KKJPD
CCDJP
CDDGP

Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren
Conférence des directrices et directeurs des départements cantonaux de justice et police
Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia

Per Mail an:
ncsc@gs-efd.admin.ch

Bern, 8. März 2022
08.02.01 cst

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrte Damen und Herren

Die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) wurde eingeladen, zur oben erwähnten Vernehmlassung Stellung zu nehmen. Wir danken Ihnen dafür bestens.

Die KKJPD begrüsst die vorgesehene Einführung einer Meldepflicht für Betreiberinnen kritischer Infrastrukturen bei Cyberangriffen und die damit verbundene Definition der Aufgaben des Nationalen Zentrums für Cybersicherheit (NCSC) explizit. Die KKJPD erachtet dies als wichtigen Beitrag zur Verbesserung der Resilienz der Schweiz im Umgang mit Cyberbedrohungen.

Die Unterstellung möglichst vieler Betreiberinnen kritischer Infrastrukturen unter die neue gesetzliche Bestimmung erachten wir als wesentlich, um eine aussagekräftige Übersicht über Cyberangriffe erstellen, Betroffene bei der Bewältigung von Cyberangriffen unterstützen und weitere Betreiberinnen kritischer Infrastrukturen rechtzeitig und angemessen warnen zu können.

Aufgrund der sehr heterogenen Landschaft bei den Betreiberinnen kritischer Infrastrukturen weisen wir darauf hin, dass den Möglichkeiten und Eigenheiten der verschiedenen Organisationen angemessen Rechnung zu tragen ist. Wir erachten es deshalb als zielführend, dass der Bundesrat gemäss Art. 74c namentlich für kleine Organisationen und solche, von denen nur ein geringes volkswirtschaftliches Schadenspotential ausgeht, eine Befreiung von der Meldepflicht vorsehen kann.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen für zusätzliche Auskünfte gerne zur Verfügung.

Freundliche Grüsse

Fredy Fässler
Präsident KKJPD

Generalsekretariat KKJPD | Haus der Kantone, Speichergasse 6, Postfach, 3001 Bern | Tel. +41 31 318 15 05 | Fax: +41 31 318 15 06 | info@kkjpd.ch | www.kkjpd.ch

Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren
Conférence des directrices et directeurs cantonaux de la santé
Conferenza delle direttrici e dei direttori cantonali della sanità

Haus der Kantone
Speichergasse 6, CH-3001 Bern
+41 31 356 20 20
office@gdk-cds.ch
www.gdk-cds.ch

Versand per Mail

Eidgenössisches Finanzdepartement
Nationales Zentrum für Cybersicherheit

ncsc@gs-efd.admin.ch

7-7-2 / MW

Bern, 10. März 2022

Stellungnahme der GDK zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Mit Schreiben vom 12. Januar 2022 laden Sie uns ein, zum Entwurf zur Änderung des Informationssicherheitsgesetzes (ISG) zur Einführung einer Meldepflicht von Cyberangriffen auf kritische Infrastrukturen Stellung zu nehmen.

Wir danken Ihnen für diese Möglichkeit und äussern uns wie folgt:

Wir teilen Ihre Einschätzung, dass Cyberrisiken zu den wichtigsten Bedrohungen der Sicherheit und der Wirtschaft der Schweiz geworden sind. Um die Bedrohungslage besser einzuschätzen und darauf angemessen reagieren zu können, ist es unumgänglich, dass Angriffe auf Unternehmen und Behörden in der Schweiz früh erkannt werden können. Die Einführung einer Meldepflicht für Betreiberinnen kritischer Infrastrukturen scheint uns dafür ein geeignetes Mittel zu sein. Mit der Integration dieser Aufgabe im ISG werden nun die Grundzüge der Meldepflicht auf einer adäquaten Rechtsgrundlage verankert und das Nationale Zentrum für Cybersicherheit (National Cyber Security Centre - NCSC) gestärkt.

Wir begrüssen, dass auf Gesetzesstufe für die Definition der von der Meldepflicht betroffenen kritischen Bereiche soweit als möglich auf klare Definitionen aus bereits bestehenden Bundesgesetzen abgestellt wird. Es stellt sich jedoch die Frage, ob im Rahmen der Verordnung noch Konkretisierungen vorgenommen werden müssen, beispielsweise ob alle Spitäler, die sich auf einer kantonalen Spitalliste befinden (Art. 74*b*, Bst. g E-ISG), also vom kleinsten Regionalspital über Rehabilitationskliniken bis hin zu den Universitätsspitälern, als für die Landesversorgung kritische Infrastrukturen betrachtet werden müssen.

Es ist zu prüfen, ob die Plattformen über die das elektronische Patientendossier (EPD) läuft, nicht auch in den Bereich der Meldepflicht fallen sollten. Mit der Verbreitung des EPDs werden die darin enthaltenen Daten zu einer Informationsquelle für die Versorgung von Patientinnen und Patienten und dadurch an Bedeutung gewinnen. Eine Störung oder ein Ausfall der zentralen Plattformen kann somit zu einer direkten Gefährdung von Patientinnen und Patienten führen.

Die Vorlage behandelt hauptsächlich die Meldepflicht für Betreiberinnen von kritischen Infrastrukturen von Cyberangriffen. Dabei darf aber die Wichtigkeit der Meldung von Cybervorfällen und Schwachstellen

auf freiwilliger Basis nicht vergessen gehen. Auch dieses bereits bestehende Mittel soll durch das NCSC weiterhin gefördert werden. Die Möglichkeit der Verwendung desselben Systems zur Übermittlung der Meldung (gemäss Art. 74*f* Abs.1 E-ISG) von Cyberangriffen, wie auch von Cybervorfällen und Schwachstellen könnte dabei für die Meldenden ein Anreiz zur freiwilligen Meldung sein.

Der Gesetzesentwurf sieht auch vor, dass Betreiberinnen von kritischen Infrastrukturen ihre Meldung auch an weitere Stellen oder Behörden übermitteln können, ev. mit Angaben, die über die durch das NCSC definierten Mindestinformationen hinausgehen, dies im Sinne einer Mehrfachnutzung der Meldung (Art. 74f, Abs. 2 und 3 E-ISG). Wir bitten Sie, sich in der konkreten Umsetzung dieser Bestimmung nicht auf die Übermittlung an nationale Stellen und Behörden zu beschränken, sondern auch die Zusammenarbeit mit kantonalen Behörden zu suchen, da es auch auf kantonaler Ebene bereits teilweise Verpflichtungen zur Meldung von Cyberangriffen von kritischen Infrastrukturen gibt. Eine möglichst einfache Übergabe der Meldungen muss auch da vorgesehen werden.

Freundliche Grüsse

Regierungsrat Lukas Engelberger
Präsident GDK

Michael Jordi
Generalsekretär

RK MZF | CG MPS | CG MPP | CG MPP
Regierungskonferenz Militär, Zivilschutz und Feuerwehr
Conférence gouvernementale des affaires militaires, de la protection civile et des sapeurs-pompiers
Conferenza governativa per gli affari militari, la protezione civile e i pompieri
Conferenza guvernativa per ils affars militars, la protecziun civila ed ils pompiers

Herr Bundesrat
Ueli Maurer, Vorsteher EFD
Bundesgasse 3, 3003 Bern
ncsc@gs-efd.admin.ch

18. März 2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe
Eröffnung des Vernehmlassungsverfahrens

Sehr geehrter Herr Bundesrat

Mit Schreiben vom 12. Januar 2022 haben Sie uns zur Stellungahme in titelerwähnter Sache eingeladen. Die Regierungskonferenz Militär, Zivilschutz und Feuerwehr (RK MZF) bedankt sich dafür. Wir nehmen wie folgt Stellung.

Der Vorstand der RK MZF begrüsst die vorgesehene Einführung einer Meldepflicht für Betreiberinnen kritischer Infrastrukturen (KI) bei Cyberangriffen.

Begründung: Der Vorstand der RK MZF erachtet diese Massnahme als wichtigen Beitrag zur Verbesserung der Resilienz der Schweiz im Umgang mit Cyberbedrohungen. Die Unterstellung möglichst vieler Betreiberinnen von KI unter die neue gesetzliche Bestimmung ist wichtig. Dies nicht zuletzt, um aussagekräftige Analysen über Cyberangriffe erstellen und damit zukünftige Attacken verhindern zu können. Zudem können so die Betroffenen bei der Bewältigung von Cyberangriffen unterstützt und weitere Betreiberinnen von KI rechtzeitig und angemessen gewarnt werden.

Der Vorstand der RK MZF empfiehlt, dass der Bundesrat eine Meldepflicht mit entsprechender Sanktionsmöglichkeit nur für Organisationen einführt, bei denen eine solche anwendbar und sinnvoll ist. Kleine Organisationen im Sinne von Art. 74 c und solche, von denen nur ein geringes volkswirtschaftliches Schadenspotential ausgeht, sollen von der Meldepflicht befreit werden können.

Begründung: Aufgrund der sehr heterogenen Landschaft bei den Betreiberinnen von KI weisen wir darauf hin, dass den Möglichkeiten und Eigenheiten der verschiedenen Organisationen angemessen Rechnung zu tragen ist. So verfügen beispielsweise kleine Behörden oder vergleichbare Organisationen (z.B. kleine Gemeinden, interkantonale Konferenzen) oftmals nicht über professionelle Strukturen im IT-Bereich, die Cyberangriffe erkennen und entsprechend darauf reagieren könnten. Solche Organisationen einer Meldepflicht zu unterstellen, erscheint uns wenig zweckmässig, da diese einer solchen ohne den Aufbau zusätzlicher, teurer Strukturen nicht nachkommen könnten. Zudem stufen wir die Bedeutung der Meldungen von Kleinstorganisationen für das Lagebild wegen ihrer geringen volkswirtschaftlichen Relevanz als niedrig ein. Wir sprechen uns aber für die restriktive Bestimmung von Ausnahmen aus und

GENERALSEKRETARIAT RK MZF
Haus der Kantone | Speichergasse 6 | 3011 Bern
Telefon 031 320 16 26 | www.rkmzf.ch

regen die von solchen Ausnahmeregelungen betroffenen Behörden an, auch im eigenen Interesse professionelle Strukturen zu schaffen bzw. auf solche zurückzugreifen und wenn immer möglich bei Cyberangriffen freiwillig Meldung zu erstatten.

Wir ersuchen Sie, sehr geehrter Herr Bundesrat, die Empfehlungen des Vorstandes der RK MZF zu berücksichtigen.

Mit freundlichen Grüssen

Regierungskonferenz
Militär, Zivilschutz und Feuerwehr

Regierungsrat Paul Winiker
Präsident RK MZF

PD Dr. phil. Alexander Krethlow
Generalsekretär RK MZF

KONFERENZ DER KANTONALEN POLIZEIKOMMANDANTEN
CONFERENCE DES COMMANDANTS DES POLICES CANTONALES
CONFERENZA DEI COMANDANTI DELLE POLIZIE CANTONALI

Der Präsident

Eidgenössisches Finanzdepartement EFD

Per E-Mail:
ncsc@gs-efd.admin.ch

Bern, 13. April 2022

Vernehmlassungsantwort der KKPKS zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Die KKPKS beobachtet im Bereich Cybercrime steigende Fallzahlen, vermehrt Geschädigte und zunehmende Schadenssummen. Auch kritische Infrastrukturen der Schweiz stehen im Visier für Cyberangriffe. Um dieser Entwicklung entgegenzuwirken und um die Schweiz, insbesondere auch deren kritische Infrastruktur, vor Schadensfällen bestmöglich zu schützen, ist die Zusammenarbeit aller involvierten Kräfte unabdingbar. Die KKPKS begrüsst und unterstützt deshalb grundsätzlich die Einführung einer Meldepflicht bei Cyberangriffen für Betreiberinnen kritischer Infrastrukturen.

Im Bezug zum vorgeschlagenen Vorgehen, welches die Meldungen beim NCSC bündelt, äussert die KKPKS aus Sicht der Strafverfolgungsbehörden jedoch folgende Vorbehalte:

Die geplante Meldepflicht ermöglicht den verbindlichen Informationsfluss an das NCSC, ist darüber hinaus jedoch aus Sicht der Strafverfolgungsbehörden stark eingeschränkt. Gemäss Vorlage erfolgt eine Weiterleitung von Meldungen oder Teilen davon nur mit Einverständnis der Betreiberin der betroffenen kritischen Infrastruktur oder anonymisiert. Für die Strafverfolgungsbehörden ist nur eine Ausnahme vorgesehen, wenn die Meldung Informationen über eine schwere Straftat enthält. Die Definition einer solchen schweren Straftat fehlt. Eine Weitergabe von Informationen, die Rückschlüsse auf die Meldenden oder Betroffenen erlauben, ist nicht verpflichtend und liegt gemäss Vorlage im Ermessen der Leiterin oder des Leiters des NCSC. Das NCSC soll von der bestehenden Anzeigepflicht von Offizialdelikten explizit ausgenommen werden (vgl. Artikel 22a des Bundespersonalgesetzes vom 24. März 2006).

Verweigern Meldende dem NCSC die Weitergabe der vollumfänglichen Informationslage und sind sie nicht Willens, Anzeige bei der Polizei zu erstatten, resultiert daraus für die Strafverfolgungsbehörden ein im Vergleich zum NCSC lückenhaftes Lagebild. Die in der Gesetzesvorlage ausformulierte Meldepflicht ist klar von einer Anzeigepflicht zu unterscheiden. Für die Strafverfolgungsbehörden bedeutet dies, dass relevante Fälle nicht erfasst, Wissen nicht geteilt und Täterschaften nicht verfolgt werden können. Ermittlungen, die in den vorliegenden Fällen relevant und für zukünftige Fälle wegweisend sein könnten, werden verunmöglicht. Um die in der

Der Präsident

Schweiz vorhandenen Kräfte zur Bekämpfung von Cybercrime seitens Gefahrenabwehr sowie Strafverfolgung zu nutzen und zu bündeln, um ein einheitliches Lagebild zu ermöglichen und damit letztendlich die effiziente Bekämpfung von Cyberangriffen in der Schweiz zu gewährleisten, ist es aus Sicht der KKPKS zwingend nötig, dass das NCSC zumindest alle gemeldeten Offizialdelikte, wie von Gesetzes wegen in Art. 22a BPG vorgesehen, an die Strafverfolgung weiterleitet.

Art. 76 Abs. 1 weist das NCSC zudem an, den NDB mit Auswertungen zu Anzahl, Art und Ausmass von Cyberangriffen sowie technischen Analysen von Cyberrisiken zu unterstützen. Die KKPKS spricht sich hiermit für eine Erweiterung dieser Unterstützung auf die Strafverfolgungsbehörden aus.

Die KKPKS begrüsst, dass Art. 76a (Unterstützung für Behörden) in Absatz 4 den Strafverfolgungsbehörden Zugriff auf Informationen im Abrufverfahren gewährt, die Aufschluss über die Identität und die Vorgehensweise der Verursacherinnen und Verursacher von Cyberangriffen geben. Dies dient als Ergänzung zu den Meldungen bezüglich Offizialdelikten. Es ist hierbei essentiell, dass die Daten hochaktuell verfügbar und direkt zugänglich sind. Die Strafverfolgungsbehörden sind darauf angewiesen, dass seitens NCSC die Dateneingabe mit kleinstmöglicher Verzögerung ausgeführt und die Qualität der Daten sichergestellt wird.

Auch rückwirkend müssen die Daten zur Verfügung stehen. Kommt ein Delikt erst später ans Licht, ist aber noch nicht verjährt, soll den Strafverfolgungsbehörden die Bearbeitung weiterhin möglich sein. Deshalb hat sich die maximale Aufbewahrungsfrist der Daten in Art. 79 an der Verfolgungsverjährung zu orientieren. Diese beläuft sich in Abhängigkeit des Strafmasses auf drei bis dreissig Jahre (Art. 97 und 109 StGB). Ansonsten würden wichtige Ermittlungsakten frühzeitig vernichtet.

Aus der Vorlage stellt sich zudem für die Strafverfolgungsbehörden die Frage, wie mit Fällen umzugehen ist, bei denen Geschädigte eines meldungspflichtigen Vorfalls sich an die Polizei, nicht jedoch an das NCSC wenden und ob dies seitens Strafverfolgung in jedem Fall proaktiv zu prüfen ist. Eine klare Regelung wird hier begrüsst.

Aufgrund vorangehender Ausführungen stellt die KKPKS folgende Anträge:

- Art. 73c Abs. 2 sei zu streichen, um die Weiterleitung der Meldungen von Offizialdelikten durch das NCSC an die Strafverfolgungsbehörden sicherzustellen.
- Die in Art. 76 Abs. 1 vorgesehene Unterstützung des NDB durch das NCSC mit Auswertungen zu Anzahl, Art und Ausmass von Cyberangriffen sowie technischen Analysen von Cyberrisiken sei auf die Strafverfolgungsbehörden zu erweitern.
- Die maximale Aufbewahrungsfrist der Daten in Art. 79 habe sich an der Verfolgungsverjährung (Art. 97 und 109 StGB) zu orientieren.
- Es sei eine gesetzliche Regelung einzufügen, die vorsieht, wie seitens der Strafverfolgungsbehörden umzugehen ist, wenn sich Geschädigte eines meldungspflichtigen Vorfalls an die Polizei, nicht jedoch an das NCSC wenden.

Besten Dank für die Berücksichtigung unserer Stellungnahme.

CONFERENCE DES COMMANDANTS DES POLICES CANTONALES (CCPCS)
CONFERENZA DEI COMANDANTI DELLE POLIZIE CANTONALI (CCPCS) .
Generalsekretariat, Haus der Kantone, Speichergasse 6, 3011 Bern, Telefon: 031 512 87 20, info@kkpks.ch

KONFERENZ DER KANTONALEN POLIZEIKOMMANDANTEN
CONFERENCE DES COMMANDANTS DES POLICES CANTONALES
CONFERENZA DEI COMANDANTI DELLE POLIZIE CANTONALI

Der Präsident

Freundliche Grüsse

Der Präsident

Mark Burkhard, Kdt Polizei Basel-Landschaft

Kopie z.K.:
- Mitglieder der KKPKS
- GS KKJPD

SSK | CPS
Schweizerische Staatsanwälte-Konferenz
Conférence des procureurs de Suisse
Conferenza dei procuratori della Svizzera

Eidg. Finanzdepartement

3003 Bern

Per E-Mail: ncsc@gs-efd.admin.ch

Bern, 8. Februar 2022

Meldepflicht von Cyberangriffen für Betreiberinnen kritischer Infrastrukturen; Änderung des Informationssicherheitsgesetzes (ISG)

Sehr geehrte Damen und Herren

Mit Schreiben vom 12. Januar 2022 haben Sie unsere Konferenz eingeladen, zur erwähnten Vorlage Stellung zu nehmen. Hierfür danken wir Ihnen bestens, enthalten uns aber einer materiellen Stellungnahme.

Mit freundlichen Grüssen

Fiona Strebel
Generalsekretärin SSK-CPS

KANTON AARGAU

REGIERUNGSRAT

Regierungsgebäude, 5001 Aarau
Telefon 062 835 12 40, Fax 062 835 12 50
regierungsrat@ag.ch
www.ag.ch/regierungsrat

A-Post Plus
Eidgenössisches Finanzdepartement
Bundesgasse 3
3003 Bern

30. März 2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe; Vernehmlassung

Sehr geehrte Damen und Herren

Mit Schreiben vom 12. Januar 2022 wurden die Kantonsregierungen eingeladen, die Unterlagen zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe zu prüfen und dazu Stellung zu nehmen. Wir danken Ihnen für diese Möglichkeit und nehmen diese gern wahr.

1. Allgemeines

Der Angriff auf eine Informatikstruktur ist bereits heute von strafrechtlicher Relevanz (zum Beispiel Art. 147 Schweizerisches Strafgesetzbuch, StGB). Obwohl die einschlägigen Strafnormen weitgehend als Offizialdelikte ausgestaltet sind, ist von einer hohen Dunkelziffer auszugehen, da die Betroffenen in aller Regel keiner Anzeigepflicht unterstehen und die Strafverfolgungsbehörden mangels Kenntnis nicht aktiv werden können. Diese Ausgangslage ist unbefriedigend, da Straftaten passieren, eine Verfolgung aber nicht stattfindet. Weit bedenklicher ist jedoch der Umstand, dass damit kein Bild über die effektive Bedrohungslage besteht und damit keine ausreichende Informationslage für zielgerichtete Abwehr- und Präventionsmassnahmen bestehen,

Mit der vorgeschlagenen Meldepflicht als Kern der vorliegenden Revisionsvorlage soll insbesondere letzteres verbessert werden. Der Regierungsrat begrüsst die Vorlage, mit welcher die Cybersicherheit verbessert werden soll.

2. Zu den Änderungsvorschlägen

Art. 73c Abs. 2

Die Aufhebung der Anzeigepflicht und die Statuierung eines Anzeigerechts des Nationalen Zentrums für Cybersicherheit (NCSC) wird begrüsst.

Art. 73c Abs. 3

Die vorgeschlagene Regelung ist nachvollziehbar und entspricht den strafprozessualen Grundsätzen.

Problematisch erscheint jedoch, dass derartige Regelungen einzelfallweise in den Spezialgesetzen Eingang finden. Zum einen wird damit die Rechtsanwendung aufwendig und unübersichtlich und zum anderen ergibt sich eine unsystematische Regelung von Privilegierungen. Die hier geregelte

Problematik stellt sich in vielen Situationen, welche zum Teil viel häufiger vorkommen, so beispielsweise im Gesundheitswesen (Kunstfehler), im Flug- und Bahnverkehr etc.

Wir regen an, anstelle von Einzelfallregelungen eine einheitliche, für alle Bereiche geltende Regelung zu erlassen.

Art. 74b

Diese Bestimmung regelt die Bereiche, für welche eine Meldepflicht besteht. Hierzu wird folgende Ergänzung beantragt:

"Objekte, Organisationen und Unternehmen, die von den zuständigen Stellen von Bund oder Kanton als kritische Infrastruktur im Sinne des Bevölkerungsschutzes erfasst sind."

Art. 74c

Angesichts des umfangreichen Katalogs der Meldepflichtigen in Art. 74b kann eine sehr hohe Zahl von Meldungen erfolgen. Es ist daher nachvollziehbar, dass die Zahl der Meldungen auf eine handhabbare Anzahl reduziert werden soll. Unseres Erachtens ist der in Art. 74c beschrittene Weg jedoch ungeeignet, da damit die Triage zwischen wichtig und unwichtig dem Betroffenen überlassen wird. Die Triage sollte vielmehr von der Fachstelle NCSC selber vorgenommen werden, da sich auch "unwichtige" Meldungen aufgrund ihrer Häufigkeit oder aus anderen Gründen als wichtig erweisen können. Abgesehen davon erscheinen die postulierten Kriterien als wenig unterscheidungskräftig.

Wir danken Ihnen für die Berücksichtigung unserer Vernehmlassung.

Freundliche Grüsse

Im Namen des Regierungsrats

Alex Hürzeler
Landammann

Joana Filippi
Staatsschreiberin

Kopie
- ncsc@gs-efd.admin.ch

KANTON
APPENZELL INNERRHODEN

Landammann und Standeskommission

Sekretariat Ratskanzlei
Marktgasse 2
9050 Appenzell
Telefon +41 71 788 93 11
info@rk.ai.ch
www.ai.ch

Ratskanzlei, Marktgasse 2, 9050 Appenzell

Per E-Mail an
ncsc@gs-efd.admin.ch

Appenzell, 14. April 2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe (Änderung des Informationssicherheitsgesetzes)
Stellungnahme Kanton Appenzell I.Rh.

Sehr geehrte Damen und Herren

Mit Schreiben vom 12. Januar 2022 haben Sie uns die Vernehmlassungsunterlagen zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe und zur Änderung des Informationssicherheitsgesetzes zukommen lassen.

Die Standeskommission hat die Unterlagen geprüft. Sie nimmt dazu wie folgt Stellung:

Die Einführung einer Meldepflicht soll ermöglichen, das Lagebild realistischer zu zeichnen, als mit freiwilligen Meldungen. Es ist durchaus nachvollziehbar, dass damit flächendeckend Informationen vorliegen, wodurch eine objektivere und lückenlosere Sicht entsteht. Aus unserer Sicht ist allerdings darauf zu achten, dass:

- der mit der Meldepflicht verbundene Aufwand in Grenzen gehalten wird;
- klar definiert wird, welche Fälle genau zu melden sind und was der Inhalt der Meldungen sein muss;
- durch die Definition von Standardprozessen und den Einsatz von technischen Hilfsmitteln so weit möglich eine gewisse Automatisation sichergestellt werden kann;
- nur Vorfälle mit einer gewissen Tragweite gemeldet werden müssen. Dazu sind ebenfalls entsprechende klar definierte Kriterien zu erlassen.

So würden etwa nach Art. 74c lit. c des Vernehmlassungsentwurfs alle Kantons- und Gemeindebehörden meldepflichtig. Im Kanton Appenzell I.Rh. haben verschiedene kommunale Körperschaften die Informationstechnologie an den Kanton ausgelagert. Das kantonale Amt für Informatik stellt im sogenannten AINet etwa auch den Bezirken die Infrastruktur und Betreuung gegen Entgelt zur Verfügung. Es ist nun zu vermeiden, dass jede am AINet angeschlossene Organisation dem Bund nach Cyberangriffen Meldung erstattet. Es muss genügen, wenn der Betreiber der IT, der Kanton Appenzell I.Rh., meldepflichtig ist.

Der organisatorische und technische Aufwand für die beteiligten Akteurinnen und Akteure muss überschaubar bleiben. Dies betrifft nicht nur die Vermeidung von Mehrfachmeldungen. Das zukünftige System muss einfach und eingängig zu bedienen sein. Der Meldeprozess muss sich einfach in die verschiedenen Organisations- und Systemlandschaften der betroffenen Akteurinnen und Akteure einfügen.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme und grüssen Sie freundlich.

Im Auftrage von Landammann und Standeskommission
Der Ratschreiber:

Markus Dörig

Zur Kenntnis an:
- Finanzdepartement Appenzell I.Rh., Marktgasse 2, 9050 Appenzell
- Ständerat Daniel Fässler, Weissbadstrasse 3a, 9050 Appenzell
- Nationalrat Thomas Rechsteiner (thomas.rechsteiner@parl.ch)

Appenzell Ausserrhoden

Regierungsrat

Obstmarkt 3
9102 Herisau
Tel. +41 71 353 61 11
kantonskanzlei@ar.ch
www.ar.ch

Regierungsrat, 9102 Herisau

Eidgenössisches Finanzdepartement EFD

per E-Mail: ncsc@gs-efd.admin.ch
[PDF- und Wordversion]

Dr. iur. Roger Nobs
Ratschreiber
Tel. +41 71 353 63 51
roger.nobs@ar.ch

Herisau, 25. März 2022

Eidg. Vernehmlassung; Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe; Stellungnahme des Regierungsrates von Appenzell Ausserrhoden

Sehr geehrte Damen und Herren

Mit Schreiben vom 12. Januar 2022 wurden die Kantonsregierungen vom Eidgenössischen Finanzdepartement EFD eingeladen, zur Einführung einer Meldepflicht für Cyberangriffe und der damit verbundenen Änderung des Informationssicherheitsgesetzes (ISG) bis 14. April 2022 Stellung zu nehmen.

Der Regierungsrat von Appenzell Ausserrhoden nimmt dazu wie folgt Stellung:

Er begrüsst die vorgesehene Einführung einer Meldepflicht für Betreiberinnen kritischer Infrastrukturen bei Cyberangriffen und die damit verbundene Definition der Aufgaben des Nationalen Zentrums für Cybersicherheit (NCSC). Er erachtet dies als wichtigen Beitrag zur Verbesserung der Resilienz der Schweiz im Umgang mit Cyberbedrohungen.

Die Unterstellung möglichst vieler Betreiberinnen kritischer Infrastrukturen unter die neue gesetzliche Bestimmung erachtet der Regierungsrat als wesentlich, um eine aussagekräftige Übersicht über Cyberangriffe erstellen, Betroffene bei der Bewältigung von Cyberangriffen unterstützen und weitere Betreiberinnen kritischer Infrastrukturen rechtzeitig und angemessen warnen zu können.

Aufgrund der sehr heterogenen Landschaft bei den Betreiberinnen kritischer Infrastrukturen ist darauf hinzuweisen, dass den Möglichkeiten und Eigenheiten der verschiedenen Organisationen angemessen Rechnung zu tragen ist. Der Regierungsrat erachtet es deshalb als zielführend, dass der Bundesrat gemäss Art. 74c namentlich für kleine Organisationen und solche, von denen nur ein geringes volkswirtschaftliches Schadenspotential ausgeht, eine Befreiung von der Meldepflicht vorsehen kann.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme.

Freundliche Grüsse

Im Auftrag des Regierungsrates

Dr. iur. Roger Nobs, Ratschreiber

Kanton Bern
Canton de Berne

Regierungsrat

Postgasse 68
Postfach
3000 Bern 8
info.regierungsrat@be.ch
www.be.ch/rr

Staatskanzlei, Postfach, 3000 Bern 8

Eidgenössisches Finanzdepartement
Per E-Mail (PDF/Word) an: ncsc@gs-efd.admin.ch

Ihr Zeichen:
Unser Zeichen: 2022.KAIO.1

16. März 2022

RRB Nr.: 267/2022
Direktion: Finanzdirektion
Klassifizierung: Nicht klassifiziert

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe. Stellungnahme des Kantons Bern

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Der Regierungsrat des Kantons Bern dankt Ihnen für die Gelegenheit zur Stellungnahme zu dieser Vorlage.

1. Grundsätzliches

Wir unterstützen die von Ihnen vorgeschlagene Ergänzung des Informationssicherheitsgesetzes (ISG). Cyberangriffe gehören zu den grössten Bedrohungen der Sicherheit und der Wirtschaft der Schweiz. Wir begrüssen es daher, dass der Bund beim Schutz des Landes vor dieser Bedrohung die Führung übernimmt und die Betreiberinnen kritischer Infrastrukturen bei der Bewältigung dieses Risikos unterstützt.

Vor diesem Hintergrund – und mit den nachstehenden Vorbehalten – unterstützen wir auch die in Art. 74a E-ISG vorgesehene Pflicht der Betreiberinnen von kritischen Infrastrukturen, dem Nationalen Zentrum für Cybersicherheit (NCSC) Cyberangriffe zu melden. Dies, obwohl die Liste der kritischen Infrastrukturen in Art. 74b E-ISG sehr weit gefasst ist: Neben Infrastrukturunternehmen im klassischen Sinne umfasst sie auch alle Kantons- und Gemeindebehörden, Hochschulen, Spitäler sowie eine Vielzahl von Privatunternehmen, deren Leistungen von nationaler Bedeutung sind. Diese breite Meldepflicht ist u.E. dennoch gerechtfertigt, weil eine wirksame Bekämpfung von Cyberangriffen ihre frühe Erkennung voraussetzt. Wir erwarten aber, dass der Bundesrat von seiner Kompetenz zum Erlass von Ausnahmen von der Meldepflicht (Art. 74c E-ISG) so Gebrauch macht, dass der Aufwand für die Meldepflicht in einer nationalen Gesamtsicht verhältnismässig bleibt.

2. Anträge

2.1 Antrag zu Art. 73a

Art. 73a ist wie folgt mit einem zweiten Absatz zu ergänzen:

[2] Das NCSC arbeitet bei der Erfüllung dieser Aufgaben mit den Polizeibehörden der Kantone zusammen.

2.1.1 Begründung

Auch die Schweizerische Kriminalprävention (SKP) sowie mehrere Polizeikorps sind im Bereich der Abwehr von Cyberrisiken tätig. Die Zuweisung von präventiven Aufgaben an das NCSC darf nicht dazu führen, dass die Kompetenz der Kantone oder der SKP im präventiven Bereich eingeschränkt wird. Der Austausch zwischen den Behörden ist daher sicherzustellen, damit sie zweckmässig zusammenarbeiten.

2.2 Antrag zu Art. 73c Abs. 2 und Art. 76a Abs. 3

Art. 73c Abs. 2 ist zu streichen. Er lautet: «Für Mitarbeitende des NCSC entfällt die Anzeigepflicht gemäss Artikel 22a des Bundespersonalgesetzes vom 24. März 2000, wenn sie im Zusammenhang mit der Meldung eines Cybervorfalls oder dessen Analyse Hinweise auf eine mögliche Straftat erhalten. Die Leiterin oder der Leiter des NCSC kann Anzeige erstatten, sofern dies aufgrund der Schwere der möglichen Straftat geboten scheint.»

Art. 76a Abs. 3 ist ebenfalls zu streichen. Er lautet: «Es [das NCSC] gewährt den Strafverfolgungsbehörden den Zugriff auf Informationen im Abrufverfahren, die Aufschluss über die Identität und die Vorgehensweise der Verursacherinnen und Verursacher von Cyberangriffen geben.»

2.2.1 Begründung

Mit der Aufhebung der Pflicht, vermutete Delikte im Cyberbereich zur Anzeige zu bringen, können die Strafverfolgungsbehörden ihre Aufgaben im Cyberbereich nicht mehr wirksam wahrnehmen. Um die Strafverfolgung solcher Delikte sicherzustellen und um den Überblick über die deliktische Aktivität im Cyberbereich zu behalten, sind sie ebenso zwingend auf die Meldungen des NCSC angewiesen, wie es das NCSC für die Wahrnehmung seiner Aufgaben auf die neu einzuführende Meldepflicht der Betroffenen ist.

Der erläuternde Bericht begründet nicht nachvollziehbar, wieso die Anzeigepflicht entfallen soll. Gemäss dem Bericht steht «diese Anzeigepflicht in einem Spannungsfeld zum Grundsatz der vertraulichen Behandlung der Meldung». Worin dieses Spannungsfeld besteht, bleibt aber unklar, zumal die Strafverfolgungsbehörden ebenfalls dem Amtsgeheimnis unterstehen. Eine Strafverfolgung dürfte in fast allen Fällen auch im Interesse der Meldenden liegen, und gegen eine Selbstbelastung im Zusammenhang mit allfälligem deliktischem Verhalten der Meldenden schützt sie Art. 73c Abs. 3. Überdies sieht Art. 76a Abs. 2–4 vor, dass der NDB, die Strafverfolgungs- und Cybersicherheitsbehörden auf (soweit ersichtlich) dieselben Informationen im Abrufverfahren Zugriff haben, einschliesslich auf allfällige Personendaten (Bericht S. 24). Es ist nicht ersichtlich, wieso dies unter dem Gesichtspunkt der Vertraulichkeit kein Problem sein soll, die Anzeigepflicht aber schon.

Unserer Meinung nach sollte das Zusammenspiel zwischen der Gefahrenabwehr und der Strafverfolgung im Zentrum stehen. Zudem führt eine erfolgreiche Strafverfolgung auch zu einer gewissen Prävention. Es ist erwiesen, dass Straftaten, bei denen eine hohe Aufklärungsrate besteht, weniger häufig begangen werden und dadurch eine gewisse Abschreckungswirkung besteht.

Das in Art. 76a Abs. 3 vorgesehene Abrufverfahren wird bei einer Streichung von Art. 73 Abs. 2 obsolet und kann entfallen. Es wäre im Bereich der Strafverfolgung ohnehin nicht zielführend, denn wenn die Strafverfolgungsbehörden keine Kenntnis von Vorfällen haben, haben sie auch keinen Anlass dazu, Daten abzurufen.

2.3 Antrag zu Art. 74c^{bis}

Folgender Artikel ist nach Art. 74c E-ISG einzufügen:

Art. 74c^{bis} Bestimmungen des kantonalen Rechts
Die Kantone können
a. nach Anhörung des NCSC unter den Voraussetzungen des Artikels 74c kantonale oder kommunale Behörden oder Träger öffentlicher Aufgaben von der Meldepflicht ausnehmen,
b. die für die Meldung verantwortlichen Personen der kantonalen oder kommunalen Behörden oder Träger öffentlicher Aufgaben bestimmen.

2.3.1 Begründung

Buchstabe a: Die sehr umfangreiche Liste der Meldepflichtigen in Art. 74a E-ISG führt dazu, dass auch Behörden oder Organisationen mit einer minimalen Bedeutung für die Cybersicherheit der Schweiz meldepflichtig werden können, beispielsweise Kleinstgemeinden. Art. 74c erlaubt es dem Bundesrat zwar, solche Organisationen von der Meldepflicht auszunehmen. Mit Rücksicht auf die Organisationsautonomie der Kantone, welche die Risikoexposition ihrer Behörden meist besser kennen werden als der Bund, sollte diese Kompetenz in Bezug auf Behörden oder Träger öffentlicher Aufgaben aber auch den Kantonen zustehen. Vor dem Entscheid sollen die Kantone aber das NCSC als Fachbehörde des Bundes konsultieren müssen.

Buchstabe b: Zur Organisationsautonomie der Kantone gehört auch die Sicherheitsorganisation, also z.B. der Entscheid, ob Informationssicherheitsverantwortliche auf gesamtkantonaler oder -kommunaler Ebene oder auf Direktions- bzw. Amtsebene eingesetzt werden sollen. Diese Organisationsautonomie würde unterlaufen, wenn das NCSC als Bundesorgan in Anwendung des ISG entscheiden würde, wen in einer Kantonsverwaltung (z.B. ein Regierungsmitglied, eine Amtsleiterin oder einen Informatikverantwortlichen) es für meldepflichtig hält und welche Behörde (der Kanton selbst, eine Direktion oder ein Amt) daher Adressatin oder Adressat einer allfälligen strafbewehrten Verfügung des NCSC (Art. 74i E-ISG) sein soll. Die Kantone und Gemeinden müssen mit anderen Worten weiterhin frei sein, eine ihrer Organisation angemessene Sicherheitsorganisation einschliesslich der Zuordnung der Meldepflicht gemäss ISG festzulegen.

2.4 Antrag zu Art. 79

Die Bestimmung ist so anzupassen, dass Daten in der Regel nicht vor dem Ende der Verfolgungsverjährung der in Frage kommenden Delikte gelöscht werden.

2.4.1 Begründung

Die vorgesehene maximale Aufbewahrungsdauer von fünf bzw. zwei Jahren ab der letzten Verwendung ist nicht angemessen, weil ein wichtiger Nutzen der Daten darin liegt, eine Strafverfolgung der für Cyberangriffe Verantwortlichen zu ermöglichen (s. oben unser Antrag zu Art. 73c). Die Verfolgungsverjährung dauert abhängig vom Strafmass drei bis dreissig Jahre (Art. 97 und 109 StGB).

Auch im Abrufverfahren durch die Strafbehörden nach Art. 76a Abs. 3 würden die Daten zu früh gelöscht, wenn die Strafverfolgungsbehörden aufgrund der nicht erfolgten Anzeige (s. oben unser Antrag zu Art. 73c) erst später Kenntnis von der Straftat erhalten. Dadurch würden wichtige Ermittlungsakten verloren gehen.

Der Regierungsrat dankt Ihnen für die Berücksichtigung seiner Anliegen.

Freundliche Grüsse

Im Namen des Regierungsrates

Beatrice Simon
Regierungspräsidentin

Christoph Auer
Staatsschreiber

Landeskanzlei
Rathausstrasse 2
4410 Liestal
T 061 552 50 06
landeskanzlei@bl.ch
www.bl.ch

BASEL LANDSCHAFT
REGIERUNGSRAT

Regierungsrat, Rathausstrasse 2, 4410 Liestal

Eidgenössisches Finanzdepartement

Per E-Mail an:
ncsc@gs-efd.admin.ch

Liestal, 29. März 2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe, Vernehmlassungsantwort

Sehr geehrter Herr Bundesrat Maurer
Sehr geehrte Damen und Herren

Mit Schreiben vom 12. Januar 2022 haben Sie uns eingeladen, im Rahmen der Vernehmlassung zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe unsere Stellungnahme abzugeben.

Wir bedanken uns für diese Einladung und stellen Ihnen im Folgenden unsere Bemerkungen innerhalb der Frist zu.

I. Allgemeine Anmerkungen

Der Regierungsrat des Kantons Basel-Landschaft befürwortet grundsätzlich die Einführung der Meldepflicht und die damit einhergehenden Änderungen des Bundesgesetzes über die Informationssicherheit beim Bund. Die Einführung der Meldepflicht beschränkt einerseits zwar geringfügig den Freiheitsgrad der kantonalen Verwaltung in Bezug auf Zeitpunkt und Umfang von Kommunikation und Information zu allfällig erfolgten Cybercrime-Angriffen. Zudem wird die Meldepflicht zu einer Zunahme von offiziellen Cyberdelikten führen, mit entsprechendem Mehraufwand bei den Strafverfolgungsbehörden. Dies kann zu personellen Ressourcen-Engpässen führen. Andererseits ermöglicht die Gesetzesrevision aber den Zugang und den Zugriff zu unterstützenden Fachkompetenzen beim Nationalen Zentrum für Cybersicherheit, um einen Angriff zu bewältigen und verbessert die Information zur nationalen Bedrohungslage. Das ist sachlich zielführend und wirksam.

II. Anmerkungen zu einzelnen Bestimmungen:

Artikel 73c Absatz 2
Wir regen an, das Weiterleitungsrecht der Leitung des Nationalen Cybersicherheitszentrums NCSC durch eine Weiterleitungs*pflicht* an die Strafverfolgungsbehörden im Falle des ausdrücklichen Wunsches der Melderin bzw. des Melders im Sinne einer Beschleunigung und zeitnahen Verfahrenseröffnung zu ergänzen.

Artikel 74d Absatz 2
Strafrechtlich relevante Begleitumstände eines Cyberangriffs sind gemäss dieser Bestimmung immer zu melden. In Ergänzung zu den bereits aufgeführten Tatbeständen der Erpressung, Drohung oder Nötigung regen wir an, zusätzlich die Datenbeschädigung, begangen durch die Verschlüsselung (encryption) bzw. das Einschleusen (Malware) von Daten, aufzuführen: Zum einen werden bei einem Ransomware-Angriff zuerst die Daten beschädigt. Eine «ransom note» wird durch die Täterschaft nicht zwingend gleichzeitig hinterlegt bzw. kann auch erst mit zeitlicher Verzögerung erfolgen. Diese Zeitspanne bis zur Meldepflicht durch die erfolgte Erpressung, Drohung oder Nötigung gilt es zu verkürzen. Zum anderen stellen staatliche Akteure meist keine Forderungen (z.B. Stuxnet, aktuelle Angriffe auf die digitale Infrastruktur der Ukraine). Diesen Fall gilt es mittels des Tatbestandes der Datenbeschädigung (Verschlüsselung/Malware) abzudecken.

Hochachtungsvoll

Thomas Weber
Regierungspräsident

Elisabeth Heer Dietrich
Landschreiberin

Regierungsrat des Kantons Basel-Stadt

Rathaus, Marktplatz 9
CH-4001 Basel

Tel: +41 61 267 85 62
Fax: +41 61 267 85 72
E-Mail: staatskanzlei@bs.ch
www.regierungsrat.bs.ch

per Email an die Geschäftsstelle
National Cyber Security Center - NCSC:
ncsc@gs-efd.admin.ch.

Basel, 5. April 2022

Präsidialnummer: 220056

Regierungsratsbeschluss vom 5. April 2022
Vernehmlassung zur «Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe»: Stellungnahme des Kantons Basel-Stadt

Sehr geehrte Damen und Herren

Mit Schreiben vom 12. Januar 2022 haben Sie uns die Vernehmlassungsunterlagen zur Einführung einer Meldepflicht für Cyberangriffe und der damit verbundenen Änderung des Bundesgesetzes über die Informationssicherheit beim Bund (ISG) zukommen lassen.
Wir danken Ihnen für die Gelegenheit zur Stellungnahme und lassen Ihnen nachstehend unsere Anträge und Bemerkungen zukommen.

Der Regierungsrat begrüsst die Einführung einer einheitlichen und auf nationaler Ebene regulierten Meldepflicht für Cyberangriffe an das Nationalen Zentrum für Cybersicherheit (NCSC). Die entsprechenden Massnahmen steigern die Früherkennung und Abwehr von Cyberangriffen auf die Daten im Datennetz Basel-Stadt (DANEBS) und den Wirtschaftsstandort Basel.

Der Regierungsrat informiert, dass aktuell in der kantonalen Verwaltung Basel-Stadt noch keine Detektoren für die Erkennung von „zu meldende Cyberangriffe" gemäss Art. 74d ISG installiert sind.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen. Für Rückfragen steht Ihnen gerne Miriam Gantner, miriam.gantner@bs.ch, Tel. 061 267 67 08, zur Verfügung.

Freundliche Grüsse
Im Namen des Regierungsrates des Kantons Basel-Stadt

Beat Jans
Regierungspräsident

Barbara Schüpbach-Guggenbühl
Staatsschreiberin

ETAT DE FRIBOURG
STAAT FREIBURG

Conseil d tat CE
Staatsrat SR

Rue des Chanoines 17, 1701 Fribourg

T +41 26 305 10 40, F +41 26 305 10 48
www.fr.ch/ce

Conseil d'Etat
Rue des Chanoines 17, 1701 Fribourg

PAR COURRIEL

Département fédéral des finances DFF
Monsieur Ueli Maurer
Conseiller fédéral
Bundesgasse 3
3003 Berne

Courriel : ncsc@gs-efd.admin.ch

Fribourg, le 21 mars 2022

2022-256
Obligation de signaler les cyberattaques contre des infrastructures critiques

Monsieur le Conseiller fédéral,

Par courrier du 12 janvier dernier, vous nous avez consultés sur l'objet cité en titre, et nous vous en remercions.

De manière générale, nous approuvons les modifications proposées, qui permettent de combler une lacune importante dans le dispositif mis en place pour lutter contre la cybercriminalité.

S'agissant de l'art. 74a du projet, nous estimons toutefois qu'il conviendrait de définir précisément le délai de signalement. La formulation *« […] le plus rapidement possible après leur découverte »* ne nous paraît pas suffisante. Cela étant dit sans remettre en cause les modalités prévues à l'art. 74e sur le contenu du signalement et la possibilité de donner un premier signalement incomplet lorsque l'exploitant ne dispose pas dans l'immédiat de toutes les informations constitutives du signalement.

Enfin, nous ne saurions manquer d'insister sur le fait que la LSI et les modifications qui font l'objet de cette consultation ne sont qu'un pan de la lutte contre la cybercriminalité. Il est indispensable que les acteurs concernés renforcent également les mesures de prévention, de sensibilisation et de formation à l'intention de la population en générale, notamment dans le cadre scolaire et de la formation post-obligatoire, des entreprises et autres personnes morales, ainsi qu'aux collectivités publiques. Dans le canton de Fribourg, cette vision transversale et globale dans le domaine de la sécurité numérique sera d'ailleurs l'un des objectifs prioritaires du programme gouvernemental de la présente législature 2022-2026.

Avec ces considérations, nous vous réitérons notre soutien au projet et vous prions de croire, Monsieur le Conseiller fédéral, à l'assurance de nos sentiments les meilleurs.

Au nom du Conseil d'Etat :

Olivier Curty, Président

Danielle Gagnaux-Morel, Chancelière d'Etat

L'original de ce document est établi en version électronique

Copie

—

à la Direction de la sécurité, de la justice et du sport, pour elle, la Police cantonale et le Service de la protection de la population et des affaires militaires ;
à la Direction de l'économie, de l'emploi et de la formation ;
à la Direction des finances, pour elle et le Service de l'informatique et des télécommunications ;
à la Direction des institutions, de l'agriculture et des forêts ;
à la Direction de la formation et des affaires culturelles ;
à la Direction de la santé et des affaires sociales ;
à la Direction du développement territorial, des infrastructures, de la mobilité et de l'environnement ;
à la Chancellerie d'Etat.

RÉPUBLIQUE ET CANTON DE GENÈVE

POST TENEBRAS LUX

Genève, le 13 avril 2022

Le Conseil d'Etat

1562-2022

Confédération Suisse
Département fédéral des finances
Monsieur Ueli Maurer
Conseiller fédéral
Bundesgasse 3
3003 Berne

Concerne : obligation de signaler les cyberattaques contre des infrastructures critiques

Monsieur le Conseiller fédéral,

Notre Conseil a pris connaissance des propositions transmises par le Département fédéral des finances (DFF) le 12 janvier 2022, concernant la consultation relative à l'obligation de signaler les cyberattaques contre des infrastructures critiques et sur la modification de la loi sur la sécurité de l'information (LSI), qui ont retenu notre meilleure attention.

Après analyse, nous sommes favorables, avec quelques réserves, aux propositions d'amendements à la LSI présentées.

Nous relevons toutefois un manque de cohérence avec la récente loi fédérale sur la protection des données (nLPD). Alors que cette dernière propose des règles et mécanismes précis d'annonce, par exemple lors de violations de la protection des données, certaines propositions – qui sont annoncées comme inspirées de la nLPD – s'appuient sur des règles et mécanismes différents. La collaboration indispensable avec le préposé fédéral à la protection des données et à la transparence est aussi absente.

En outre, certains points nécessitent d'être améliorés. Par exemple, alors que la loi spécifie explicitement que les communes sont concernées, le projet de loi fait implicitement porter tout le poids des interactions et responsabilités avec celles-ci sur le canton.

Vous trouverez en annexe de la présente réponse l'ensemble de nos commentaires.

En vous remerciant de nous avoir consulté, nous vous prions de croire, Monsieur le Conseiller fédéral, à l'expression de notre haute considération.

AU NOM DU CONSEIL D'ÉTAT

La chancelière :

Michèle Righetti

Le président :

Serge Dal Busco

Annexe mentionnée

Copie à : ncsc@gs-efd.admin.ch

REPUBLIQUE ET CANTON DE GENEVE
Département des infrastructures
Office cantonal des systèmes d'information et du numérique

NOTE D'ACCOMPAGNEMENT

De :	Christian Geffcken et Pascal Verniory
A :	Confédération Suisse, Département fédéral des finances
Date :	23 mars 2022
Objet :	Loi fédérale sur la sécurité de l'information au sein de la Confédération (Loi sur la sécurité de l'information, LSI) Annexe

Ci-après, vous trouverez les commentaires ou propositions de changements formulées par l'office cantonal des systèmes d'information et du numérique (OCSIN) du canton de Genève.

Article 5, lettres d à e :
Il manque une définition de "cyberrisque" à l'art 1,1, b

Article 73b alinéa 1
Le paragraphe n'est pas clair.

En effet, la première phrase mentionne que le NCSC fera une analyse.

La seconde phrase précise « *pour autant que la situation ne nécessite pas d'analyses ou clarifications supplémentaires* ».

Dès lors, est-ce que ces « suppléments » se rapportent au signalement ou à l'analyse initiale du NCSC ? Le rapport explicatif n'évoque pas cette restriction.

Article 73b alinéa 1
[...] **pour autant que la situation ne nécessite pas d'analyses ou clarifications supplémentaires**
Nous proposons de remplacer cette partie de phrase comme suite :
[...] pour autant qu'il ne soit pas nécessaire d'instruire d'enquête complémentaire.

Article 73b alinéa 2
"Le NCSC **peut"** [...]

Cela n'engendre donc pas d'obligation. Néanmoins, quels seront les critères, et qui les déterminera ?

Article 73b alinéa 2
[...] et aux organisations **intéressées** [...]

Cela signifie-t-il que celles-ci doivent explicitement s'annoncer ? Et si oui, est-ce pour chaque cas, ou pour tous les cas ?

Article 73b alinéa 2
Nous estimons que ce terme « intéressées » est trop vague et pas forcément adéquat. Nous proposons de le remplacer par « concernées ».

Article 73b alinéa 2
[...] **et que la personne concernée ait donné son accord.**

Si deux millions de personnes sont concernées, est-ce que cela signifie que les 2 millions de personnes doivent donner leur accord ? Plus concrètement, qui est la personne concernée ?

Article 73b alinéa 2
[...] **et que la personne concernée ait donné son accord.**

Les personnes concernées n'ont pas à donner leur accord pour les raisons suivantes :
- Seules les organisations concernées sont contactées (cf. modification proposée ci-dessus)
- La démarche vise à améliorer la sécurité, donc se fait en faveur des personnes concernées
- Il s'agit de savoir quelle information transmettre aux personnes concernées.

Ces activités n'ont pas à être couvertes par l'accord des personnes intéressées. Il s'agit d'activités « internes » et dans un cercle limité. Quant aux communications au grand public et de nature préventive, la transmission de données personnelles ne devrait pas être nécessaire.

Article 73b alinéa 3
Le NCSC informe immédiatement **le fabricant [...]**

Nous estimons que tant le concepteur que le diffuseur devraient être concernés par l'annonce effectuée par le NCSC. Ainsi, nous proposons de répondre à la volonté affichée par la Confédération d'agir sur le matériel et le logiciel, et proposons la variante suivante : "le fabricant et/ou l'éditeur".

Article 73c alinéa 3
[...] ne peuvent être utilisées dans une procédure pénale contre **cette personne** [...]

Qu'en est-il de l'entreprise ou de l'administration qui emploie ladite personne ?
Nous estimons que cette disposition devrait plutôt s'appuyer sur la protection assurée par la loi sur les lanceurs d'alerte.

Article 73c alinéa 4
[...] **informations qui révèlent des secrets pénalement protégés**

L'article 320 du code pénal concerne un périmètre d'informations beaucoup plus large. Pourquoi le limiter ici ?

Article 74 alinéa 2, lettre c
Qui prend en charge la communication au grand public ? Comment est-ce fait ?

Article 74 alinéa 3
[...] correction des vulnérabilités lorsqu'il existe un risque **imminent** [...]

Comment est déterminée l'imminence du risque ?

Nous estimons que l'imminence des risques couverts par le PL implique que le NCSC conseille et aide les exploitants d'infrastructures critiques de manière immédiate à survenance du risque encouru. Ainsi, dès l'instant où ce soutien est de toute manière conditionné à la non-existence d'une alternative fournie par le marché privé, le "risque" de voir le NCSC fournir une prestation indue est faible.

Article 74a
[...] afin que **celui-ci** [...]

Est-ce le NCSC ou l'exploitant ? S'il s'agit du NCSC, il conviendrait de le préciser par « ce dernier ».

Article 74a
[...] **avertir les victimes potentielles** [...]

Cette phrase est en contradiction avec la LPD, qui prévoit que cette communication relève d'une décision du PFPDT. Une collaboration du NCSC avec ce dernier doit être prévue, car le signalement au PFPDT double celui prévu au NCSC et entraîne un risque important d'incohérence.

A notre sens, il incombe en premier lieu au NCSC de répondre à l'urgence commandée par une situation critique. Il lui revient de déclarer – dans un second temps administratif – au préposé fédéral à la protection des données tout incident touchant à la sphère de la LPD. Pour éviter tout risque de doublon entre le PL et la LPD, il conviendrait peut-être de faire figurer l'obligation pour le NCSC de déclarer l'événement au PFPDT.

Article 74b lettre b
[...] aux autorités fédérales, cantonales ou **communales** [...]

Dans ce cas, la Confédération doit communiquer directement avec les communes (ou les associations de communes), et ne pas se contenter de laisser les cantons s'en charger. Les urgences de la sécurité s'accommodent mal d'une telle hiérarchie verticale.

Quand bien même il est bien compris que la liste des infrastructures critiques est une reprise des sous-secteurs critiques tels que définis dans la stratégie nationale pour la protection des infrastructures critiques, il nous semble que les éléments suivants peuvent faire l'objet d'un commentaire :

- Généralités : les lettres f) et s) semblent recouvrir l'ensemble des acteurs directement concernés par l'action à mener par la NCSC. De fait, les interlocuteurs "en première ligne" vis-à-vis des événements critiques dont dispose le PL en question sont les exploitants, fabricants, éditeurs et/ou de prestataires de services (internes ou externes) à l'endroit des infrastructures critiques. Par ailleurs, sauf à connaître que la liste des infrastructures critiques figurent plutôt dans l'ordonnance d'application (adaptation facilitée) et non dans la loi, nous suggèrerions de structurer l'article en deux sous-section : la première qui concernerait les acteurs compris dans les lettres f) et s) avec obligation de signalement en premier chef vu leur responsabilité d'ordre technique, et une seconde, avec les entités considérées comme infrastructures critiques, avec une obligation de signalement basée sur leur qualité de propriétaire des données.

- Lettre f) : les notions de "grand nombre d'utilisateurs" et de "grande importance pour l'économie" gagneraient à être mieux précisées dans l'ordonnance que l'intention annoncée dans le commentaire de l'article considéré.

Article 74b, lettre f. 3.
offrent **des services de sécurité et de confiance;**

Cette notion de « services de sécurité et de confiance » est-elle définie dans une autre loi, par exemple la Loi sur la signature électronique ? À défaut, dans l'ordonnance d'application prévue ?

Article 74b, lettre g
La référence à l'article de la LAMAL est erronée. Il s'agit de l'article 39, al.1 (au lieu de l'article 9).

Nous proposons de changer la formulation de cet article de la manière suivante :"aux hôpitaux figurant sur la liste hospitalière cantonale des hôpitaux conformément à l'article 39, al. 1 let.e. de la loi fédérale du 18 mars 1994 sur l'assurance maladie, et, par analogie, aux établissements mentionnés à l'art. 39 al. 3 LAMAL.

Article 74b, lettre s. 4
[...] **cryptage** [...]

Le terme correct en français est « chiffrement » (source : ANSSI). Le terme « cryptage » est réservé à l'encodage de la télévision, style Canal+

Article 74c
Le Conseil fédéral exempte [...]

Cet article est en contradiction avec la LPD si l'obligation de signalement est au NCSC. Les causes d'exception sont par ailleurs inadéquates car il ne s'agit pas de savoir s'il convient de signaler les risques aux personnes concernées, mais au NCSC et cela devrait être à lui de trier de telles informations.

Par ailleurs, il convient de rappeler que la communication d'un risque non critique pour une entité peut s'avérer très critique pour d'autres. D'autre part, la communication simultanée de plusieurs attaques « non critiques » pourrait permettre au NCSC d'en déduire le début d'attaques concertées de plus grande échelle.

Article 74c, lettre b
n'ont qu'un impact limité [...]

Le projet d'article 74b liste un grand nombre d'institutions qui sont considérées comme suffisamment importantes.

Cette lettre b est contradictoire avec le but du 74b.

Article 74d, alinéa 1, lettre a
[...] **une autre infrastructure critique;**

Cette appréciation échappe très souvent à l'entité intéressée. Il serait donc préférable qu'elle communique d'office – même de manière succincte – au NCSC sans en faire une condition de la communication.

Article 74d, alinéa 2
Le principe de cet alinéa est louable. Cependant, dans la pratique, bien des entreprises et institutions ne pourraient se permettre de perdre leurs données chiffrées par un rançongiciel.

En violant cet article, elles s'infligeraient une double peine.

Au niveau de la teneur du signalement d'une cyberattaque, il nous apparaît que les informations devraient également inclure le produit logiciel ainsi que l'identité du prestataire de services informatiques

Article 74e, alinéa 1
[...] son **déroulement** et ses conséquences [...].

Nous proposons de préciser la phrase comme suite :
[...] déroulement, notamment les informations temporelles, et ses conséquences [...].

Article 74e, alinéa 1
[...] **ainsi que les mesures que compte prendre** l'exploitant [...]

Nous proposons de remplacer cette partie de phrase par :
[...] ou que l'entité concernée a commencé à mettre en œuvre

Article 74e, alinéa 2
[...] **dès que celles-ci lui parviennent**

Nous proposons de compléter cette phrase par [...] ou qu'elles peuvent être obtenues.

Article 74f, alinéa 1
Le NCSC **met** à disposition [...].

Nous proposition d'ajouter [...] **gratuitement** à disposition [...].

Article 74f, alinéa 2
Ce système doit permettre **à l'exploitant d'une infrastructure** [...]

Si cela se passe par le système du NCSC, c'est ce dernier qui communique, à la suggestion de l'entité concernée.

Article 74f, alinéa 3
[...] l'autorité concernés **ont besoin** [...]

Nous proposons de préciser : [...] ont **légitimement** besoin [...].

Article 74g
L'exploitant de l'infrastructure critique **fournit au NCSC** [...].

Nous proposons : [...] fournit **dans les meilleurs délais** au NCSC [...].

Article 74i, alinéa 1
Est puni **d'une amende de 100 000 francs** [...].

Au niveau du montant de l'amende encourue en cas de non-signalement, il peut raisonnablement être estimé que le faible montant de l'amende maximale ne remplisse pas son rôle incitatif pour des entreprises réalisant un chiffre d'affaires conséquent, Partant, nous nous demandons dans quelle mesure il ne serait pas opportun d'envisager soit un montant nominal max. plus important, soit un montant rapporté au chiffre d'affaires."

Article 75, alinéa 1, lettre a
[...] **le traitement des données** n'est admissible [...]

Nous proposons de préciser : [...] le traitement **de ces** données [...].

Article 76
Dans cet article, considère-t-on que « les exploitants d'infrastructures critiques » le sont pour les infrastructures décrites à l'article 74b, à l'article 74b réduit du 74c, ou autrement ?

Article 76
Collaboration sur le plan national

Nous estimons qu'une collaboration avec le PFPDT s'avère indispensable au vu de l'obligation d'annonce à ses services prévus par la LPD.

Article 79, al 1, 1
[...] la durée de conservation est limitée à deux ans.

Nous proposons de préciser : [...] « après leur dernière utilisation ».

Chapitre II
2. Loi du 25 septembre 2020 sur la protection des données.

Article 24, al 5bis
Le PFPDT peut, avec l'accord du responsable tenu à l'obligation de signalement, transmettre le signalement au Centre national pour la cybersécurité à des fins d'analyse de l'incident.

Nous estimons que la collaboration doit être plus étroite, et qu'il convient de prévoir une communication contraignante de la part du NCSC au PFPDT ; la communication du PFPDT au bénéfice du NCSC n'a pas à obtenir l'autorisation de la personne responsable du signalement si ce dernier remplit les conditions de la présente loi.

Nous restons bien entendu à votre disposition pour tout complément d'information.

kanton glarus

Telefon 055 646 60 11/12/15
E-Mail: staatskanzlei@gl.ch
www.gl.ch

Regierungsrat
Rathaus
8750 Glarus

per E-Mail
ncsc@gs-efd.admin.ch

Glarus, 22. März 2022
Unsere Ref: 2022-29

Vernehmlassung i. S. Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Hochgeachteter Herr Bundesrat
Sehr geehrte Damen und Herren

Das Eidgenössische Finanzdepartement gab uns in eingangs genannter Angelegenheit die Möglichkeit zur Stellungnahme. Dafür danken wir und lassen uns gerne wie folgt vernehmen:

Wir teilen Ihre Einschätzung, dass Cyberrisiken zu den wichtigsten Bedrohungen der Sicherheit und der Wirtschaft der Schweiz geworden sind. Um die Bedrohungslage besser einzuschätzen und darauf angemessen reagieren zu können, ist es unumgänglich, dass Angriffe auf Unternehmen und Behörden in der Schweiz früh erkannt werden können. Die Einführung einer Meldepflicht für Betreiberinnen kritischer Infrastrukturen scheint uns dafür ein geeignetes Mittel zu sein. Mit der Integration dieser Aufgabe im Informationssicherheitsgesetz (ISG) werden nun die Grundzüge der Meldepflicht auf einer adäquaten Rechtsgrundlage verankert und das Nationale Zentrum für Cybersicherheit (National Cyber Security Centre – NCSC) gestärkt.

Wir begrüssen, dass auf Gesetzesstufe für die Definition der von der Meldepflicht betroffenen kritischen Bereiche soweit als möglich auf klare Definitionen aus bereits bestehenden Bundesgesetzen abgestellt wird. Es stellt sich jedoch die Frage, ob im Rahmen der Verordnung noch Konkretisierungen vorgenommen werden müssen, beispielsweise ob alle Spitäler, die sich auf einer kantonalen Spitalliste befinden (Art. 74b Bst. g E-ISG), also vom kleinsten Regionalspital über Rehabilitationskliniken bis hin zu den Universitätsspitälern, als für die Landesversorgung kritische Infrastrukturen betrachtet werden müssen.

Es ist zu prüfen, ob die Plattformen über die das elektronische Patientendossier (EPD) läuft, nicht auch in den Bereich der Meldepflicht fallen sollten. Mit der Verbreitung des EPDs werden die darin enthaltenen Daten zu einer Informationsquelle für die Versorgung von Patientinnen und Patienten und dadurch an Bedeutung gewinnen. Eine Störung oder ein Ausfall der zentralen Plattformen kann somit zu einer direkten Gefährdung von Patientinnen und Patienten führen.

Die Vorlage behandelt hauptsächlich die Meldepflicht für Betreiberinnen von kritischen Infrastrukturen von Cyberangriffen. Dabei darf aber die Wichtigkeit der Meldung von Cybervorfällen und Schwachstellen auf freiwilliger Basis nicht vergessen gehen. Auch dieses bereits be-

stehende Mittel soll durch das NCSC weiterhin gefördert werden. Die Möglichkeit der Verwendung desselben Systems zur Übermittlung der Meldung (gemäss Art. 74f Abs.1 E-ISG) von Cyberangriffen, wie auch von Cybervorfällen und Schwachstellen könnte dabei für die Meldenden ein Anreiz zur freiwilligen Meldung sein.

Der Gesetzesentwurf sieht auch vor, dass Betreiberinnen von kritischen Infrastrukturen ihre Meldung auch an weitere Stellen oder Behörden übermitteln können, ev. mit Angaben, die über die durch das NCSC definierten Mindestinformationen hinausgehen, dies im Sinne einer Mehrfachnutzung der Meldung (Art. 74f Abs. 2 und 3 E-ISG). Wir bitten Sie, sich in der konkreten Umsetzung dieser Bestimmung nicht auf die Übermittlung an nationale Stellen und Behörden zu beschränken, sondern auch die Zusammenarbeit mit kantonalen Behörden zu suchen, da es auch auf kantonaler Ebene bereits teilweise Verpflichtungen zur Meldung von Cyberangriffen von kritischen Infrastrukturen gibt. Eine möglichst einfache Übergabe der Meldungen muss auch da vorgesehen werden.

Genehmigen Sie, hochgeachteter Herr Bundesrat, sehr geehrte Damen und Herren, den Ausdruck unserer vorzüglichen Hochachtung.

Freundliche Grüsse

Für den Regierungsrat

Marianne Lienhard
Landammann

Hansjörg Dürst
Ratsschreiber

E-Mail an (PDF- und Word-Version):
- ncsc@gs-efd.admin.ch

Die Regierung
des Kantons Graubünden

La Regenza
dal chantun Grischun

Il Governo
del Cantone dei Grigioni

Sitzung vom	Mitgeteilt den	Protokoll Nr.
5. April 2022	6. April 2022	284/2022

Eidgenössisches Finanzdepartement EFD
Bundesrat Ueli Maurer
Bundesgasse 3
3003 Bern

Per E-Mail (PDF und Word-Version) zustellen an:
ncsc@gs-efd.admin.ch

Vernehmlassung zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Mit Schreiben vom 12. Januar 2022 haben Sie uns die Gelegenheit gegeben, zur erwähnten Vorlage Stellung zu nehmen. Dafür danken wir Ihnen bestens.

1. Allgemeine Bemerkungen

Der Schutz kritischer Infrastrukturen und die Erhöhung der Cybersicherheit ist für das Wohlergehen der Bevölkerung, die Wirtschaft und die öffentlichen Verwaltungen von zentraler Bedeutung. Wir halten die Einführung einer Meldepflicht für Cyberangriffe vor diesem Hintergrund für eine sinnvolle Massnahme und ein wertvolles Instrument für eine koordinierte Cyberabwehr in der Schweiz. Die Meldepflicht trägt zur Steigerung der Cyber-Resilienz der Betreiberinnen von kritischen Infrastrukturen bei und dient diesen unmittelbar. Die erforderlichen Kompetenzen und Erfahrungen werden beim Nationalen Zentrum für Cybersicherheit (NCSC) gebündelt. Aus diesen Gründen begrüssen wir die Änderung des Bundesgesetzes über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG).

Ziel der Massnahmen muss es sein, Angriffe frühzeitig zu erkennen, die Bedrohungslage möglichst genau einzuschätzen und die Angriffe abzuwehren. Die aussagekräftige Analyse von Cyberangriffen ist ein entscheidendes Element für die Prävention zukünftiger Angriffe.

Die Meldepflicht sollte mit einem Mehrwert für die beteiligten Akteure im Sinne einer Unterstützung verbunden sein. Neben einer technischen Analyse steht dabei eine rasche Verteilung von Informationen an alle Akteure im Vordergrund. Betroffene sollen bei der Bewältigung von Cyberangriffen unterstützt und alle anderen Betreiberinnen kritischer Infrastrukturen gewarnt werden.

Aufgrund der vorgesehenen Meldeformalitäten erscheint die Meldepflicht als Eingriff von beschränkter Tragweite in die Rechte von Privaten bzw. die föderale Autonomie. Die finanziellen Auswirkungen auf die Kantonale Verwaltung oder die betroffenen, im Kanton Graubünden ansässigen, Betriebe dürften überschaubar sein. Insgesamt sprechen daher keine Gründe gegen die Vorlage.

Bei der Umsetzung ist darauf zu achten, dass

- der mit der Meldepflicht verbundene Aufwand für die Betreiberinnen kritischer Infrastrukturen überschaubar bleibt;
- sich der Meldeprozess durch den Einsatz technischer Hilfsmittel möglichst einfach in die bestehende Organisations- und Systemlandschaft integrieren lässt;
- die Vertraulichkeit und die Weitergabe der übermittelten Informationen klar geregelt ist;
- klar umschrieben wird, welche Fälle und mit welchem Inhalt zu melden sind;
- nur Vorfälle mit einer gewissen Tragweite gemeldet werden müssen;
- das NCSC seine Aufgaben schnell und professionell erfüllt und dass die diesbezüglich nötigen Vorgaben und Prozesse klar definiert sind.

2. Besondere Bemerkungen zu einzelnen Bestimmungen

Art. 73c (Weiterleitung von Informationen)
Laut dem Erläuternden Bericht erfolgt eine Weiterleitung von Meldungen oder Teilen davon – abgesehen von zwei Ausnahmen – nur mit Einverständnis der Betreiberin der betroffenen kritischen Infrastruktur oder anonymisiert (Ziff. 1.2.2). Dieser Grundsatz muss angesichts der Geheimhaltungsverpflichtungen der Betreiberinnen deutlicher im Erlass zum Ausdruck kommen. Die Vertraulichkeit und Weitergabe der übermittelten Informationen muss klar geregelt sein.

Art. 74
Absatz 3 ist wie folgt zu ergänzen: «[…] wenn für die kritische Infrastruktur ein unmittelbares Risiko von gravierenden Auswirkungen besteht oder dieses bereits eingetreten ist und, […]».

Art. 74a (Meldepflicht)
Die zeitliche Vorgabe «so rasch als möglich» sollte genauer definiert werden.

Art. 74b (Bereiche)
Die Meldepflicht gilt für eine Vielzahl von Bereichen und Akteuren. Es sollte geprüft werden, ob eine Priorisierung und eine entsprechend zeitliche Staffelung vorzunehmen ist. So könnten im Rahmen einer Pilotphase Erfahrungen mit einer kleineren Anzahl von Akteuren gesammelt und frühzeitig mögliche Prozessverbesserungen abgeleitet werden.

Viele der aufgeführten Akteure verfügen nicht über die notwendigen Mittel, Cyberangriffe über ein aktives Monitoring zu erkennen. Es ist deshalb zu prüfen, wie bspw. Gemeindeverwaltungen bei der Erkennung von Cyberangriffen unterstützt werden können.

Art. 74d (Zu meldende Cyberangriffe)
Die Definition der zu meldenden Cyberangriffe ist allgemein gehalten. Dies lässt einen grossen Interpretationsspielraum zu. Für die praktische Handhabung wäre eine

leicht verständliche und nachvollziehbare Umschreibung der zu meldenden Cyberangriffe hilfreich.

Art. 74e (Inhalt der Meldungen)
Wie bereits erwähnt, bleibt zu definieren, welche Informationen genau gemeldet werden müssen.

Art. 74f (Übermittlung der Meldung)
Es ist unklar, welche Informationen an welche Behörden gelangen und wer diese einsehen darf. Zudem gilt es, den organisatorischen und technischen Aufwand für die beteiligten Akteure überschaubar zu halten und Mehrfachmeldungen zu vermeiden.

Art. 75 (Bearbeitung von Personendaten)
Das Wort «enthalten» ist in Absatz 1 Litera a und Litera b zu entfernen, da es bereits im Einführungssatz vorkommt.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und die Berücksichtigung unserer Anliegen.

GRISCHUN * GRIGIONE * GRAUBÜNDEN

Namens der Regierung

Der Präsident:	Der Kanzleidirektor:
Marcus Caduff	Daniel Spadin

Hôtel du Gouvernement
2, rue de l'Hôpital
CH-2800 Delémont

t +41 32 420 51 11
f +41 32 420 72 01
chancellerie@jura.ch

Hôtel du Gouvernement – 2, rue de l'Hôpital, 2800 Delémont

Confédération suisse
Département fédéral des finances DFF
M. le Conseiller fédéral Ueli Maurer
Bundesgasse 3
3003 Berne

ncsc@gs-efd.admin.ch

Delémont, le 29 mars 2022

Obligation de signaler les cyberattaques contre des infrastructures critiques : ouverture de la procédure de consultation

Monsieur le Conseiller fédéral,

Le Gouvernement jurassien a pris connaissance de votre courrier du 12 janvier 2022 relatif au sujet cité en marge.

Les cyberattaques sont devenues une menace importante dans l'exploitation des systèmes critiques de la République et Canton du Jura. Par l'intermédiaire du Service de l'informatique cantonal (SDI) nous prenons régulièrement des mesures afin de nous adapter à ces risques.

L'obligation d'annonces des cyberattaques par les entreprises et les autorités publiques (Cantons et communes) aide les autorités fédérales compétentes à évaluer le niveau de menace et à identifier les modes opératoires à un stade précoce. Ils peuvent ainsi alerter à temps les services informatiques en leur qualité d'exploitant d'infrastructures critiques. Le SDI annonce déjà de manière réactive toutes les cyberattaques à sa connaissance au *Centre national pour la cybersécurité* (NCSC). Dès lors, le Gouvernement est favorable à l'obligation d'annoncer les cyberattaques contre les infrastructures critiques.

Le présent projet se limite toutefois à l'introduction d'une obligation de notification. Nous regrettons qu'il n'impose pas aux opérateurs de services critiques des mesures de sécurité minimales, en fait, à mettre en place, ceci afin de garantir un niveau de sécurité adapté pour les réseaux et les systèmes d'information et pour limiter l'impact des incidents.

Le Gouvernement jurassien est donc favorable à la modification de la LSI et plus précisément à l'obligation d'annonce des cyberattaques. Il demande également qu'un soutien fort soit établi entre les services informatiques cantonaux avec le NCSC en cas de cyberattaques, dans l'objectif de capitaliser sur l'expérience acquise par celle-ci.

Le Gouvernement vous prie d'agréer, Monsieur le Conseiller fédéral, l'expression de notre très haute considération.

AU NOM DU GOUVERNEMENT DE LA RÉPUBLIQUE ET CANTON DU JURA

David Eray
Président

GOUVERNEMENT DE LA RÉPUBLIQUE ET CANTON DU JURA

Jean-Baptiste Maître
Chancelier d'État

KANTON LUZERN

Justiz- und Sicherheitsdepartement
Bahnhofstrasse 15
Postfach 3768
6002 Luzern
Telefon 041 228 59 17
justiz@lu.ch
www.lu.ch

Eidgenössisches Finanzdepartement

per E-Mail
ncsc@gs-efd.admin.ch

Luzern, 5. April 2022

Protokoll-Nr.: 432

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrte Damen und Herren

Im Namen und Auftrag des Regierungsrates danken wir Ihnen für die Gelegenheit zur Stellungnahme und äussern uns wie folgt.

Wir begrüssen die vorgeschlagene Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe und die weiteren Änderungen des Informatiksicherheitsgesetzes. Uns ist es aber wichtig, dass die Meldepflicht von den Betreiberinnen kritischer Infrastrukturen mit vertretbarem Aufwand umgesetzt werden kann. In diesem Sinn erachten wir es als positiv, dass ein elektronisches Meldeformular für die rasche Erfassung und einfache Übermittlung der Meldungen zur Verfügung gestellt wird.

Wir haben ebenfalls die Erfahrung gemacht, dass Cyberangriffe – beispielsweise auf Energieversorger, Hochschulen, Spitäler oder Telekommunikationsanbieterinnen – immer realistischer werden. Es ist deshalb wichtig, frühzeitig Cyberangriffe auf Schweizer Unternehmen und Behörden zu erkennen, um die Bedrohungslage möglichst genau einschätzen zu können. Die vorgeschlagene Meldepflicht unterstützt diese Absicht.

Um aussagekräftige Analysen über Cyberangriffe erstellen und damit zukünftige Attacken verhindern zu können, ist es wichtig, möglichst viele Betreiberinnen der Meldepflicht zu unterstellen. Wir empfehlen aber, dass der Bundesrat eine Meldepflicht mit entsprechender Sanktionsmöglichkeit nur für Organisationen einführt, bei denen eine solche anwendbar und auch sinnvoll ist. Kleine Organisationen im Sinn von Artikel 74c des Entwurfs und solche, von denen nur ein geringes volkswirtschaftliches Schadenspotential ausgeht, sollen von der Meldepflicht befreit werden können. So verfügen beispielsweise kleinere Gemeinden oder vergleichbare Organisationen oftmals nicht über professionelle Strukturen im IT-Bereich, die Cyberangriffe erkennen und entsprechend darauf reagieren könnten. Solche Organisationen einer Meldepflicht zu unterstellen, erscheint uns wenig zweckmässig, da diese einer solchen ohne den Aufbau zusätzlicher, teurer Strukturen nicht nachkommen könnten. Zudem stufen

wir die Bedeutung der Meldungen von Kleinstorganisationen für das Lagebild wegen ihrer geringen volkswirtschaftlichen Relevanz als niedrig ein. Wir sprechen uns aber für die restriktive Bestimmung von Ausnahmen aus und regen die von solchen Ausnahmeregelungen betroffenen Behörden an, auch im eigenen Interesse professionelle Strukturen zu schaffen und wenn immer möglich bei Cyberangriffen freiwillig Meldung zu erstatten.

Das Nationale Zentrum für Cybersicherheit (NCSC) ist die richtige Organisation, um solche Angriffe zu erkennen und potentielle Opfer zu warnen. Wir begrüssen es auch, dass das NCSC Betroffene bei der Bewältigung von Cybervorfällen und der Behebung von Schwachstellen berät und unterstützt. Schliesslich wird den betroffenen Unternehmen mit der Meldepflicht auch klar aufgezeigt, dass die Erhöhung der Cybersicherheit ein wichtiger Punkt in der Unternehmenskultur sein müsse.

Freundliche Grüsse

Paul Winiker
Regierungsrat

LE CONSEIL D'ÉTAT
DE LA RÉPUBLIQUE ET
CANTON DE NEUCHÂTEL

Envoi par courrier électronique :
Département fédéral des finances
Bundesgasse 3
3003 Berne

Obligation de signaler les cyberattaques contre les infrastructures critiques - procédure de consultation

Monsieur le conseiller fédéral,

Votre correspondance du 12 janvier 2022 relative à l'objet susmentionné nous est bien parvenue et a retenu notre meilleure attention. Nous vous remercions d'avoir consulté le canton de Neuchâtel sur le dossier mentionné en titre.

Le gouvernement neuchâtelois préavise favorablement cet avant-projet qui permettra aux autorités fédérales compétentes d'évaluer le niveau de menace, d'identifier les modes opératoires à un stade précoce et d'alerter à temps les services informatiques en leur qualité d'exploitant d'infrastructures critiques.

L'avant-projet oblige en contrepartie la Confédération à fournir une assistance en cas de cyberattaques. Les tâches de soutien attribuées au Centre national pour la cybersécurité (NCSC) seront attendues par les services assurant l'exploitation d'infrastructures critiques et par les autorités cantonales et communales. Nous comprenons ainsi que les ressources du NCSC seront adaptées en conséquence.

Cela étant, le projet ne se limite toutefois qu'à l'introduction d'une obligation de notification. Il n'impose pas aux opérateurs de services essentiels des mesures de sécurité à prendre, par exemple pour prévenir les risques, pour garantir un niveau de sécurité adapté pour les réseaux et les systèmes d'information ou pour limiter l'impact des incidents compromettant la sécurité. Le Canton le déplore tout en comprenant la complexité d'imposer dans une loi, ces mesures sécuritaires.

Nous rendons attentive la Confédération sur la section 3 « Protection des données et échanges d'information », qui doit être strictement respectée et surveillée afin de limiter les dégâts d'image et les pressions à contre-emploi.

Finalement, et en réponse à votre demande, Monsieur Daniel Crevoisier (daniel.crevoisier@ne.ch), chef du service informatique de l'Entité neuchâteloise (SIEN) est à votre disposition pour répondre à d'éventuelles questions.

NE

En vous remerciant de nous avoir donné la possibilité de prendre position sur cet objet, nous vous prions d'agréer, Monsieur le conseiller fédéral, l'expression de notre haute considération.

Neuchâtel, le 28 mars 2022

Au nom du Conseil d'État :

Le président,
L. FAVRE

La chancelière,
S. DESPLAND

RÉPUBLIQUE ET CANTON DE NEUCHÂTEL * CONSEIL D'ÉTAT *

KANTON NIDWALDEN
LANDAMMANN UND REGIERUNGSRAT
Dorfplatz 2, Postfach 1246, 6371 Stans
Telefon 041 618 79 02, www.nw.ch

CH-6371 Stans, Dorfplatz 2, Postfach 1246, STK

PER E-MAIL
Eidgenössisches Finanzdepartement FD
Herr Bundesrat Ueli Maurer
Bundesgasse 3
3003 Bern

Telefon 041 618 79 02
staatskanzlei@nw.ch
Stans, 5. April 2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe. Stellungnahme

Sehr geehrter Herr Bundesrat

Mit Schreiben vom 12. Januar 2022 eröffnete das Eidgenössische Finanzdepartement (FD) unter anderem bei den Kantonen das Vernehmlassungsverfahren zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe und der damit verbundenen Änderung des Informationssicherheitsgesetzes (ISG). Für die Möglichkeit zur Stellungnahme bedanken wir uns herzlich.

Der Kanton Nidwalden nimmt den Entwurf zur Kenntnis und stimmt diesem grundsätzlich zu. Die vorgesehene Einführung einer Meldepflicht für Betreiberinnen kritischer Infrastrukturen bei Cyberangriffen und die damit verbundene Definition der Aufgaben des Nationalen Zentrums für Cybersicherheit (NCSC) wird begrüsst. Wir erachten dies als wichtigen Beitrag zur Verbesserung der Resilienz der Schweiz im Umgang mit Cyberbedrohungen. Die gesetzlichen Grundlagen richten sich nicht nur auf die Repression, sondern auch auf die Prävention zur Cybersicherheit aus. Sie trägt auch dazu bei, die Bevölkerung für Cyberrisiken zu sensibilisieren.

Die Unterstellung möglichst vieler Betreiberinnen kritischer Infrastrukturen unter die neue gesetzliche Bestimmung erachten wir als wesentlich, um eine aussagekräftige Übersicht über Cyberangriffe erstellen, Betroffene bei der Bewältigung von Cyberangriffen unterstützen und weitere Betreiberinnen kritischer Infrastrukturen rechtzeitig und angemessen warnen zu können. Aufgrund der sehr heterogenen Landschaft bei den Betreiberinnen kritischer Infrastrukturen weisen wir aber darauf hin, dass den Möglichkeiten und Eigenheiten der verschiedenen Organisationen angemessen Rechnung zu tragen ist. Die Meldepflicht bei Cyberangriffen betrifft nebst den öffentlichen Infrastrukturen auch private Firmen, die voraussichtlich einer solchen teilweise eher kritisch gegenüberstehen werden. Der Gesetzestext weist darauf hin, dass ein relativ breites Spektrum an Unternehmen und Organisationen betroffen sein kann. Der Begriff "kritische Infrastrukturen" umfasst nicht nur Energieversorgungsunternehmen, Krankenhäuser, die Zivilluftfahrt oder Telekommunikationsanbieter. Auch Hochschulen, Behörden aller föderalen Ebenen, Banken, Versicherungen und Finanzmarktinfrastrukturen sind mitgemeint. Zu dieser Definition hinzu kommen Hersteller von Hard- und Software sowie Anbieter von digitalen Diensten, die "über das Internet Dienste anbieten, die von einer grossen Zahl von Nutzern in der Schweiz nachgefragt werden". Wir erachten es deshalb als zielführend, dass der Bundesrat gemäss Art. 74c namentlich für kleine Organisationen und solche, von

denen nur ein geringes volkswirtschaftliches Schadenspotential ausgeht, eine Befreiung von der Meldepflicht vorsehen kann.

Falls eine Meldepflicht besteht oder eine Meldung an das NCSC gemacht wird, sollten die Informationen vollständig an die Strafverfolgungsbehörden übermittelt werden. Art. 73c Abs. 2 hält aber fest, dass grundsätzliche keine Anzeigepflicht der Mitarbeitenden des NCSC bei Hinweisen auf eine Straftat besteht. Die Möglichkeit einer eingeschränkten Weitergabe von Informationen an die Strafverfolgungsbehörden, sei es hinsichtlich der Meldung an sich oder deren Vollständigkeit, wird jedoch als problematisch erachtet. Der Leiter oder die Leiterin des NCSC entscheidet aktuell nach freiem Ermessen über die Schwere der Straftat und die Abwägung zwischen dem Interesse des Staates an einer Strafverfolgung gegenüber demjenigen der meldenden Person an der Vertraulichkeit der Meldung im Einzelfall. Dies kann sich auf ein unvollständiges Lagebild und Wissenslücken insbesondere bezüglich Auftreten von neuen Phänomenen auswirken, was wiederum eine koordinierte Strafverfolgung erschwert. Dies sollte überdacht und geändert werden.

Die Bestimmung von Art. 76a ISG regelt Art, Umfang und Zweck der Zurverfügungstellung von Informationen des NCSC gegenüber anderen Behörden (vgl. auch S. 24 des Erläuternden Berichts). Die Abs. 2, 3 und 4 besagter Bestimmung regeln die Zurverfügungstellung von Informationen gegenüber dem Nachrichtendienst des Bundes (NDB), den Strafverfolgungsbehörden und den kantonalen Cybersicherheits-Stellen in genereller Hinsicht. Abs. 1 beschränkt die Auswertungs- und Analyseunterstützung durch das NCSC aber nur auf den NDB. Hier beantragen wir, dass auch diese Informationen (inklusive darauf gestützter Erkenntnisse) ebenfalls allen Strafverfolgungsbehörden zur Verfügung gestellt werden.

Der Regierungsrat Nidwalden bedankt sich für die Möglichkeit zur Stellungnahme. Er unterstützt den Entwurf der Änderung des Informationssicherheitsgesetzes (ISG) und bedankt sich für die Berücksichtigung der Hinweise und Anträge.

Freundliche Grüsse
NAMENS DES REGIERUNGSRATES

REGIERUNGSRAT · KANTON NIDWALDEN

Karin Kayser-Frutschi
Landammann

lic. iur. Armin Eberli
Landschreiber

Geht an:
- ncsc@gs-efd.admin.ch

Kanton Obwalden

Die Vorsteherin des Finanzdepartements

CH-6061 Sarnen, St. Antonistrasse 4, FD

Elektronisch an:
ncsc@gs-efd.admin.ch

Sarnen, 5. April 2022

Stellungnahme: Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Wir beziehen uns auf die mit Nachricht vom 18. Januar 2022 zugestellte Einladung zur Stellungnahme im Rahmen des Vernehmlassungsverfahrens zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe und danken für die Gelegenheit zur Stellungnahme.

Der Kanton Obwalden verzichtet in diesem Vernehmlassungsverfahren auf eine Stellungnahme.

Freundliche Grüsse

Maya Büchi-Kaiser
Landstatthalter

St. Antonistrasse 4, 6060 Sarnen
Tel. 041 666 61 70
finanzdepartement@ow.ch
www.ow.ch

kanton glarus

Telefon 055 646 60 11/12/15
E-Mail: staatskanzlei@gl.ch
www.gl.ch

Regierungsrat
Rathaus
8750 Glarus

per E-Mail
ncsc@gs-efd.admin.ch

Glarus, 22. März 2022
Unsere Ref: 2022-29

Vernehmlassung i. S. Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Hochgeachteter Herr Bundesrat
Sehr geehrte Damen und Herren

Das Eidgenössische Finanzdepartement gab uns in eingangs genannter Angelegenheit die Möglichkeit zur Stellungnahme. Dafür danken wir und lassen uns gerne wie folgt vernehmen:

Wir teilen Ihre Einschätzung, dass Cyberrisiken zu den wichtigsten Bedrohungen der Sicherheit und der Wirtschaft der Schweiz geworden sind. Um die Bedrohungslage besser einzuschätzen und darauf angemessen reagieren zu können, ist es unumgänglich, dass Angriffe auf Unternehmen und Behörden in der Schweiz früh erkannt werden können. Die Einführung einer Meldepflicht für Betreiberinnen kritischer Infrastrukturen scheint uns dafür ein geeignetes Mittel zu sein. Mit der Integration dieser Aufgabe im Informationssicherheitsgesetz (ISG) werden nun die Grundzüge der Meldepflicht auf einer adäquaten Rechtsgrundlage verankert und das Nationale Zentrum für Cybersicherheit (National Cyber Security Centre – NCSC) gestärkt.

Wir begrüssen, dass auf Gesetzesstufe für die Definition der von der Meldepflicht betroffenen kritischen Bereiche soweit als möglich auf klare Definitionen aus bereits bestehenden Bundesgesetzen abgestellt wird. Es stellt sich jedoch die Frage, ob im Rahmen der Verordnung noch Konkretisierungen vorgenommen werden müssen, beispielsweise ob alle Spitäler, die sich auf einer kantonalen Spitalliste befinden (Art. 74b Bst. g E-ISG), also vom kleinsten Regionalspital über Rehabilitationskliniken bis hin zu den Universitätsspitälern, als für die Landesversorgung kritische Infrastrukturen betrachtet werden müssen.

Es ist zu prüfen, ob die Plattformen über die das elektronische Patientendossier (EPD) läuft, nicht auch in den Bereich der Meldepflicht fallen sollten. Mit der Verbreitung des EPDs werden die darin enthaltenen Daten zu einer Informationsquelle für die Versorgung von Patientinnen und Patienten und dadurch an Bedeutung gewinnen. Eine Störung oder ein Ausfall der zentralen Plattformen kann somit zu einer direkten Gefährdung von Patientinnen und Patienten führen.

Die Vorlage behandelt hauptsächlich die Meldepflicht für Betreiberinnen von kritischen Infrastrukturen von Cyberangriffen. Dabei darf aber die Wichtigkeit der Meldung von Cybervorfällen und Schwachstellen auf freiwilliger Basis nicht vergessen gehen. Auch dieses bereits be-

stehende Mittel soll durch das NCSC weiterhin gefördert werden. Die Möglichkeit der Verwendung desselben Systems zur Übermittlung der Meldung (gemäss Art. 74f Abs.1 E-ISG) von Cyberangriffen, wie auch von Cybervorfällen und Schwachstellen könnte dabei für die Meldenden ein Anreiz zur freiwilligen Meldung sein.

Der Gesetzesentwurf sieht auch vor, dass Betreiberinnen von kritischen Infrastrukturen ihre Meldung auch an weitere Stellen oder Behörden übermitteln können, ev. mit Angaben, die über die durch das NCSC definierten Mindestinformationen hinausgehen, dies im Sinne einer Mehrfachnutzung der Meldung (Art. 74f Abs. 2 und 3 E-ISG). Wir bitten Sie, sich in der konkreten Umsetzung dieser Bestimmung nicht auf die Übermittlung an nationale Stellen und Behörden zu beschränken, sondern auch die Zusammenarbeit mit kantonalen Behörden zu suchen, da es auch auf kantonaler Ebene bereits teilweise Verpflichtungen zur Meldung von Cyberangriffen von kritischen Infrastrukturen gibt. Eine möglichst einfache Übergabe der Meldungen muss auch da vorgesehen werden.

Genehmigen Sie, hochgeachteter Herr Bundesrat, sehr geehrte Damen und Herren, den Ausdruck unserer vorzüglichen Hochachtung.

Freundliche Grüsse

Für den Regierungsrat

Marianne Lienhard
Landammann

Hansjörg Dürst
Ratsschreiber

E-Mail an (PDF- und Word-Version):
- ncsc@gs-efd.admin.ch

Kanton Schaffhausen
Regierungsrat
Beckenstube 7
CH-8200 Schaffhausen
www.sh.ch

T +41 52 632 71 11
F +41 52 632 72 00
staatskanzlei@sh.ch

Regierungsrat

Eidgenössisches Finanzdepartement EFD
3003 Bern

per E-Mail an:
ncsc@gs-efd.admin.ch

Schaffhausen, 5. April 2022

Vernehmlassung zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe und als Folge davon zur Änderung des Informationssicherheitsgesetzes (ISG)

Sehr geehrte Damen und Herren

Mit Schreiben des Eidgenössischen Finanzdepartements vom 12. Januar 2022 wurden die Kantonsregierungen zur Vernehmlassung in oben genannter Angelegenheit eingeladen. Wir bedanken uns für diese Möglichkeit.

Cyberrisiken sind zu einer der grössten Bedrohungen der Sicherheit und der Wirtschaft der Schweiz geworden. Hier gilt es mit vereinten Kräften das gesammelte Wissen zu bündeln und gezielt ein- und umzusetzen. Die Fachstellen des Kantons Schaffhausen schätzen die Bedrohungslage als durchaus akut ein und begrüssen grundsätzlich die Einführung einer Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe sowie die damit einhergehende Änderung des Bundesgesetzes über die Informationssicherheit (ISG).

Die geplante Meldepflicht beim Nationalen Zentrum für Cybersicherheit (NCSC) sollte ein guter Anfang für eine verbesserte Übersicht über Cyberangriffe in der Schweiz sein. Ziel der Meldepflicht ist - unter anderem - die Frühwarnung und eine bessere Einschätzung der aktuellen Bedrohungslage. Nach einem Cyberangriff soll aus unserer Sicht das NCSC die betroffene Betreiberin kritischer Infrastrukturen bei der Vorfallbewältigung unterstützen können. Zudem wäre ein regelmässiges Reporting an die Sicherheitsverantwortlichen der Kantone sinnvoll. Interessant wäre dabei insbesondere, wenn nach einer erfolgten Meldung an das NCSC diese - wie auch

für Schwachstellen/aktuelle Bedrohungen - über eine gemeinsame Informations- und Austauschplattform bereitgestellt werden. So könnte das Cyberwissen besser ausgetauscht werden. Dies wäre ein Mehrwert für alle Betreiberinnen kritischer Infrastrukturen und hätte aus unserer Sicht den Vorteil, dass dadurch die Akzeptanz der Meldepflicht erhöht wird.

Wir erlauben uns zudem noch folgende artikelspezifische Anmerkungen:

- Art. 74 Abs. 2 lit. b ISG
  Damit die darin erwähnten Informationen und Empfehlungen zugänglich gemacht werden können, wäre die Einführung einer gemeinsamen Plattform zu begrüssen.
- Art. 74 Abs. 4 ISG
  Die Voraussetzung des Einverständnisses der Betreiberin ist hier besonders hervorzuheben. Ein solches könnte unter Definition gewisser Bedingungen (Dringlichkeit und Gefährdungsgrad) auch im Voraus erteilt werden.

Für Ihre Kenntnisnahme und die Berücksichtigung unser Stellungnahme danken wir Ihnen.

Freundliche Grüsse
Im Namen des Regierungsrates
Die Präsidentin:

REGIERUNGSRAT DES KANTONS SCHAFFHAUSEN

Dr. Cornelia Stamm Hurter

Der Staatsschreiber-Stv.:

Christian Ritzmann

KANTON solothurn

Finanzdepartement

Rathaus
Barfüssergasse 24
4509 Solothurn
Telefon 032 627 20 57
finanzdepartement@fd.so.ch
so.ch

Peter Hodel
Regierungsrat

Eidgenössisches Finanzdepartement
Herr Bundesrat Ueli Maurer
Bernerhof
Bundesgasse 3
3011 Bern

23. Februar 2022

Vernehmlassung zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Mit Schreiben vom 12. Januar 2022 haben Sie uns die Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe zur Vernehmlassung unterbreitet. Wir danken Ihnen für die Gelegenheit zur Stellungnahme und nehmen diese gerne wahr.

Die Meldepflicht wird sehr positiv aufgenommen. Sowohl die Vernehmlassung als auch der zugehörige erläuternde Bericht sind fortschrittlich und zukunftsgerichtet. Die darin beschriebene Meldepflicht entspricht auch der des Kantons Solothurns in Bezug auf die Cybersicherheit und unseren Reaktionen auf Cyberangriffe.

Die Vorteile der Meldepflicht sind nachvollziehbar, einfach umsetzbar und wichtig für die Bekämpfung der Cyberkriminalität. Die Umsetzung soll so rasch als möglich erfolgen. Massnahmen wie die zentrale Anlaufstelle beim Bund, gleiche Prozesse für alle Behörden, ein Austausch dieser wichtigen Informationen sowie die Unterstützung durch das Nationale Zentrum für Cybersicherheit (NCSC) bei einem Vorfall werden als sehr wertvoll angesehen. Sie helfen, um künftig noch besser gegen Cyberrisiken geschützt zu sein.

Die Verteilung von Informationen hilft präventiv auf Gefahren reagieren zu können. Mit dem NCSC und dessen Unterstützung steht den öffentlichen Verwaltungen ein starker Partner zur Seite.

Dennoch gibt es aus Sicht des Kantons Solothurn folgende Punkte, die präzisiert werden müssten. Diese sollen helfen, Akzeptanz und Durchsetzung der Meldepflicht zu erhöhen.

- Bei einer Verletzung der Melde- oder Auskunftspflicht kann das NCSC eine Verfügung mit Bussandrohung erlassen. Die Obergrenze der Busse liegt bei Fr. 100'000.00. Die Busse kommt als ultima ratio erst nach einer Kaskade von Massnahmen zum Zug und hat weitgehend symbolischen Charakter. Wir bezweifeln allerdings, ob eine Bussandrohung in dieser Höhe bei den kritischen Infrastrukturen auf die nötige Akzeptanz stösst und dazu beiträgt, die Verantwortlichen zu pflichtgemässem Verhalten zu bewegen.
- Zwingend zu beschreiben ist des Weiteren, wie der Vorgang der Melde- oder Auskunftspflicht abläuft. Die beschriebene Kontaktaufnahme des NCSC muss sicher vor der Verfügung mit Bussandrohung erfolgen.

- Der administrative Aufwand sowie der eigentliche Meldeprozess müssen schlank gehalten werden. Mit jeder zusätzlichen technischen oder organisatorischen Hürde wächst das Risiko, dass weniger Vorfälle erfasst und dem NCSC gemeldet werden. Dies würde den Nutzen erheblich schmälern.

Der Kanton Solothurn begrüsst die Anpassungen im „Bundesgesetz über die Informationssicherheit beim Bund". Sie sind, nebst den technischen Massnahmen, ein wichtiger Schritt in der Bekämpfung von Cyberrisiken.

Freundliche Grüsse

Peter Hodel
Regierungsrat

Regierungsrat des Kantons Schwyz

VERSENDET AM 12. APR. 2022

kantonschwyz

6431 Schwyz, Postfach 1260

per E-Mail
Eidgenössisches Finanzdepartement
Bundeshaus
3003 Bern

ncsc@gs-efd.admin.ch

Schwyz, 5. April 2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe
Vernehmlassung des Kantons Schwyz

Sehr geehrter Herr Bundesrat

Mit Schreiben vom 12. Januar 2022 hat das Eidgenössische Finanzdepartement den Kantonsregierungen die Unterlagen zur Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen zur Vernehmlassung bis 14. April 2022 unterbreitet.

Der Regierungsrat unterstützt die Schaffung einer Meldepflicht für die Betreiber kritischer Infrastrukturen. Mit der Meldeplicht können Betroffene gezielter unterstützt werden und durch eine schnelle und koordinierte Reaktion auf einen Cyberangriff lässt sich das Schadenpotenzial minimieren. In Art. 73c sowie Art. 74b nSIG verortet der Regierungsrat jedoch Anpassungsbedarf.

Das Entfallen der Anzeigepflicht gemäss Art. 73c Abs. 2 nISG wird kritisch beurteilt. Insbesondere bei schweren Straftaten ist der Ermessensspielraum der Leitung des NCSC einzuschränken bzw. sind geeignete Massnahmen zu treffen, um sicherzustellen, dass schwere Straftaten konsequent zur Anklage gebracht werden. Zudem werden die Betreiber der elektronischen Patientendossiers (Gemeinschaften und Stammgemeinschaften) nach Art. 10 des Bundesgesetzes über das elektronische Patientendossier vom 19. Juni 2015 (SR 816.1) in Art. 74b nISG nicht explizit genannt. Aus Sicht des Regierungsrats ist es zu prüfen, diese Gemeinschaften aufgrund des Schadenpotenzials ebenfalls der Meldepflicht zu unterstellen.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und versichern Sie, Herr Bundesrat, unserer vorzüglichen Hochachtung.

Im Namen des Regierungsrates:

Petra Steimen-Rickenbacher
Landammann

Regierungsrat Kanton Schwyz

Dr. Mathias E. Brun
Staatsschreiber

Kopie an:
– die Schwyzer Mitglieder der Bundesversammlung.

Der Regierungsrat des Kantons Thurgau

Thurgau

Staatskanzlei, Regierungsgebäude, 8510 Frauenfeld

Eidgenössisches Finanzdepartement
(EFD)
Herr Ueli Maurer
Bundesrat
3003 Bern

Frauenfeld, 12. April 2022

Bundesgesetz über die Informationssicherheit beim Bund: Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Vernehmlassung

Sehr geehrter Herr Bundesrat

Wir danken Ihnen für die Gelegenheit, zu den geplanten Änderungen des Bundesgesetzes über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) betreffend Meldepflicht von Betreiberinnen und Betreibern kritischer Infrastrukturen für Cyberangriffe Stellung zu nehmen.

Die Einführung einer Meldepflicht für Betreiberinnen und Betreiber kritischer Infrastrukturen bei Cyberangriffen ist grundsätzlich zu begrüssen. Es ist für staatliche und private Stellen von Bedeutung, dass eine aussagekräftige Übersicht über Cyberangriffe erstellt wird, Betroffene bei der Bewältigung von Cyberangriffen unterstützt werden und Betreiberinnen und Betreiber kritischer Infrastrukturen rechtzeitig und angemessen gewarnt werden können. Dies ist ein wichtiger Beitrag zur Verbesserung der Resilienz der Schweiz im Umgang mit Cyberbedrohungen. Allerdings wird das auch zur Folge haben, dass im Kanton Thurgau der Dienst Cybercrime der Kantonspolizei ausgebaut werden muss.

Der vorliegende Entwurf für die Änderung des ISG geht allerdings sehr weit und führt zu einem grossen Ausbau der Kompetenzen des Nationalen Zentrums für Cybersicherheit (NCSC). Insbesondere ist unzureichend definiert, welche Vorfälle zu melden sind und welchen Umfang Meldungen zu enthalten haben. Der mit einer Meldepflicht verbundene Aufwand muss aus ökonomischen und sicherheitstechnischen Gründen in Grenzen gehalten werden.

Regierungsgebäude, 8510 Frauenfeld
T +41 58 345 53 10, F +41 58 345 53 54
www.tg.ch

Titel des Erlasses

Wir erachten den Titel des Erlasses „Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG)“ als unangemessen. Dieser Erlass regelt nicht nur die Informationssicherheit beim Bund, sondern damit sollen auch Kantone und Gemeinden sowie private Betreiberinnen und Betreiber von kritischen Infrastrukturen vor Cyberangriffen besser geschützt werden. Der Titel des Erlasses ist daher zu präzisieren und gleichzeitig zu kürzen: Informationssicherheitsgesetz (ISG).

Art. 1 Abs. 1 Zweck

Die Zweckbestimmung weist keinen normativen Gehalt auf. Sollte an der Zweckbestimmung festgehalten werden, so ist Abs. 1 nicht in lit. a und lit. b aufzuteilen. Die Aufteilung führt zu einer künstlichen Verkomplizierung der Bestimmung.

Art. 73a Grundsatz

Die Aufzählung der Aufgaben des nationalen Zentrums für Cybersicherheit (NCSC) ist zu umfassend. Dieser Ausbau führt zu erheblichen Kosten, wobei zu bezweifeln ist, dass ein entsprechender Nutzen gegenübersteht. Die Aufgabenliste ist daher zu kürzen. Insbesondere sollte lit. c dieser Bestimmung in lit. a integriert werden:

lit. a: Sensibilisierung der Öffentlichkeit auf Cyberrisiken und zur Cybersicherheit.

Art. 74b und 74c Bereiche/Ausnahmen von der Meldepflicht

Die Meldepflichten in Art. 74b sind zu umfassend; sie sind in dieser Form nicht erforderlich. Die Ausnahmen gemäss Art. 74c sind unübersichtlich und wenig praktikabel. Beide Bestimmungen sind daher zu überarbeiten. Der Ausbau der Zuständigkeiten des NCSC und der Meldepflichten wird nicht zu einer Reduktion von Cyberangriffen führen. Es ist zweifelhaft, dass damit die Widerstandsfähigkeit der Schweiz gegenüber Cyberrisiken erhöht wird. Die Meldepflicht sollte ohnehin an den zuständigen IT-Betreiber delegiert werden können. Die Formulierung in dieser Bestimmung würde sonst dazu führen, dass in Fällen, in denen eine Gemeinde ihre IT-Infrastruktur an den Kanton ausgelagert hat, sowohl die Gemeinde als auch der Kanton bei einem Vorfall meldepflichtig wären.

Art. 74d Zu meldende Cyberangriffe

Der Begriff „kritisch“ in Abs. 1 lit. a ist nicht definiert. Es fehlen genauere Angaben, worauf sich der Begriff „kritisch“ beziehen soll.

Nach Abs. 1 lit. b sind Cyberangriffe eines fremden Staates anders zu werten als landesinterne Cyberangriffe. Es ist nicht nachvollziehbar, weshalb dies ein wesentliches Kriterium sein sollte, um die Bedeutung eines Cyberangriffs zu qualifizieren.

Laut Abs. 1 lit. d ist ein Cyberangriff meldepflichtig, wenn Anzeichen dafür bestehen, dass dieser länger als 30 Tage unentdeckt blieb.

Ein anerkanntes Modell zur Beschreibung der Stufen eines Cyberangriffs ist die „Cyber Kill Chain". Diese beschreibt ein schrittweises, immer tieferes Vordringen eines Angreifers. In den ersten Phasen eines Cyberangriffs werden typischerweise Organisationen und Systeme ausgekundschaftet, bevor in der Folge Schwachstellen gezielt ausgenutzt werden und das eigentliche Ziel des Angriffs erreicht wird. Die zu Beginn eingesetzten Schadprogramme oder Vorgehensweisen gefährden die Funktionsfähigkeit einer kritischen Infrastruktur in aller Regel noch nicht unmittelbar. Wenn ein Angriffsversuch in einer der frühen Phasen verhindert wird, so bleibt ein Cyberangriff erfolglos. Spuren solcher Angriffswerkzeuge bleiben aber häufig in der IT-Infrastruktur für längere Zeit bestehen. Mit der vorgeschlagenen Bestimmung ist nicht klar, ob das Auffinden früherer, möglicherweise gestoppter oder nicht erfolgreicher Angriffskomponenten meldepflichtig ist. Wenn bei einer Betreiberin oder einem Betreiber kritischer Infrastrukturen Instrumente gefunden werden, die aktiv für einen Cyberangriff verwendet wurden, so sind diese, ungeachtet der Dauer seit ihrer Entdeckung, gemäss Art. 74d Abs. 1 lit. a bis c ohnehin meldepflichtig. Abs. 1 lit. d ist daher entsprechend zu präzisieren:

> *d. die direkt und unmittelbar für das Ziel des Cyberangriffs verwendeten Instrumente länger als 30 Tage unentdeckt blieben.*

Art. 74e Inhalt der Meldung

Es fehlen Angaben, welche Informationen zur kritischen Infrastruktur bei einer Meldung anzugeben sind. Es dürfen in solchen Fällen keine technischen Informationen eingefordert werden, die der Geheimhaltung entgegenwirken. Andernfalls bestünde durch das Weitergeben vertraulicher Infrastrukturinformationen die Gefahr von weiteren Informationslecks.

Art. 74g Auskunftspflicht

Diese absolute Formulierung ist problematisch. Sowohl kantonale Behörden als auch Private sind diesbezüglich den eigenen IT-Sicherheits-Richtlinien verpflichtet.

Art. 74i Widerhandlungen gegen Verfügungen des NCSC

Die für eine Verletzung der Melde- oder Auskunftspflichten vorgesehene Busse von Fr. 100'000 ist unverhältnismässig. Es gibt keinen Grund, die Verfügungen einer einzelnen Behörde mit einer solchen Strafandrohung zu versehen. Für Ungehorsam gegen amtliche Verfügungen existiert ohnehin die Strafbestimmung von Art. 292 Strafgesetzbuch (StGB; SR 311.0). Auf Art. 74i ist daher zu verzichten.

Art. 75 Bearbeitung von Personendaten

Es geht zu weit, dem NCSC zu erlauben, Personendaten zu bearbeiten, die religiöse, weltanschauliche oder politische Ansichten enthalten. Die – gesetzestechnisch unschön als Nachsatz in einer Aufzählung eingefügte – Einschränkung, die Bearbeitung sei nur zulässig, wenn sie für die Bewertung von konkreten Bedrohungen und Gefahren im Bereich der Cybersicherheit erforderlich ist, ändert nichts daran. Es ist zudem problematisch, dass das NCSC diese Personendaten bearbeiten kann, ohne dass dies für die betroffenen Personen erkennbar ist. Diese Bestimmung ist dahingehend zu ändern, dass das NCSC verpflichtet ist, die betroffenen Personen zumindest nachträglich über die Bearbeitung ihrer Personendaten zu informieren.

Art. 76, Art. 76a und Art. 77 Zusammenarbeit

Diese Bestimmungen erlauben es dem NCSC, Daten unkontrolliert mit Behörden im Inland und Ausland auszutauschen. Die Einschränkung, dies müsse zum Schutz von kritischen Infrastrukturen vor Cyberrisiken erforderlich sein, ist unzureichend. Es ist dem NCSC nicht zu gestatten, nach eigenem Gutdünken über solche Daten zu verfügen.

Mit freundlichen Grüssen

Die Präsidentin des Regierungsrates

Der Staatsschreiber

DER REGIERUNGSRAT · DES KANTONS THURGAU ·

Numero			Bellinzona
1407	cl	0	23 marzo 2022

Consiglio di Stato
Piazza Governo 6
Casella postale 2170
6501 Bellinzona
telefono +41 91 814 41 11
fax +41 91 814 44 35
e-mail can@ti.ch
web www.ti.ch

Repubblica e Cantone
Ticino

Il Consiglio di Stato

Consigliere federale
Ueli Maurer
Direttore del Dipartimento federale
delle finanze
Bundesgasse 3
3003 Berna

ncsc@gs-efd.admin.ch

Procedura di consultazione "Obbligo di notifica di ciberattacchi per i gestori di infrastrutture critiche"

Onorevole Consigliere federale,

vi ringraziamo per averci dato l'opportunità di esprimere la nostra opinione in merito alla summenzionata procedura di consultazione. Qui di seguito formuliamo le nostre osservazioni.

Lo scrivente Consiglio di Stato si esprime sostanzialmente a favore dell'introduzione dell'obbligo di notifica di ciberattacchi per i gestori delle infrastrutture critiche come da voi proposto. Riteniamo per contro che vadano considerate le caratteristiche eterogenee dei diversi gestori e che sarebbe opportuno prevedere l'esenzione dalla notifica per quelle organizzazioni le cui dimensioni o il possibile danno per l'economia nazionale sono ridotti.

Voglia gradire, Onorevole Consigliere federale, i sensi della nostra massima stima.

PER IL CONSIGLIO DI STATO

Il Presidente
Manuele Bertoli

Il Cancelliere
Arnoldo Coduri

Copia a:
- Consiglio di Stato (decs-dir@ti.ch; dfe-dir@ti.ch; di-dir@ti.ch; dss-dir@ti.ch; dt-dir@ti.ch; can-sc@ti.ch)
- Delegato cantonale per le relazioni esterne (francesco.quattrini@ti.ch)
- Deputazione ticinese alle Camere federali (can-relazioniesterne@ti.ch)
- Pubblicazione in internet
- Divisione delle risorse (dfe-dr@ti.ch)
- Centro sistemi informativi (csi@ti.ch)

Landammann und Regierungsrat des Kantons Uri

Eidgenössisches Finanzdepartement (EFD)
Geschäftsstelle NCSC
Schwarztorstrasse 59
3003 Bern

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe; Vernehmlassung

Sehr geehrte Damen und Herren

Der Bundesrat hat am 12. Januar 2022 das Eidgenössische Finanzdepartement (EFD) beauftragt, bei den Kantonen ein Vernehmlassungsverfahren zur Einführung einer Meldepflicht für Cyberangriffe und der damit verbundenen Änderung des Informationssicherheitsgesetzes (ISG) durchzuführen.

Der Kanton Uri betrachtet Cyberrisiken wie der Bund als eine der wichtigsten Bedrohungen der Sicherheit von Bürgerinnen und Bürgern, Wirtschaft und Verwaltung. Eine schweizweite Einschätzung der Bedrohungslage kann durch eine Meldepflicht von Cyberangriffen mit höherer Qualität gestaltet werden. Die Sammlung der Meldungen im nationalen Zentrum für Cybersicherheit (NCSC früher MELANI) macht sehr viel Sinn damit eine Gesamtübersicht/Lagebild gewonnen werden kann, die Erkenntnisse weitergegeben und Betroffene unterstützt werden können. Die positiven Erfahrungen aus dem geschlossenen Kundenkreis von MELANI können durch die Meldepflicht auch sektorbezogen fortgeführt und erweitert werden. Der Kanton Uri ist seit 2014 Mitglied des geschlossenen Kundenkreises und schätzt die Arbeit dessen sehr. Die Verankerung der Meldepflicht im Informationssicherheitsgesetz ist naheliegend und wird befürwortet.

Der Kanton Uri nimmt zu einzelnen Artikeln wie folgt Stellung:

Artikel 74a In diesem Artikel steht wörtlich geschrieben: «Die Betreiberinnen von kritischen Infrastrukturen müssen dem NCSC Cyberangriffe nach deren Entdeckung so rasch als möglich melden, etc..»

Wir schlagen folgende Änderung vor: «Die Betreiberinnen von kritischen Infrastrukturen müssen dem NCSC Cyberangriffe sofort nach Vermutung oder Erkennung eines Cypberangriffs melden».

Artikel 74b Eine Meldung sollte für alle weiteren Organisationen empfohlen werden. Sie muss möglichst umfassend, landesweit und sektorenübergreifend sein.

Artikel 74c Wir würden diesen Artikel ersatzlos streichen.

Artikel 74i Eine Busse wird erst nach nicht befolgter, schriftlich belegter Rücksprache des NCSC mit dem Meldenden ausgesprochen.

Artikel 76a Informationen über Angreifende, Methoden und Taktiken sind wichtig und sollten vollumfänglich weitergegeben werden dürfen.

Artikel 79 Besonders schützenswerte Personendaten dürfen höchstens zwei Jahre aufbewahrt werden. Leider fehlen ergänzende Aussagen, wie dies überprüft werden soll.

Damit die Meldung eines Cyberangriffs nicht an verschiedene Organisationen wie Strafverfolgungsbehörden, Nachrichtendienst Bund, Eidgenössische Finanzmarktaufsicht (FINMA) oder Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB) einzeln gemacht werden muss, sollte das NCSC die notwendigen Weiterleitungen in Absprache mit der meldenden Organisation direkt vornehmen.

Die Meldepflicht für kritische Infrastrukturen mit einem einfachen NCSC-Meldeformular hat in unserem Kanton keine Zusatzkosten oder weitere Ressourcen für diese Informationssicherheitsgesetzeserweiterung zur Folge.

Sehr geehrte Damen und Herren, wir bedanken uns für die Möglichkeit zur Stellungnahme und grüssen Sie freundlich.

Altdorf, 29. März 2022

Im Namen des Regierungsrats

Der Landammann Der Kanzleidirektor

REGIERUNGSRAT DES KANTONS URI

Urban Camenzind Roman Balli

canton de vaud
LIBERTÉ ET PATRIE

CONSEIL D'ETAT

Château cantonal
1014 Lausanne

Monsieur le Conseiller fédéral
Ueli Maurer
Chef du Département fédéral des finances
DFF
3000 Berne

Par courrier électronique à
ncsc@gs-efd.admin.ch

Lausanne, le 13 avril 2022

Obligation de signaler les cyberattaques contre des infrastructures critiques

Monsieur le Conseiller fédéral,

Le Conseil d'Etat du Canton de Vaud vous remercie de l'avoir consulté sur l'obligation de signaler les cyberattaques contre des infrastructures critiques.

Le Conseil d'Etat partage la préoccupation globale de la Confédération concernant la vulnérabilité des infrastructures critiques face aux cyberrisques et soutient le projet mis en consultation.

L'introduction d'une obligation d'annonce des cyberattaques dans une loi est une nécessité qui permet de mieux apprécier le niveau de menaces et contribue à améliorer la cyberrésilience de notre société numérique. Cette disposition devrait en particulier permettre de diminuer le chiffre noir, soit les infractions non dénoncées à la Police, qui est aujourd'hui estimé entre 85% et 90% des infractions dans le cyberespace au niveau des annonces à la Police. Le Conseil d'Etat est également d'avis que l'absence d'indicateurs fiables empêche aujourd'hui les instances gouvernementales de prendre la mesure de la gravité de la situation et ainsi d'adopter les mesures nécessaires et adaptées à la réalité en matière de réponse sécuritaire.

Le Conseil d'Etat est également favorable à l'approche décrite dans le rapport explicatif consistant à soutenir les entreprises dans leurs démarches de signalement (simplification des formulaires, incitations positives de type évaluation technique par le Centre national pour la cybersécurité (NCSC) ou soutien dans la gestion de l'attaque) sans exclure néanmoins la possibilité de sanctions répressives et pécuniaires. Les expériences de la déclaration obligatoire pour le secteur financier pourraient ainsi être utiles vu le constat mitigé posé par le Contrôle fédéral des finances en février 2021. Dès lors que les concernés seront soumis à plusieurs obligations d'annonces, le Conseil d'Etat relève la nécessité de coordonner les différentes démarches par une adaptation des formulaires pour éviter de compliquer la tâche des responsables des infrastructures critiques, le Conseil d'Etat souhaite éviter le risque de perdre en qualité ou quantité d'informations dans ce contexte.

Concernant le domaine hospitalier, le Conseil d'Etat estime par ailleurs nécessaire que l'art. 73b soit coordonné avec l'Ordonnance sur les dispositifs médicaux (ODim). La publication d'une vulnérabilité, voire de mesures à prendre, peut en effet mettre l'hôpital dans une situation difficile. Toute modification d'un dispositif médical, si elle n'est pas faite par le fabriquant, lui fait perdre son certificat de conformité. L'hôpital serait, dans les faits, dans l'impossibilité de suivre les recommandations du Centre national pour la cybersécurité. Le Conseil d'Etat estime donc nécessaire que le NCSC puisse les imposer aux fabricants.

En conclusion, le Conseil d'Etat réitère son soutien à la mise en application législative de l'obligation de signaler les cyberattaques contre des infrastructures critiques.

Nous vous prions de croire, Monsieur le Conseiller fédéral, à l'assurance de notre meilleure considération.

AU NOM DU CONSEIL D'ETAT

LA PRESIDENTE	LE CHANCELIER
Nuria Gorrite	Aurélien Buffat

Copies

- Direction générale du numérique et des systèmes d'information
- Office des affaires extérieures

Conseil d'Etat
Staatsrat
CP 478, 1951 Sion

CANTON DU VALAIS
KANTON WALLIS

2022.01503

P.P. CH-1951 Sion A Poste CH SA

Département fédéral des finances
Monsieur Ueli Maurer
Conseiller fédéral
Bundesgasse 3
3003 Berne

Date 6 avril 2022

Obligation de signaler les cyberattaques contre des infrastructures critiques
Prise de position cantonale

Monsieur le Conseiller fédéral,

Le Conseil d'Etat du canton du Valais vous remercie de lui avoir soumis la consultation sur les modifications apportées à la loi sur la sécurité de l'information (LSI).

Le Gouvernement valaisan relève positivement l'introduction de l'obligation, pour les infrastructures critiques, d'annoncer les cyberattaques subies au Centre national de cybersécurité (NCSC). Cette mesure permettra au NCSC d'obtenir une vue d'ensemble plus complète et plus précise de la situation. La résilience globale du pays face aux cybermenaces sera ainsi améliorée.

Nous saluons également le rôle de soutien aux infrastructures critiques nouvellement dévolu au NCSC. L'expérience de cette unité est précieuse et son support en cas de cyberattaques sera profitable à toutes les infrastructures critiques bénéficiaires.

Nous relevons que l'article 74b, définit les cantons, mais aussi les communes et certaines organisations exécutant des tâches régaliennes, notamment celles en lien avec l'approvisionnement en eau potable, le traitement des eaux usées et des déchets, l'approvisionnement énergétique, la sécurité, comme des infrastructures critiques soumises à l'obligation d'annonce. L'article 74c, al. b, interroge toutefois sur le devoir d'annonce des petites structures comme les communes. Une précision dans la version finale de la loi modifiée ou dans le cadre de l'ordonnance serait bienvenue.

D'autre part, l'art. 5 précise la différence entre un cyberincident et une cyberattaque. Seules les cyberattaques devront être annoncées au NCSC. Toutefois les articles 73a à 73c utilisent le terme cyberincident, ce qui pourrait créer une certaine confusion.

En conclusion, le canton du Valais est favorable aux modifications de la LSI proposées par la consultation du Conseil fédéral du 12 janvier 2022 et est convaincu que ces évolutions permettront de renforcer le rôle du NCSC et d'améliorer la résilience du pays face aux cybermenaces.

Nous vous remercions de nous avoir consultés et vous prions d'agréer, Monsieur le Conseiller fédéral, l'expression de notre considération distinguée.

Au nom du Conseil d'Etat

Le président

Frédéric Favre

CANTON DU VALAIS CONSEIL D'ETAT

Le chancelier

Philipp Spörri

Copie à ncsc@gs-efd.admin.ch

Place de la Planta 3, CP 478, 1951 Sion
Tél. 027 606 21 00

Kanton Zug

Regierungsrat

Regierungsrat, Postfach, 6301 Zug

Nur per E-Mail
Eidgenössisches Finanzdepartement
Herr Bundesrat Ueli Maurer
Bernerhof
3003 Bern

Zug, 15. März 2022 rv

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe
Vernehmlassung des Kantons Zug

Sehr geehrter Herr Bundesrat Maurer
Sehr geehrte Damen und Herren

Mit Schreiben vom 12. Januar 2022 hat das Eidgenössische Finanzdepartement (EFD) das Vernehmlassungsverfahren eröffnet und die Kantonsregierungen zur Einreichung einer Stellungnahme bis am 14. April 2022 eingeladen.

Wir stellen folgende

Anträge:

1. nArt. 73b Abs. 2 sei dahingehend zu ergänzen, dass mit gemeldeten Sicherheitsvorfällen nicht vertrauliche interne Informationen wie interner Netzaufbau mit IP-Adressen oder Anmeldeinformationen an Dritte weitergeleitet werden dürfen. Ausserdem sei explizit festzuhalten, dass das NCSC aufgrund von gemeldeten Sicherheitsvorfällen kein Bewertungs-Dashboard im Sinne einer qualitativen Informationssicherheitsbewertung pro Unternehmen oder Behörden erstellt.

2. nArt. 73c Abs. 2 sei dahingehend zu ändern, dass durch eine nähere Definition der Schwere der Straftat der Ermessensspielraum der Leiterin oder des Leiters der NCSC bei der Weitergabe von Informationen an die Strafverfolgungsbehörden eingegrenzt wird.

3. Die Geltungsbereiche und die Menge der meldepflichtigen Betreiberinnen kritischer Infrastrukturen gemäss nArt. 74b sei zu überprüfen und zu reduzieren.

4. Der Adressatenkreis der Auswertungen und technischen Analysen gemäss nArt. 76a Abs. 1 sei auf die Strafverfolgungsbehörden auszuweiten.

Regierungsgebäude, Seestr. 2, 6300 Zug
T +41 41 728 33 11
www.zg.ch

Begründung:

Allgemeines
Kaum ein Risikofeld wird in den nächsten Jahren von der öffentlichen und privaten Hand einen derart hohen Effort fordern wie die Cyberkriminalität. Cyberrisiken sind zu einer der wichtigsten Bedrohungen der Sicherheit und der Wirtschaft der Schweiz geworden.

Das Nationale Zentrum für Cybersicherheit (NCSC) als geplante, neue Meldestelle kann auf die mehrjährige Erfahrung der vormaligen Stelle «MELANI» aufbauen. Das NCSC hat sich die Reputation erarbeitet, sehr professionelle und wertvolle Arbeit zu leisten. Die geplante Meldepflicht ermöglicht dem NCSC eine verbesserte Übersicht über Cyberangriffe und erlaubt, Betroffene bei der Bewältigung von Cyberangriffen zu unterstützen und andere Betreiberinnen kritischer Infrastrukturen zu warnen. Die Meldepflicht soll im Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) als Rechtsgrundlage verankert werden.

Aufgrund des Systemwechsels von einer bisher freiwilligen Meldung zu einer Pflichtmeldung wird der Aufwand steigen, zumal auch eine Unterstützungsleistung an die betroffenen Infrastrukturbetreiberinnen und -betreiber vorgesehen ist. Entsprechend muss der Bund das NCSC personell aufstocken.

Zum Antrag 1:
Art. 73b Abs. 2 umfasst den Schutz von datenschutzrelevanten Informationen. Bei Sicherheitsvorfällen fallen aber weitere vertrauliche Informationen wie Zugangsdaten, Benutzernamen, Netzwerkadressen, Systembeschreibungen, interne Organisationsdaten etc. an, die unter keinen Umständen an die Öffentlichkeit gelangen dürfen.

Gemäss Vorlage werden die gemeldeten Sicherheitsvorfälle ausgewertet. Die Auswertung darf nicht an die Öffentlichkeit gelangen, da sonst Rückschlüsse auf die Schwachstellen der einzelnen Vorfälle publik werden und dadurch durch Hacker ausgenutzt werden könnten. Zudem besteht die Gefahr, dass Politik und Gesellschaft Ranglisten erstellen und dadurch falsche Eindrücke der gemeldeten Vorfälle entstehen. Beispielsweise könnten Firmen, die viele auch weniger gravierende Vorfälle melden, als unsicher angesehen werden. Solche Vergleiche müssen vermieden werden, weil gerade in öffentlichen Unternehmen die Meldungen dann begründet werden müssten. Allfällige öffentlich zugängliche grafische Vergleiche zwischen den Unternehmen und Bereichen könnten deshalb dazu führen, dass weniger Sicherheitsvorfälle gemeldet werden, da die IT, anstelle Gegenmassnahmen einzuleiten, sich mit Rechtfertigungen beschäftigen muss.

Zum Antrag 2:
Die Weitergabe von Informationen an die Strafverfolgungsbehörden betrachten wir als sinnvoll (vgl. den erläuternden Bericht, Seiten 5 und 15 zu nArt. 73c Abs. 2). Problematisch erachten wir jedoch die Möglichkeit einer von erheblichem Ermessen abhängigen *eingeschränkten* Wei-

tergabe von Informationen an die Strafverfolgungsbehörden, sei es hinsichtlich der Meldung an sich oder deren Vollständigkeit. Die Leiterin oder der Leiter des NCSC entscheidet hiernach mittels eigenem Ermessen über die Schwere der Straftat und die Abwägung zwischen dem Interesse des Staates an einer Strafverfolgung und dem Interesse der meldenden Person an der Vertraulichkeit der Meldung. Dies birgt das Risiko eines unvollständigen Lagebildes einerseits und Wissenslücken, insbesondere bezüglich des Auftretens neuer Phänomene, andererseits. Die koordinierte Strafverfolgung wird damit erschwert.

Begrüsst wird dagegen die Spezifizierung der Meldepflicht gemäss nArt. 74d Abs. 2 (vgl. Seite 21 des erläuternden Berichts) hinsichtlich der Vorgabe, dass ein Cyberangriff bei strafrechtlich relevanten Begleitumständen immer zu melden ist. Dies erlaubt eine umfassende Einschätzung der Bedrohungslage für kritische Infrastrukturen durch Cyberkriminelle.

Zum Antrag 3:
Wir begrüssen die Einführung einer Meldepflicht bei Cyberangriffen für Betreiberinnen kritischer Infrastrukturen, die Schaffung der erforderlichen gesetzlichen Grundlage durch entsprechende Ergänzung des Informationssicherheitsgesetzes (ISG) sowie die Verankerung des nationalen Zentrums für Cybersicherheit als zentrale Meldestelle.

Gleichzeitig sehen wir, dass mit der Meldepflicht ein potenziell grosser administrativer Aufwand auf das NCSC und die Betreiberinnen kritischer Infrastrukturen zukommt. Zu wenig erkennbar ist, wie stark und mit welchen Aufgaben allenfalls die Kantone von dieser Gesetzesrevision betroffen sein werden. So liegt etwa die Zuständigkeit für die Verfolgung und Beurteilung von Widerhandlungen einer Verfügung des NCSC gemäss nArt. 74i bei den Kantonen. Es scheint uns, dass die Liste der Betreiberinnen kritischer Infrastrukturen (nArt. 74b) grosszügig ausgefallen ist.

Zum Antrag 4:
Die Bestimmung von nArt. 76a regelt Art, Umfang und Zweck der Zurverfügungstellung von Informationen des NCSC gegenüber anderen Behörden (vgl. auch Seite 24 des erläuternden Berichts). Während Abs. 2, 3 und 4 die Zurverfügungstellung von Informationen gegenüber dem Nachrichtendienst des Bundes (NDB), den Strafverfolgungsbehörden und den kantonalen Cybersicherheitsstellen in genereller Hinsicht regeln, beschränkt Abs. 1 die Auswertungs- und Analyseunterstützung durch das NCSC auf den NDB.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und bitten Sie, unsere Anliegen zu berücksichtigen.

Zug, 15. März 2022

Freundliche Grüsse
Regierungsrat des Kantons Zug

Martin Pfister
Landammann

Tobias Moser
Landschreiber

Kopie per E-Mail an:
- Eidgenössisches Finanzdepartement (ncsc@gs-efd.admin.ch) im Word- und PDF-Format
- Zuger Mitglieder der Bundesversammlung
- Finanzdirektion (info.fd@zg.ch)
- Volkswirtschaftsdirektion (info.vd@zg.ch)
- Sicherheitsdirektion (info.sd@zg.ch)

Kanton Zürich
Regierungsrat

Eidgenössisches Finanzdepartement
3003 Bern

30. März 2022 (RRB Nr. 541/2022)

Änderung des Bundesgesetzes über die Informationssicherheit beim Bund (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), Vernehmlassung

Sehr geehrter Herr Bundesrat

Mit Schreiben vom 12. Januar 2022 haben Sie uns eingeladen, zur Änderung des Bundesgesetzes über die Informationssicherheit beim Bund (SR 126) Stellung zu nehmen. Wir danken für diese Gelegenheit und äussern uns wie folgt:

Wir halten die Einführung einer Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe für eine sinnvolle ergänzende Massnahme und ein wertvolles Instrument in einer koordinierten Cyberabwehr. Sie sollte jedoch mit einem angemessenen Mehrwert für die beteiligten Akteurinnen und Akteure verbunden sein. Mit den nachstehenden Bemerkungen möchten wir die Entwicklung in diesem Sinne unterstützen.

Allgemeine Bemerkungen

Der erläuternde Bericht setzt sich mit Anreizen und Sanktionen auseinander. Nach unserem Dafürhalten sollte insbesondere der Mehrwert für die verpflichteten Akteurinnen und Akteure im Sinne einer Unterstützung verstärkt werden. Neben der vorgesehenen technischen Einschätzung und Unterstützung steht dabei die frühzeitige Verteilung von Informationen an alle Akteurinnen und Akteure im Vordergrund, beispielsweise über auffällige Aktivitäten oder Anomalien sowie drohende oder laufende Angriffe. Art. 73b Abs. 2 E-ISG sollte daher weiter formuliert werden. In Art. 74 E-ISG sollte sodann klarer umschrieben werden, was mit «Informationen zu aktuellen Cyberrisiken» als Unterstützungsleistung gemeint ist.

Zudem weisen wir darauf hin, dass die Meldepflicht ein nach innen gerichtetes Instrument des Nationalen Zentrums für Cybersicherheit (NCSC) ist. Schutzbedarf besteht allerdings auch nach aussen. Deshalb sind an den Netzübergängen zwischen Ausland und Inland (CH data carriers) Instrumente und Sicherheitsmassnahmen einzusetzen, damit die Schweiz und damit auch der Kanton Zürich vor internationaler Cyberkriminalität geschützt werden kann. Dieses Thema ist allerdings nicht Gegenstand der Vorlage.

Bemerkungen zu einzelnen Bestimmungen

Art. 74 Unterstützung von Betreiberinnen von kritischen Infrastrukturen

Gemäss Art. 74 Abs. 3 E-ISG soll das NCSC private Betreiberinnen bei der Bewältigung von Cybervorfällen und der Behebung von Schwachstellen beraten und unterstützen, wenn die Beschaffung gleichwertiger Unterstützung auf dem Markt nicht rechtzeitig möglich ist. Dies birgt die Gefahr von Fehlanreizen: Eine von einem Cyberangriff betroffene Betreiberin kann sich so auf Staatskosten vom NCSC unterstützen lassen, ohne ein angemessenes Service-Level-Agreement mit einem Incident Containment Service abzuschliessen. Wir regen daher an, jede Betreiberin einer kritischen Infrastruktur zum Bezug eines Incident Containment Service mit vorgegebenen Mindestanforderungen zu verpflichten.

Art. 74b Bereiche

Wir regen an, die Meldepflicht stufenweise (z. B. nach Sektoren) einzuführen. So lassen sich Erfahrungen mit den ersten Beteiligten sammeln und daraus frühzeitig mögliche Verbesserungen ableiten. Zudem erhält das NCSC Zeit, um sich auf seine neue Aufgabe einzustellen. So kann eine Überlastung des NCSC durch viele gleichzeitige Meldungen vermieden werden, was trotz seiner langen Erfahrung im Umgang mit Meldungen eine Gefahr darstellt.
Des Weiteren setzt eine Meldepflicht voraus, dass Cyberangriffe erkannt werden können. Viele Betreiberinnen in den in Art. 74b E-ISG aufgeführten Bereichen verfügen jedoch nicht über die dafür notwendigen Mittel. Es ist daher zu überlegen, wie insbesondere Städte und Gemeinden bei der Erkennung von Cyberangriffen unterstützt werden können. Eine Möglichkeit wäre der Aufbau von kantonalen oder regionalen Cyber Defence Centers.

Art. 74d Zu meldende Cyberangriffe

Art. 74d E-ISG umschreibt die zu meldenden Cyberangriffe in allgemeiner Form. Diese Bestimmung lässt einen allzu grossen Auslegungsspielraum. Für die praktische Handhabung und die erforderliche Handlungssicherheit der verpflichteten Akteurinnen und Akteure bedürfte es einer leicht verständlichen und nachvollziehbaren Umschreibung der zu meldenden Cyberangriffe.
Das NCSC sollte zudem gesetzlich dazu verpflichtet werden, Meldungen von Cyberangriffen, die gemäss Art. 74d Abs. 2 E-ISG mit Erpressung, Drohung oder Nötigung verbunden sind, an die Strafverfolgungsbehörden weiterzuleiten, soweit sich diese Pflicht nicht aus dem Bundespersonalrecht ergibt.

Art. 74f Übermittlung der Meldung

Der organisatorische und technische Aufwand für die beteiligten Akteurinnen und Akteure muss überschaubar bleiben. Dies betrifft nicht nur die Vermeidung von Mehrfachmeldungen. Das zukünftige System muss einfach und eingängig zu bedienen sein. Der Meldeprozess muss sich einfach in die verschiedenen Organisations- und Systemlandschaften der betroffenen Akteurinnen und Akteure einfügen.

Genehmigen Sie, sehr geehrter Herr Bundesrat,
die Versicherung unserer ausgezeichneten Hochachtung.

Im Namen des Regierungsrates

Die Präsidentin: Die Staatsschreiberin:

Jacqueline Fehr Dr. Kathrin Arioli

Schweizerische Volkspartei
Union Démocratique du Centre
Unione Democratica di Centro
Partida Populara Svizra

Generalsekretariat / Sécrétariat général
Postfach, 3001 Bern / www.svp.ch
Tel. 031 300 58 58 / gs@svp.ch
IBAN: CH80 0900 0000 3000 8828 55

Bundesrat Ueli Maurer
Eidgenössisches Finanzdepartement
Bundesgasse 3
3003 Bern

Elektronisch an:
ncsc@gs-efd.admin.ch

Bern, 11. April 2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Vernehmlassungsantwort der Schweizerischen Volkspartei (SVP)

Sehr geehrte Damen und Herren

Wir nehmen im Rahmen der rubrizierten Vernehmlassung Stellung zur Vorlage. Wir äussern uns dazu wie folgt:

Die SVP lehnt die Änderungen des Informationssicherheitsgesetzes (ISG) ab. Das Gesetz führt zu erheblichen Mehrkosten für die Wirtschaft, ohne die Cybersicherheit bedeutend zu verbessern. Der heute freiwillige Informationsaustausch zwischen kritischen Infrastrukturen und dem Bund funktioniert bereits auf einem bewährten Vertrauensverhältnis zwischen Behörden und den betroffenen Unternehmen. Die angestrebte Meldepflicht ist daher überflüssig und würde nur weiteren administrativen Aufwand und zusätzliche Kosten für weite Teile der Wirtschaft bedeuten.

Bereits 2018 lehnte die SVP die erste Vorlage (Botschaft zum Informationssicherheitsgesetz) ab, da diese einen erheblichen bürokratischen Aufwand für die betroffenen Unternehmen zur Folge hat. Die positiven Auswirkungen auf die Sicherheit im Cyber-Space sind minim und die finanziellen Auswirkungen auf die Unternehmen sind bis heute noch nicht vollumfänglich geklärt.
Die Einführung eines neu meldepflichtigen Informationsaustausches lehnt die SVP ab, obwohl die SVP die Förderung der Cybersicherheit als Verbundsaufgabe durchaus unterstützt. Anstatt eine gesetzliche Meldepflicht durchzusetzen, macht es jedoch mehr Sinn, innerhalb der verschiedenen Branchen, beispielsweise im Rahmen der Selbstregulierungsorganisationen (SRO), Melde-Standards zu entwickeln. Von Strafbestimmungen ist generell abzusehen, da die Unternehmen andauernd gezwungen wären, den Zeitpunkt der Kenntnisnahme von Cyber-Angriffen nachzuweisen. Zudem widersprechen die Strafbestimmungen dem angestrebten Vertrauensprinzip.

Die vorgeschlagenen Änderungen des Gesetzes nehmen sich in keiner Form der bereits 2018 angesprochenen Probleme (konkreter Nutzen und Kostenfolge) an. Der Bundesrat unterschätzt die Kosten, welche einerseits für das NCSC und andererseits für die meldenden Akteure anfallen. Er geht davon aus, dass keine direkten Auswirkungen auf die Volkswirtschaft zu erwarten sind, obwohl gleichzeitig mit den

zunehmenden Aufgaben, verbunden mit den steigenden Meldungen der Unternehmen, die Ressourcen des NCSC aufgestockt werden müssen (Erläuternder Bericht, S. 27).

Aus den obenerwähnten Gründen kann die SVP die Änderungen im Informationssicherheitsgesetz nicht unterstützen.

Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme und grüssen Sie freundlich.

SCHWEIZERISCHE VOLKSPARTEI

Der Parteipräsident	Der Generalsekretär
Marco Chiesa	Peter Keller
Ständerat	Nationalrat

Sozialdemokratische Partei der Schweiz

Zentralsekretariat
Theaterplatz 4
3011 Berne

Tel. 031 329 69 69
Fax 031 329 69 70

info@spschweiz.ch
www.spschweiz.ch

Eidgenössisches Finanzdepartement
Bundesgasse 3
3003 Bern

Per Email an:
ncsc@gs-efd.admin.ch

Bern, 12. April 2022

Stellungnahme zu einer Meldepflicht bei Cyberangriffen auf kritische Infrastrukturen

Sehr geehrter Herr Bundesrat Maurer
sehr geehrte Damen und Herren

Wir bedanken uns für die Gelegenheit zur Stellungnahme, die wir gerne nutzen.

SP begrüsst Einführung einer Meldepflicht für Cyberangriffe

Die SP begrüsst die Einführung eine Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen. Seit Jahren verlangt die SP einen Ausbau der Massnahmen gegen Cyberangriffe – eine Gefahr, die mit der Aggression Russlands gegen die Ukraine noch akuter werden dürfte. Eine Meldepflicht für Cyberangriffe auf kritische Infrastrukturen ist eine wichtige Massnahme, da sie die Datenlage in diesem Bereich verbessert und so erst ermöglicht, darauf zu reagieren. Da auch die allermeisten Betreiber von kritischen Infrastrukturen einer Meldepflicht grundsätzlich positiv eingestellt sind und es (mit Ausnahme eines kleinen administrativen Aufwands) keine effektiven Nachteile gibt, stellt sich die SP hinter die Einführung einer Meldepflicht.

Die SP stellt jedoch zwei Forderungen zur weiteren Verbesserung der Vorlage:

1. **Forderung: Das NCSC soll die Pflicht haben, möglicherweise von Cyberangriffen Betroffene davor zu warnen und entsprechende Empfehlungen auszusprechen (Art. 74a ISG)**

Die SP schlägt folgende Änderung von Art. 74a vor:

«Die Betreiberinnen von kritischen Infrastrukturen müssen dem NCSC Cyberangriffe nach deren Entdeckung so rasch als möglich melden, damit das NCSC Angriffsmuster frühzeitig erkennt~~en~~, mögliche Betroffene warn**ten** ~~ten~~ und ihnen geeignete Präventions- und Abwehrmassnahmen empf**iehlt**~~tehlen kann~~. **Die Warnung möglicher Betroffener und die Empfehlung geeigneter Präventions- und Abwehrmassnahmen stellt grundsätzlich eine Pflicht des NCSC dar**.»

Präventive Massnahmen sind zentral, weshalb weitere möglicherweise von Cyberangriffen Betroffene zeitnah zu warnen sind. Ausnahmen von dieser Pflicht können vorgesehen werden, müssen aber explizit aufgeführt werden.

2. **Forderung: Überprüfung der Liste von kritischen Infrastrukturen (Art. 74b ISG)**

Art. 74b ISG definiert den Begriff der «Betreiberinnen von kritischen Infrastrukturen», welche nach Art. 74a ISG einer Meldepflicht unterstehen. Dies ist mit anderen Worten eine Liste der besonders schützenswerten Infrastrukturen. Was schützenswert ist und was nicht, kann sich aber im Laufe der Zeit ändern, weshalb die SP fordert, dass die Liste in Art. 74b ISG alle fünf Jahre überprüft und ggf. ergänzt wird.

3. **Forderung: Überprüfung der Massnahmen bei Widerhandlungen gegen Verfügungen des NCSC (Art. 74i ISG)**

Die in Art. 74i ISG festgehaltenen Massnahmen bei Widerhandlungen gegen Verfügungen des Nationalen Zentrums für Cybersicherheit (NCSC) erachtet die SP grundsätzlich als sinnvoll. Der Übergang vom Prinzip der Freiwilligkeit zur Pflicht bei Meldungen bei Cyberangriffen ist zu begrüssen. Allerdings muss nach fünf Jahren überprüft werden, ob die in Art. 74i ISG genannten Sanktionsmöglichkeiten ausreichen, um auch tatsächlich eine flächendeckende Meldung möglichst aller Cyberangriffe auf kritische Infrastrukturen sicherzustellen. Dies, zumal Anreize bestehen können, einen Angriff zu verschweigen – beispielsweise aus Reputationsgründen. Art. 74i Abs. 4 ISG hält fest: «Bei einer Widerhandlung gegen eine Verfügung des NCSC obliegt die Verfolgung und die Beurteilung den Kantonen.» Bei einer Überprüfung nach fünf Jahren soll auch evaluiert werden, ob eine schweizweite Gleichbehandlung sichergestellt ist, obwohl die Beurteilung von Widerhandlungen in der Kompetenz der Kantone liegt.

Wir danken Ihnen, geschätzte Damen und Herren, für die Berücksichtigung unserer Anliegen und verbleiben mit freundlichen Grüssen

Sozialdemokratische Partei der Schweiz

Mattea Meyer
Co-Präsidentin

Cédric Wermuth
Co-Präsident

Sozialdemokratische Partei der Schweiz
Theaterplatz 4
Case postale · 3001 Berne
Tel. 031 329 69 69
Fax 031 329 69 70
info@spschweiz.ch
www.spschweiz.ch

Severin Meier
Politischer Fachsekretär

Sozialdemokratische Partei der Schweiz
Theaterplatz 4
Case postale · 3001 Berne
Tel. 031 329 69 69
Fax 031 329 69 70
info@spschweiz.ch
www.spschweiz.ch

FDP
Die Liberalen

FDP.Die Liberalen
Generalsekretariat
Neuengasse 20
Postfach
CH-3001 Bern

+41 (0)31 320 35 35
www.fdp.ch
info@fdp.ch
/fdp.dieliberalen
@FDP_Liberalen

FDP.Die Liberalen, Postfach, 3001 Bern

Herr Manuel Sauter
Geschäftsstelle NCSC
Schwarztorstrasse 59
3003 Bern

Bern, 13. April 2022

Per Mail an:
ncsc@gs-efd.admin.ch

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe - Vernehmlassungsantwort der FDP.Die Liberalen

Sehr geehrte Damen und Herren

Für Ihre Einladung zur Vernehmlassung oben genannter Vorlage danken wir Ihnen. Gerne geben wir Ihnen im Folgenden von unserer Position Kenntnis.

Die Gefahren für Wirtschaft und Staat im Cyberraum haben in den letzten Jahrzehnten rasant zugenommen. FDP.Die Liberalen hat dies frühzeitig erkannt und auf eine Stärkung der Cyber-Resilienz hingewirkt. Federführend waren dabei die Motionen der FDP (Motion Dittli 17.3507 und Motion Eder 17.3508), die zum Cyber-Lehrgang der Armee bzw. der Umgestaltung der Melde- und Analysestelle Informationssicherung (Melani) geführt haben. Ganz im Sinne unserer Motionen wurde das Nationale Zentrum für Cybersicherheit (NCSC) geschaffen, das wertvolle Arbeit leistet. Jedoch besteht eine gesetzgeberische Lücke, da dem Kompetenzzentrum des Bundes die nötige rechtliche Grundlage fehlt, um seine Aufgaben wahrzunehmen. Somit begrüsst die FDP die Vorlage, die für das Kompetenzzentrum des Bundes das nötige rechtliche Fundament schafft.

Ebenfalls befürwortet die FDP das Kernstück der Vorlage, nämlich die Einführung einer Meldepflicht bei Cyberangriffen auf kritische Infrastrukturen. Eine freiwillige Meldemöglichkeit besteht bereits heute, mit der Einführung einer Meldepflicht für eine ausgewählte Gruppe soll jedoch ein vollständiges und unverzerrtes Lagebild ermöglicht werden. Dieses Lagebild ist unerlässlich, um die Aus- und Breitenwirkung einer Bedrohung korrekt einzuschätzen. Ein auf Freiwilligkeit beruhendes Prinzip, bei welchem nur ein Bruchteil der Akteure teilnimmt, kann kein unverzerrtes Lagebild ermöglichen. Zudem führt das Freiwilligkeitsprinzip zu einer Ungleichbehandlung von Akteuren, da die eingegangenen Meldungen aus Sicherheitsgründen allen Akteuren weitergegeben werden müssen, sprich auch an jene Akteure, die sich nicht mit Meldungen beteiligen.

Bei der Umsetzung der Meldepflicht ist darauf zu achten, dass der Aufwand für die betroffenen Unternehmen möglichst kleingehalten wird. So ist bei der Meldestelle das Prinzip eines «One-Stop-Shop» einzuführen, das den betroffenen Unternehmen ermöglicht mit einer Meldung all ihren Meldepflichten nachzukommen. Des Weiteren ist auf Verordnungsstufe ein abschliessender Katalog der zu meldenden Vorfälle zu definieren, um allfälligen Unklarheiten oder Missverständnissen entgegenzuwirken. Besonders da auf Gesetzesstufe noch Unklarheiten bestehen, was alles unter einem Cyberangriff fallen könnte.

Als Kompetenzzentrum besitzt das NCSC ein fundiertes Fachwissen, welches es der Wirtschaft und Wissenschaft zur Verfügung stellen sollte. Jedoch ist darauf zu achten, dass das NCSC und seine Angebote nicht mit Diensten von privaten Anbietern konkurrenzieren. Die Cybersicherheit einzelner Unternehmen zu gewährleisten ist und bleibt in der Selbstverantwortung dieser. Der Staat muss seine Rolle subsidiär ausüben: Er darf erst einschreiten, wenn die Bedrohung die Kapazitäten der betroffenen Akteure, Branchen oder Anbietern übersteigt.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und für die Berücksichtigung unserer Überlegungen.

Freundliche Grüsse
FDP.Die Liberalen

Der Präsident

Der Generalsekretär

Thierry Burkart
Ständerat

Jon Fanzun

Allianza dal Center | Alleanza del Centro | Le Centre | Die Mitte

Per Mail: ncsc@gs-efd.admin.ch

Bern, 28. März 2022

Vernehmlassung: Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrte Damen und Herren

Sie haben uns eingeladen, zur obengenannten Vernehmlassungsvorlage Stellung zu nehmen. Für diese Gelegenheit zur Meinungsäusserung danken wir Ihnen bestens.

Cyberangriffe auf Unternehmen, Behörden auf ganz verschiedenen Stufen oder auf Privatpersonen haben in den letzten Jahren stark zugenommen. Dies mit teils gravierenden Auswirkungen für die Sicherheit unserer Bürger und Bürgerinnen, Wirtschaft und Verwaltung. Der vorliegende Entwurf will nun eine Meldepflicht für Cyberangriffe auf kritische Infrastrukturen einführen, um solche Angriffe frühzeitig zu entdecken, ihre Angriffsmuster zu analysieren und andere Betreiber rechtzeitig zu warnen.

Die Mitte begrüsst diese Meldepflicht und die Beauftragung des nationalen Zentrums für Cybersicherheit (NCSC) als Meldestelle. Zentral ist eine Umsetzung, die eine einfache und rasche Handhabung solcher Meldungen ermöglicht. Die Meldestelle soll idealerweise in die bestehenden Strukturen des NCSC und MELANI integriert werden. Aus Sicht der Mitte ist es beispielsweise wichtig, dass mit der digitalen Erfassung auch andere Meldepflichten (z.B. an die FINMA, EDÖB) bei einem Ereignis einfach erfüllt werden können.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme und verbleiben mit freundlichen Grüssen.

Die Mitte

Sig. Gerhard Pfister
Präsident Die Mitte Schweiz

Sig. Gianna Luzio
Generalsekretärin Die Mitte Schweiz

Die Mitte
Schweiz

Hirschengraben 9
Postfach
CH-3001 Bern

T 031 357 33 33
info@die-mitte.ch
www.die-mitte.ch

GRÜNE Schweiz
Waisenhausplatz 21
3011 Bern

rahel.estermann@gruene.ch
031 326 66 15

Eidgenössisches Finanzdepartement,
Herr Bundesrat Ueli Maurer
3003 Bern

per E-Mail an:
ncsc@gs-efd.admin.ch

Bern, 13. April 2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe (Revision Informationssicherheitsgesetz ISG): Vernehmlassung

Sehr geehrter Herr Bundesrat, sehr geehrte Damen und Herren

Sie haben die GRÜNEN eingeladen, sich zum Entwurf zur Änderung des Informationssicherheitsgesetzes (Meldepflicht für Cyberangriffe auf kritische Infrastrukturen) zu äussern. Wir danken Ihnen dafür und nehmen gerne Stellung.

Die GRÜNEN begrüssen die Revision des Gesetzes in der vorgesehenen Richtung. Dies ist ein wichtiger Schritt, der die gesteigerte Bedeutung der Datensicherheit im digitalen Zeitalter aufnimmt und auf eine neue Kultur der gemeinsamen Verantwortung für Cyber-Security verweist. Aus unserer Sicht sollte der Bereich Cyber-Security sogar durch ein eigenes Bundesamt oder ein Staatssekretariat (Vorstoss 21.4389) verankert sein. Bis dahin plädieren wir im Rahmen dieser Gesetzesrevision dafür, die Kompetenzen und Ressourcen des National Cyber Security Centers (NCSC) auszubauen. Wichtig ist, dessen Sensibilisierungsaufgabe umfassend auszulegen: Unsere Gesellschaft ist darauf angewiesen, dass Behörden wie auch Unternehmen und Privatpersonen Massnahmen für die Datensicherheit ernst nehmen. Im Gesetz muss zudem der Begriff der «kritischen Infrastrukturen» erweitert werden, beispielsweise durch kritische Komponenten oder den Bereich der Demokratie. Zudem soll das Gesetz nicht nur die Meldung von Cyberangriffen, sondern von Cybervorfällen verpflichtend machen. Die Anreize für möglichst viele Meldungen (auch freiwillige) müssen hoch, die Hürden dafür tief gesetzt sein. Die Gesetzesrevision soll der Anfang einer neuen gemeinsamen Verantwortungskultur sein, so wie sie beispielsweise im Bereich der Flug- oder Nuklearsicherheit bereits etabliert ist.
Zu den einzelnen Artikeln nehmen wir wie folgt Stellung:

Grundsätzliche Überlegungen und Art. 73a

Wir begrüssen die weitreichende Ausgestaltung der Aufgaben des NCSC in Art. 73a, insbesondere die Sensibilisierung der Öffentlichkeit in lit. a. Der Schutz von Cyber-Risiken ist nur so stark wie sein schwächstes Glied – das heisst, dass eine Gesellschaft darauf angewiesen ist, dass alle Akteurinnen – von Behörden über Unternehmen bis hin zu Privatpersonen –

Massnahmen zur Cyber-Security ernst nehmen. Der Bund schreibt selbst treffend in den Erläuterungen (Seite 28): «Eine erhöhte Cyberkompetenz der Bevölkerung ist eine wichtige Voraussetzung für die erfolgreiche Digitalisierung der Gesellschaft.»

Gerade deshalb ist es nötig, dass das NCSC eine aktivere Rolle einnehmen kann. Es muss Schwachstellen und Bedrohungen aktiv erkennen – einerseits durch die Überwachung der globalen Geschehnisse im Bereich Cybersicherheit; andererseits durch das aktive Überwachen der Bedrohungslage durch Scans nach Sicherheitslücken in sämtlichen Informatikmitteln im Geltungsbereich des Gesetzes. Die so erlangten Erkenntnisse sind sodann analog zu passiv erhaltenen Meldungen zu verarbeiten.

Art. 73a lit. a (Sensibilisierung der Öffentlichkeit) muss aus Sicht der GRÜNEN weit ausgelegt und konsequent umgesetzt werden – Information und damit Opfer-Prävention ist auch in diesem Bereich genauso wichtig wie das Beheben von Problemen und Schäden. Der Bund bzw. das NCSC sollen auf Basis der Gesetzes Sensibilisierungskampagnen durchführen und Anreize setzen, damit Cyber-Security-Massnahmen und die Meldung von Vorfällen zur üblichen Praxis werden für alle Organisationen und Personen. Auch wenn es sich dabei nicht nur um (aus gesellschaftlicher Sicht) kritische Infrastrukturen handelt, kann der Missbrauch von persönlichen Daten (beispielsweise Gesundheitsdaten) für Einzelne genauso gravierende Folgen haben. Auch kleinere Firmen ohne gut bestückte IT-Abteilung, die oftmals wichtige Glieder im Wirtschaftsgeschehen sind, müssen spezifisch sensibilisiert und unterstützt werden. Die enge Vernetzung verschiedenster Akteure im wirtschaftlichen und gesellschaftlichen Leben verlangt es, dass wir Cyber-Security umfassend und nicht auf kritische Infrastrukturen beschränkt verstehen.

Die «Unterstützung von Betreiberinnen von kritischen Infrastrukturen» (Art. 73a lit. f) muss ebenfalls breiter gedacht werden, als die Erläuterungen und Definitionen das bisher vorsehen. Denn einzelne Komponenten oder Teile von Software können ebenfalls kritisch sein. Entdeckte Sicherheitslücken in weit verbreiteten Einzelkomponenten (beispielsweise Heartbleed 2014 oder Log4j 2021) zeigen, dass dadurch schnell eine grosse Anzahl an kritischen Einfallstoren entstehen. Art.74 lit. s erwähnt genau solche «Hard- und Software, deren Produkte von kritischen Infrastrukturen genutzt werden» als Bereiche der Meldepflicht und anerkennt deren Bedeutung. Im Sinne der Vorbeugung sollte der Bund die Sicherung und Verbesserung solcher Komponenten aktiv unterstützen, beispielsweise durch ein Public-Private-Partnership für einen Fonds für die Wartung solcher Komponenten.

Im Sinne der Prävention von Cyber-Security-Vorfällen regen wir zudem an, dass der Bund verbindliche Mindeststandards schaffen muss, welche sich an den anerkannten Regeln der Technik orientieren sowie messbare und überprüfbare Massnahmen und damit «best practices» definieren. Dies würde es auch erleichtern, Haftungsfragen zu klären und somit die Rechte von Nutzer*innen und Abnehmer*innen von Software zu stärken. Wir verweisen an dieser Stelle auf die detaillierten Ausführungen der Vernehmlassungsantwort der Digitalen Gesellschaft.

Art. 73b – Meldungen zu Cybervorfällen und Schwachstellen

Für die Sensibilisierung für Cyber-Risiken und eine Erhöhung des Sicherheitsniveaus insgesamt ist es aus Sicht der GRÜNEN zentral, dass möglichst viele Vorfälle und deren Details öffentlich sind. Deshalb verlangen wir eine Umkehrung der Vorzeichen bezüglich Veröffentlichung (Art. 73 Abs. 2 und Abs. 3): Sprechen nicht gewichtige Gründe dagegen, soll das NCSC gemeldete Vorfälle und Schwachstellen veröffentlichen. Dies unter der Einhaltung des

Schutzes von persönlichen oder sonst sensiblen Daten und natürlich unter der Berücksichtigung, dass damit Angreiferinnen keine zusätzlichen, nützlichen Informationen zur Verfügung stehen. Zudem erscheint es zweckmässig, dass das NCSC kontinuierlich und in aggregierter Form über Vorfälle und Schwachstellen berichtet und damit ein breiteres Publikum erreicht. So ist es möglich, dass die Öffentlichkeit sich einen aktuellen Überblick über die Sicherheitslage im Cyber-Bereich verschaffen kann und weiss, welche Angriffsarten und Schwachstellen besonders verbreitet sind.

Für eine tragfähige Lagebeurteilung ist es zentral, dass möglichst viele Ereignisse (also Vorfälle und Schwachstellen) gemeldet werden. Die Meldepflicht bzw. der Begriff der kritischen Infrastrukturen (Art. 74b) müssen grosszügig ausgelegt sowie die Anreize für eine Meldung hoch und die Hürden dafür tief gelegt werden (siehe auch Überlegungen zu Art. 73a lit. a oben).

Zudem muss das NCSC grössere Kompetenzen erhalten bei gravierenden Vorfällen. Es soll dann Weisungen und Fristen gegenüber Hersteller- und Betreiberorganisationen erlassen dürfen, welche diese verpflichten, Schwachstellen schnell zu beheben und Schäden zu mindern. Wichtig ist hier insbesondere, dass Abs. 3 auch auf Betreiberorganisationen ausgedehnt wird – Sicherheitsupdates beispielsweise nützen nur dann, wenn sie auch wirklich eingespielt werden.

Das NCSC soll die Fristen und Weisungen dabei gemäss einem risikobasierten Ansatz gestalten: Je kritischer eine Infrastruktur bzw. grösser der potenzielle Schaden, desto kürzer die Fristen.

Wird dem NCSC eine Sicherheitslücke bekannt, die ein Drittprodukt betrifft und bei der nicht davon auszugehen ist, dass sie der Herstellerin bereits bekannt ist, muss die Sicherheitslücke vom NCSC umgehend im Rahmen eines «responsible disclosure»-Verfahrens der betroffenen Herstellerin gemeldet werden. Zusätzlich sollten dem NCSC Mittel an die Hand gegeben werden, um bei meldenden Organisationen auf der Behebung einer Sicherheitslücke zu bestehen.

Der Grundsatz, entdeckte (aber noch nicht bekannte) Sicherheitslücken («Zero Day Exploits») im Rahmen eines «responsible-disclosure»-Verfahrens zu veröffentlichen, sollte neben dem NCSC für alle Bundesstellen gelten, auch für den Nachrichtendienst. Alle Bundesstellen sollen auf den Einsatz von Informatikmitteln verzichten, welche diese Lücken ausnutzen – denn mit solchen «Staatstrojanern» wird das Geschäft mit Sicherheitslücken und damit Unsicherheit vorangetrieben.

Art 73c (insbesondere Abs. 3) – Strafverfahren

Wir begrüssen, dass der verantwortungsvolle Umgang mit Sicherheitsrisiken («responsible disclosure» beispielsweise) vor der Strafverfolgung geschützt ist.

Art. 74 – Unterstützung durch das NCSC

Die GRÜNEN begrüssen es sehr, dass das NCSC die Betreiberinnen bezüglich Cyber-Risiken unterstützt.

Art. 74a – Meldepflicht

Die Revision sieht im eigentlichen Kernpunkt, Art. 74a, eine Meldepflicht von kritischen Infrastrukturen nur für Cyberangriffe vor (definiert in Art. 5 als «Cybervorfall, der von Unbefugten absichtlich ausgelöst wurde»). Dies geht zu wenig weit. Die Meldepflicht von kritischen Infrastrukturen sollte allgemeine Cybervorfälle einschliessen, definiert in Art. 5 als «Ereignis beim Betrieb von Informatikmitteln, das dazu führen kann, dass die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist.» Mit Blick auf das Schadenspotential ist es unerheblich, ob ein Ereignis absichtlich von Unbefugten («Cyberangriff») oder unabsichtlich, von Befugten oder von Informatikmitteln («Cybervorfall») ausgelöst wurde. Die Definition von Cybervorfällen umfasst zudem algorithmische Entscheidungssysteme (Künstliche Intelligenz, KI) und entsprechende Fehlfunktionen. Es ist essenziell, dass auch KI unter die Meldepflicht fällt, da diese Systeme über zunehmende Leistungsfähigkeit verfügen und in immer mehr kritischen Infrastrukturen eingesetzt werden. Zudem ist es etwa in der Flug- oder Nuklearsicherheit etablierte Praxis, dass nicht nur schwere Unfälle oder Angriffe, sondern auch sonstige Zwischenfälle rapportiert und aufgearbeitet werden. Eine solche moderne Sicherheitskultur sollte auch im Cyber- und KI-Bereich Einzug finden.

Dies ist auch deshalb sinnvoll, weil sich die Tragweite und Ursache eines Vorfalls zu Beginn des Ereignisses oft gar nicht abschätzen lassen. Um den möglichen Sicherheitsrisiken, die davon ausgehen, trotzdem Rechnung zu tragen, ist eine unmittelbare Meldung von allen Vorfällen nötig, möglichst innerhalb von 24 Stunden.

Art. 74b – Bereiche der Meldepflicht

Der Artikel legt fest, für welche Bereiche die Meldepflicht gilt. Die GRÜNEN regen an, dass die Bereiche der in lit. c genannten Organisationen mit öffentlich-rechtlichen Aufgaben erweitert werden um den Bereich der Demokratie. Dies würde insbesondere Parteien in Parlamenten und Politiker*innen in relevanten Ämtern umfassen. Diese nehmen gewichtige öffentlich-rechtliche Aufgaben wahr und ein Cyberangriff auf sie hat potenziell grosse Auswirkungen auf die Demokratie. Während in der Schweiz bisher wenig über Cyber-Angriffe auf die Demokratie bekannt ist, ist dies in anderen Ländern bereits gängige Praxis. Die Schweiz hat sich in diesem Thema bisher erstaunlich sorglos gezeigt, obwohl die schweizerische direkte Demokratie so viele politische Prozesse in der Öffentlichkeit bewirkt wie kaum in einem anderen Land. Es erscheint wenig plausibel, wenn Organisationen der Postdienste, der Rheinschifffahrt oder Nachrichtenagenturen der Meldepflicht unterliegen – nicht aber im nationalen Parlament vertretene Parteien.

Zudem soll der Bereich von lit. f sich nicht auf die Anzahl Nutzende beziehen, da dies nichts darüber aussagt, ob es sich um ein für einen Cyberangriff lohnendes Ziel handelt. Ausserdem soll an derselben Stelle von «Wirtschaft» die Rede sein, nicht von «digitaler Wirtschaft».

Art. 74c – Ausnahmen der Meldepflicht

Die GRÜNEN beantragen die gesamte Streichung des Ausnahmen-Artikels. Der erste Teil (lit. a) – eine geringe Abhängigkeit von Informatikmitteln – erscheint im 21. Jahrhundert zunehmend unwahrscheinlich. Der zweite Teil (lit. b) scheint schwer abschätzbar und ermöglicht deshalb zahlreiche Schlupflöcher, der Meldepflicht zu entgehen – was erhöhte Risiken für die Cyber-Sicherheit der Gesellschaft bedeutet.

Art. 74e und Art. 74f – Inhalt und Übermittlung der Meldungen

Der Artikel 74e ist aus Sicht der GRÜNEN so zu überarbeiten, dass die Automatisierung von Meldungen möglich und wünschenswert werden. Mit den zur Verfügung stehenden technischen Möglichkeiten ist die Auswertung eines grossen Volumens von Meldungen möglich, auch wenn diese eher Anhaltspunkte denn kompletten Meldungen entsprechen. Dies ist insbesondere wichtig, weil mit der Meldung von Cybervorfällen (siehe oben, Ausführungen zu Art. 74a) eine erhöhte Anzahl Interaktionen zu erwarten ist. Die Anforderungen an die Meldungen müssen dementsprechend je nach Art des Ereignisses (Angriff oder Vorfall) abgestuft sein. Dies ist wichtig, um die Schwelle für eine Kontaktaufnahme zu senken.

Neben manuellen Meldungen soll eine IT-Schnittstelle (API) auch automatisierte Meldungen an das NCSC erlauben. So können Cyber-Überwachungssysteme von kritischen Infrastrukturen etwa automatisch verdächtige Signale an das Zentrum weiterleiten. Die Datengrundlage des NCSC wird damit umfassender und zeitnaher als bei rein manuellen Eingaben nach grösseren Vorfällen.

In jedem Fall sollte in der Umsetzung nach Möglichkeit sichergestellt werden, dass sich überschneidende Meldepflichten (DSG, Finma, etc.) durch einen einzigen Meldevorgang erfüllt werden können.

Art. 74i – Widerhandlungen und Verantwortlichkeit

Der Artikel-Text muss expliziter machen, dass die vorgesehenen Sanktionen auf der Leitungsebene der Organisationen greifen, und nicht auf der Ebene der Fachspezialist*innen (allenfalls sind Organe zu nennen). Dies ist wichtig, um die Verantwortlichkeiten für Cyber-Security in den Leitungsgremien zu verankern.

Die GRÜNEN regen zudem an, den höchsten Führungsorganen Verantwortung für die Cyber-Governance zuzuordnen, wie dies beispielsweise bereits bei Verwaltungsräten von Aktiengesellschaften für die Ausgestaltung des Rechnungswesens und die Finanzplanung und -kontrolle der Fall ist. Im digitalen Zeitalter gebührt der Ausgestaltung einer Daten-Governance in Unternehmen das gleiche Gewicht wie den Finanzen. Eine solche Verantwortung müsste der Bund im Aktienrecht verankern.

Wir danken Ihnen, Herr Bundesrat, sehr geehrte Damen und Herren, für die Berücksichtigung unserer Vorschläge in der Revision des Gesetzes.

Freundliche Grüsse

Balthasar Glättli
Präsident

Rahel Estermann
stv. Generalsekretärin, Leiterin Politik

Grünliberale Partei Schweiz
Monbijoustrasse 30, 3011 Bern

Eidgenössisches Finanzdepartement
Nationales Zentrum für Cybersicherheit (NCSC)
3003 Bern

Per E-Mail an: ncsc@gs-efd.admin.ch

12. April 2022
Ihr Kontakt: Ahmet Kut, Co-Generalsekretär, Tel. +41 31 311 33 03, E-Mail: schweiz@grunliberale.ch

Stellungnahme der Grünliberalen zur Änderung des Informationssicherheitsgesetzes (Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe)

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Wir bedanken uns für die Vorlage und den erläuternden Bericht zur Änderung des Informationssicherheitsgesetzes (Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe) und nehmen dazu wie folgt Stellung:

Die **Stärkung des Schutzes vor Cyberrisiken** ist für die Grünliberalen ein zentrales Thema. Die Grünliberalen begrüssen daher, dass eine Meldepflicht für Betreiberinnen kritischer Infrastrukturen eingeführt werden soll.

Soweit es um *freiwillige* Meldungen geht, ist wichtig, dass diese auch anonym erfolgen können. Gemäss dem erläuternden Bericht (S. 5) erfolgt eine Weiterleitung von Meldungen oder Teilen davon nur mit Einverständnis der Betreiberin der betroffenen kritischen Infrastruktur oder anonymisiert. Die Weitergabe von Informationen, die Rückschlüsse auf die Meldenden oder Betroffenen erlauben, soll dem Nationalen Zentrum für Cybersicherheit (NCSC) nur in zwei Fällen auch ohne deren Einverständnis erlaubt sein: (i) In Form einer Strafanzeige, wenn die Schwere der möglichen Straftaten das geboten erscheinen lässt (Interessenabwägung durch den oder die Leiter:in des NCSC) und (ii) in bestimmten Fällen an den Nachrichtendienst des Bundes (NDB). Für eine möglichst grosse Rechtssicherheit und Rechtsklarheit sollte die Möglichkeit **anonymer Meldungen** an das NCSC im Gesetzestext ausdrücklich vorgesehen werden (z.B. in Art. 73b Abs. 1 VE-ISG).

Im Unterschied zu den freiwilligen Meldungen soll die Meldepflicht gemäss Vorentwurf nicht für **Schwachstellen** gelten, sondern nur für erfolgte Cyberangriffe. Im erläuternden Bericht (S. 9) wird dazu lapidar ausgeführt, man habe davon «abgesehen, die Meldepflicht auf Schwachstellen in Informatikmitteln auszudehnen». Eine Begründung dafür fehlt, und es überzeugt auch nicht. Die Meldepflicht sollte richtigerweise auch für Schwachstellen gelten – zumindest Schwachstellen in der Lieferkette. Das würde es der NCSC ermöglichen, Angriffsmuster frühzeitig zu erkennen, mögliche Betroffene zu warnen und ihnen geeignete Präventions- und Abwehrmassnahmen zu empfehlen.

Kritisch beurteilen die Grünliberalen den Umfang der Personendaten, welche der NCSC bearbeiten gemäss Vorentwurf bearbeiten darf. Gemäss Art. 75 Abs. 1 Bst. a VE-ISG darf er u.a. **besonders schützenswerte Personendaten** bearbeiten, die Informationen «über religiöse, weltanschauliche oder politische Ansichten enthalten.» Es ist zwar einschränkend vorgesehen, dass die Bearbeitung nur zulässig ist, wenn sie für die Bewertung von konkreten Bedrohungen und Gefahren im Bereich der Cybersicherheit erforderlich ist. Da es hier um sehr sensible Daten geht, sollte eindeutig geklärt sein, weshalb der NCSC diese Daten benötigt. Das ist nicht der Fall. Im Gegenteil: Die Aufgabenteilung insbesondere gegenüber NDB und fedpol, welche diese Daten zum gleichen Zweck bearbeiten, ist unklar. Hinzu kommt, dass vorliegend keine besondere Aufsicht vorgesehen ist. Damit ist nicht sichergestellt, dass es zu keiner

missbräuchlichen Verwendung dieser Daten kommt. Diese Fragen sind mit Blick auf die Botschaft zu klären und Lösungen vorzuschlagen.

Neben der Meldepflicht nach ISG gibt es weitere Meldepflichten bei Cybervorfällen, so etwa nach dem neuen Datenschutzgesetz (Art. 24: Meldung von Verletzungen der Datensicherheit). Im erläuternden Bericht (S. 11) werden weiter Beispiele genannt. Um im Fall eines Cyberangriffs rasch reagieren zu können und die administrative Belastung der betroffenen Unternehmen so gering wie möglich zu halten, ist eine **gemeinsame Meldeplattform** der verschiedenen Behörden vorzusehen. Diese soll es erlauben, mit einer Meldung alle relevanten Meldepflichten zu erfüllen. Der Entwurf ist entsprechend zu ergänzen.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und die Prüfung unserer Anmerkungen und Vorschläge.

Bei Fragen dazu stehen Ihnen die Unterzeichnenden sowie unsere zuständigen Fraktionsmitglieder, Nationalrat François Pointet und Nationalrätin Melanie Mettler, gerne zur Verfügung.

Mit freundlichen Grüssen

Jürg Grossen
Parteipräsident

Ahmet Kut
Co-Generalsekretär

piratenpartei
www.piratenpartei.ch

Piratenpartei Schweiz, 3000 Bern

Sehr geehrter Herr Bundesrat Maurer

Sehr geehrte Damen und Herren

Stellungnahme der Piratenpartei Schweiz zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe (Vernehmlassung 2021/70)

Bezugnehmend auf Ihre Vernehmlassungseröffnung vom 12.01.2022 nehmen wir gerne Stellung und würden es zukünftig sehr begrüssen, wenn wir als politische Partei in ihre Adressatenliste aufgenommen werden.

Im Weiteren finden wir Piraten es sehr bedenklich, dass Sie für die Stellungnahme auf eine proprietäre Software verweisen (Word der Firma Microsoft), wo es doch heute zahlreiche offene und freie Dateiformate gibt. Wir entsprechen ihrem Wunsch mit einer docx-Datei, welche auch in neueren Word Versionen geöffnet werden kann.

Die Piratenpartei Schweiz setzt sich seit Jahren für eine humanistische, liberale und progressive Gesellschaft ein. Dazu gehören die Privatsphäre der Bürger, die Transparenz des Staatswesens, inklusive dem Abbau der Bürokratie, Open Government Data, den Diskurs zwischen Bürgern und Behörden, aber auch die Abwicklung alltäglicher Geschäfte im Rahmen eines E-Governments. Jede neue digitale Schnittstelle und Applikation bedingt aber eine umfassende Risikoanalyse und Folgeabschätzung.

Stellungnahme zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Gerne nehmen wir zur wie folgt Stellung: Die Piratenpartei macht sich grundsätzlich für eine Politik stark, welche Probleme ursächlich bekämpft. Deshalb möchten wir vorab darauf hinweisen, dass präventives Schützen statt defensiven Reagierens in Bezug auf Cybersicherheit besser wäre. Wir erachten es darum als wichtig, den Fokus der Cybersicherheit auf Resilienz zu legen. Aus diesem Grund fordern wir frühe Kompetenzförderung in der breiten Masse, sowie eine bessere

Ausbildung von Spezialisten in der IT, der Ausbau der Förderung der Entwicklung von neuen Technologien und die Bereitstellung der dafür notwendigen Ressourcen.

Des Weiteren wäre es zeitgemäss, Mindeststandards für die IT-Sicherheit definieren und diese auch für verbindlich zu erklären. Die in der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken [1] enthaltenen Vorschläge dürfen als gute Ausgangslage hierfür betrachtet werden. Ergänzt werden sollte dies mit einem Gebot zur sicheren Verschlüsselung von jeglicher Kommunikation und Daten.

Gleichzeitig steht im Raum, ob auch eine Haftungsfrage bezüglich IT-Sicherheitsstandards eingeführt werden sollte. Dies könnte durch eine Erweiterung des Produktehaftpflichtgesetzes auf unkörperliche, digitale Produkte ergänzt werden. Insbesondere müssten Hersteller von netzwerkfähigen Geräten verpflichtet werden, Patches oder Updates über einen langfristigen Zeitraum (mindestens 5 Jahre) bereitzustellen.

Darüber hinaus halten wir es für fragwürdig, dass nur Betreiber kritischer Infrastruktur verpflichtet werden sollen Cyberangriffe zu melden. Es werden von "normalen" Unternehmen kaum Fälle gemeldet, dabei könnten durch eine zentrale Meldestelle beispielsweise Ransomware-Angriffe auf viele weitere Unternehmen verhindert werden. Eine Meldepflicht sollte deshalb im Minimum auch auf Organisationen, die im Auftrag vom Staat Aufgaben ausführen, alle Unternehmen, die zu einer ordentlichen Revision, oder gemäss DSG 11a [2] zur Anmeldung einer Datensammlung verpflichtet sind, erweitert werden.

Die Meldemöglichkeit ist dabei so niedrigschwellig wie möglich zu gestalten. Als positiver Anreiz müsste auch ein Angebot analog Art. 74 Abs. 3 seitens des Staates zur Bewältigung eines Vorfalls den meldenden Unternehmen in Aussicht gestellt werden.

Die Piratenpartei vermisst ebenso den Einbezug der zukünftigen Entwicklung in der Digitalisierung. Die aktuelle Vorlage geht mit keinem Wort auf "Künstliche Intelligenz" (oder das was gemeinhin darunter verstanden wird) ein, jedoch wird in absehbarer Zeit immer mehr Entscheidungen von solcher Software getroffen werden und auch zu kritischer Infrastruktur gehören.

Bezüglich der Betreiber kritischer Infrastruktur sollte vor allem auch aus der Vergangenheit gelernt werden. Die Crypto AG hat gezeigt, wie gefährlich Closed Source Systeme für die Sicherheit sind. Die immer noch aktive "Schwesterfirma" der Crypto AG, die Infoguard AG [3], beliefert weiterhin Betreiber kritischer Infrastrukturen in der Schweiz. Dies ist ein enormes, unkalkulierbares Klumpenrisiko. Wir fordern deshalb, dass bei kritischer Infrastruktur in Zukunft nur noch Open Source Software (OSS) verwendet werden darf. Dazu braucht es natürlich eine Übergangsregelung

bis zum EOL (end of life) von bestimmten Systemen. Jedoch *muss* OSS zeitnah ein Grundkriterium für jede Beschaffung in diesem Bereich sein.

Um tatsächlich kritische Infrastruktur auf einem angemessenen hohen Niveau zu betreiben, muss die Schweiz langfristig Ressourcen aufbauen, um Hard- und Software für kritische Infrastruktur selbst zu entwickeln UND zu produzieren. Entsprechende Mittel für Förderung, Ausbildung, Forschung in diesem Bereich sind zur Verfügung zu stellen.

Das NCSC (und nicht der NDB) soll die gemeinsame Cyberlage führen, dokumentieren, kontinuierlich und zeitnah transparent veröffentlichen, Art. 73b Abs 2 ist deshalb entsprechend von "kann" auf "muss" abzuändern. Mit einer solchen Regelung halten wir damit die explizite Weiterleitung an den NDB nach Art. 73c Abs. 1 für obsolet. In jedem Fall muss dieser Passus gestrichen werden, da das Risiko besteht, dass der NDB solche Sicherheitslücken hortet und ausnutzt - entgegen dem Interesse der Bevölkerung.

Darüber hinaus fordert die Piratenpartei einen Kurswechsel, um die Interessenskonflikte zu beheben, die sich aus der aktuellen Cybersicherheitsstruktur der Bundesverwaltung ergeben. Offensiv agierende Akteure wie die Armee, die zivilen Nachrichtendienste und die Justiz verfolgen der Cybersicherheit nicht zuträgliche Interessen. Wir begrüssen, dass in Art. 73b Abs. 3 Sicherheitslücken sofort mit den Betreibern von kritischen Infrastrukturen geteilt werden und fordern eine Ergänzung, dass diese nicht für offensive Cyberspielchen gemäss NDG missbraucht werden dürfen. Ebenso muss Hackern automatisch Straffreiheit im Rahmen von Responsible Disclosure zugesichert werden.

Das UVEK aber auch andere Departemente müssen unserer Meinung nach stärker in die Cybersicherheitsorganisation eingebunden werden. Wir erhoffen uns dadurch eine stärkere Gewichtung der Interessen der Betreiber kritischer Infrastrukturen.

Ferner fordern wir dringlich die Bildung eines finanziell gut ausgestatteten Fonds, aus dem Sicherheitsaudits von weit verbreiteter Software (bspw. Open Source / FOSS) finanziert wird. Es ist in Zukunft mit weiteren Sicherheitsvorfällen in der Grössenordnung wie log4j [4] oder heartbleed [5] zu rechnen und es ist im Interesse Aller, diese von non-profit Organisationen in grösstenteils ehrenamtlicher Arbeit erstellte Software, welche grosse Verbreitung geniesst, auf Herz und Nieren überprüfen zu lassen.

Die in Art. 74b genannten Bereiche sollen auf grosse Medienunternehmen erweitert werden.

Art. 74i ist zu starr formuliert. Für grosse Unternehmen ist eine angedrohte Busse von maximal 100'000 Franken lächerlich. Der Gesetzgeber sollte dies anteilig zum Umsatz des Unternehmens definieren, z.B. auf 4% des Jahresumsatzes.

Abschliessend stellt sich für die Piratenpartei die Frage, ob man im Jahr 2022 immer noch an der mentalen Haltung festgehalten werden soll, dass Informatik, Digitalisierung etc. als reiner Kostenblock angesehen wird, und damit immer noch im EFD anzusiedeln ist. Wir finden es an der Zeit, die Digitalisierung in ihrer Gänze die Wichtigkeit zuzusprechen, die sie auch für unser alltägliches Leben, die Wirtschaft und unsere Zukunft hat. Deshalb fordern wir erneut die Schaffung eines eigenen Departments für Digitalisierung, welches ressourcenmässig den tatsächlichen gesellschaftlichen und volkswirtschaftlichen Wert widerspiegelt.

Schlussbemerkungen

Wir beschränken uns in dieser Stellungnahme auf unsere Kernanliegen. Bei Verzicht unsererseits auf umfassende allgemeine Anmerkungen oder auf Anmerkungen zu einzelnen Regelungen, ist damit keine Zustimmung durch die Piraten zu solchen Regelungen verbunden.

Kontaktdetails für Rückfragen finden Sie in der Begleit-E-Mail.

Quellen:

[1] https://www.ncsc.admin.ch/ncsc/de/home/strategie/strategie-ncss-2018-2022.html

[2] https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/de#art_11_a

[3] https://www.republik.ch/2020/11/11/die-mysterioese-schwesterfirma

[4] https://de.wikipedia.org/wiki/Log4j#Bekanntwerden_einer_Sicherheitslücke_im_Dezember_2021

[5] https://de.wikipedia.org/wiki/Heartbleed

———

Piratenpartei Schweiz, Arbeitsgruppe Vernehmlassungen, 12. April 2022

AERO SUISSE

AEROSUISSE

Dachverband der schweizerischen Luft- und Raumfahrt

Fédération faîtière de l'aéronautique et de l'aérospatiale suisses

Associazione mantello dell'aeronautica e dello spazio svizzeri

Umbrella Organisation of Swiss Aerospace

Sekretariat:
Kapellenstrasse 14
Postfach
CH-3001 Bern
T +41 (0)58 796 98 90
F +41 (0)58 796 99 03

info@aerosuisse.ch
www.aerosuisse.ch

Eidgenössisches Finanzdepartement
3003 Bern

per Mail: ncsc@gs-efd.admin.ch

Bern, 14. April 2022

Stellungnahme AEROSUISSE zur Vernehmlassung Meldepflicht von BetreiberInnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrte Damen und Herren

Die AEROSUISSE dankt für die Einladung zum Vernehmlassungsverfahren und nimmt dazu wie folgt Stellung:

Die AEROSUISSE stimmt der Vorlage zu. Kritische Infrastrukturen müssen besser vor Cyberangriffen geschützt werden. Die Betreiber kritischer Infrastrukturen brauchen Ansprechpartner beim Bund, die die Informationen der Betreiber mit Erkenntnissen der Verwaltung und des Nachrichtendienstes ergänzen.

Gleichzeitig dürfen aber mit der Meldepflicht für sicherheitsrelevante Ereignisse keine zusätzlichen Kosten und Aufgaben für die Betreiber kritischer Infrastrukturen entstehen. Auch wenn die Verantwortung für IT-Sicherheit bei den Unternehmen liegt, braucht es staatliche Kapazitäten für die Frühwarnung und für die Unterstützung bei Verteidigungsmassnahmen gegen Cyberangriffe. In diesem Zusammenhang ist für die AEROSUISSE entscheidend, dass die Meldepflicht mit geringem Mehraufwand verbunden ist. Schliesslich erwarten die Betreiber von kritischen Infrastrukturen, dass sie von den Behörden, insbesondere vom NCSC und vom Nachrichtendienst frühzeitig auf etwaige Bedrohungen aufmerksam gemacht werden.

Ein weiterer wichtiger Punkt für die AEROSUISSE ist, dass im vorgeschlagenen Gesetzestext zu präzisieren ist, dass gestützt auf Artikel 74d nur Angriffe zu melden sind, die ein gewisses Schadenspotential aufweisen bzw. erfolgreich waren. Ohne diese Präzisierung besteht die Gefahr, dass jeder Cyberangriff der Meldepflicht untersteht. In Kombination mit der Schwierigkeit, was genau ein Cyberangriff ist, ist für die Rechtssicherheit der betroffenen Unternehmen wichtig, dass klar ist, dass Art. 74d der Massstab ist, wann ein Angriff auf eine kritische Infrastruktur zu melden ist.

Im Interesse der Rechtssicherheit ist mit Blick auf die Definition der kritischen Infrastruktur das Verhältnis des Informationssicherheitsgesetzes (ISG) und der nationalen Strategie zum Schutz kritischer Infrastrukturen zu klären. In der Strategie gehören die beiden Landesflughäfen Zürich und Genf zu diesen kritischen Infrastrukturen, aber gestützt auf Art. 74b lit p ISG könnte man zum Schluss kommen, dass lediglich Fluggesellschaften mit Bewilligung des Bundesamtes für Zivilluftfahrt (BAZL) von der Meldepflicht betroffen wären.

Mit Blick auf die Meldepflicht erfolgt bereits heute eine Meldung von erfolgreichen Cyber-Angriffen an das BAZL statt. Eine Harmonisierung und Koordination der Meldepflicht auf Bundesebene und damit die Förderung des Informationsaustauschs zwischen den Sektoren ist grundsätzlich begrüssenswert. Hier stellt sich die Frage, ob mit der Meldung an die NCSC die Meldepflicht an das BAZL erlischt.

Schliesslich ist die AEROUSISSE überzeugt, dass die in Artikel 74i vorgeschlagene Sanktionsmöglichkeit bei der Verletzung der Meldepflicht der falsche Weg ist, um den im erläuternden Bericht vorgesehenen Ausbau des Informationsaustausches mit Hilfe einer Kultur der Zusammenarbeit und gegenseitigen Vertrauens auszuarbeiten. Hier sind andere Mittel zu wählen.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und verbleiben

mit freundlichen Grüssen.

AEROSUISSE
Dachverband der schweizerischen
Luft- und Raumfahrt
Der Geschäftsführer:

Philip Kristensen

Generalsekretariat des Eidgenössischen
Finanzdepartements
Nationales Zentrum für Cybersicherheit
NCSC

Per E-Mail an: ncsc@gs-efd.admin.ch

Bern, 12. April 2022

Stellungnahme zum Entwurf des Bundesgesetzes über die Informationssicherheit beim Bund (ISG): Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrter Herr Bundesrat,
sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit zu oben genanntem Geschäft Stellung zu beziehen und nehmen diese hiermit gerne fristgerecht wahr.

asut, der Schweizerische Verband der Telekommunikation repräsentiert die Telekommunikations- und Netzwerkbranche und sämtliche Wirtschaftszweige sind im Verband vertreten. Wir gestalten und prägen gemeinsam mit unseren Mitgliedern die digitale Transformation der Schweiz und setzen uns für optimale politische, rechtliche und wirtschaftliche Rahmenbedingungen für die digitale Wirtschaft ein. Die vorgeschlagene Änderung des ISG ist für unsere Branche von hoher Relevanz.

asut unterstützt das Ziel, die Widerstandsfähigkeit der Schweiz gegenüber Cyberrisiken zu erhöhen und begrüsst die vorgeschlagenen Anpassungen des ISG im Grundsatz. asut regt jedoch die Schaffung einer zentralen Meldestelle für sämtliche Cybervorfälle an. Zu präzisieren ist zudem die Meldepflicht (Art. 74a), die ausdrücklich nur bei Cybervorfällen auf die eigene kritische Infrastruktur bestehen soll. Abzulehnen ist zudem Art. 74h bezüglich Strafbestimmungen die zur persönlichen Strafbarkeit der Verantwortlichen führen. In diesem Zusammenhang ist der Grundsatz des Selbstbelastungszwangsverbots bei Cyberangriffen und Cybervorfällen in Art. 73c Abs. 3 zu präzisieren.

asut begrüsst die vorgeschlagenen Anpassungen des ISG im Grundsatz, schlägt jedoch folgende Anpassungen vor:

NCSC als zentrale Meldestelle definieren
Um das Schadensausmass eines Cybervorfalls zu minimieren, müssen diese unter Umständen rasch gemeldet und ebenso rasch bearbeitet werden können. Die innerbetrieblichen Ressourcen werden in einer ersten Phase jedoch vor allem für die Krisenbewältigung, also für die Abwehr und Schadensbegrenzung eingesetzt. Der bürokratische Aufwand für die Erfüllung der verschiedenen Meldepflichten muss deshalb so gering und der Prozess so einfach wie möglich sein.

asut schlägt vor, beim Bund eine einzige und zentrale Meldestelle für sämtliche Cybervorfälle zu schaffen, deren Meldung gesetzlich vorgeschrieben ist. Mit dieser zentralen Meldestelle würde die Wirtschaft administrativ entlastet und die Prozesse vereinfacht werden. Prädestiniert für diese Aufgabe dürfte das NCSC sein. Statt es den Meldenden zu überlassen, einen Vorfall auch anderen Bundesstellen weiterzuleiten, könnte dies durch die zentrale Meldestelle geschehen. Wo nötig, könnte der Meldepflichtige mit der Meldung auch gleich sein Einverständnis für die Weitergabe der Meldung geben. Im erläuternden Bericht ist ein solcher Prozess angedacht.

asut
Schweizerischer Verband der Telekommunikation
Hirschengraben 8
3011 Bern

+41 (0)31 560 66 66
info@asut.ch
www.asut.ch

@asut_ch

Wir schlagen zudem ein einheitliches Vorgehen in allen Bundesbereichen vor. Im Revisionsentwurf zur «FDV – Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten» (Vernehmlassung bis 18. März 2022) war beispielsweise vorgesehen, dass Störungen in Telekomnetzen (wie z.B. Störungen der Netze, Cyberangriffe und andere böswillige Eingriffe) künftig nicht mehr an das BAKOM, sondern an die Nationale Alarmzentrale (NAZ) gemeldet werden müssen. asut hat sich in ihrer Stellungnahme zur Revision der FDV ebenfalls für das NCSC als zentrale Meldestelle für Störungen in Telekommunikationsnetzwerken ausgesprochen. Wichtig ist, dass die Revision der FDV und die Anpassung des ISG koordiniert erfolgen.

Meldepflicht präzisieren

«Internet Access Provider» (IAP) stellen anderen kritischen Infrastrukturen den Zugang zum Internet zur Verfügung. Die IAP sind stets bestrebt, bei Cybervorfällen ihre Kunden zu unterstützen. Ein IAP kann jedoch unmöglich zur Meldung sämtlicher Cyberangriffe verpflichtet werden, die über sein Netzwerk auf Betreiberinnen von kritischen Infrastrukturen erfolgen. Auch ist unter Umständen eine Meldung durch den IAP aufgrund von Vorgaben des Datenschutzgesetzes oder von vertraglichen Vereinbarungen gar nicht möglich. asut schlägt darum in Art. 74a ISG folgende präzisierende Ergänzung vor (zu ergänzender Text ist unterstrichen):

Art. 74a	Die Betreiberinnen von kritischen Infrastrukturen müssen dem NCSC Cyberangriffe auf ihre eigenen Infrastrukturen nach deren Entdeckung so rasch als möglich melden, damit das NCSC Angriffsmuster frühzeitig erkennen, mögliche Betroffene warnen und ihnen geeignete Präventions- und Abwehrmassnahmen empfehlen kann.

Strafbestimmungen zur persönlichen Strafbarkeit

Die Stossrichtung der Vernehmlassungsvorlage lässt auf ein partnerschaftliches Vorgehen zwischen Staat und Wirtschaft bei der Eindämmung von Cyber-Bedrohungen schliessen. Dieses kooperative Vorgehen widerläuft Art. 74h E-ISG und ist gänzlich abzulehnen. Solche Bestimmungen, die zur persönlichen Strafbarkeit der Verantwortlichen führen, sind für die Bekämpfung von Cyber-Bedrohungen vielmehr schädlich als förderlich, führen zu Fehlanreizen und können insbesondere die Bereitschaft der zuständigen Personen reduzieren, in Fragen der Cyber-Security Verantwortung zu übernehmen.

Art. 74h	ist gänzlich abzulehnen

In diesem Zusammenhang ist zudem der Grundsatz des Selbstbelastungszwangsverbots bei Cyberangriffen und Cybervorfällen eminent wichtig. asut schlägt eine Präzisierung von Art. 73c Abs. 3 vor.

Art. 73c Abs. 3	Informationen, die dem NCSC im Rahmen einer Meldung bekanntgegeben wurden und die meldende Person selbst belasten könnten, dürfen in einem Strafverfahren gegen diese Person nur mit Einverständnis dieser Person verwendet werden.

Wir danken ihnen bestens für die Berücksichtigung unserer Anliegen und stehen Ihnen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Peter Grütter
Präsident

Association of Foreign Banks in Switzerland
Verband der Auslandsbanken in der Schweiz
Association des banques étrangères en Suisse
Associazione delle banche estere in Svizzera

foreign banks . in switzerland .

Bundesrat
Ueli Maurer
Federal Department of Finance
ncsc@gs-efd.admin.ch

Zürich, 12. April 2022

Bundesgesetz über die Informationssicherheit

Sehr geehrter Herr Bundesrat

Gerne nehmen wir die Gelegenheit wahr, den Revisionsentwurf des Gesetzes für Informationssicherheit ISG, zu kommentieren. Unser Verband war an den Arbeiten der Schweiz. Bankiervereinigung beteiligt und unterstützt deren Stellungnahme. Daher werden wir uns nur zu ausgewählten Punkten äussern.

Unser Augenmerk liegt auf dem Abschnitt Pflicht zur Meldung. Wir verstehen, dass unterschiedliche Behörden und Ämter eigene Ansprüche gegenüber Form und Inhalt der Meldung haben. Auch bearbeiten die Behörden die Meldung aus unterschiedlicher Perspektive. Dennoch sollen die Abläufe standardisiert und die Meldungsinhalte harmonisiert sein. Auch sollen klare und einfach anwendbare Kriterien bestehen, nach denen Meldungen zu erstatten sind.

Aus diesen Gründen wünscht unser Verband, dass das Melderegime präzisiert wird und dabei folgende Punkte berücksichtigt werden:

- Das Gefährdungspotential des Zwischenfalls, ab der Meldung zu erstatten ist, ist zu definieren. Es ist klarzustellen, dass nur diejenigen Zwischenfälle zu melden sind, deren Auswirkungen weitere Finanzplatzteilnehmer betreffen können, bzw. deren Gefährdungspotential als hoch eingestuft wird. Zwischenfälle, deren Auswirkungen sich auf das Unternehmen beschränken, sind von der Meldepflicht auszunehmen.
- Eindeutig quantifizierbare Kriterien sind festzusetzen, nach denen eine Meldung zu erfolgen hat.
- Zeitpunkt und realistisch wahrnehmbare Fristen sind festzusetzen, innert derer eine Meldung zu erstatten ist. Es ist allenfalls ein zweistufiges Verfahren vorzusehen, nach dem in einem ersten Schritt der Vorfall zu melden ist und in einem zweiten Schritt Einzelheiten dazu nachzuliefern sind.
- Meldeinhalte sind zwischen den einzelnen Meldungsempfängern zu koordinieren. Doppelspurigkeiten sind zu vermeiden. Jeder Empfänger soll festlegen, welche Information er erhalten will.
- Ein standardisiertes Formular soll zur Verfügung stehen für alle Meldungen an unterschiedliche Meldungsempfänger. Wir unterstützen den Vorschlag der SBVg, ein derartiges Formular zu kreieren, das die Bedürfnisse aller Meldungsempfänger abdeckt.
  Dieser Ansatz ist auch im Sinne von Art 74f, der vorsieht, dass die erstattete Meldung an weitere Empfänger übermittelt werden kann.
  Dieser Punkt ist umso wichtiger, wenn man bedenkt, dass die Meldungsempfänger Rückfragen stellen werden. Auch hier ist Koordination und/ bzw. Arbeitsteilung sicherzustellen.
- Meldungen sollen in Englisch und den Landessprachen abgefasst werden können. Für Auslandsbanken, aber auch bei internationalen Sachverhalten, ist Englisch die übliche Sprache.

Usteristrasse 23 · CH-8001 Zürich
T +41 44 224 40 70 · F +41 44 221 00 29
www.afbs.ch · info@afbs.ch

Viele der hier vorgeschlagenen Elemente können in der Verordnung definiert werden. Unser Verband steht gerne zur Verfügung, um bei der Ausformulierung der Einzelheiten mitzuarbeiten und auch Erfahrung und Erkenntnis von Plattformen ausländischer Finanzplätze einzubringen.

Wir danken für die Aufmerksamkeit, die Sie unserer Stellungnahme entgegenbringen.

Freundliche Grüsse

VERBAND DER AUSLANDSBANKEN IN DER SCHWEIZ

Raoul Würgler
Geschäftsführer

Jonathan Deneys
Wissenschaftlicher Mitarbeiter

Centre Patronal

Monsieur le Conseiller fédéral
Ueli Maurer
Chef du Département fédéral des finances
3003 Berne

Par courrier électronique :
ncsc@gs-efd.admin.ch

Paudex, le 31 mars 2022
PGB

Procédure de consultation : obligation de signaler les cyberattaques contre des infrastructures critiques

Monsieur le Conseiller fédéral,

Nous avons pris connaissance du projet cité en titre, mis en consultation par vos services et qui a retenu toute notre attention. Par la présente, nous prenons la liberté de vous faire connaître notre position.

Généralités

Le projet consiste en une modification de la loi fédérale sur la sécurité de l'information (LSI), afin d'y intégrer un chapitre intitulé «Mesures de la Confédération visant à protéger la Suisse contre les cyberrisques». Les deux éléments essentiels de ce chapitre sont, d'une part, la description des tâches dévolues au Centre national pour la cybersécurité (NCSC) et, d'autre part, la création d'une obligation de signaler les cyberattaques contre des infrastructures critiques (domaines d'activités concernés par l'obligation, types de cyberattaques à signaler, contenu et modalités du signalement, etc.)

Le Centre national pour la cybersécurité (NCSC, autrefois MELANI) existe depuis un certain nombre d'années. A notre connaissance, il constitue une référence appréciée des professionnels de la cybersécurité, qui souhaiteraient toutefois, notamment, un service d'annonce des cyberrisques plus complet, plus rapide, plus réactif – ce qui suppose qu'un maximum de cybermenaces lui soient annoncées.

Dès lors, la volonté de mieux définir les tâches du NCSC, d'une part, et d'obliger les infrastructures critiques à annoncer toutes les cyberattaques dont elles ont connaissance, d'autre part, répond à une demande et contribuera certainement à améliorer la connaissance des menaces et la rapidité de réaction.

Nous soutenons donc, dans son principe, le projet mis en consultation.

Nous regrettons toutefois de constater, à la lecture du rapport explicatif, que l'obligation de signaler les cyberattaques – que nous soutenons – ne repose pas sur une base constitutionnelle explicite et satisfaisante et que le législateur fédéral, suivant sa mauvaise habitude, prévoit d'invoquer une «compétence fédérale inhérente». Nous plaidons pour que les questions constitutionnelles soient traitées avec davantage de soin par le monde politique fédéral, même si, en l'occurrence, l'obligation proposée ne porte guère atteinte aux compétences des cantons ni aux droits individuels.

Route du Lac 2
1094 Paudex
Case postale 1215
1001 Lausanne
T +41 58 796 33 00
F +41 58 796 33 11
info@centrepatronal.ch

Kapellenstrasse 14
Postfach
3001 Bern
T +41 58 796 99 09
F +41 58 796 99 03
cpbern@centrepatronal.ch

www.centrepatronal.ch

Remarques de détail

Nous constatons que la définition des infrastructures critiques soumises à l'obligation d'annonce (art. 74b) représente une liste longue et complexe, qui peut être source d'incertitude pour des entreprises qui hésiteraient à se sentir concernées. Les exceptions prévues ensuite à l'art. 74c sont susceptibles de renforcer cette incertitude. Nous prenons note du fait que des précisions pourront être apportées par voie d'ordonnance. Nous sommes surtout rassurés de constater que les éventuelles infractions à l'obligation d'annonce (art. 74h) seront traitées de manière pragmatique et constructive, avec d'abord une information du NCSC à l'exploitant concerné, puis, cas échéant, une décision du NCSC concernant les obligations qui incombent à l'exploitant, décision assortie d'un délai. Il est ainsi garanti qu'aucune entreprise ne pourra être sanctionnée pour une négligence ou un malentendu.

En conclusion, nous approuvons le projet mis en consultation, tout en faisant remarquer que le développement probable des activités de la Confédération en matière de cybersécurité appelle certainement la création d'une base constitutionnelle explicite.

Nous vous remercions de l'attention que vous porterez à ce qui précède et vous prions de croire, Monsieur le Conseiller fédéral, à l'expression de notre haute considération.

Centre Patronal

Pierre-Gabriel Bieri

CH++

Eidgenössisches Finanzdepartement EFD
Bundesrat Ueli Maurer
Bundesgasse 3, 3003 Bern
Eingabe per Mail an: ncsc@gs-efd.admin.ch

Lausanne, 12. April 2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe
Stellungnahme zum Bundesgesetz über die Informationssicherheit beim Bund

Sehr geehrter Herr Bundesrat Maurer,
Sehr geehrter Delegierter des Bundes für Cybersicherheit Schütz,
Sehr geehrte Damen und Herren;

Mit grossem Interesse haben wir die Vernehmlassung zur Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen und die weiteren vorgesehen Änderungen im Informationssicherheitsgesetz ISG zur Kenntnis genommen. Unsere Organisation CH++ widmet sich unabhängig einer nachhaltigen, wohlhabend und handlungsfähigen Schweiz durch Wissenschaft und Technologie — und dazu gehört fraglos und immer mehr auch die Cybersicherheit. Gerne nehmen wir entsprechend hiermit von der Möglichkeit gebrauch, Ihnen unsere Vernehmlassungsantwort zukommen zu lassen, die wir in den vergangenen Monaten mit einer Reihe namhafter ExpertInnen haben ausarbeiten können.

Wir bedanken uns für Ihr Interesse und stehen Ihnen für weiteren Dialog stets gerne zur Verfügung.

Marcel Salathé, Präsidium
Hannes Gassert, Präsidium
Olga Baranova, Geschäftsleitung

CH++

Allgemeine Würdigung

CH++ begrüsst die Einführung einer Meldepflicht im ISG: Ein verlässliches Lagebild muss Grundlage sein unserer Abwehrmassnahmen, in der Verwaltung ebenso wie in der Wirtschaft.

Ebenfalls unterstützt CH++ die erhöhte Verbindlichkeit auf Gesetzesstufe, sowohl bei den Verpflichtungen des NCSC wie auch auf jenen der Betreiberorganisationen kritischer Infrastruktur, inklusive Sanktionsmöglichkeiten. Punkte wie die Definition der zu meldenden Cyberangriffe oder der Auskunftspflichten sind aus Sicht CH++ gut gelungen.

CH++ ist jedoch der Ansicht, dass verschiedentlich Schärfungen vorzunehmen sind am aktuellen Entwurf, welche wir in der Folge darlegen. Namentlich ist aus Sicht von CH++ das Mandat des NCSC robuster auszugestalten und die Meldepflicht breiter zu gestalten — und gleichzeitig sie effizienter zu gestalten.

Darüber hinaus unterstützt CH++, wie Sie der Presse haben entnehmen können[1], die bereits von Bundesrat Maurer angekündigte Überführung des NCSC in ein Staatssekretariat, um den Stellenwert des Themas, den Ressourcenbedarf und die Mitwirkungsmöglichkeiten und die internationale Verhandlungsfähigkeit der Behörde auf das aus unserer Sicht angebrachte Niveau zu heben.

[1] https://magazin.nzz.ch/meinungen/die-schweiz-muss-ihre-digitale-souveraenitaet-verteidigen-ld.1653935

CH++

Artikel 73

1. Grundsatz

Die hier aufgeführten Tätigkeiten beschreiben ein breites Aufgabengebiet, sind aber noch zu passiv ausgestaltet und weisen dem NCSC eine entsprechend zu kleine und zu wenig aktive Verantwortungsposition zu.

Hinzuzufügen ist aus Sicht CH++ die aktive Erkennung von Schwachstellen und Bedrohungen, einerseits durch die Überwachung der globalen Geschehnisse im Bereich Cybersicherheit und andererseits durch das aktive Überwachen der Bedrohungslage durch Scans nach Sicherheitslücken in sämtlichen Informatikmitteln im Geltungsbereich des Gesetzes. Die so erlangten Erkenntnisse sind sodann analog zu passiv erhaltenen Meldung zu verarbeiten.

2. Bearbeitung von Meldungen zu Cybervorfällen und Schwachstellen

Nach Ansicht von CH++ sind die Bedingungen für eine Veröffentlichung sowohl in den lit. 2 und 3 (“sofern ..”) umzukehren in eine grundsätzliche Verpflichtung zur Veröffentlichung, unter Vorbehalt übergeordneter Interessen. Der “Default” kann nicht “security through obscurity” sein oder aktive Zurückhaltung sicherheitsrelevanter Informationen, sondern die aktive Transparenz — mit begründeten Ausnahmen. Über diese Ausnahmen ist sodann regelmässig Bericht zu erstatten an den Bundesrat und die zuständige parlamentarische Kommission.

Die möglichen Massnahmen in der Bearbeitung von Meldungen sind aus Perspektive von CH++ zudem noch zu wenig klar zu wenig robust. In Ergänzung zu den genannten Möglichkeiten schlägt CH++ vor, dass das NCSC in besonders gravierenden Fällen Weisungen mit Fristen erlassen kann, die Hersteller und

Betreiberorganisationen dazu verpflichten, die entsprechenden Produkte oder Infrastrukturen nachweislich abzusichern.

Darüber hinaus erscheint es angebracht, lit. 3 um eine Sanktionsmöglichkeit zuzüglich zur Veröffentlichung zu ergänzen, beispielsweise durch den Ausschluss des Herstellers von jeglichen öffentlichen Beschaffungen im Bereich kritischer Infrastruktur bis zur Behebung der Schwachstelle. Ein entsprechender Absatz im Bundesgesetz über das öffentliche Beschaffungswesen erscheint angebracht.
Im Weiteren sind in einem weiteren Absatz analog zu Absatz 3 nicht nur Hersteller, sondern auch auf Betreiberorganisationen entsprechender Hard- und Software in die Pflicht zu nehmen. Das Forcieren der Bereitstellung eines Sicherheitsupdates verbessert die Sicherheitslage wenig, wenn dieses sodann nicht zügig und flächendeckend eingespielt wird.

3. Weiterleitung von Informationen

CH++ begrüsst lit. 3 klar. Der verantwortungsvolle Umgang mit Sicherheitslücken (responsible disclosure etc.) darf nicht mit dem Risiko einer Strafverfolgung belegt werden.

Artikel 74

Meldepflicht

Die Meldepflicht ist aus Sicht von CH++ schneller, automatisierter und breiter auszugestalten:

- Die Meldungen haben nicht “so schnell wie möglich”, sondern umgehend zu erfolgen, im Regelfall innert 24 Stunden.
- Lit. f ist zu präzisieren: Die Auslegung von “grossen Zahl von Nutzenden” birgt die Gefahr, dass etwas kleinere Anbieter mit weniger Sicherheits-Ressourcen,

die aber womöglich sehr lohnenswerte Ziele darstellen und deren Nutzende hohen Risiken wie etwa Identitätsdiebstahl ausgesetzt sind, von der Regulierung nicht betroffen wären. Eine konkrete, im Zweifelsfall eher niedrige Zahl ist hier spätestens auf Verordnungsstufe zu definieren. Im Weiteren ist der in Punkt 2 verwendete Begriff “digitale Wirtschaft” abzuändern zu “Wirtschaft”.

- Lit s. begrüsst CH++ explizit, die Lieferketten sind miteinzubeziehen.

Ausnahmen von der Meldepflicht

CH++ steht dem gesamten Artikel 74c kritisch gegenüber und schlägt vor, diesen zu streichen. A priori die Eintretenswahrscheinlichkeit eines Risikos und die Grösse des erwartbaren Schadens verlässlich so gut einschätzen zu können, dass solche Ausnahmen bedenkenlos für gesamte Bereiche erteilt werden können, scheint schwierig — und entsprechend riskant.

Inhalt und Art. 74f Übermittlung der Meldung

Diese Artikel sind aus Sicht CH++ so zu überarbeiten, dass die Automatisierung von Meldungen möglich und wünschenswert werden. Mit den zur Verfügung stehenden technischen Möglichkeiten ist die Auswertung auch eines grossen Volumens von Meldungen möglich, auch wenn diese eher Anhaltspunkte denn kompletten Meldungen entsprechen. Art. 74e wäre entsprechend abzuschwächen auf eine Kann-Formulierung, sodass auch Meldungen wie Signale verdächtiger Aktivität andere auffällige Muster gemeldet werden können. Damit sinkt die Schwelle zur Interaktion mit dem NCSC.

Art. 74f wäre anzupassen hin zur expliziten Nennung der Datenanlieferung via gesicherter Schnittstelle als zusätzliche Möglichkeit. Dank dieser Automatisierung sinkt potentiell die administrative Belastung seitens der Meldepflichtigen, was die Akzeptanz der neuen Pflicht erhöhen dürfte. In der Industrie ist dies ein weit

verbreiteter Ansatz, sich innerhalb einer Community mit “Threat Intelligence” gegenseitig zu unterstützen. Ein API-zentrierter Ansatz wie er zum Beispiel in den Partnernetzwerken von Meta/Facebook oder AT&T erfolgreich praktiziert wird, ist aus Sicht CH++ durch das NCSC weiter zu verfolgen, wofür nun eine entsprechende gesetzliche Grundlage zu schaffen ist.

In jedem Fall sollte in der Umsetzung nach Möglichkeit sichergestellt werden, dass sich überschneidende Meldepflichten (DSG, Finma, usw.) durch einen einzigen Meldevorgang erfüllt werden können.

Widerhandlungen gegen Verfügungen des NCSC

CH++ schlägt vor, im Text klarer zu machen, dass die Sanktionen auf der Leitungsebene der Unternehmen zu greifen haben, nicht auf Ebene der Fachspezialisten, allenfalls durch Nennung spezifisch haftbarer Organe bzw. deren Mitglieder.

Art. 79 Abs. 1

Hier schlägt CH++ vor, den Begriff Verwendung zu qualifizieren, z.B. mit “zwingende Verwendung”. Das blosse Öffnen eines Datensatzes kann selbstverständlich nicht zur Verlängerung der erlaubten Aufbewahrungsdauer führen.

DIGITALE | GESELLSCHAFT

Digitale Gesellschaft, CH-4000 Basel

Eidgenössischen Finanzdepartements EFD
Generalsekretariat EFD
Bundesgasse 3
3003 Bern

Per E-Mail an: ncsc@gs-efd.admin.ch

14. April 2022

Stellungnahme zur Änderung des Informationssicherheitsgesetzes (ISG) (Vernehmlassung 2021/70)

Sehr geehrte Damen und Herren

Am 17. November 2021 eröffnete der Bundesrat die Vernehmlassung zur Einführung einer Meldepflicht für Cyberangriffe und der damit verbundenen Änderung des Informationssicherheitsgesetzes (ISG). Wir danken Ihnen für die Einladung am Vernehmlassungsverfahren teilzunehmen.

Die Digitale Gesellschaft ist eine gemeinnützige Organisation, die sich für Grund- und Menschenrechte, eine offene Wissenskultur, weitreichende Transparenz sowie Beteiligungsmöglichkeiten an gesellschaftlichen Entscheidungsprozessen einsetzt. Die Tätigkeit orientiert sich an den Bedürfnissen der Bürgerinnen und Konsumenten in der Schweiz und international. Das Ziel ist die Erhaltung und die Förderung einer freien, offenen und nachhaltigen Gesellschaft vor dem Hintergrund der Persönlichkeits- und Menschenrechte.

Gerne nehmen wir zum Entwurf wie folgt Stellung:

Vorbemerkung

Die Digitalisierung und ihr bisher wohl grösstes Werk – das Internet – haben die letzten 20 Jahre geprägt wie keine andere Neuerung. Die wirtschaftlichen und gesellschaftlichen Möglichkeiten, welche der digitale Wandel mit sich bringt, sind enorm und haben schon zu vielen positiven Veränderungen in der Gesellschaft geführt. Im letzten Jahrzehnt hat sich der technologische Wandel aber auch vermehrt von einer dunklen Seite gezeigt: Desinformationskampagnen über soziale Netzwerke, Massenüberwachung und Cyberangriffe sind zu realen Bedrohungen für Wirtschaft und Gesellschaft geworden. Insbesondere Angriffe auf IT-Systeme haben in den letzten Jahren massiv zugenommen. So wurden laut einer Untersuchung der ZHAW ein Drittel aller Schweizer KMU schon einmal Opfer eines Cyberangriffs [1]. Diese Vorfälle kosten die Schweiz jährlich schätzungsweise 9.5 Milliarden CHF [2] und betreffen auch immer öfters Betreiber kritischer Infrastrukturen [3].

Im Lichte dieser Entwicklungen unterstützt die Digitale Gesellschaft den Änderungsvorschlag zum ISG. Zusätzlich sind jedoch weitere Massnahmen dringend nötig.

Meldepflicht für alle

Die Erstellung eines möglichst umfassenden, aktuellen Lagebildes ist ein unabdingbarer Schritt in Richtung höherer IT-Sicherheit in der Schweiz. Aktuell ergibt sich dieses Lagebild aus den freiwilligen Meldungen von Bevölkerung und Wirtschaft an das Nationale Zentrum für Cybersicherheit (NCSC). Im ersten Halbjahr 2021 wurden dem NCSC so rund 10'234 Vorfälle gemeldet. Betrachtet man diese Zahl etwas genauer, wird ersichtlich, dass diese Meldungen grossmehrheitlich aus der Bevölkerung kamen.

So trafen beim NCSC knapp 8'000 Meldungen zu «Fake-Sextortion», Vorschussbetrug, Fake-Support-Anrufen und falschen Paketbenachrichtigungen ein. Angriffstaktiken, welche hingegen auf Unternehmen abzielen, wurden kaum gemeldet. So gingen beim NCSC im ersten Halbjahr 2021 lediglich 94 Meldungen zu Malware ein (insbesondere Verschlüsselungstrojanern; wobei 39 Fälle ein von Privaten eingesetztes Produkt betreffen) [4]. Vergleicht man diese Zahl mit den Schätzungen der Anzahl Schweizer Unternehmen, die bereits Opfer eines Cyberangriffs wurden (siehe oben), kommt man zum Schluss, dass die dem NCSC gemeldeten Angriffe auf Unternehmen die absolute Minderheit darstellen. In anderen Worten: Aus den Meldungen der Schweizer

Wirtschaft an das NCSC lässt sich kein aktuelles Lagebild zur IT-Sicherheit Schweizer Unternehmen ableiten. Es muss also davon ausgegangen werden, dass den politischen und wirtschaftlichen Entscheidungsträgern in der Schweiz aktuell kein hinreichendes Lagebild zur IT-Sicherheit zur Verfügung steht.

Mit Blick auf kritische Infrastrukturen ist dieser Informationsmangel besonders verheerend. Grosse Teile der kritischen Infrastruktur erbringen Dienstleistungen, welche für die Gesellschaft von grundlegender Bedeutung sind. Entsprechend hoch müssen die Ansprüche an ihre Sicherheit sein. Die Digitale Gesellschaft unterstützt deshalb die geplante, im revidierten ISG vorgesehene, verbindliche Meldepflicht von IT-Sicherheitsvorfällen für Betreiber von kritischer Infrastruktur.

Die vorgesehene Meldepflicht ist ein erster, wichtiger Schritt; aus unserer Sicht jedoch nicht hinreichend. Die kritische Infrastruktur stellt nur einen Bruchteil der Schweizer IT-Landschaft dar. Wie oben ausgeführt, betreffen IT-Sicherheitsvorfälle aber Unternehmen in allen Sektoren (und die Gesellschaft insgesamt). Zudem kann davon ausgegangen werden, dass die Bedrohungen, denen Betreiberinnen von kritischen Infrastrukturen ausgesetzt sind, sich nur teilweise mit jenen überschneiden, mit denen der Rest der Wirtschaft zu kämpfen hat. Aus den Daten der neuen Meldepflicht wird sich deshalb nicht ein Lagebild für die ganze Schweiz ableiten lassen. Wir schlagen deshalb vor, dass die Meldepflicht künftig auf alle Bereiche der Schweizer Wirtschaft sowie auf staatliche Behörden und NGO ausgedehnt wird, auch wenn diese keine Betreiber von kritischer Infrastruktur sind, sobald der Vorfall eine entsprechende Relevanz hat.

Wird dem NCSC eine Sicherheitslücke bekannt, die ein Drittprodukt betrifft und bei der nicht davon auszugehen ist, dass sie der Herstellerin bereits bekannt ist, muss die Sicherheitslücke vom NCSC umgehend im Rahmen eines «responsible Disclosure»-Verfahrens der betroffenen Herstellerin gemeldet werden. Zusätzlich sollten dem NCSC Mittel an die Hand gegeben werden, um bei meldenden Organisationen auf die Behebung einer Sicherheitslücke bestehen zu können.

Der Grundsatz, entdeckte (aber noch nicht bekannte) Sicherheitslücken («Zero Day Exploits») im Rahmen eines «responsible-Disclosure»-Verfahrens zu veröffentlichen, sollte neben dem NCSC für alle Bundesstellen gelten, auch für den Nachrichtendienst. Alle Bundesstellen sollen auf den Einsatz von Informatikmitteln verzichten, welche diese Lücken ausnutzen – denn mit solchen «Staatstrojanern» wird das Geschäft mit Sicherheitslücken und damit Unsicherheit vorangetrieben.

Die Digitale Gesellschaft ist sich bewusst, dass eine verbindliche Meldepflicht für die gesamte Wirtschaft nicht unproblematisch ist. Eine Meldepflicht bedeutet technischen und administrativen Aufwand zu einer Zeit, in der eine Organisation einen potenziell existenzgefährdenden Vorfall zu bewältigen hat. Zudem wäre diese Meldepflicht unter Umständen nicht die einzige Meldepflicht, welcher im Falle eines Sicherheitsvorfalls nachgekommen werden müsste. Denkbar – und sogar wahrscheinlich – ist, dass ein Sicherheitsvorfall auch eine Meldepflicht nach dem nDSG nach sich zieht. Zudem wird das betroffene Unternehmen typischerweise auch eine Strafanzeige einreichen wollen. Die Hürden für diese Meldungen sollten deshalb so tief wie möglich gehalten werden. Optimalerweise stünde den Organisationen eine einzige, zentrale Anlaufstelle innerhalb der Bundesverwaltung zur Verfügung, bei der allen Meldepflichten – und potenziell Strafanzeigen – mittels einem einzigen Online-Formular nachgekommen werden kann.

Verbindliche Mindeststandards und Haftung

Neben reaktiven Massnahmen – wie der Meldepflicht – braucht es aber auch proaktive Massnahmen. Wichtig wäre es, verbindliche Mindeststandards zu schaffen, welche überprüfbare «best Practices» definieren. Die im Rahmen der aktuellen Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) erarbeiteten IKT-Mindeststandards sind ein guter Ansatz, weisen aber folgende drei Mängel auf. Erstens richten sie sich lediglich an Betreiber von kritischer Infrastruktur. Zweitens sind sie für diese nicht verbindlich. Und drittens sind die darin definierten Massnahmen nur sehr schwierig messbar und damit kaum einer Überprüfung zugänglich. Die Digitale Gesellschaft schlägt deshalb die Einführung von verbindlichen Mindeststandards vor, welche sich an den anerkannten Regeln der Technik orientieren und zudem messbare und damit überprüfbare Massnahmen definieren.

Verbindliche Mindeststandards würden es sodann erlauben, eine weitere Herausforderung anzugehen: Die Klärung von Haftungsfragen. Aktuell ist die Frage nach der Haftung für Schäden aus IT-Sicherheitsvorfällen weitgehend ungeklärt. Betroffene, welche durch einen Sicherheitsmangel in der IT einen Schaden erleiden, haben diesen oftmals selbst zu tragen. Grund dafür ist primär die Unklarheit in Bezug auf die Frage, wann IT-Infrastruktur überhaupt einen Sicherheitsmangel aufweist. Verbindliche Mindeststandards würden diese Unsicherheit beseitigen. Die Mindeststandards fungieren in diesem Kontext als ein Mindestmass an «due Diligence», welches eine Betreiberin erreichen muss, um ihre Abnehmer (oder sonstige

mögliche Betroffene) vor Schäden aus Sicherheitsvorfällen zu bewahren. Tut sie das nicht, haftet sie für die Schäden, welche die Betroffenen erleiden.

Zu klären bliebe die Frage nach der Beweislast in diesen Konstellationen. Nach Art. 8 ZGB trägt grundsätzlich jene Partei die Beweislast, welche ein Recht geltend machen will – in Haftungsfragen also grundsätzlich die geschädigte Person. Im Kontext von Schäden, die im Zuge eines IT-Sicherheitsvorfalls entstehen, ist diese Beweislastverteilung aber nicht sinnvoll. Es ist davon auszugehen, dass es dem geschädigten Abnehmer schon allein aufgrund von fehlendem Zugang zur Infrastruktur der Betreiberin in der Regel unmöglich wäre, nachzuweisen, dass die Betreiberin schuldhaft einen Sicherheitsstandard nicht eingehalten hat. Für die Betreiberin hingegen wäre es ein Leichtes, die Einhaltung von Mindestsicherheitsstandards zu protokollieren und somit nachzuweisen. Entsprechend muss im Zusammenhang mit Haftungsfragen betreffend IT-Infrastrukur – in Anlehnung an bereits bestehende Konsumentenschutzgesetze wie das Produktehaftpflichtgesetz (PrHG) – auch über Beweislasterleichterungen oder gar über eine Beweislastumkehr nachgedacht werden.

Ausblick

Die oben aufgeführten Massnahmen stellen einen ersten, entscheidenden Schritt in Richtung mehr IT-Sicherheit dar. Darauf aufbauend sollte aber über weitere Massnahmen nachgedacht werden. Im folgenden werden einige vorgeschlagen.

Die oben diskutierten Mindeststandards bieten zwar eine Hilfestellung zur Klärung von Haftungsfragen bei Schäden aus fehlerhafter IT-Infrastruktur, nicht aber bei Schäden aus fehlerhaften IT-Produkten – also in Konstellationen, in denen eine Herstellerin einem Kunden ein fehlerhaftes IT-Produkt zum eigenen Betrieb übergibt und dem Kunden oder Dritten daraus ein Schaden entsteht. Als Beispiel sind fehlerhafte IoT-Produkte (netzwerkfähige Geräte) oder fehlerhafte Software zu nennen. Das PrHG, welches Haftungsfragen im Kontext von fehlerhaften Produkten klärt, füllt diese Lücke nur teilweise, denn das PrHG ist nur auf bewegliche Sachen anwendbar. In Fällen, in denen das Produkt eine gewisse Körperlichkeit aufweist – wie beispielsweise bei einem Staubsaugerroboter – werden Haftungsfragen also durch das PrHG geklärt. In Fällen, in denen das Produkt jedoch lediglich in digitaler Form vorliegt – wie beispielsweise bei einem Textverarbeitungsprogramm, welches der Kunde direkt von der Website der Herstellerin herunterlädt – fehlt diese Körperlichkeit und das PrHG ist nicht anwendbar. Um diese Lücke zu schliessen, sollte über eine Ausweitung

des Anwendungsbereichs des PrHG auf unkörperliche, digitale Produkte (die gegen ein Entgelt angeboten werden) nachgedacht werden, wie es ein Teil der juristischen Lehre fordert [BSK OR I-Fellmann, Art. 3 PrHG, RZ 10].

Herstellerinnen von netzwerkfähigen Geräten (IoT-Produkte) müssten zudem über einen Zeitraum (abhängig von der durchschnittlichen Nutzungsdauer dieser Geräte) verpflichtet werden, Firmware- und Security-Updates für ihre Geräte allen Nutzern bereitzustellen. Diese «garantierte Nutzungsdauer» entspricht einem Mindeshaltbarkeitsdatum zur sicheren Nutzung und wäre eine Erweiterung der gesetzlichen Gewährleistung.

Wenn Sicherheitsforscher einen Sicherheitsmangel in der Infrastruktur, der Dienstleistung oder dem Produkt eines Unternehmens aufdecken, stellt sich regelmässig die Frage nach der Art und Weise, wie dieser Mangel dem betroffenen Unternehmen gemeldet werden soll. Traditionell waren solche «responsible Disclosures» ein äusserst heikles Unterfangen: Die Sicherheitsforscher mussten trotz ihren guten Absichten damit rechnen, vom Unternehmen, dessen Sicherheitsmangel sie aufgedeckt hatten, verklagt zu werden. In den letzten Jahren hat sich diese Situation etwas entschärft: Das gestiegene Bewusstsein für IT-Sicherheit trägt dazu bei, dass immer mehr Unternehmen dankbar sind für gemeldete Sicherheitsmängel. Einige grössere Unternehmen zahlen im Rahmen von «bug Bounty»-Programmen den Entdeckerinnen von Sicherheitsmängeln gar Belohnungsgelder aus. Insgesamt ist die Situation aber dennoch unbefriedigend. So sorgt insbesondere der Artikel 143bis StGB (sog. «Hackerparagraph»), welcher ein unbefugtes Eindringen in ein Datenverarbeitungssystem oder das Zugänglichmachen von Werkzeugen mit einer Freiheitsstrafe bis zu drei Jahren sanktioniert, weiterhin für erhebliche Rechtsunsicherheit und behindert die Aufdeckung von Sicherheitsmängeln durch Sicherheitsforscher.

Trifft bei einem Unternehmen die Meldung einer Sicherheitslücke ein, so haben insbesondere kleine und mittlere Unternehmen oft nicht die Ressourcen, um umgehend auf die Meldung zu reagieren und die Schwachstelle zu beheben. Das Resultat sind Sicherheitslücken, die zwar erkannt wurden, aber dennoch über lange Zeit offenstehen. Eine zentrale Meldestelle für Sicherheitsmängel könnte Abhilfe schaffen. Eine zentrale Meldestelle innerhalb der Bundesverwaltung – beispielsweise das NCSC – könnte Meldungen von Sicherheitslücken entgegennehmen und alle potenziell betroffenen Unternehmen gleichzeitig informieren. Daraus würden sich

zwei Vorteile ergeben. Einerseits könnte so der Finder bzw. die Finderin der Sicherheitslücke von einer potenziell feindseligen Reaktion des Unternehmens geschützt werden. Andererseits könnte das NCSC auf die Behebung der Sicherheitslücke hinwirken.

Schlussbemerkung

Wir beschränken uns in dieser Stellungnahme auf unsere Kernanliegen. Bei Verzicht auf umfassende allgemeine Anmerkungen oder auf Anmerkungen zu einzelnen Artikeln bedeutet dies keine Zustimmung der Digitalen Gesellschaft.

Freundliche Grüsse

Erik Schönenberger

digitalswitzerland

Eidgenössisches Finanzdepartement EFD
Bundesrat Ueli Maurer
Bundesgasse 3, 3003 Bern

Eingabe per Mail an: ncsc@gs-efd.admin.ch

Bern, 13. März 2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Stellungnahme zum Bundesgesetz über die Informationssicherheit beim Bund

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, uns zu den Änderungen im Bundesgesetz über die Informationssicherheit beim Bund, äussern zu können. digitalswitzerland nimmt diese Gelegenheit gerne wahr.

Betroffenheit digitalswitzerland
digitalswitzerland ist eine schweizweite, branchenübergreifende Initiative, welche die Schweiz als weltweit führenden digitalen Innovationsstandort stärken und verankern will. Unter dem Dach von digitalswitzerland arbeiten an diesem Ziel mehr als 240 Organisationen, bestehend aus Vereinsmitgliedern und politisch neutralen Stiftungspartnern, transversal zusammen. digitalswitzerland ist Ansprechpartner in allen Digitalisierungsfragen und engagiert sich für die Lösung vielfältiger Herausforderungen.

1. Begrüssung der Meldepflicht

digitalswitzerland unterstützt grundsätzlich die Einführung einer Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe. Die Mitglieder von digitalswitzerland beschäftigen sich täglich mit der Cybersicherheit ihrer eigenen Unternehmen oder betreuen IT-Systeme ihrer Kunden in diesem Bereich. Die Anzahl von Cyberangriffen nimmt rasant zu. Ein adäquater Schutz ist generell für jedes Unternehmen angezeigt. Dies gilt insbesondere für Betreiberinnen von kritischen Infrastrukturen, die eine wichtige Funktion für Wirtschaft und Gesellschaft übernehmen und auch im Falle eines Cybervorfalls oder -angriffs diese gewährleisten müssen. Deswegen begrüsst digitalswitzerland grundsätzlich eine Meldepflicht für Betreiberinnen von kritischer Infrastrukturen. Nichtdestotrotz gibt es aus Sicht von digitalswitzerland braucht Gesetzesentwurf noch Präzisierungen, damit die Regulierung für die Unternehmungen verträglich und damit zielführend für alle Beteiligten wird.

2. Präzisierungen der Meldepflichtigen und des Meldegegenstands

Im Zuge der Gesetzgebung darf nicht vergessen werden, dass eine Meldepflicht an die Behörden zu einer administrativen Belastung der Unternehmen führt. Es braucht daher klare Aussagen dazu, «wer» «wem» «was» unter welchen Bedingungen liefern muss.

Der Gesetzesentwurf erwähnt unter Art. 74b E-ISG eine Vielzahl von betroffenen Branchen. Insbesondere Art. 74b lit. s E-ISG nennt Betreiber von Hard- und Software, deren Produkte von kritischen Infrastrukturen genutzt werden. Damit wird der Geltungsbereich der Meldepflicht auf die Lieferketten ausgedehnt, was auf eine noch grössere Betroffenheit schliessen lässt, als die Aufzählung unter Art. 74b E-ISG zeigt. Die gewählte Formulierung lässt im derzeitigen Fall auf einen grossen Kreis an betroffenen Firmen schliessen.

Einführung Terminologie «Meldepflichtigen»

Um eine höhere Präzision zu erreichen und Missverständnisse zu vermeiden, wird die Einführung der Terminologie des «Meldepflichtigen» vorgeschlagen. Auch wenn im Kontext der kritischen Infrastrukturen eine klarere Definition schwierig sein dürfte, da sie sicherheitsrelevant ist, braucht es trotzdem möglichst klare Anhaltspunkte zum Geltungsbereich. Gerade die Ausdehnung auf Unternehmungen in der Lieferkette weist auf eine breite Betroffenheit der Wirtschaft hin.

Sollte der Geltungsbereich, wie von uns verstanden, grosse Teile der Wirtschaft betreffen, wird eine Regulierungfolgenabschätzung notwendig. Denkbar wäre auch ein abgestufter Regulierungsansatz, der sich an der Kritikalität der Unternehmen orientiert. Durch Definierung von Ambitionsniveaus könnten Erfahrungen mit der Meldepflicht gesammelt werden, bevor sie auf weite Teile der Wirtschaft ausgedehnt würde. Als oberste Stufe wären die Betreiberinnen von kritischen Infrastrukturen wie etwa die Energie- und Wasserversorger zu nennen. Alsdann könnte die Meldepflicht entlang von Ambitionsniveaus ausgerollt werden. Denn gerade für kleine Unternehmen und Startups sind zusätzliche Regulierungsaufwände so klein wie möglich zu halten.

Meldegegenstand klar benennen

Damit keine Missverständnisse beim Meldegegenstand entstehen, sollte zudem klar definiert werden, was gemeldet werden muss. Hier bleibt der Gesetzestext unscharf, da er wahlweise von Cybervorfällen, Cyberangriffen oder Schwachstellen spricht. Auch scheint die Definiton des Begriffs «Cybervorfall» kaum handhabbar, weil sie mit der blossen – auch theoretischen – Möglichkeit der Beeinträchtigung der Schutzziele operiert. Eine Möglichkeit kann oft nicht ausgeschlossen werden. Die Definition sollte daher angepasst werden. Es drängt sich auf, sich hier an Art. 4 Nr. 7 der NIS-Richtlinie anzulehnen. Sie definiert den «Sicherheitsvorfall» als «alle Ereignisse, die tatsächlich nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssystemen haben». Im Ergebnis sollte Art. 5 lit. d daher wie folgt lauten:

Änderung Art. 5 lit. d E-ISG (Änderung kursiv markiert) «Cybervorfall: Ereignis beim Betrieb von Informatikmitteln, das ~~dazu führen kann~~ *dazu führt*, dass die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist.»

Unklare Defintion von Online-Marktplatz

Art. 74b lit. f E-ISG definiert zwei Bedingungen bei welchen Anbieterinnen von Online-Marktplätze, Cloudcomputing und weiteren digitalen Diensten unter die Meldepflicht fallen. Das Gesetz nennt 1) «eine grosse Zahl von Nutzenden» und 2) eine «hohe Bedeutung für die digitale Wirtschaft». Diese Definitionen sind aus Sicht von digitalswitzerland sehr unklar gewählt. Sie müssten entweder bereits im Gesetzestext präziser definiert oder spätestens dann in der Verordnung geklärt werden.

Wir geben zudem grundsätzlich zu bedenken, dass die Definition von Online-Marktplätzen als «kritische Infrastruktur» zweifelhaft erscheint. So sollte sich die Definition dieses Begriffs an etablierten regulatorischen Grundsätzen orientieren und einen Gleichklang mit der Gesetzgebung innerhalb des europäischen Auslands herstellen (siehe unter anderem hier: Annex zum Entwurf einer EU-Richtlinie zum Schutz kritischer Infrastrukturen). Dies sind per definitionem Dienste, die für die Aufrechterhaltung lebenswichtiger gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten unerlässlich sind, z.B. aus den Bereichen Finanzwesen, Gesundheit, Verkehr. Es wird vorgeschlagen, den Gesetzestext in diesem Sinne zu präzisieren.

Änderung Art. 74b, Abs. f E-ISG «Bereiche» (Änderung kursiv markiert) «Die Meldepflicht gilt für: […] f. Anbieterinnen von ~~*Online-Marktplätzen,*~~ Cloudcomputing, Suchmaschinen und weiteren digitalen Diensten sowie Registrare von Domain-Namen und Betreiberinnen von Rechenzentren, die in der Schweiz: […]

Durch die angestrebte Breite und Tiefe der Meldepflicht ist es aus Sicht von digitalswitzerland unabdingbar, dass die Verletzung von Rechten von Dritten im Falle einer Meldung nicht gefährdet sind. Daher wird eine Präzisierung von Art. 74 Abs. 4 E-ISG gefordert. Es sollte klarer dargelegt werden, wie das NCSC die Geheimhaltungspflichten schützt.

3. Überschneidungen mit anderen Meldepflichten vermeiden

Die Wirtschaft kennt bereits in anderen Bereichen Meldepflichten. Überschneidungen mit bestehenden sektoriellen Meldepflichten im Bereich Cybersicherheit sollten vermieden werden. So kennt der Finanzsektor gemäss Art. 29 Abs. 2 FINMAG bereits eine Meldepflicht von Cyber-Attacken. Entsprechend wichtig ist eine Alignierung des NCSC mit den anderen Meldeempfängern. Eine möglichst weitestgehende Standardisierung oder zumindest Interoperabilität sollte angestrebt werden. Dies betrifft auch den Inhalt der Meldung und die Meldefristen. Dies muss in der entsprechenden Verordnung festgehalten werden. Der administrative Aufwand für die Unternehmen könnte mit einem «one-stop-shop» für Meldepflichten erheblich vermindert werden. So würde eine einzige Meldung genügen, die je nach Erfüllung der relevanten Kriterien bzw. Überschreiten der relevanten Schwellen direkt von NCSC, mit dem Einverständnis des Meldepflichtigen, an weitere Meldeempfänger (z.B. FINMA) weitergeleitet würde. Aus Sicht von digitalswitzerland ist hier der Bund in der Pflicht, eine optimale Koordination sicherzustellen, damit statt der verschiedenen staatlichen Anlaufstellen und Sektorregulierungen eine einzige Ansprechstelle geschaffen wird, welche die erforderliche Koordination garantiert. Dies gilt sowohl für die Meldepflicht seitens des Unternehmens als auch für eine allfällige Reaktion seitens der Behörden. Gerade im Momenten der Bedrohung kann es nicht sein, dass Unternehmen durch unterschiedliche Meldepflichten unnötig belastet werden.

4. Gegenwert klar erkennbar machen

Damit die Meldepflicht die vorgesehene «Servicementalität» erhält, muss ihr ein klarer Mehrwert entspringen. Gemäss den Vernehmlassungsunterlagen ziehen die Betreiberinnen kritischer Infrastrukturen einen Mehrwert aus den technischen Einschätzungen und Unterstützung bei schwerwiegenden Cyber-Vorfällen. Die Meldepflicht soll eine verlässliche Einschätzung der Bedrohungslage und ein «Frühwarnsystem» darstellen. Diese Vorteile werden von digitalswitzerland begrüsst. Die Meldepflicht muss stets von diesem Service-Gedanken geprägt sein und darf nicht zu einem Kontrollinstrument gegenüber betroffenen Firmen werden. Es muss darum gehen, partnerschaftlich

Risiken zu identifizieren, diese zu kommunizieren und dadurch einen Beitrag zur besseren Cybersicherheit für alle zu leisten. Das gemeinsame Ziel und der Nutzen muss für die Unternehmen von Anfang an plastisch und konkret dargelegt werden. Nur so können sie Vertrauen in den Nutzen der Institution aufbauen. Der unmittelbare und übergeordnete Nutzen muss im Verhältnis zu den Pflichten klar ersichtlich sein – gerade für KMU und Startups ist die Verhältnismässigkeit der Massnahmen ein wichtiges Kriterium. Dieser wichtige Gegenwert wird in der Vorlage noch zu wenig ersichtlich und muss entsprechend besser dargelegt werden.

5. Keine persönliche Strafbarkeit

digitalswitzeralnd ist überzeugt, dass Cyber-Bedrohungen nur partnerschaftlich zwischen Staat und Wirtschaft effektiv eingedämmt werden können. Diesem kooperativen Geist widerlaufen Art. 74h und 74i E-ISG. Strafbestimmungen die zur persönlichen Strafbarkeit der Verantwortlichen führen können, sind gänzlich abzulehnen. Solche Bestimmungen sind für die Compliance von Unternehmen vielmehr schädlich als förderlich. Fachkräfte, die in einem inhärent fehleranfälligen Bereich wie der Cyber-Sicherheit mit Sanktionen rechnen müssen, obwohl sie alle zumutbaren Vorkehrungen getroffen haben, werden verständlicherweise zur Übernahme dieser Verantwortung weniger bereit sein. Es wird für die Unternehmen also noch schwieriger, im bereits ausgetrockneten Stellenmarkt entsprechende IT-Fachkräfte zu rekrutieren. Im schlimmsten Fall werden durch den Fokus auf die Sanktionsrisiken, die sowieso schon knappen Ressourcen noch für die Absicherung gegen Sanktionsrisiken anstelle der Cyberrisiken verwendet. Und dies in einem Bereich, in dem eigentlich gleichgerichtete Interessen bestehen.
In diesem Zusammenhang ist auch der Grundsatz des Selbstbelastungszwangsverbots bei Cyberangriffen und Cybervorfällen eminent wichtig. digitalswitzerland schlägt in diesem Zusammenhang eine Präzisierung von Art. 73c Abs. 3 vor.

Änderung Art. 73c Abs. 3 E-ISG
Informationen, die ~~von einer Person~~ dem NCSC im Rahmen einer Meldung ~~dem NCSC~~ bekanntgegeben wurden und die meldende Person selbst belasten könnten, dürfen in einem Strafverfahren gegen diese Person nur mit ~~deren~~ Einverständnis dieser Person verwendet werden.

Wir danken Ihnen für die Aufmerksamkeit, die Sie unseren Anliegen entgegenbringen und stehen für weitere Auskünfte gerne zur Verfügung.

Freundliche Grüsse

Stefan Metzger
Managing Director digitalswitzerland

Andreas W. Kaelin
Senior Advisor Cyber Security digitalswitzerland

Für weitere Auskünfte:
Andreas Kaelin, digitalswitzerland | Geschäftsstelle Bern
Tel. +41 31 311 62 45 | andreas@digitalswitzerland.com

eAHV/IV – eAVS/AI
p.a. mundi consulting ag
Marktgasse 55
Postfach
3001 Bern
Mail info@eahv-iv.ch
Web www.eahv-iv.ch
Tf. +41 31 326 76 76

Geht an
Eidgenössisches Finanzdepartement
EFD
Herr Bundesrat Ueli Maurer

Via Mail an
ncsc@gs-efd.admin.ch

Bern, 12. April 2022

Antwort zur Vernehmlassung:
Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe (Änderung des Informationssicherheitsgesetz, ISG)

Sehr geehrter Herr Bundesrat Maurer
Sehr geehrte Damen und Herren

Wir danken Ihnen bestens für die Gelegenheit, uns zum erwähnten Gesetzesentwurf zu äussern. eAHV/IV ist verantwortlich für den Datenaustausch und Digitalisierung in der 1. Säule der Sozialversicherungen und Familienzulagen. Der sichere und zuverlässige Betrieb der Infrastrukturen bei den verschiedenen beteiligten Partnern ist ein zentrales gemeinsames Anliegen. Unsere Vereinsmitglieder sind die Konferenz der kantonalen Ausgleichskassen (KKAK), die Vereinigung der Verbandsausgleichskassen (VVAK), die IV-Stellen-Konferenz (IVSK) sowie die Zentrale Ausgleichsstelle (ZAS). Die drei Vereinigungen der Durchführungsstellen unterstützen die vorliegende Vernehmlassungsantwort.

Die vertretenen rund 110 Durchführungsstellen, deren IT-Dienstleister und der Verein selbst sind potenziell von der geplanten Meldepflicht betroffen.

1. Im Grundsatz

Wir teilen die Einschätzung der grossen Wichtigkeit, die der Cybersicherheit zukommt und sind überzeugt, dass Koordinations- und Unterstützungsmassnahmen im Rahmen der Aktivitäten des Nationalen Zentrums für Cybersicherheit (NCSC) eine wichtige Ergänzung der verantwortungsvollen Planung und Durchführung von Cybersicherheitsaktivitäten in der 1. Säule der Sozialversicherungen durch unsere Mitglieder darstellt.

Die Meldepflicht, sofern die Umsetzung zweckmässig erfolgt – sehen wir als sinnvolle Massnahme, um die Information und Koordination zusätzlich zu verbessern. Wir tragen diese Grundidee ausdrücklich mit, unter der Bedingung, dass die Verpflichtung für vergleichbare Akteure gemäss der Liste in *Artikel 74b* beibehalten wird.

2. Akteure und Verantwortlichkeiten klar regeln

Der reibungslose Betrieb der ersten Säule der Sozialversicherungen hängt von unterschiedlichen Akteuren ab, die – je nach Bereich – stärker oder weniger stark miteinander kooperieren und Daten austauschen. Das angepasste Gesetz und vor allem die

nachgelagerten Bestimmungen müssen diesem Umstand Rechnung tragen und die Verantwortlichkeiten für die Meldung generisch für unterschiedliche Konstellationen festlegen. Insbesondere muss die Verpflichtung für die IT-Lieferanten der Durchführungsstellen geklärt werden, deren Situation in *Art. 72b Buchstabe s* nicht eindeutig festgeschrieben ist.

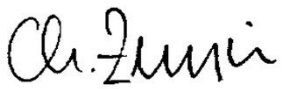
3. Aufwand für die initiale Meldung begrenzen

Die gesetzlichen Vorgaben bauen darauf auf, dass eine schnelle erste Meldung an das NCSC gemacht werden soll. Im Gesetz (*Art. 74a, 74e, 74f*) und vor allem in den nachgelagerten Bestimmungen soll spezifiziert werden, dass eine Meldung auch verschiedene betroffene Organisationen umfassen kann und dass die Meldung explizit auch durch Dritte erfolgen kann. Damit kann der dem Umstand Rechnung getragen werden, dass bereits innerhalb der 1. Säule Absprachen und Koordination im Falle eines Angriffes stattfinden. Zudem wird verhindert, dass mehrfache Meldungen erfasst werden und damit der Aufwand gesteigert wird.

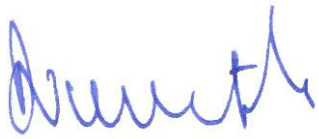
Abschliessend möchten wir nochmals betonen, dass eine zweckmässige Ausgestaltung der Meldepflicht im Sinne der Akteure der 1. Säule ist und die verbesserte Information und Koordination durch das NCSC einen Beitrag zum zuverlässigen Funktionieren der 1. Säule leisten kann.

Wir danken Ihnen für die Kenntnisnahme unserer Anregungen und bitten um deren Berücksichtigung.

Freundliche Grüsse



Christian Zeuggin
Präsident eAHV/IV



Andreas Dummermuth
Präsident Konferenz der Kantonalen Ausgleichskassen

Yvan Béguelin
Präsident der Schweizerischen Vereinigung der Verbandsausgleichskassen

Martin Schilt
Vize-Präsident der IV-Stellen-Konferenz, Leiter Ressort ICT

Eidgenössisches Finanzdepartement
Bundesgasse 3
3003 Bern

Per E-Mail an: ncsc@gs-efd.admin.ch

13. April 2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe: Stellungnahme economiesuisse

Sehr geehrter Herr Bundesrat Maurer
Sehr geehrte Damen und Herren

Mit Schreiben vom 12. Januar haben Sie uns eingeladen, zur Einführung einer Meldepflicht für Betreiberinnen kritischer Infrastrukturen für Cyber-Angriffe Stellung zu nehmen. Wir danken Ihnen für diese Möglichkeit.

Als Dachverband der Schweizer Wirtschaft bündelt economiesuisse die Interessen von rund 100'000 Unternehmen mit etwa 2 Mio. Beschäftigten im Inland und weiteren 2 Mio. Beschäftigten im Ausland. Unser Mitgliederkreis umfasst 100 Branchenverbände, 20 Handelskammern und diverse Einzelfirmen. Alle diese Mitglieder sind an einem effizienten Schutz vor Cyber-Risiken interessiert.

economiesuisse teilt die Einschätzung, dass aufgrund der rasant steigenden Zahl der Cyber-Angriffe auf Schweizer Unternehmen und Institutionen in passende Schutzmassnahmen investiert werden muss. Dies gilt im Speziellen für sog. kritische Infrastrukturen, welche aus systemischer Sicht eine erhöhte Resilienz aufweisen müssen, damit sie ihre wichtige Funktion für Wirtschaft und Gesellschaft auch angesichts eines Cybervorfalls oder -angriffs erfüllen können. Folglich bestehen gegen eine Meldepflicht für die Betreiberinnen kritischer Infrastrukturen grundsätzlich keine Einwände. Dennoch muss diese aus Sicht der Wirtschaft gewisse entscheidende Anforderungen erfüllen:

1. Es braucht frühzeitige und umfassende Klarheit darüber, «wer» «wem» «was» unter welchen Bedingungen melden muss. Besonders über das «wer» und «was» gibt die Vernehmlassungsvorlage aus Sicht der Wirtschaft nicht ausreichend Aufschluss. Die im Gesetzesentwurf erwähnten Branchen und Bereiche lassen auf einen sehr umfassenden Geltungsbereich schliessen. Eine Meldepflicht, die weite Teile der Wirtschaft betrifft und bei der viele Akteure gerade zum aktuellen Zeitpunkt der Vernehmlassung noch nicht einmal wissen, ob sie nicht auch betroffen sind, ist nicht zielführend.

2. Die Meldepflicht muss den betroffenen Unternehmen und der Volkswirtschaft letztlich mehr bringen, als sie kostet. Sie muss einen verhältnismässigen, subsidiären, risikobasierten Ansatz verfolgen, der administrative und finanzielle Aufwände auf ein Minimum reduziert. Grundsätzlich sollte

economiesuisse
Hegibachstrasse 47
Postfach
CH-8032 Zürich
Telefon +41 44 421 35 35

Verband der Schweizer Unternehmen
Fédération des entreprises suisses
Federazione delle imprese svizzere
Swiss Business Federation
www.economiesuisse.ch

sie einer «Servicementalität» entspringen und nicht einseitig als Kontrollinstrument aufgesetzt werden. Die Interessen der Behörden und der Unternehmen sind umfassend identisch. Beide wollen einen bestmöglichen Schutz vor Cyber-Angriffen. Dies darf nur ein absolutes Minimum an Zwang mit sich bringen. Betroffene Unternehmen müssen aus der Meldepflicht schliesslich einen Mehrwert erhalten, der zu einer konstruktiven Zusammenarbeit animiert und eine an sich schon unerwünschte Situation nicht noch unnötig verkompliziert.

3. economiesuisse erkennt keinen Sinn darin, die neuen Pflichten mit Strafbestimmungen durchzusetzen und lehnt diese prinzipiell ab. Gerade im vorliegenden Fall wird klar, dass diese zu Fehlanreizen führen und insbesondere die Bereitschaft der zuständigen Personen reduzieren, in Fragen der Cyber-Security Verantwortung zu übernehmen. Die im Cyber-Bereich so wichtige Fehlerkultur und der kooperative Geist der Vernehmlassungsvorlage werden durch unnötige und schädliche Sanktionen beeinträchtigt.

Aus Sicht der Wirtschaft würden solche Präzisierungen und Änderungen der Vorlage für Betreiberinnen kritischer Infrastrukturen die Rechtssicherheit stärken und wohl auch Berührungsängste mit der Meldepflicht abbauen. Sollte die Vorlage in diesen Punkten nicht nachgebessert werden, behält sich economiesuisse vor, eine ablehnende Haltung einzunehmen.

Weitere Ausführungen zu dieser Position finden Sie nachfolgend:

1 Abschliessende und klare Bezeichnung der von der Regulierung adressierten Unternehmen

Generell stellen Meldepflichten an Behörden für Unternehmen eine zusätzliche administrative Belastung dar. Diese geht auf Kosten von Investitionen und Produktivitätssteigerungen. Klare Aussagen darüber, welche Unternehmen in welchen Bereichen konkret betroffen sind, sind deshalb im vorliegenden Fall besonders wichtig. Der Gesetzesentwurf und die begleitenden Unterlagen müssen eindeutig erkennbar machen, welche Firmen wann von der Meldepflicht betroffen sind. Im Kontext der kritischen Infrastrukturen ist dies nachvollziehbarerweise schwierig, da solche Definitionen sicherheitsrelevant sind. Dennoch sind genauere Anhaltspunkte nötig. Die Liste der Bereiche, welche einer Meldepflicht unterstehen (Art. 74b E-ISG), ist zu breit gefasst. Eine Meldepflicht ist auf diejenigen Bereiche zu beschränken, deren Ausfall oder Beeinträchtigung zu nachhaltig wirkenden Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen führen würden. Der aktuelle Entwurf lässt auf eine breite und tiefe wirtschaftliche Betroffenheit der geplanten Meldepflicht schliessen, wobei sich «breit» auf die Anzahl Branchen und Unternehmen bezieht und «tief» auf die vor- und nachgelagerten Lieferketten der betroffenen Unternehmen. Insbesondere ist nicht nachvollziehbar, warum Hersteller (Art. 74b, Ziff. s E-ISG) eingebunden werden. Nicht nur nimmt dadurch die Unklarheit bezüglich Betroffenheit zu, die Hersteller passen zudem nicht in die Systematik der Betreiberinnen von kritischen Infrastrukturen, welcher das E-ISG zugrunde liegt. Sollte sich unsere Einschätzung einer derart ausgedehnten Betroffenheit in weiten Teilen der Wirtschaft bewahrheiten, ist zwingend eine Regulierungsfolgeabschätzung notwendig. Sodann wäre beispielsweise ein mehrstufiger Regulierungsansatz zu prüfen, der zuerst eine Meldepflicht für Infrastrukturen mit höchster Kritikalität vorsieht, bevor man die gesamte Wirtschaft mit neuen und vielleicht unverhältnismässigen Auflagen beschwert.

2 Abschliessende und klare Bezeichnung der zu meldenden Sachverhalte

Die vorgeschlagene Definition ist zu generisch und zu breit (Art. 5 E-ISG). Es gibt keine klare Differenzierung zwischen Vorfällen, welche keinen oder nur einen unwesentlichen Einfluss auf die Geschäftsprozesse haben und solchen, die den Betrieb kritischer Infrastrukturen grundsätzlich gefährden oder ein hohes Risiko bergen. Nach momentanem Wortlaut des Entwurfes müssten ausserdem sowohl erfolgreiche als auch nicht erfolgreiche Cyber-Angriffe dem NCSC gemeldet werden. Aufgrund der vorhandenen Informationen müssen wir davon ausgehen, dass bereits lediglich Anzeichen auf einen Angriff zur Meldepflicht führen könnten, was aus unserer Sicht über das Ziel hinausschiesst. Ausnahmen von der Meldepflicht sind nur für bestimmte Kategorien von Betreiberinnen nach Art. 74c E-ISG, nicht aber für bestimmte Arten von Angriffen geplant. Art. 74d E-ISG, welcher die zu meldenden Cyberangriffe definiert, ist deshalb zwingend zu überarbeiten. Die Kriterien sind zu weit gefasst und für die Unternehmen so kaum greif- oder umsetzbar. Zielführender wäre es eine eingeschränktere (Positiv-)Liste der zu meldenden Vorfälle zur Verfügung zu stellen und die Meldepflicht generell nur auf erfolgreiche oder besonders schwerwiegende Versuche zu begrenzen. Dass, z.B. Cyberangriffe, welche länger als 30 Tage unentdeckt blieben, gemeldet werden müssen (vor allem in Kombination mit der ebenfalls abzulehnenden Strafbarkeit) ist nicht sinnvoll und scheint auch für die Zielsetzung der Einführung einer Meldepflicht nicht relevant. Ebenso schwierig ist das Kriterium der Involvierung eines fremden Staates. Je nachdem kann ein Unternehmen dies zum Zeitpunkt der Entdeckung gar nicht wissen. Das Ziel einer Meldepflicht soll es sein, dass ein Unternehmen in bestimmten und klar definierten Fällen mit den Behörden in den Dialog tritt. In diesem Dialog können dann weitere Fragen geklärt werden, wie zum Beispiel auch der Absender. Die Anforderungen an die Meldung an sich müssen jedoch einfach gehalten werden, um die Hürden für die Unternehmen tief zu halten. Letztlich müssen auch die Grenzen der zu meldenden Sachverhalte klar abgesteckt sein, bspw. wenn sie das Anwaltsgeheimnis oder Fabrikations- und Geschäftsgeheimnisse eines Unternehmens tangieren.

3 Keinen Mehraufwand durch Überschneidungen mit anderen Meldepflichten schaffen

Als problematisch beurteilen wir darüber hinaus Überschneidungen mit anderen, sektoriellen Meldepflichten im Bereich Cyber-Sicherheit oder weiteren Bereichen. Diesbezüglich stellt der erläuternde Bericht zur Vernehmlassungsvorlage klar, dass a priori keine Synergien mit der neuen Meldepflicht genutzt werden können. economiesuisse ist derweil der Ansicht, dass einem zusätzlichen Aufwand für die Unternehmen entgegenzuwirken ist. Ein diesbezüglich prüfenswerter Ansatz könnte ein One-Stop-Shop sein. Aus Sicht der Wirtschaft ist der Bund hier in der Pflicht, eine optimale Koordination sicherzustellen. Dies gilt sowohl für die Meldepflicht seitens des Unternehmens als auch für eine allfällige Reaktion seitens der Behörden. Dabei sollte aber beachtet werden, dass, im Sinne der Datensparsamkeit, die unterschiedlichen Behörden nur die für sie relevanten Informationen erhalten, unabhängig von der Ausgestaltung der Datenablieferung.

4 Massnahmen müssen ein positives Kosten-Nutzen-Verhältnis aufweisen

Gemäss Vernehmlassungsunterlagen sollen die Betreiberinnen kritischer Infrastrukturen als Mehrwert aus der Meldepflicht technische Einschätzungen und Unterstützung bei schwerwiegenden Cyber-Vorfällen erhalten. Darüber hinaus erlaubt die Meldepflicht eine verlässlichere Einschätzung der Bedrohungslage und ein «Frühwarnsystem» aufgrund besserer Kenntnisse über Angriffsmethoden und -muster. Dies ist voll und ganz im Sinne der Wirtschaft. Eine Meldepflicht muss generell einem Service-Gedanken folgen und darf nicht als Kontrollinstrument gegenüber den betroffenen Firmen eingesetzt werden. Nur so kann das Vertrauen der Unternehmen in den Nutzen der Institution gestärkt werden. Damit die Meldepflicht akzeptiert wird, muss bereits jetzt plastisch dargelegt werden, wie diese Unterstützungsleistungen ganz konkret den betroffenen Unternehmen zugutekommen sollen. Ebenso muss klar dargelegt werden, wie weit die neuen Pflichten in einem sinnvollen Verhältnis zum Ertrag stehen, dies insbesondere bei KMU und kleineren Betreiberinnen kritischer Infrastrukturen, bei denen der Zusatzaufwand stärker ins Gewicht fällt. Eine Meldepflicht «als Selbstzweck» einzuführen, um

Handlungsbereitschaft in einem die Unternehmen stark belastenden Bereich zu markieren, ist nicht akzeptabel. Es braucht einen klaren Gegenwert, der sich aktuell aus der Vorlage noch zu wenig erschliesst.

5 Fehlanreize vermeiden

Insgesamt lässt die Stossrichtung der Vernehmlassungsvorlage auf eine partnerschaftliche Grundhaltung hinter den vorgeschlagenen Massnahmen schliessen. Dies ist für die Wirtschaft entscheidend und muss entsprechen konsequenter herausgearbeitet werden. Nur gemeinsam und im Sinne einer Partnerschaft zwischen der Wirtschaft und dem Staat lassen sich Cyber-Bedrohungen eindämmen. Ein wesentlicher Punkt im Vorentwurf sind daher die Strafbestimmungen in Art. 74h und 74i E-ISG. Diese lehnen wir gänzlich ab. Solche Bestimmungen, die zur persönlichen Strafbarkeit der Verantwortlichen führen, sind für die Compliance von Unternehmen eher schädlich als förderlich. Personen, die in einem inhärent fehleranfälligen Bereich wie der Cyber-Sicherheit mit Sanktionen rechnen müssen, obwohl sie alle zumutbaren Vorkehrungen getroffen haben, werden klar weniger zur Übernahme dieser Verantwortung bereit sein. Dadurch wird ein Stellenmarkt, der bereits heute ausgetrocknet ist und nicht ausreichend Experten und Fachkräfte anbietet, noch weiter unter Druck gesetzt. Durch den unnötigen Fokus auf Strafbestimmungen in einem Themenfeld, bei dem gleichgerichtete Interessen bestehen und es keinerlei Sanktionsgründe gibt, wird darüber hinaus noch die Gefahr geschaffen, dass knappe Ressourcen in die Absicherung gegen die Sanktionsrisiken anstelle der Cyber-Risken fliessen.

Wir danken Ihnen vielmals für die Berücksichtigung unserer Argumente. Ergänzend unterstützten wir die Stellungnahmen unserer Mitglieder (unter anderem von scienceindustries, SwissBanking, Schweizerischer Versicherungsverband und Swissmem) und stehen für eine Zusammenarbeit im Sinne eines Austausches zum Gesetzesentwurf sowie für Fragen gerne zur Verfügung.

Freundliche Grüsse
economiesuisse

Erich Herzog
Leiter Wettbewerb & Regulatorisches
Mitglied der Geschäftsleitung

Lukas Federer
Projektleiter Infrastruktur, Energie & Umwelt

eGov schweiz
innovation and network

Eidgenössisches Finanzdepartement

3003 Bern

Per Mail an ncsc@gs-efd.admin.ch

Bern, 5. April 2022

Antwort auf die Vernehmlassung Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe (Änderung des Informationssicherheitsgesetz ISG)

Sehr geehrte Damen und Herren

Wir bedanken uns für die Gelegenheit, uns zum erwähnten Gesetzesentwurf zu äussern und nehmen diese gerne wahr. Der Verein eGov-Schweiz bezweckt die Förderung der Innovation im eGovernment. Die Sicherheit und der kontinuierliche Betrieb behördlicher Angebote ist in dieser Perspektive von besonderem Interesse für unseren Verein.

Wir begrüssen die vorgesehene Schaffung einer Meldepflicht für Cybervorfälle für einen klar definierten Kreis von Betreiberinnen kritischer Infrastrukturen. Die Liste der betroffenen Organisationen unter Art. 74b erscheint uns als sinnvoll, die Ausnahmeregelung unter Art. 74c ist mit der Berücksichtigung des Schadensausmasses zweckmässig und stellt sicher, dass elektronische Angebote nicht generell mit höheren Anforderungen belastet werden.

Die unter Art. 74d aufgeführten Kriterien für die Meldung von Vorfällen erscheinen uns als zu wenig eindeutig. Eine konsistentere Herleitung würde die Anwendung erleichtern, klärende Verordnungsbestimmungen sind zwingend.

Aus der Perspektive unserer Mitglieder wünschen wir uns zudem, dass die Informationen der Nationalen Zentrums für Cybersicherheit NCSC auch in umfassender Art und Weise an die Betreiberinnen zurückfliessen und auch die Lieferanten Teil des Informationsaustausches sind. Eine entsprechende Grundlage in Art. 74 würden wir begrüssen. Mit der geeigneten Aufbereitung der Informationen kann eine Verbesserung der Cybersicherheit bei allen Akteuren erreicht werden.

Kritisch bewerten wir die Kompetenzen zur Bearbeitung von besonderes schützenswerten Personendaten durch das NCSC gemäss Art. 75, insbesondere in der Verbindung mit den Möglichkeiten der Weitergabe im In- und Ausland gemäss Art. 76 und Art. 77. Wir gehen davon aus, dass bei Bedarf polizeiliche und geheimdienstliche Unterstützung herzbeigezogen werden kann und nicht die eigene Bearbeitung durch das NCSC abgestrebt wird.

Insgesamt sind wir davon überzeugt, dass mit der Schaffung der Meldepflicht im Rahmen der vorgeschlagenen Gesetzesänderung eine Verbesserung der Cybersicherheit in der Schweiz erreicht werden kann.

Freundliche Grüsse

eGov-Schweiz

Renato Gunc

Präsident

Christoph Beer

Geschäftsführer

Fédération des
Entreprises
Romandes

FER Genève - FPE Bulle - UPCF Fribourg
FER Arcju - FER Neuchâtel - FER Valais

Monsieur Ueli Maurer,
Conseiller fédéral

ncsc@gs-efd.admin.ch

Département fédéral des finances (DFF)
3003 Berne

Genève, le 13 avril 2022
DZ/3489 – FER No 13-2022

Introduction d'une obligation de signaler les cyberattaques contre des infrastructures critiques

Monsieur le Conseiller fédéral,

La FER a pris connaissance avec intérêt du projet mis en consultation par vos services et vous prie de trouver ci-après sa prise de position y relative.

Notre Fédération salue les modifications proposées en vue de l'introduction d'une obligation de signaler les cyberattaques contre les infrastructures critiques. L'attractivité de la place économique suisse se mesure en effet à l'aune de nombreux facteurs parmi lesquels figure le niveau de sécurité informatique des infrastructures critiques.

Il convient effectivement d'adresser et traiter les enjeux nés des évolutions des usages numériques et des menaces qui y sont liées. Le renforcement de la sécurité numérique fait bien entendu partie des missions qu'un Etat se doit d'assumer, au même titre que la sécurité des personnes et des biens, menacés parfois eux-mêmes lors d'une cyberattaque. Ainsi est-il indispensable que la Suisse se dote d'une stratégie et de moyens techniques propres à faire face efficacement à la cybercriminalité, non seulement en termes d'information, de prévention, mais aussi d'assistance technique à la résolution des cyberattaques.

L'actualité récente nous a démontré que les cyberattaques visent non seulement des entreprises privées, de toutes tailles, mais aussi des établissements publics, tels que l'université de Neuchâtel, ou des organisations non gouvernementales, tels que le CICR. Les Etats sont aussi directement visés par des hackers au service d'Etats étrangers.

Le maintien de la compétitivité suisse dépend d'une politique en matière de cybersécurité performante et ambitieuse assurant une protection de haut niveau aux organismes implantés sur le territoire. En effet, la sécurité informatique constitue un réel avantage concurrentiel pour les entreprises implantées sur notre sol.

Dès lors, notre Fédération soutient les mesures préventives et informatives, qui s'ajoutent à l'obligation de signalement, afin d'intervenir en amont d'une éventuelle attaque, et plaide en faveur d'une action technique de soutien aux services attaqués.

Nous vous prions de croire, Monsieur le Conseiller fédéral, à l'assurance de notre parfaite considération.

Blaise Matthey
Secrétaire général

Raoul Diez
Directeur Contrôle et Sécurité
FER Genève

La Fédération des Entreprises Romandes en bref
Fondée le 30 juillet 1947 à Morat, son siège est à Genève. Elle réunit six associations patronales interprofessionnelles cantonales (GE, FR, NE, JU, VS), représentant la quasi-totalité des cantons romands. La FER comprend plus de 45'000 membres.

Groupement des
Entreprises
Multinationales

Rue de Saint-Jean 98
Case postale - 1211 Genève 3
T : 058 715 32 99
info@gemonline.ch
www.gemonline.ch

Monsieur le Conseiller fédéral
Ueli Maurer
Chef du Département des finances
3003 Berne

Par courriel : ncsc@gs-efd.admin.ch

Genève, le 13 avril 2022/RN

Procédure de consultation : obligation de signaler les cyberattaques contre des infrastructures critiques

Monsieur le Conseiller fédéral,

Le GEM a pour objectif de représenter et de défendre les intérêts communs de ses membres auprès des autorités et du public en général. Les 100 sociétés membres qui composent notre groupement sont des entreprises multinationales, d'origine suisse et étrangère, de toute taille, dont les sièges sont situés en Suisse romande, principalement dans les cantons de Genève, Vaud et Fribourg. Notre groupement représente près de 90'000 emplois directs et indirects, dont 35'000 emplois directs dans cette région. Le GEM s'investit pour garantir des conditions cadres propices à la compétitivité et à l'attractivité économique de la Suisse.

Le GEM a pris connaissance avec intérêt du projet mis en consultation par vos services et vous prie de trouver ci-après sa prise de position y relative.

Notre Groupement salue les modifications proposées qui prévoient d'introduire une obligation de signaler les cyberattaques contre les infrastructures critiques. L'attractivité de la place économique suisse se mesure en effet à l'aune de nombreux facteurs parmi lesquels figure le niveau de sécurité informatique des infrastructures critiques.

Les enjeux nés des évolutions des usages numériques et des menaces qui y sont liées doivent être adressés et traités. Le renforcement de la sécurité numérique fait en effet partie des missions qu'un Etat se doit d'assumer, au même titre que la sécurité des personnes et des biens, lesquels sont d'ailleurs parfois menacés lors d'une cyberattaque. Pour ce faire, il est indispensable que la Suisse se dote d'une stratégie et de moyens techniques propres à faire face efficacement à la cybercriminalité, non seulement en termes d'information, de prévention, mais aussi d'assistance technique à la résolution des cyberattaques.

L'actualité récente nous a en effet démontré que les cyberattaques visent non seulement des entreprises privées, de toutes tailles, mais aussi des établissements publics (telle que l'université de Neuchâtel), ou des organisations non gouvernementales (telle que le CICR). Les Etats sont aussi directement visés par des hackers au service d'Etats étrangers.

La sécurité informatique est un avantage concurrentiel pour les entreprises implantées sur notre sol. Le maintien de la compétitivité suisse dépend d'une politique en matière de cybersécurité efficace et ambitieuse assurant une protection de hauts niveaux aux organismes implantés sur le territoire.

Notre groupement soutient donc les mesures de prévention et d'information, en sus de l'obligation de signalement, afin d'intervenir en amont d'une éventuelle attaque, et plaide en faveur d'une action technique de soutien aux organismes attaqués.

Nous vous prions de croire, Monsieur le Conseiller fédéral, à l'assurance de notre parfaite considération.

Olivier Straub
Vice-Président du GEM

Larissa Robinson
Secrétaire Générale

Per Mail (PDF / Word) an:
ncsc@gs-efd.admin.ch
Eidgenössisches Finanzdepartement
3003 Bern

Bern, 14. April 2022

Stellungnahme der IG eHealth: Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrte Damen und Herren

Die IG eHealth nimmt gerne die Möglichkeit wahr, im Rahmen der Vernehmlassung zur Meldepflicht für Cyberangriffe für Betreiberinnen von kritischen Infrastrukturen (Revision Informationssicherheits-gesetz) Stellung zu beziehen.

Cyberattacken und Sicherheitsprobleme haben in der Vergangenheit zugenommen, z.B. bei meineimpfungen.ch, beim Transplantationsregister oder bei Primärsoftware im Kanton Neuenburg. Auch Lösegeldforderungen treten vermehrt auf. Der Handlungsbedarf ist also unbestritten.

Einleitende Bemerkungen

Im Grundsatz begrüsst die IG eHealth die Ergänzungen des Bundesgesetzes über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG). Namentlich die Verpflichtung wesentlicher Bereiche des Gesundheitswesens erachten wir als wichtig und richtig. Gemäss Art. 74b werden Spitäler, medizinische Laboratorien, Zulassungsinhaberinnen von Arzneimitteln oder Medizinprodukten und die Sozialversicherungen meldepflichtig. **Wir bitten das EFD/NSCS die Frage zu prüfen, weshalb Geburtshäuser und ambulante Anbieter wie Gruppenpraxen von Ärztinnen und Ärzten, Spitex-Organisationen oder Apotheken-Ketten und -Gruppierungen von der Meldepflicht ausgenommen sind?**

Konkrete Punkte

Aus Sicht der IG eHealth braucht es im Gesetz folgende Präzisierungen

Art. 5 Bst. d–e ISG Begriffe

Im Artikel werden die Begriffe Cybervorfall und Cyberangriff definiert. Im Gesetz wird verschiedentlich von Schwachstellen gesprochen, z.B. im Art. 73a Grundsatz.

⇒ Die Begriffe Cybervorfall, Cyberrisiko und Schwachstelle sind im Gesetz zentral, die Abgrenzung sollte präziser festgelegt werden. Wir bitten das EFD, den Begriff der Schwachstelle ebenfalls zu definieren und sich dabei an internationale Begrifflichkeiten zu halten (z.B. Common Vulnerabilities Scoring System CVSS).

Art. 73b Abs. 2 ISG Bearbeitung von Meldungen von Cybervorfällen und Schwachstellen

Die Veröffentlichung und Weiterleitung von Informationen zu Cybervorfällen können gegen Geschäftsinteressen verstossen. Die Frage, ob durch die Veröffentlichung und Weiterleitung Cyberangriffe verhindert oder bekämpft werden können, kann allenfalls erst nachträglich beurteilt werden.

⇒ Die IG eHealth schlägt zwei Punkte vor:

- es braucht im ISG einen Öffentlichkeitsvorbehalt, falls Geschäftsinteressen der Organisation / Firma betroffen sind, die den Mitbewerbern zu Vorteilen verhelfen oder zu einer Umsatzeinbusse führen könnten.
- Im ISG ist festzuhalten, dass die Meldung von Cybervorfällen, Cyberrisiken und Schwachstellen vom Geltungsbereich des Öffentlichkeitsgesetz BGÖ ausgenommen sind.

Art. 74d ISG Zu meldende Cyberangriffe

Ein Cyberangriff muss gemäss dem Gesetz immer gemeldet werden, wenn die Punkte a bis d erfüllt werden. Punkt b, wonach ein fremder Staat den Cyberangriff ausgeführt oder veranlasst hat, erachten wir als eher theoretischer Natur. Vielfach dürfte nicht ersichtlich sein, wer hinter dem Cyberangriff steht.

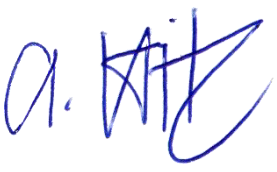
⇒ Die IG eHealth schlägt vor, Punkt d (Cyberangriff bleibt länger als 30 Tage unentdeckt) keiner Meldepflicht zu unterstellen, wenn die Punkte a (Funktionsfähigkeit gefährdet) und c (möglicher Abfluss oder zur Manipulation von Informationen) nicht erfüllt sind, d.h. der Angriff eine Bagatelle war oder einen tiefen bis mittleren Schweregrad aufwies.

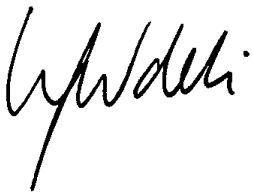
Schlussbemerkungen

Die Vorgaben auf Gesetzesstufe sind genereller Natur. Bei der Ausarbeitung der Verordnungen ist es zentral, die betroffenen Akteure frühzeitig einzubinden. So sind der Meldeprozess und der Gegenstand und der Umfang einer Meldung klar zu definieren.

Der Bundesrat und das Parlament müssen sicherstellen, dass das Nationale Zentrum für Cybersicherheit NCSC genügend Personalressourcen erhält, um die vielfältigen Aufgaben bewältigen zu können. Ressourcen sind namentlich auch für die Unterstützung des NCSC bei Cybervorfällen und Schwachstellen vorzusehen, die im Art. 74 Abs. 3 ISG festgehalten ist. Wichtig ist auch, dass die Daten an die Behörden nur einmal erfasst und gemeldet werden müssen (Umsetzung Once-Only-Prinzip).

Besten Dank für die Kenntnisnahme und freundliche Grüsse





Anna Hitz
Präsidentin IG eHealth

Walter Stüdeli
Geschäftsführer IG eHealth

Die IG eHealth ist der einzige Fachverband mit Expertise in den Bereichen Gesundheitspolitik, Organisation, ICT, Semantik und Technik.

Sie unterstützt die digitale Transformation im Gesundheitswesen in der Schweiz proaktiv, damit Qualitäts- und Sicherheitslücken in der Behandlung abgebaut und administrative Prozesse verbessert werden.

inter pension
Interessengemeinschaft autonomer
Sammel- und Gemeinschaftseinrichtungen

NCSC
Nationales Zentrum für Cybersicherheit

Versand per E-Mail an:
ncsc@gs-efd.admin.ch

Ittigen, 14. April 2022

Vernehmlassung zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrter Herr Bundesrat, sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit zur Stellungnahme im Rahmen der Vernehmlassung zur Änderung des Informationssicherheitsgesetzes (ISG) betreffend Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe. Der Vorstand von inter-pension nimmt dazu gerne wie folgt Stellung:

1. Allgemeine Bemerkungen

Wir unterstützen grundsätzlich die Einführung der neuen Meldepflicht – auch für die Pensionskassen (Vorsorgeeinrichtungen). Unseres Erachtens überwiegen die Vorteile (Gleichbehandlung und Unterstützung der Betreiber*innen kritischer Infrastrukturen durch das NCSC) die administrativen Mehraufwände. Wir erachten es aber als wichtig, dass – wie in der Vorlage erwähnt – das neue Meldeverfahren möglichst *administrativ einfach und schlank* gehalten werden wird.

2. Bemerkungen zu Art. 74b Bst. j ISG

Diese Bestimmung soll die Rechtsgrundlage darstellen für die Einrichtungen der beruflichen Vorsorge. Im Gesetzestext ist von «Organisationen, die Leistungen der Sozialversicherungen [...] erbringen» die Rede. Im Erläuterungsbericht verweisen Sie auf das ATSG und bemerken, dass auch *nicht-registrierte Vorsorgeeinrichtungen* bzw. *überobligatorische Leistungen* der beruflichen Vorsorge von der Meldepflicht erfasst sein sollen. Inhaltlich stimmen wir mit dieser Zielsetzung überein, jedoch erachten wir den Gesetzestext diesbezüglich zu wenig präzise. Weder ist der Begriff «Sozialversicherungen» in der beruflichen Vorsorge klar definiert, noch werden die überobligatorischen Leistungen vom ATSG erfasst. Auch stellt sich z.B. die Frage, ob Anlagestiftungen, die bekanntlich nicht unter der FINMA-Aufsicht stehen, sondern von der Oberaufsichtskommission berufliche Vorsorge (OAK BV) beaufsichtigt werden, von der Meldepflicht

betroffen sind. Wir bitten Sie um entsprechende Präzisierung, gegebenenfalls dann auf Verordnungsstufe.

Wir danken Ihnen für die Beachtung unserer obigen Bemerkungen. Gerne stehen wir für die Beantwortung weiterer Fragen zu Ihrer Verfügung.

Freundliche Grüsse

inter-pension

Sergio Bortolin
Präsident

Therese Vogt
Geschäftsstelle

/SSS information security society switzerland

Kochergasse 6
3011 Bern
sekretariat@isss.ch
+41 31 311 53 00

Generalsekretariat des Eidgenössischen
Finanzdepartements
Nationales Zentrum für Cybersicherheit (NCSC)
3003 Bern

Per E-Mail an: ncsc@gs-efd-admin.ch

BETREFF

Stellungnahme zum Entwurf des Bundesgesetzes über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG)

DATUM

14. April 2022

Sehr geehrter Herr Bundesrat Maurer,
sehr geehrte Damen und Herren,

Wir bedanken uns für die Möglichkeit zum rubrizierten Geschäft Stellung zu beziehen und nehmen diese gerne fristgerecht wahr.

Die Information Security Society Switzerland ISSS setzt sich in Theorie und Praxis mit der Sicherheit der Verarbeitung, Speicherung und Kommunikation von Information auseinander und beleuchtet die technischen, wirtschaftlichen, regulatorischen und gesellschaftspolitischen Aspekte der Informationssicherheit. ISSS setzt sich insbesondere konsequent für den Informationsaustausch von Information Security Professionals untereinander und mit Security Interessierten, das frühzeitige Erkennen von sicherheitsrelevanten Entwicklungen des Informationsmanagements, die nachhaltige Berücksichtigung der Sicherheitsaspekte bei bestehenden und zukünftigen Architekturen, Konzepten und Systemen und den bedarfsgerechten und ausgewogenen Auf- und Ausbau von Sicherheitsinfrastrukturen aufgrund aktueller Ereignisse und Trends ein.

ISSS unterstützt das Ziel, die Resilienz der Schweiz gegenüber Cyberrisiken zu erhöhen, anerkennt den Bedarf verschiedener Behörden an, Zugriff auf einen grössen Pool von Informationen zu erlangen und begrüsst im Grundsatz die vorgeschlagenen Anpassungen des ISG.

ISSS regt allerdings an, dass den Abgleich der Meldung mit anderen Meldeprozessen z.B. mit dem EDÖB (nach Art. 24 revDSG), dem BAKOM (Art. 48a FMG) oder der FINMA zu verbessern und detaillierter auszuarbeiten. Insbesondere, wenn man eine zentrale Meldestelle schaffen würde, aber auch nur schon auf Grundlage des vorliegenden Entwurfes, fehlt Klarheit darüber, an wen welche Information weitergegeben werden (dürfen) und mit welchem Inhalt. So ist z.B. nicht klar, ob Meldungen an das NCSC, die an den EDÖB weitergeleitet werden, ebenfalls unter dem Vorbehalt der Nichtbelastung im Strafverfahren nach Art. 24 Abs. 6 revDSG fallen würden oder nicht. Da gemäss Art. 74g E-ISG der NCSC weitere Auskünfte verlangen kann, erweitert dies sodann den Umfang der Kommunikation gegenüber

Dritten. Eine solche, oft auch sehr informelle Kommunikation auf technischer Ebene, soll nicht Gegenstand eines Strafverfahrens nach dem neuen Datenschutzgesetz werden können, wenn denn Personendaten involviert sind. Es braucht folglich eine detailliertere Regelung, mit wem welche Informationen geteilt werden können und welche Konsequenzen dies haben kann oder eben nicht hat.

Ausserdem ist die Meldepflicht von kritischen Infrastrukturbetreibern einseitig ausgestaltet. Es fehlt eine Informationspflicht des NCSC an kritische Infrastrukturbetreiber oder gar an die Allgemeinheit betreffend konkreten Cybervorfällen, - angriffen sowie Schwachstellen. Es wäre hilfreich, wenn NCSC auch eine anonymisierte Rückmeldung geben würde über die erlangten Erkenntnisse. Ausserdem könnte auch eine Informationspflicht des NSCS für betroffene Personen etabliert werden z.B. durch Eingabe von Benutzerkennung / E-Mail / oder andere Detection-Codes.

Im Detail schlagen wir die nachfolgenden Änderungen bzw. Ergänzungen vor:

1. Informationsschutzgesetz (ISG)

Art. 1 - Ergänzung

[1] Dieses Gesetz soll:

a. die sichere Bearbeitung der Informationen, für die der Bund zuständig ist, sowie den sicheren Einsatz der Informatikmittel des Bundes gewährleisten, es sei denn eine Spezialgesetzgebung sehe eine gesonderte Zuständigkeit vor;

Begründung

Es sollte explizit erwähnt werden, dass eventuelle Spezialgesetzgebungen vorgehen können.

Art. 2 – Präzisierung

[5] Für Organisationen des öffentlichen und privaten Rechts, die kritische Infrastrukturen gemäss Artikel 74b betreiben, die aber nicht unter die Absätze 1–3 fallen, gelten die Artikel 73a–79. Die Spezialgesetzgebung kann weitere Teile dieses Gesetzes für anwendbar erklären.

Begründung

Es sollte klar sein, dass man die kritischen Infrastrukturen gemäss der Definition im ISG meint.

Art. 5 Bst. f-g - Ergänzung

Hinzufügen von lit. f mit der Definition von Cyberrisiko.

Hinzufügen von lit. g mit der Definition von Schwachstellen von Informatikmitteln

Begründung

Beide Begrifflichkeiten werden in Art. 73a ff. ISG erwähnt, jedoch erscheint deren Unterscheidung nicht geläufig. Deren Abgrenzung ist für die Erfüllung der Meldepflicht jedoch von grosser Bedeutung, weswegen wir empfehlen, die beiden Begriffe in Art. 5 ISG zu definieren.

Zudem sollten Begrifflichkeiten gesetzesübergreifend definiert und mit dem revDSG abgeglichen werden. Art. 5 Abs. 1 lit. h. revDSG spricht von Verletzung der Datensicherheit. Eine Verletzung der Datensicherheit liegt vor, wenn eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden.

Art. 73a Grundsatz Ergänzung

f. Subsidiäre Unterstützung von Betreiberinnen von kritischen Infrastrukturen.

Begründung

Da die Subsidiarität auch im erläuternder Bericht aufgewiesen wird, sollte diese auch im Gesetzestext statuiert werden. Das NCSC soll nur unterstützen, wenn die freie Wirtschaft dazu nicht in der Lage ist, weil es sich z.B. um einen Fall nationaler Bedeutung handelt.

Art. 73b Bearbeitung von Meldungen zu Cybervorfällen und Schwachstellen - Ergänzung

[2] Das NCSC kann Informationen zu Cybervorfällen veröffentlichen oder an interessierte Behörden und Organisationen weiterleiten, sofern der Geheimhaltungs- und Datenschutz sichergestellt ist und sofern dies dazu dient, Cyberangriffe zu verhindern oder zu bekämpfen. Diese Informationen dürfen Personendaten und Daten juristischer Personen enthalten, sofern es sich um missbräuchlich verwendete Identifikationsmerkmale und Adressierungselemente handelt und die betroffene Person einwilligt. Gleiches gilt für Immaterialgüterrechte im weitesten Sinne.

[3] Werden dem NCSC Schwachstellen gemeldet, so informiert es umgehend den Hersteller und setzt ihm zur Behebung der Schwachstelle eine angemessene Frist. Behebt der Hersteller die Schwachstelle nicht innert dieser Frist, so veröffentlicht das NCSC die Schwachstelle unter Angabe der betroffenen Soft- oder Hardware und des Herstellers, sofern dies zum Schutz vor Cyberrisiken beiträgt. Diese Meldungen werden vom Öffentlichkeitsprinzip ausgeschlossen.

Begründung

Betr. Abs. 1: Es muss präziser geregelt werden, welche Schwachstellen vom NCSC den Herstellern gemeldet werden müssen. Auch sollte aufgezeigt werden, ob diese Meldung lediglich optional erfolgen kann. Ebenfalls muss diese Meldung mit anderen Meldungen koordiniert werden, sodass Doppelspurigkeiten vermieden werden.

Betr. Abs. 2: Da die Bekanntgabe von Cybervorfällen negative Konsequenzen für die Reputation des angegriffenen Unternehmens nach sich ziehen kann, sollte präziser geregelt werden, unter welchen Umständen der Cybervorfall unter Nennung welcher Angaben veröffentlicht werden soll. Idealerweise ist mit dem betroffenen Unternehmen die Kommunikation sogar abzustimmen. Zudem muss der Daten- und Geheimhaltungsschutz von vertraulichen Informationen gewährleistet sein, es sei denn die betroffene Person hat zugestimmt Wenn eine Kommunikation eine Firma, Marke oder dergleichen einer Firma beinhaltet, so gilt die Zustimmung auch für diese Immaterialgüterrechte.

Betr. Abs. 3: Da auch der erläuternde Bericht die Angabe des Herstellers erwähnt, empfehlen wir auch eine explizite Nennung des Herstellers im Gesetzestext.

Art. 74 Unterstützung von Betreiberinnen von kritischer Infrastruktur -Ergänzung

[2] Es stellt ihnen dazu insbesondere folgende Hilfsmittel zur Verfügung:

a. ein Kommunikationssystem für den sicheren Informationsaustausch sowie eine sichere Datenablage;

[3] Es berät und unterstützt sie bei der Bewältigung von Cybervorfällen und der Behebung von Schwachstellen in subsidiärer Weise zu IT-Dienstleistungen, die auf dem Markt erhältlich sind, wenn für die kritische Infrastruktur ein unmittelbares Risiko von gravierenden Auswirkungen besteht und, sofern es sich um private Betreiberinnen handelt, die Beschaffung gleichwertiger Unterstützung auf dem Markt nicht rechtzeitig möglich ist.

[4] Es kann zur Analyse eines Cybervorfalls mit dem Einverständnis der betroffenen Betreiberin auf deren Informationen und Informatikmittel zugreifen. Der Zugriff kann gewährt werden ohne allfällige Geheimhaltungspflichten zu verletzen.

Begründung

Betr. lit. a: Es sollte explizit auch erwähnt werden, dass der NCSC eine sichere Datenablage gewährleistet.

Betr. lit. c: Was ist unter technischen Hilfsmittel zu verstehen?

Betr. Abs. 2: Da die Subsidiarität auch im erläuternder Bericht aufgewiesen wird, sollte diese auch im Gesetzestext statuiert werden.

Art. 74a Meldepflicht - Präsizierung

Die Betreiberinnen von kritischen Infrastrukturen müssen dem NCSC Cyberangriffe und -vorfälle nach deren Entdeckung so rasch als möglich melden, damit das NCSC Angriffsmuster frühzeitig erkennen, mögliche Betroffene warnen und ihnen geeignete Präventions- und Abwehrmassnahmen empfehlen kann.

Begründung

Bereits Cybervorfälle sollen gemeldet werden. Auch Schwachstellen sollte man freiwillig melden können, damit das NCSC Hersteller darauf hinweisen kann.

Art. 74b Bereiche - Ergänzung

r. Unternehmen, die die Bevölkerung mit unentbehrlichen Gütern des täglichen Bedarfs versorgen. Der Bundesrat bezeichnet die betroffenen Unternehmen.

Oder alternativ ganz streichen und eine gesetzliche Grundlage schaffen, um dies auf Verordnungsstufe zu definieren.

Begründung

Da der erläuternde Bericht die Präzisierung durch den Bundesrat auf dem Verordnungsweg explizit erwähnt, sollte dies auch im Gesetzestext aufgenommen werden. Es fragt sich, ob nicht die gesamte Definition der Kritischen Infrastrukturbetreiber durch den Bundesrat erfolgen soll.

Art. 74d Zu meldende Cyberangriffe – und Vorfälle– Ergänzung und Löschung

[1] Ein Cyberangriff oder ein Cybervorfall auf eine kritische Infrastruktur muss gemeldet werden, wenn die ernsten Befürchtungen bestehen, dass:

Streichung von lit. b.

Begründung

Die Ausführungen in lit. a-d verdeutlichen, dass Bagatellfälle nicht gemeldet werden sollen, sondern lediglich, wenn der Cyberangriff weitgehende Konsequenzen beinhalten kann und somit schweizweit zum Tragen kommt. Dass bereits Anzeichen der Meldepflicht gemäss Art. 74d unterliegen, widerspricht demnach der ratio legis. Lit. b ist zu streichen, da in der Regel oft nicht belegt werden kann, dass ein fremder Staat einen Cyberangriff tätigt. Lit. d ist auch zu streichen.

Art. 74e Inhalt der Meldung – Ergänzung + Bemerkung

[1] Die Meldung muss Informationen zur kritischen Infrastruktur, zur Art und Ausführung des Cyberangriffs, des Cybervorfalles, zu seinen Auswirkungen und zum geplanten weiteren Vorgehen der Betreiberin der kritischen Infrastruktur enthalten.

Begründung

Der Inhalt der Meldung sollte präziser formuliert werden, auch im Hinblick auf die Gefahr von Bussgeldern. Vorstellbar wäre die Präzisierung auch auf Stufe der Verordnung vorzunehmen.

Auch sollte der Inhalt der Meldung mit anderen Meldungspflichten an anderen Behörden abgestimmt werden, um Doppelspurigkeiten zu vermeiden.

Art. 74f Übermittlung der Meldung – Bemerkung + Streichung

[1] Für die elektronische Meldung von Cyberangriffen stellt das NCSC ein sicheres System zur Übermittlung der Meldung an das NCSC zur Verfügung.

[2] Das System muss der Betreiberin einer kritischen Infrastruktur ermöglichen, die Meldung des Cyberangriffs oder seiner Auswirkungen gesamthaft oder in Teilen an weitere Stellen und Behörden zu übermitteln.

Neuer Vorschlag

Abs. 3 ist zu streichen.

Begründung

Es kann nicht angehen, dass hier Meldungen an das NCSC und an die Datenschutzbehörde, BAKOM oder FINMA vermischt wird. Es ist sicherzustellen, dass andere «Stelle» und Behörden, nur den

Umfang an Information erhalten, zu dem sie gesetzlich berechtigt sind oder im Rahmen des Zweckes der zugrundeliegenden Gesetzgebung eine Rechtfertigung besteht.

Abs. 3 ist zu streichen oder sonst ist eine klare Governance-Regelung aufzunehmen, welche es der betroffenen Infrastruktur ermöglicht zu erkennen, an welche andere(n) Behörde, Stelle oder Dritten die Informationen über ihren Cybervorfall oder -angriff mitgeteilt wurden. Das Transparenzgebot staatlichen Handelns gebietet dies.

Art. 74g Auskunftspflicht - Ergänzung

Es ist festzulegen, wie weit eine Auskunftspflicht gehen kann.

Begründung

Mit der Meldung sollte die Pflicht der kritischen Infrastrukturanbieter erfüllt sein. U.U. müsste man sich überlegen, ob man die Meldepflicht detaillierter in einer Verordnung fasst. Ausserdem ist mit der Erteilung der ergänzenden Auskünfte die Meldepflicht erfüllt. Auch die ergänzenden Auskünfte dürfen nicht zu einer Belastung in einem Strafverfahren führen und sie können nicht endlos sein.

Art. 74i Widerhandlungen gegen Verfügungen des NCSC

Neuer Vorschlag

Komplett streichen

Begründung

Die Verletzung der Meldepflicht wie auch die nachträgliche Auskunft soll nicht unter Strafe gestellt werden. Dies ist kontraproduktiv und verhindert freiwillige Meldungen, die über die reine Pflicht hinausgehen.

4. Abschnitt: Datenschutz und Informationsaustausch

Art. 76 Zusammenarbeit im Inland

[2] Die Betreiberinnen von kritischen Infrastrukturen können dem NCSC Personendaten bekanntgeben, sofern dies zum Schutz ihrer kritischen Infrastrukturen vor Cyberrisiken erforderlich ist.

[3] Das NCSC kann den Fernmeldedienstanbieterinnen, die nicht kritische Infrastrukturanbieterinnen sind, Adressierungselemente und damit zusammenhängende Personendaten bekanntgeben, sofern dies zum Schutz von kritischen Infrastrukturen vor Cyberrisiken erforderlich ist.

[4] Die Fernmeldedienstanbieterinnen, die nicht kritische Infrastrukturanbieterinnen sind, können dem NCSC Adressierungselemente und damit zusammenhängende Personendaten bekanntgeben, sofern dies zum Schutz von kritischen Infrastrukturen vor Cyberrisiken erforderlich ist.

Begründung

Personendaten von kritischen Infrastrukturbetreiberinnen sollte nicht ins Ausland bekannt gegeben werden. Darüber hinaus sind in Abs. 3 und 4 wohl nur die Fernmeldedienstanbieterinnen gemeint, sofern sie nicht bereits unter kritische Infrastrukturanbieterin erfasst sind.

Art. 77 Internationale Zusammenarbeit

[1]Das NCSC kann mit ausländischen und internationalen Stellen, die für die Cybersicherheit zuständig sind, Informationen austauschen, wenn sie diese zur Erfüllung von Aufgaben benötigen, die denjenigen des NCSC entsprechen. Umfasst der Informationsaustausch auch Personendaten nach Artikel 75, ist Artikel 6 und Art. 10a DSG zu beachten.

[2] Der Informationsaustausch nach Absatz 1 ist nur dann zulässig, wenn die ausländischen und internationalen Stellen die bestimmungsgemässe datenschutzkonforme Verwendung gewährleisten.

Begründung

Der Transfer von Personendaten hat sich an die allgemeinen datenschutzrechtlichen Grundsätze zu halten, insbesondere auch Art. 10a DSG.

Art. 79 Abs. 1

[1] Das NCSC bewahrt Personendaten nur so lange auf, wie dies zur Abwehr von Gefahren oder zur Erkennung von Vorfällen zweckmässig ist, höchstens jedoch ein Jahr ab der letzten Verwendung; bei besonders schützenswerten Personendaten beträgt die Frist 6 Monate. In anonymisierter Form sowie als erkannte Muster dürfen die aus Personendaten gewonnen Erkenntnisse unbefristet aufbewahrt werden.

Begründung

Das Verhältnissmässigkeitsprinzip im Datenschutz gebietet, dass Daten nur so lange aufbewahrt bleiben, wie sie für die Zweckerfüllung benötigt werden. Aus den Personendaten können anonymisierte Muster generiert werden.

II. Die nachstehenden Erlasse werden wie folgt geändert:

2. Datenschutzgesetz vom 25. September 2020

Art. 24 Abs. 5bis

Streichen.

Begründung

Sofern eine zentrale Stelle zu schaffen wäre, welche sämtlichen Meldungen aufnimmt, erübrigt sich diese Ergänzung.

Nach dem Gesagten danken wir Ihnen, sehr geehrte Frau Bundesrätin Keller-Sutter, sehr geehrter Herr Amstutz, sehr geehrte Damen und Herren, bestens für die Berücksichtigung unserer Anliegen und stehen Ihnen für allfällige Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Arié Malz

Co-Präsident ISSS

Marcel Zumbühl

Co-Präsident ISSS

Schweizerischer Pensionskassenverband
Association suisse des Institutions de prévoyance
Associazione svizzera delle Istituzioni di previdenza
Kreuzstrasse 26
8008 Zürich

Telefon 043 243 74 15/16
Telefax 043 243 74 17
E-Mail info@asip.ch
Website www.asip.ch

Eidgenössisches Finanzdepartement
EFD
Generalsekretariat EFD
Bundesgasse 3
ncsc@gs-efd.admin.ch

3003 Bern

Zürich, 14. April 2022

Stellungnahme zur Vernehmlassung betreffend Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrte Damen und Herren,

Gerne nehmen wir zum Entwurf des Bundesgesetzes über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) Stellung.

Angesichts der Tatsache, dass Cyberrisiken schon seit etlichen Jahren auch für Pensionskassen und deren Versicherte bzw. Rentnerinnen und Rentner ein grosses Risiko darstellen, befürworten wir grundsätzlich das neue ISG.

Wir begrüssen dabei die im Erläuterungsbericht, S. 18f., erwähnte Möglichkeit der Einschränkung der Meldepflicht aller registrierten und nicht registrierten Vorsorge- und Freizügigkeitseinrichtungen gemäss Art. 74a i.V.m. Art. 74b lit. j E-ISG.

Bezüglich der vom Bundesrat zu definierenden «geeigneten Kriterien» ersuchen wir Sie jedoch um eine Vernehmlassung des angekündigten Verordnungstextes, so dass wir die Definition der «geeigneten Kriterien» vorsorgerechtlich prüfen können.

Wir danken Ihnen für die Berücksichtigung unserer Hinweise.

Mit freundlichen Grüssen

A S I P

Schweizerischer Pensionskassenverband

Jean Rémy Roulet

Präsident

Hanspeter Konrad

Direktor

Eidgenössisches Finanzdepartement EFD
Bundesrat Ueli Maurer
Bundesgasse 3, 3003 Bern

Eingabe per Mail an: ncsc@gs-efd.admin.ch

Bern, 13. April 2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe
Stellungnahme zum Bundesgesetz über die Informationssicherheit beim Bund

Sehr geehrter Herr Bundesrat Maurer,
Sehr geehrter Herr Delegierter des Bundes für Cybersicherheit Schütz,
Sehr geehrte Damen und Herren,

Die Vernehmlassung zur Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen sowie die weiteren vorgesehenen Änderungen im Informationssicherheitsgesetz ISG verfolgen wir mit grossem Interesse. Um die Vorreiterrolle der Schweiz betreffend Wissenschaft und Wirtschaft weiter zu stärken, arbeitet der Thinktank Pour Demain an gesellschaftlichen Themen, welche ein grosses Nutzen- und Schadenspotential aufweisen. Die Verknüpfung von Cybersicherheit und kritischen Infrastrukturen ist ein solches Thema.

Deshalb nehmen wir hiermit gerne die Möglichkeit wahr, Ihnen unsere Vernehmlassungsantwort zukommen zu lassen. Diese haben wir in den letzten Monaten mit einer Reihe namhafter Expert:innen ausgearbeitet (siehe Liste der Unterstützer:innen).

Für einen weiteren Dialog stehen wir gerne zur Verfügung und bedanken uns für Ihr Interesse.

Patrick Stadler, Geschäftsführer & Mitgründer, Pour Demain
David Marti, Mitgründer, Pour Demain

Beilage:
- Liste der 30 Unterstützer:innen

Allgemeine Würdigung

Pour Demain begrüsst die Revision des Informationssicherheitsgesetzes (ISG) mit der Ausweitung des Schutzes vor Cyberangriffen. Der vorliegende Entwurf überzeugt in weiten Teilen, insbesondere in folgenden Punkten:

- Breite Definition von kritischen Infrastrukturen inklusive Anbieterinnen von Online-Diensten sowie Herstellern von Hard- und Software in sicherheitsrelevanten Bereichen.
- Positive wie negative Anreize, inklusive Bussen, sind vorhanden.
- Administrativer Aufwand wird tief gehalten durch kombinierte Übertragungsformulare.
- Weiterleitung von Informationen zur frühzeitigen Erkennung/Verhinderung von Sicherheitsbedrohungen.
- Internationale Zusammenarbeit.
- Unterstützung der Betreiber:innen kritischer Infrastrukturen.

Die Revision unterstreicht die Bedeutung von Cybersicherheit in einem weiten Sinne und stärkt das Nationale Zentrum für Cybersicherheit (NCSC). Somit verfügt das NCSC über eine starke Grundlage, die auch einen Ausbau in ein Amt/Staatssekretariat möglich machen wird (siehe Interpellation 21.4389).

Artikel 5

d-e Meldepflicht auf Cybervorfälle ausweiten

Die Revision sieht eine Meldepflicht von kritischen Infrastrukturen nur für Cyberangriffe vor, definiert in Art. 5 als “Cybervorfall, der von Unbefugten absichtlich ausgelöst wurde”. Dies geht zu wenig weit. Die Meldepflicht von kritischen Infrastrukturen sollte allgemeine Cybervorfälle einschliessen, definiert in Art. 5 als “Ereignis beim Betrieb von Informatikmitteln, das dazu führen kann, dass die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist.” Mit Blick auf das Schadenspotential ist es unerheblich, ob ein Ereignis absichtlich von Unbefugten (Cyberangriff) oder unabsichtlich/von Befugten/von Informatikmitteln (Cybervorfall) ausgelöst wurde.

Die Definition von Cybervorfällen umfasst zudem algorithmische Entscheidungssysteme (Künstliche Intelligenz, KI) und entsprechende Fehlfunktionen (z.B. häufig eingesetzter KI-Algorithmus führt zu Stromausfall in Elektrizitätswerk oder Flugzeugabsturz wie bei Boeing 737 Max). Es ist essenziell, dass auch KI unter die Meldepflicht fällt, da diese Systeme über zunehmende Leistungsfähigkeit verfügen und in immer mehr kritischen Infrastrukturen eingesetzt werden. Zudem ist es etwa in der Flug- oder Nuklearsicherheit etablierte Praxis, dass nicht nur schwere Unfälle oder Angriffe, sondern auch sonstige Zwischenfälle rapportiert und

aufgearbeitet werden. Eine solche moderne Sicherheitskultur sollte auch im Cyber- und KI-Bereich Einzug finden.

Artikel 73

a Grundsatz; Aktives Monitoring

Die in Art. 73 festgehaltenen Aufgaben des NCSC, insbesondere die “Warnung für Cyberrisiken und Schwachstellen von Informatikmitteln” sollten, wo relevant, mit einem nationalen Monitoring zu Chancen und Risiken von KI verknüpft werden (siehe Motion 22.3298, welche anregt, dass der Bund eigene Kapazitäten entwickelt, um Fortschritte bei KI zu antizipieren und zu überwachen). Unabhängig davon schlagen wir vor, dass das NCSC eine aktivere Monitoring-Rolle übernimmt. Anstatt primär eingehende Berichte zu verwerten, kann das Zentrum die Bedrohungslage durch Monitoring und Scans von Sicherheitslücken aktiv verfolgen.

b Weisungen zur Behebung der Schwachstellen verschärfen; Transparenz über Schwachstellen

Fristen zur Behebung von Schwachstellen (Art 73b, lit. 3) sollen nicht nur für Hersteller, sondern auch für Betreiber gesetzt werden können. Nur so ist sichergestellt, dass ein Sicherheitsupdate nicht nur von Herstellern entwickelt, sondern von kritischen Infrastrukturen auch tatsächlich eingespielt wird.

Auf Basis der zwingenden Meldungen an das NCSC sollte dieses mindestens jährlich in aggregierter Form über Schwachstellen bei kritischen Infrastrukturen berichten (in einer Form, die Angreifern keine spezifischen verwertbaren Informationen zur Verfügung stellt). Diese Praxis - analog der Sicherheitskultur im Flugverkehr (siehe SUST) - schärft das Problembewusstsein und ermöglicht schnelleres Handeln bei Schwachstellen.

Artikel 74

a Klare Definition der Meldefrist

Cyberangriffe sind “nach deren Entdeckung so rasch als möglich” zu melden. Eine schärfere Definition wäre begrüssenswert. So heisst es im erläuternden Bericht, dass bei Cyberangriffen oft “längere Zeit” unklar sei, wie gravierend ein Angriff ist und eine Meldung erst bei “ausreichendem Kenntnisstand” verlangt werde. Dies könnte dazu führen, dass Angriffe mit Verweis auf diese Definition erst verzögert gemeldet werden, weil die Informationen “unvollständig” seien. Zudem ist der Schaden grösser, wenn ein gravierender Angriff zu lange nicht gemeldet wird, als wenn ein weniger gravierender Angriff (unnötigerweise) gemeldet wird.

c Ausnahmen von der Meldepflicht

Einschränkung der Ausnahmen der Meldepflicht: Art. 74c Abs. a ist nicht zeitgemäss und sollte gestrichen werden. Angesichts der Durchdringung von IT-Mitteln trifft es nicht (mehr) zu, dass Cyberangriffe auf gewisse kritische Infrastrukturen “unwahrscheinlich sind, insbesondere wegen der geringen Abhängigkeit von Informatikmitteln”. Es ist nicht ersichtlich, bei welchen der unter Art. 74b aufgeführten kritischen Infrastrukturen Störungen an Informatikmitteln keine gravierenden Auswirkungen zur Folge hätten. Selbst eine tiefe Zahl oder ältere Informatikmittel schützen nicht vor Angriffen oder Zwischenfällen. Während Art. 74c Abs. a besonders problematisch erscheint, wäre es begrüssenswert, Ausnahmen generell auszuschliessen (d.h. Streichung gesamter Artikel Art. 74c).

f Übermittlung der Meldung

Automatisierte Meldungen: Neben manuellen Meldungen soll eine IT-Schnittstelle (API) auch automatisierte Meldungen an das NCSC erlauben. So können Cyber-Überwachungssyteme von kritischen Infrastrukturen etwa automatisch verdächtige Signale an das Zentrum weiterleiten. Die Datengrundlage des NCSC wird damit umfassender und zeitnäher als bei rein manuellen Eingaben nach grösseren Vorfällen.

privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

Nationales Zentrum für Cybersicherheit
Schwarztorstrasse 59
3003 Bern

Per Mail:
ncsc@gs-efd.admin.ch

Bern, 11. April 2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe; Vernehmlassungsverfahren

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, zum Vorentwurf für eine Änderung des Bundesgesetzes über die Informationssicherheit beim Bund (VE-ISG) betreffend die Einführung einer Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe Stellung nehmen zu können. Gerne äussern wir uns dazu wie folgt:

1. Allgemeine Bemerkungen

Das wirkungsvolle Erkennen und die Abwehr von Cyberangriffen kann sich auch positiv auf den Datenschutz auswirken. Deshalb stehen wir dem Vorhaben grundsätzlich zustimmend gegenüber.

Neben der geplanten Einführung einer Meldepflicht werden die Kompetenzen des Nationales Zentrums für Cybersicherheit (NCSC) erweitert.

Vor dem Hintergrund, dass es sich bei Cyberangriffen um Straftaten (Bedrohung der inneren oder äusseren Sicherheit) handeln kann, erscheint eine Zusammenarbeit des NCSC mit Strafverfolgungsbehörden und dem NDB als notwendig und nachvollziehbar. Die Aufgabentrennung zwischen NCSC und den Strafverfolgungsbehörden und dem Nachrichtendienst ist uns in der aktuellen Ausgestaltung allerdings zu wenig klar. Es muss sichergestellt werden, dass das NCSC strafrechtliche oder nachrichtendienstliche Ermittlungstätigkeiten nur soweit ausführt, wie dies zur Abwehr von Cyber-Angriffen zwingend notwendig ist. Rechtliche Einschränkungen oder die Aufsicht über solche Tätigkeiten dürfen nicht umgangen werden, wenn die Bearbeitung (teilweise) durch das NCSC erfolgt.

privatim
c/o Datenschutzbeauftragter des Kantons Bern
Poststrasse 25, CH-3072 Ostermundigen
Tel. +41 (31) 633 74 10
praesident@privatim.ch, www.privatim.ch

In Anbetracht der Abhängigkeit von digitalen Hilfsmitteln erscheint der breit gefasste Kreis der meldepflichtigen Bereiche nach Art. 74b VE-ISG als nachvollziehbar. Der umfassende Geltungsbereich hat aber auch zur Folge, dass sehr viele und sensitive Informationen bearbeitet werden. Entsprechend ist bei der Umsetzung dem Schutz der bearbeiteten Informationen besondere Beachtung zu schenken. Dazu gehört auch die konsequente Einschränkung der Zugriffsmöglichkeiten. Es muss sichergestellt sein, dass zu jedem Zeitpunkt ausschliesslich die Informationen in geeigneter Form zur Verfügung stehen, welche zur Abwehr notwendig sind. Sind Daten ohne Personenzug ausreichend, hat die Bearbeitung mit anonymisierten Daten zur erfolgen.

2. Einschränkung der Bearbeitung von besonderen Personendaten (Art. 75)

In Anbetracht des Umstandes, dass das NCSC weder die Aufgaben des NDB übernimmt noch eine Strafverfolgungsbehörde ist, erscheint der Umfang der bearbeiteten Personendaten nach Art. 75 Abs. 1 VE-ISG ohne weitere Einschränkungen (namentlich auf die *zwingende* Notwendigkeit zur Aufgabenerfüllung) als nicht verhältnismässig. Wir empfehlen, die nötigen Einschränkungen vorzusehen.

3. Zusammenarbeit mit ausländischen Strafverfolgungsbehörden (Art. 77)

Da sich Cyberangriffe oft nicht ausschliesslich auf einzelne Länder beziehen, ist es nachvollziehbar und erscheint als erforderlich, dass das NCSC auch mit ausländischen Behörden Informationen austauschen muss (Art. 77 Abs. 1 VE-ISG). Beim NCC handelt es sich jedoch nicht um eine Strafverfolgungsbehörde. Wir gehen deshalb davon aus, dass der Verweis auf die Bestimmungen über die Amts- und Rechtshilfe in Art. 77 Abs. 3 VE-ISG eine von Abs. 1 unabhängige Vorschrift darstellt und sich die innerstaatlichen Zuständigkeiten für die Amts- und Rechtshilfe ausschliesslich aus den betreffenden Bestimmungen ergibt; wir empfehlen, dies in der Botschaft entsprechend klarzustellen.

4. Trennung der Kompetenzen

Der Trennung der Kompetenzen zwischen NCSC, den Strafbehörden und dem NDB sollte deutlich mehr Beachtung geschenkt werden. So müsste Art. 75 Abs. 2 VE-ISG (Bearbeiten von Personendaten, ohne dass dies für die betroffene Person ersichtlich ist) auf Fälle bei laufenden Strafverfahren eingeschränkt werden. Der Zugriff im Abrufverfahren für den NDB (Art. 76a Abs. 2 VE-ISG), für Strafverfolgungsbehörden (Art. 76a Abs. 3 VE-ISG) sowie für kantonale Stellen für Cybersicherheit (Art. 76a Abs. 3 VE-IST) muss eingeschränkt oder mittels eines «Push-Verfahrens» realisiert werden. Unklar erscheint auch, wie die Aufgaben zwischen kantonalen Stellen für Cybersicherheit und dem NCSC aufgeteilt werden bzw. ob die kantonalen Stellen für Cybersicherheit weiterhin notwendig sind. Eine mehrfache Bearbeitung derselben Informationen führt zu zusätzlichen Risiken und behindert im schlechtesten Fall eine effiziente Bekämpfung von Cyberangriffen.

5. Definition von schwerwiegenden Sicherheitsvorfällen (Art. 74*d*)

Auch wenn im erläuternden Bericht ausgeführt wird, dass nur schwerwiegende Sicherheitsvorfälle gemeldet werden müssen, bleibt der erläuternde Bericht eine Antwort schuldig, was unter schwerwiegend zu verstehen ist. Die Formulierung in Art. 74d Abs. 1 VE-ISG «Ein Cyberangriff auf eine kritische Infrastruktur muss gemeldet werden, wenn Anzeichen dafür bestehen, dass […]» legt den Schluss nahe, dass Vorfälle auch dann gemeldet werden müssen, wenn ihre Schwere noch nicht abgeschätzt werden kann. Die Kombination der

breit gefassten Definition der kritischen Infrastrukturen (Art. 74b VE-ISG) und der faktisch tiefen Schwelle, bei der eine Meldung zu erfolgen hat, birgt die Gefahr, dass grosse Mengen an personenbezogenen Daten gesammelt werden. Nach Art. 73b Abs. 1 VE-ISG analysiert das NCSC die Cybervorfälle oder Schwachstellen auf ihre Bedeutung für den Schutz der Schweiz vor Cyberrisiken. Kommt die NCSC zum Schluss, dass es sich um keinen schwerwiegenden Sicherheitsvorfall handelt und liegt keine Einwilligung der betroffenen Person(en) vor, sind personenbezogene Informationen unverzüglich zu löschen. In anonymisierter Form können die Daten weiterhin bearbeitet werden.

6. Löschen von Informationen

Aufgrund der Aufgaben des NCSC müssen die personenbezogenen Daten unseres Erachtens nach einer allfälligen Übermittlung an die Strafverfolgungsbehörden oder an den NDB beim NCSC selbst nach einer kurzen Frist gelöscht werden. Die Aufbewahrungsfrist von höchstens fünf (für «normale» Personendaten) und zwei (für besondere Personendaten) Jahren erscheint aufgrund der Aufgaben des NCSC (Erkennen von gerade stattfinden Cyberangriffen) als lang. Falls es für eine Mustererkennung weiterhin notwendig ist, könnten die Daten anonymisiert und weiterhin verwendet werden.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Ueli Buri
Präsident privatim

RAILplus
Die Meterspurigen
La voie métrique
A scartamento metrico

Département fédéral des finances (DFF)
Bundesgasse 3
3003 Bern

Aarau, le 14 avril 2022

Par courriel à: ncsc@gs-efd .admin.ch

Objet : Prise de position de RAILplus dans le cadre de la procédure de consultation relative à l'introduction d'une obligation de signaler les cyberattaques.

Madame, Monsieur,

Nous vous remercions de nous donner la possibilité de prendre position sur l'introduction d'une obligation de signaler les cyberattaques au titre de la présente procédure de consultation.

Remarques générales :

Dans le contexte actuel d'augmentation constante des cyberattaques, RAILplus soutient l'initiative de rendre obligatoire leur signalement au sein des infrastructures critiques. Nous comprenons que l'objectif de cette évolution est multiple : il s'agit à la fois pour le NSCS d'avoir une idée de la réalité, d'anticiper, d'analyser et de proposer de l'aide aux organisations victimes de cyberattaques. Ce dernier point est accueilli très favorablement par RAILplus.

Remarques particulières :

- RAILplus salue la possibilité de réutiliser le formulaire existant du NCSC (avec si besoin quelques adaptations). En effet pour des raisons de simplicité et de pragmatisme, il semble pertinent de le conserver. De plus, la possibilité d'échanges d'informations avec d'autres organismes exigeants également une notification (PFPDT, etc.) est accueillie très favorablement. Cela limite les notifications en doublon et permet à nos équipes de maintenir l'attention sur la gestion de la cyberattaque.

- Concernant l'étendue de l'obligation de signalement, RAILplus souhaiterait partager quelques remarques et propositions :

RAILplus
Die Meterspurigen
La voie métrique
A scartamento metrico

Article 74d : *« Une cyberattaque contre une infrastructure critique doit être signalée si des indices laissent présumer :*

a. qu'elle met en péril le bon fonctionnement de l'infrastructure critique touchée ou une autre infrastructure critique;
b. qu'elle a été exécutée par un État étranger ou à son instigation;
c. qu'elle a entraîné ou pourrait entraîner une fuite ou la manipulation d'informations, ou
d. qu'elle est passée inaperçue pendant plus de 30 jours. »

RAILplus se questionne sur la pertinence de la deuxième condition (b.). De nos jours, les cyber-attaques perpétrées par les Etats sont de plus en plus sophistiquées, difficiles à détecter et réalisées par des groupes d'attaquants divers. L'attribution de l'attaque à un Etat peut s'avérer complexe, d'autant plus que la priorité de la victime est mise sur la résolution de l'incident et non pas sur l'identification de l'attaquant.

A la place de cette condition, RAILplus souhaiterait rajouter un critère cumulatif lié à l'impact (exemple : « nombre d'utilisateurs touchés », « nombre de systèmes touchés », « criticité du système » à définir par secteur). Selon RAILplus, ce critère permettrait de préciser davantage l'étendue de l'obligation de signalement ayant le plus de conséquences pour nos usagers.

- Concernant la confidentialité des données transmises au NCSC en cas de cyberattaques, RAILplus insiste sur le fait que toute publication d'information au sujet d'une attaque doit a minima recueillir le consentement de l'entreprise victime ou alors garantir son anonymat.

- En cas de non-respect de l'obligation de déclaration, RAILplus souligne que le montant maximum de la sanction financière (100 000 francs auprès d'une personne physique) est plus qu'incitatif. De notre compréhension, si l'amende infligée est supérieure à 20 000 francs, cette dernière sera infligée à une personne physique (chef d'entreprise, employeur, mandant ou représenté). Jusqu'à un montant de 20 000 francs, l'amende peut ainsi être directement infligée à l'infrastructure critique à la place de la personne physique responsable, afin d'éviter des frais excessifs lors de l'enquête. RAILplus propose que seules les personnes morales soient condamnables (quel que soit le montant de la sanction). En effet il parait plus pertinent de sanctionner directement les entreprises et non les employés.

- Enfin, en cas de cyberattaque chez un prestataire impactant l'activité de l'infrastructure critique, RAILplus se questionne sur les responsabilités et rôles de chacun. Pour RAILplus, il revient au prestataire de signaler la cyberattaque étant amène de détenir la majorité des informations clés la concernant. De plus, si plusieurs clients du prestaire sont touchés, la communication avec un seul interlocuteur (en l'occurrence le prestataire) sera simplifiée. Le prestataire doit être tenu d'informer RAILplus et les potentiels autres clients tout au long de l'attaque. Par conséquent, la sanction incombera au prestataire en cas de non-respect de l'obligation de déclaration. La question se pose également en cas de sous-traitants se situant en dehors du territoire suisse : est-il de leur responsabilité de déclarer la cyberattaque ? Qu'en est-il de la sanction ?

RAILplus
Die Meterspurigen
La voie métrique
A scartamento metrico

Conclusion :

RAILplus soutient le projet de loi sur l'obligation de signaler les cyberattaques. Toutefois certaines clarifications apparaissent encore nécessaires. Enfin, RAILplus tient à préciser que le montant de l'amende prévu en cas d'infraction à la nouvelle disposition doit rester proportionné.

Nous vous remercions de tenir compte de la présente prise de position. M. Greuter, directeur de RAILplus, se tient à votre disposition si vous avez besoin de précisions.

Nous vous prions d'agréer, Madame, Monsieur, l'expression de notre considération distinguée.

Joachim Greuter	Urs Siegenthaler	Nicolas Murbach
		
Directeur RAILplus	Responsable du groupe de travail informatique RAILplus en Suisse alémanique	Responsable du groupe de travail informatique RAILplus en Suisse romande

RAILplus AG | Hintere Bahnhofstrasse 85 | 5001 Aarau | 062 832 83 66 | info@railplus.ch | www.railplus.ch

santésuisse | Die Schweizer Krankenversicherer
Les assureurs-maladie suisses
Gli assicuratori malattia svizzeri

santésuisse
Römerstrasse 20
Postfach
CH-4502 Solothurn
Tel. +41 32 625 41 41
Fax +41 32 625 41 51
mail@santesuisse.ch
www.santesuisse.ch

Per E-Mail an:
ncsc@gs-efd.admin.ch

Für Rückfragen:
Agnes Stäuble
Direktwahl: +41 32 625 4266
Agnes.Staeuble@santesuisse.ch

Solothurn, 12. April 2022

Vernehmlassungsverfahren zur Meldepflicht von Betreiberinnen und Betreibern kritischer Infrastrukturen für Cyberangriffe; Stellungnahme santésuisse

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit, zur Einführung einer Meldepflicht für Cyberangriffe und der damit verbundenen Änderung des Informationssicherheitsgesetzes (ISG) Stellung nehmen zu können.

1. santésuisse erachtet eine entsprechende Meldepflicht als sinnvoll

Die Krankenversicherer sehen sich aufgrund der fortschreitenden Digitalisierung zunehmend mit Cyber-Bedrohungen konfrontiert. Es erweist sich daher als sachgerecht, mittels einer Meldepflicht bezüglich Cyberattacken ein Frühwarnsystem zu etablieren und dadurch eine bessere Übersicht zur Bedrohungslage zu schaffen und die Cybersicherheit zu stärken. Dementsprechend begrüsst santésuisse die vorgesehene Einführung einer solchen Meldepflicht für Cyberangriffe auf kritische Infrastrukturen.

2. Klärung von Begrifflichkeiten und Definitionen

- **Cyberrisiko**

  Der Begriff «Cyberrisiko» wird unseres Erachtens im vorliegenden Kontext nicht korrekt verwendet. Es müsste Cyberbedrohungen heissen. Das Risiko ist keine Bedrohung.

  Ein Unternehmen hat Schwachstellen die durch Bedrohungen aus dem Cyberraum ausgenutzt werden können. Das Risikoszenario beschreibt wie eine Schwachstelle durch die Bedrohung ausgenutzt werden kann. Das Risiko ist dann die Einschätzung der Eintrittswahrscheinlichkeit und des Schadenmasses für dieses Risikoszenario.

- **Art. 5 Bst. d E-ISG: Cybervorfall**

  Cybervorfall: Ereignis beim Betrieb von Informatikmitteln, das dazu führen kann, dass die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist;

  Die hier gewählte Definition kann zu Missverständnissen führen. Solche Ereignisse können nämlich auch auftreten, ohne dass sie durch einen Cyberangriff ausgelöst werden, z.B. Ausfall von IT Komponenten oder Programmierfehler. Diese Ereignisse dürfen nicht unter die Meldepflicht fallen.

- **Art. 74d Abs. 1 Bst. b E-ISG**

  Ein Cyberangriff auf eine kritische Infrastruktur muss gemeldet werden, wenn Anzeichen dafür bestehen, dass ein fremder Staat ihn ausgeführt oder veranlasst hat.

  Die Zuordnung eines Angriffs zu einem ausländischen Staat ist eine besonders komplexe Aufgabe, für deren Durchführung die Krankenversicherer weder über die notwendigen Ressourcen noch über die erforderlichen Fähigkeiten verfügen. Im besten Fall kann ein solcher Angriff nur mit Unterstützung des NCSC gemeldet werden, d.h. das NCSC würde vor einer Meldung involviert werden, was keinen Sinn macht.

  Überdies sollte Art. 74d E-ISG präziser formuliert werden. Zusammen mit der betreffend Cybervorfall gewählten Definition in Art. 5 Bst. d E-ISG lässt der Artikel unseres Erachtens zu viel Spielraum offen für die Interpretation, was als meldepflichtiger Cyberangriff qualifiziert wird. Nicht klar zugeordnet werden können z.B. folgende Vorfälle:
  - DDoS Attacke: Diese ist für das Unternehmen spürbar. Der Service ist kurzzeitig nicht verfügbar, aber unter der in der BIA tolerierten maximalen Ausfallzeiten. Der Provider blockiert nach kurzer Zeit die Attacke.
  - Scans aus dem Internet, welche ausloten, ob ein Unternehmen verwundbare Systeme betreibt.
  - Vorhandene Software-Schwachstellen, die ausgenutzt werden können bis sie gepatched werden. Es gibt aber noch keine bekannten Exploits.
  - Phishing E-Mails, mit der Aufforderung auf einen Link zu klicken oder interne Informationen preiszugeben.

3. Es ist darauf zu achten, dass die administrative Belastung im Zusammenhang mit der Meldepflicht klein bleibt

Gemäss Art. 74a E-ISG sind die Betreiberinnen und Betreiber von kritischen Infrastrukturen gehalten, dem nationalen Zentrum für Cybersicherheit (NCSC) Cyberangriffe nach deren Entdeckung so rasch als möglich zu melden. Für die elektronische Übermittlung der Meldung stellt das NCSC ein sicheres System zur Verfügung (vgl. Art. 74f Abs. 1 E-ISG). Vor dem Hintergrund, dass die administrative Belastung im Zusammenhang mit der Meldepflicht möglichst klein sein sollte, unterstützt santésuisse die Zurverfügungstellung eines solchen Systems.

4. Verhältnis zu anderen Meldepflichten und Informationsaustausch unter den Behörden

Die Einführung einer Meldepflicht für Cyberangriffe tangiert bereits bestehende Meldepflichten, wie insbesondere die Meldepflicht nach Art. 24 des revidierten Datenschutzgesetzes (revDSG), wonach der Verantwortliche dem EDÖB so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt, zu melden hat.

santésuisse erachtet es auch im Verhältnis zu anderen Meldepflichten als wichtig, dass der Aufwand für die Erfüllung der jeweiligen Obliegenheit möglichst geringgehalten wird. Entsprechend befürworten wir, unter Gewährleistung des vollumfänglichen Datenschutzes, die vorgesehene Regelung betreffend die Weiterleitung der Meldung eines Cyberangriffs. Es soll den Meldenden offenstehen, die Meldung gleichzeitig mit der Übermittlung an das NCSC anderen Meldestellen weiterzuleiten, um damit anderweitige Meldepflichten zu erfüllen. Umgekehrt soll das NCSC auch Meldungen zu Cyberangriffen entgegennehmen, welche in Erfüllung einer anderweitigen Meldepflicht abgegeben wurden. Damit wird verhindert, dass Betroffene den gleichen Vorfall unterschiedlichen Stellen über unterschiedliche Verfahren melden müssen und dabei unterschiedlichen Meldepflichten mit divergierenden Meldeinhalten/Meldefristen für unterschiedliche Behörden zu berücksichtigen haben.

Vielen Dank für die Kenntnisnahme und Berücksichtigung unserer Anmerkungen. Für Fragen stehen wir gerne zur Verfügung.

Freundliche Grüsse

santésuisse

Direktion

Verena Nold
Direktorin

Rechtsdienst

Isabel Kohler Muster
Leiterin Rechtdienst santésuisse-Gruppe

Swiss Banking

Eidgenössisches Finanzdepartement
Nationales Zentrum für Cybersicherheit NCSC
Schwarztorstrasse 59
CH-3003 Bern

Per Mail: ncsc@gs-efd.admin.ch

Basel, 13. April 2022

Meldepflicht von Betreiber/-innen kritischer Infrastrukturen für Cyberangriffe
Vernehmlassung – unsere Stellungnahme

Sehr geehrter Herr Bundesrat Maurer
Sehr geehrter Herr Schütz
Sehr geehrte Damen und Herren

Wir nehmen Bezug auf die vom Bundesrat am 12.01.2022 eröffnete Vernehmlassung zur Revision des Informationssicherheitsgesetzes (ISG) betr. Einführung einer Meldepflicht für Betreiber/-innen kritischer Infrastrukturen bei Cyberangriffen. Zu Ihrem Entwurf äussern wir uns wie folgt.

Zusammenfassung

Die Schweizerische Bankiervereinigung (SBVg) befürwortet die Verankerung der Aufgaben des Nationalen Zentrums für Cybersicherheit (NCSC) auf Gesetzesstufe (s. nachstehend 2.1 und 2.2); sie sollen als Dienstleistungen des Bundes die eigenverantwortlich zu treffenden Massnahmen der Unternehmen ergänzen.

Die SBVg unterstützt die Einführung einer Pflicht der Betreiberinnen kritischer Infrastrukturen, Cyberangriffe den Behörden zu melden, unter Vorbehalt nachfolgender Anliegen.

Die von der FINMA beaufsichtigten Institute sind gemäss Art. 29 Abs. 2 FINMAG bereits heute verpflichtet, der FINMA unverzüglich Vorkommnisse zu melden, die für die Aufsicht von wesentlicher Bedeutung sind. Diese umfassen auch Cyberangriffe (FINMA-Aufsichtsmitteilung 05/2020 betr. Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG).

Um zu vermeiden, dass unterschiedliche Meldungen sowohl dem NCSC als auch der FINMA erstattet werden müssen, schlagen wir vor:

- Das Meldeformular ist so zu konzipieren, dass es parallel und ohne zusätzlichen Aufwand auch weiteren Behörden (z.B. FINMA, EDÖB) geschickt werden kann.
- Rückfragen involvierter Behörden müssen über das Formular und den dafür zu schaffenden Kanal beantwortet werden können.

In jedem Fall müssen die verschiedenen Meldepflichten für die betroffenen Unternehmen konsistent ausgestaltet sein.

Die Meldepflicht muss verhältnismässig ausgestaltet sein, wie es der Entwurf zu einem guten Teil bereits vorsieht: Wo wir es als sinnvoll erachten, schlagen wir nachstehend Anpassungen und Ergänzungen vor. Wir befürworten insbesondere:

- eine Meldepflicht nur für Cyberangriffe, nicht für blosse Cybervorfälle (so bereits vorgesehen, Art. 74a);
- eine zwingende Meldepflicht nur bei Cyberangriffen mit einem gewissen Schadenspotenzial gemäss unserem Vorschlag zu Art. 74d.

Das Melderegime muss praxisfreundlich ausgestaltet sein. Zu diesem Zweck schlagen wir vor, auf Verordnungsstufe einen Beispielkatalog auszuarbeiten, und sind gerne bereit, daran mitzuwirken (s. nachstehend 2.4).

Übereinstimmend mit economiesuisse schlagen wir zudem die Streichung der Strafdrohung in Art. 74h und 74i vor (s. nachstehend 2.7), da sie sich im Blick auf die Compliance des Unternehmens kontraproduktiv auswirken könnte.

Das elektronische Meldesystem (Art. 74f) muss höchsten Sicherheitsanforderungen genügen.

Den Bestimmungen über Anpassungen beim Datenschutz und die Zusammenarbeit mit in- und ausländischen Behörden, die im Bereich der Cybersicherheit tätig sind (Art. 75–77), stimmen wir zu. Wir schlagen vor, im Gesetz explizit festzuhalten, dass bei Meldungen an das NCSC allfällige Berufsgeheimnisse zu wahren sind.

1. Allgemeines

Die Schweizerische Bankiervereinigung (SBVg) und ihre Mitglieder engagieren sich mit hoher Priorität für Massnahmen zur Stärkung der Cyberresilienz am Wirtschaftsstandort Schweiz. Ausdruck dieses Engagements war nicht zuletzt die mit dem Expertengremium Information Security & Cyber Defence erarbeitete Strategie der SBVg (parallel zur Nationalen Cyber Strategie des Bundes, NCS II). Die darin postulierten Massnahmen sind teilweise schon umgesetzt (so z.B. die Schaffung des Nationalen Zentrums für Cybersicherheit, NCSC) oder befinden sich in der Umsetzung (so z.B. die Bildung eines Swiss Financial Sector Cyber Security Centre, FS-CSC). Umsetzbar ist eine solche Strategie nur als **Public-Private Partnership (PPP) mit den Bundesbehörden, insbesondere dem NCSC**. Für die in diesem Sinne sehr erfolgreiche Zusammenarbeit möchten wir Ihnen auch an dieser Stelle danken.

Die Meldepflicht bei Cyberangriffen stellt einen **wichtigen Schritt auf dem Weg der Umsetzung dieser gemeinsamen Bemühungen** dar – einen Schritt, der notwendigerweise dem Gesetzgeber, also der staatlichen Seite der Partnership zukommt. Wir unterstützen Sie dabei und äussern uns nachstehend zu einzelnen Gesichtspunkten, insbesondere dort, wo wir noch Verbesserungsbedarf sehen.

2. Bemerkungen zu einzelnen Bestimmungen des Entwurfs

2.1 Gesetzeszweck und Begriffsumschreibungen (Art. 1 und 5)

Wir begrüssen, dass der **Gesetzeszweck** (Art. 1 Abs. 1 Bst. b) neu ausdrücklich die Erhöhung der «Widerstandsfähigkeit der Schweiz gegenüber Cyberrisiken» (Cyberresilienz) mitenthalten soll. Dadurch untermauert das Gesetz die in Art. 73a ff. festgehaltenen Aufgaben des NCSC.

Wir sind einverstanden mit der Umschreibung der **Schlüsselbegriffe**:

- *«Cybervorfall» (Art. 5 Bst. d: «Ereignis beim Betrieb von Informatikmitteln, das dazu führen kann, dass die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist») und*
- *«Cyberangriff» (Art. 5 Bst. e: «Cybervorfall, der von Unbefugten absichtlich ausgelöst wurde»).*

Der Cybervorfall ist heute in **Art. 3 Bst. b Cyberrisikenverordnung (CyRV)** so umschrieben, dass er auch den Cyberangriff abdeckt. Art. 5 Bst. d des Gesetzesentwurfs übernimmt materiell diesen Begriff, und Art. 5 Bst. e führt einen gesonderten Begriff des Cyberangriffs ein, um die Meldepflicht auf diesen zu beschränken. Das erscheint uns sinnvoll. Art. 3 CyRV wird entsprechend anzupassen sein.

2.2 Umschreibung der Aufgaben des NCSC (Art. 73a ff.)

Wir begrüssen die **gesetzliche Verankerung der Aufgaben und Zuständigkeiten des NCSC**.

Nach unserem Verständnis ist der Gesetzestext so zu verstehen, dass die «Anleitungen für präventive und reaktive Massnahmen gegen Cyberrisiken» gemäss Art. 73a Bst. c den Unternehmen als Grundlage zu

freiwilligen Massnahmen in eigener Verantwortung dienen sollen. Verbindliche Anweisungen wären u.E. nicht sinnvoll, weil das NCSC die Lage in den Unternehmen nicht detailliert selber einschätzen kann. Das gilt insbesondere auch für Art. 74 Abs. 1–3.

Wir schlagen zudem vor, in diesen Abschnitt eine **ausdrückliche Ermächtigung des NCSC zur Kooperation mit privatrechtlichen Organisationen der Wirtschaft (Art. 73bis)**, aufzunehmen. Ein Beispiel dafür ist der derzeit im Aufbau befindliche Verein Financial Swiss Sector Cyber Security Centre (Swiss FS-CSC). So lässt sich einerseits eine Selbstverständlichkeit festhalten. Andererseits werden künftige Diskussionen um die Zulässigkeit von Public-Private Partnerships dadurch vermieden. Die entsprechende Bestimmung könnte wie folgt lauten:

> *«Zusammenarbeit mit Organisationen der Privatwirtschaft*
>
> *[1] Das NCSC kann im Rahmen seiner Aufgaben gemäss diesem Abschnitt mit Organisationen der Privatwirtschaft, insbesondere Unternehmen und ihren Verbänden, zusammenarbeiten.*
> *[2] Dabei sind die Berufs- und Geschäftsgeheimnisse der betroffenen Unternehmen zu wahren.»*

2.3 Meldepflicht der Betreiberinnen von kritischen Infrastrukturen (Art. 74a ff.)

Wir begrüssen die Einführung einer Meldepflicht und deren **Begrenzung auf Cyberangriffe mit erheblichem Schadenspotenzial unter Ausklammerung blosser Vorfälle**, die aber freiwillig gemeldet werden können (Erläuternder Bericht, S. 10 oben) (s. dazu nachstehend 2.5).

Zur Vermeidung mehrfacher Meldungen in unterschiedlichen Verfahren unterbreiten wir Ihnen einen Vorschlag, der **einfache Parallelmeldungen mit dem Formular des NCSC** erlaubt (s. nachstehend 3).

Wir schlagen vor, die Meldepflicht im Sinne der **Verhältnismässigkeit** – und in Anlehnung an die FINMA-Aufsichtsmitteilung 05/2020 – auf erfolgreiche oder teilweise erfolgreiche Cyberangriffe auf kritische Funktionen von Beaufsichtigten einzuschränken, deren Ausfall oder Fehlfunktion erhebliche Auswirkungen auf die Geschäftstätigkeit hätte und diese stark beeinträchtigen würde (s. nachstehend 2.4).

Als «Betreiberinnen von kritischen Infrastrukturen» (Art. 74a) lässt der Gesetzesentwurf u.a. **sämtliche Banken, Versicherungen und Finanzmarktinfrastrukturen** unter die Meldepflicht fallen (Art. 74b Bst. e), sofern diese nicht die Kriterien für eine Ausnahme gemäss Art 74c erfüllen Wir schlagen zur Wahrung der Verhältnismässigkeit und zur Schaffung von Rechtssicherheit vor, dass die Ausnahmen von der Meldepflicht auf Verordnungsstufe weiter konkretisiert werden.

In diesem Sinn schlagen wir vor, Art. 74c zu überarbeiten. Abs. 1 kann somit wie folgt lauten:

> *«[1] Der Bundesrat legt auf Verordnungsstufe klare Kriterien fest, anhand derer die Infrastrukturen meldepflichtig werden. Sinn dieser Kriterien ist es, jene Betreiberinnen kritischer Infrastrukturen von der Meldepflicht auszunehmen, bei denen durch Cyberangriffe ausgelöste Funktionsausfälle oder Fehlfunktionen [Rest unverändert]»*

Sodann regen wir an, die vage Formulierung in Art. 74a durch einen Abs. 2 mit einer **Fristregelung** zu ergänzen. Dabei sollte die zweistufige Regelung gemäss der FINMA Aufsichtsmitteilung 05/2020 übernommen werden (innert 24 Std. erste Meldung; innert 72 Std. ergänzte, ausführlichere Meldung). Das vereinfacht nicht zuletzt auch die Vertragslage mit Lieferanten.

2.4 Kriterien für zu meldende Angriffe (Art. 74d)

Die vorgeschlagenen Kriterien sind ungeeignet, um die Meldepflicht auszulösen, denn im Zeitpunkt, da eine Meldung sinnvoll und erwünscht wäre, dürften sie in einer Vielzahl der Fälle noch nicht absehbar sein. Wir schlagen deshalb die **vollständige Ersetzung von Art. 74d durch eine Formulierung im Sinn der FINMA-Aufsichtsmitteilung 05/2020** vor, die z.B. wie folgt lauten könnte:

> *«Zu melden sind Cyberangriffe mit erheblichen Auswirkungen auf die Geschäftstätigkeit des Unternehmens, insbesondere erfolgreiche oder teilweise erfolgreiche Angriffe auf kritische Funktionen, deren Ausfall oder Störung den Schutz der Kundinnen und Kunden oder das Funktionieren der Märkte stark beeinträchtigen würde.»*

Das Ziel, eine uferlose Meldepflicht mit unscharfen Grenzen zu vermeiden, spricht für die von uns vorgeschlagene Schaffung eines **Beispielkatalogs aus der Praxis** auf Verordnungsstufe. Gerne sind wir bereit, an dessen Ausarbeitung mitzuwirken.

Entsprechend der vom Gesetzgeber bestimmten Regelung wird insbesondere auch **die FINMA-Aufsichtsmitteilung 05/2020 betr. Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG anzupassen** sein.

Es wird der Bank ohnehin freistehen, **weitergehend als vorgeschrieben** zu melden, insbesondere auch blosse Cybervorfälle (Erläuternder Bericht, ebd.). Diese Möglichkeit, freiwillig weitere Cybervorfälle und -angriffe als vorgeschrieben zu melden, erwähnt der Gesetzesentwurf nicht ausdrücklich. Im Sinn der Rechtssicherheit schlagen wir eine **Bestimmung über die Zulässigkeit freiwilliger Meldungen (Art. 74d Abs. 2)** vor, die z.B. so lauten könnte:

> *«[2] Über die Meldepflicht aufgrund von Artikel 74a ff. hinaus darf eine Betreiberin von kritischen Infrastrukturen auch Cybervorfälle und -angriffe melden, welche die Kriterien gemäss Artikel 74d nicht vollständig erfüllen.»*

Damit wird explizit ausgeschlossen, dass eine überschiessende Erfüllung der Meldepflicht als Verletzung des Berufsgeheimnisses missverstanden werden könnte, und **einer denkbaren Rechtsunsicherheit vorgebeugt.**

2.5 Inhalt der Meldung (Art. 74e)

Die **offene, knappe Formulierung** über den Inhalt der Meldung ist zu begrüssen. Es gilt zu vermeiden, dass eine zu detaillierte Umschreibung bei den meldepflichtigen Unternehmen zu unverhältnismässigem Aufwand führt. Dies wird insbesondere bei der Ausgestaltung der Verordnung durch den Bundesrat zu berücksichtigen sein.

2.6 Elektronische Übermittlung der Meldung (Art. 74f)

Wir begrüssen die Schaffung eines elektronischen Systems für die Meldung von Cyberangriffen. Art. 74f legt die **Anforderungen für das Meldesystem** fest. Es muss

- sicher sein (Art. 74f Abs. 1). Dieses Erfordernis ist durch die Erfüllung höchster Standards zu gewährleisten;
- dem meldenden Unternehmen erlauben, die erfolgte Meldung ganz oder teilweise auch weiteren Behörden zukommen zu lassen (Art. 74f Abs. 2) und
- dem meldenden Unternehmen ermöglichen, einer solchen Zweitbehörde von ihr benötigte Zusatzinformationen zu übermitteln, die das NCSC nicht benötigt (Art. 74f Abs. 3).

Das Gesetz wird aber den Unternehmen nicht verbieten, **Meldungen dem NCSC auch auf anderen Wegen, z.B. per E-Mail oder telefonisch**, zu übermitteln (Erläuternder Bericht, S. 21).

Und das Meldesystem wird auch für **freiwillige Meldungen an weitere Behörden** zur Verfügung stehen (Erläuternder Bericht, S. 21).

2.7 Verletzungen der Meldepflicht (Art. 74h und 74i)

Übereinstimmend mit economiesuisse ersuchen wir Sie um **Streichung der Strafdrohung**, da sie nach bisherigen Erfahrungen der Branche kontraproduktive Auswirkungen hinsichtlich der Compliance haben und das initiative, eigenverantwortliche Handeln der Mitarbeitenden in den betroffenen Unternehmen lähmen könnte.

3. Abgrenzung zu bestehenden Meldepflichten anderer Gesetze

Bestehende Meldepflichten aufgrund anderer Gesetze – beispielsweise Art. 29 Abs. 2 FINMAG für die Banken und Art. 24 nDSG – sollen durch die neue Meldepflicht gemäss Art. 74a ff. (s. vorstehend 2.3–2.4) *«nicht ersetzt, sondern nur ergänzt»* werden (Erläuternder Bericht, S. 5).

> *«Dabei wurde darauf geachtet, dass die gesetzlichen Grundlagen eine gleichzeitige Erfüllung verschiedener Meldepflichten erlauben. Der Aufwand für die Erfüllung der verschiedenen Meldepflichten soll so möglichst geringgehalten werden. Dies gilt vor allem, aber nicht nur für das Verhältnis zur datenschutzrechtlichen Meldepflicht nach Artikel 24 des revidierten Datenschutzgesetzes (nachfolgend: nDSG), da es in der Praxis häufig der Fall ist, dass Cyberangriffe zu Datenverlusten führen. Die*

gewählte Lösung sieht vor, dass es den Meldenden offensteht, die Meldung des Cyberangriffs gleichzeitig mit der Übermittlung an das NCSC anderen Meldestellen weiterzuleiten, um damit anderweitige Meldepflichten zu erfüllen. Umgekehrt wird das NCSC auch Meldungen zu Cyberangriffen entgegennehmen, welche in Erfüllung einer anderweitigen Meldepflicht abgegeben wurden, sofern sie die benötigten Inhalte umfasst. Damit soll verhindert werden, dass Betroffene den gleichen Vorfall unterschiedlichen Stellen über unterschiedliche Verfahren melden müssen.»

Zur Lösung dieses richtig erkannten Problems schlagen wir vor, das Meldeformular so zu konzipieren, dass es **im Sinn einer Parallelmeldung** gleichzeitig verschiedenen Behörden (z.B. FINMA, EDÖB) zugestellt werden und ohne zusätzlichen Aufwand auch für Antworten auf Rückfragen involvierter Behörden verwendet werden kann. Mit anderen Worten muss das Formular und der dafür zu schaffende Kanal die verschiedenen durch einen Cyberangriff ausgelösten Meldepflichten abdecken (also insbesondere auch die Meldepflicht gegenüber der FINMA gemäss Art. 29 Abs. 2 FINMAG).

In jedem Fall müssen die verschiedenen Meldepflichten für die betroffenen Unternehmen konsistent ausgestaltet sein.

Gern sind wir bereit, bei der **Entwicklung** dieses Meldesystems mitzuwirken.

Als Konsequenz der einen wie der anderen Variante wäre, wie schon erwähnt, insbesondere auch die **Aufsichtsmitteilung 05/2020 der FINMA betr. Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG anzupassen**.

4. Anpassungen beim Datenschutz und Informationsaustausch mit anderen Behörden (Art. 75 ff.)

4.1 Datenschutz (Art. 73b Abs.2 Satz 2, 75 und 76), Berufsgeheimnisse

Die vorgesehenen Anpassungen beim Datenschutz verdienen **Zustimmung**.

Mit dem **Erfordernis der Einwilligung der betroffenen Person** in Art. 73b Abs. 2 Satz 2 ist dem Anliegen, dass Daten nicht oder eben nur mit Zustimmung der betroffenen Person weitergegeben werden sollen, Rechnung getragen.

Wir sind zudem der Auffassung, dass bei Meldungen im Sinn der neuen Regelung allfällige **Berufsgeheimnisse zu wahren** sind. Das betrifft insbesondere auch das Bankkundengeheimnis. Wir bitten Sie, diesem Anliegen bei der Überarbeitung des Gesetzestextes Rechnung zu tragen, beispielsweise durch die Einfügung einer expliziten Regelung.

4.2 Informationsaustausch mit anderen Behörden (Art. 76a und 77)

Wir stimmen der **Regelung über die Zusammenarbeit des NCSC mit dem Nachrichtendienst des Bundes (NDB) und den inländischen Strafverfolgungsbehörden** zu (Art. 76a).

Wir sind auch mit der Regelung für den **Informationstausch zwischen dem NCSC und ausländischen Behörden gleicher Funktion** einverstanden (Art. 77), wenn die Informationen für die Bekämpfung von Cyberrisiken und insbesondere die Zwecke dieses Gesetzes nötig sind (eine in Art. 77 Abs. 1 Satz 1 ausdrücklich vorgesehene und begrüssenswerte Einschränkung).

Sind Personendaten im Sinne von Art. 75 involviert, ist bei deren **Übermittlung ins Ausland** Art. 6 DSG zu beachten.

Wichtig ist der **Spezialitätsvorbehalt** (Art. 77 Abs. 2): Beim Informationsaustausch muss gewährleistet sein, dass die ausländische Schwesterbehörde die erhaltenen Informationen nur für den Zweck der Bekämpfung von Cyberrisiken verwendet.

Wir schlagen vor, die Regelung durch einen **Art. 76 über die Vertraulichkeit der Informationen** zu ergänzen, der z.B. wie folgt lautet:

> *«Weitergegebene Informationen sind durch die Empfängerbehörde vertraulich zu behandeln. Sie dürfen nicht weitergegeben werden, wenn dadurch die Sicherheit des betroffenen Unternehmens oder der betroffenen Personen gefährdet würde.»*

Sobald es um ein *«rechtliches Verfahren»* geht (also z.B. aufsichts- oder steuerrechtlicher Natur), kommen die **Bestimmungen über die Amts- und Rechtshilfe** zur Anwendung (Art. 77 Abs. 3).

Wir bitten Sie um die wohlwollende Prüfung unserer vorstehend geschilderten Anliegen und stehen auf Ihren Wunsch für deren gesprächsweise Erläuterung gerne zur Verfügung.

Freundliche Grüsse

August Benz
Stv. CEO
Leiter Private Banking & Asset Management

Alexandra Arni
Mitglied der Direktion
Leiterin ICT

Schweizerische Bankiervereinigung
Association suisse des banquiers
Associazione Svizzera dei Banchieri
Swiss Bankers Association

Aeschenplatz 7
Postfach 4182
CH-4002 Basel

office@sba.ch
www.swissbanking.ch

scienceINDUSTRIES
SWITZERLAND

scienceindustries
Wirtschaftsverband
Chemie Pharma Life Sciences

Nordstrasse 15
Postfach
8021 Zürich
Schweiz

T +41 44 368 17 11
F +41 44 368 17 70
info@scienceindustries.ch

Eidgenössisches Finanzdepartement
Bundesgasse 3
3003 Bern

Per E-Mail an: ncsc@gs-efd.admin.ch

Zürich, 11. April 2022

Vernehmlassung zur Einführung einer Meldepflicht für Cyberangriffe im Rahmen der Revision des Bundesgesetz über die Informationssicherheit beim Bund (ISG): Stellungnahme scienceindustries

Sehr geehrter Herr Bundesrat Maurer
Sehr geehrte Damen und Herren

Mit Schreiben vom 12. Januar haben Sie uns eingeladen, zur Einführung einer Meldepflicht für Betreiberinnen kritischer Infrastrukturen für Cyber-Angriffe Stellung zu nehmen. Wir danken Ihnen für diese Möglichkeit.

scienceindustries, der Wirtschaftsverband Chemie Pharma Life Sciences, nimmt hiermit gerne Stellung zur angedachten Meldepflicht von Cyberangriffen für Betreiberinnen kritischer Infrastrukturen. Alle diese Mitglieder sind an einem effizienten Schutz vor Cyber-Risiken interessiert. Als Branchenvertretung haben wir die verschiedenen Rückmeldungen zum Revisionsentwurf zusammengefasst und reichen diese Ihnen hiermit gerne zur Berücksichtigung ein.

Grundsätzlich ist scienceindustries der Ansicht, dass mit diesem Vorschlag die Verwaltung ihre Verantwortung an die Unternehmen auslagert und vom bisherigen, zielführenden Weg der Kooperation Abstand nimmt, indem Unternehmen lediglich als Informationslieferanten eingespannt werden. Unserem Verständnis nach muss eine primäre Aufgabe des NCSC dagegen sein, Betreibern kritischer Infrastrukturen und weiteren exponierten Industrien und Gewerben durch internationale Informationsbeschaffung und proaktiver zur Verfügungstellung relevanter Informationen bezüglich Cyber Security (Bring-Schuld NCSC) an eben diese einen möglichst hohen Stand der vorbereitenden Abwehrmassnahmen durch diese Unternehmen zu ermöglichen. Wir erachten deshalb eine Formalisierung der **Melde-Möglichkeit** als den zielführenderen Weg, sicherheitsrelevante Informationen an das NCSC weiterzureichen. Eine **Meldepflicht** mit Sanktionsandrohungen ist hingegen kaum zielführend.

Grundsätzliche Bemerkungen – Sicherheit und Prävention durch Kooperation
Wir stehen einer Meldepflicht skeptisch gegenüber und lehnen Sanktionsvorgaben gemäss vorliegendem Entwurf grundsätzlich ab. Wie im erläuternden Bericht festgehalten, funktioniert der freiwillige Informationsaustausch früher mit MELANI und heute mit dem NCSC. Im erläuternden Bericht wird erwähnt, dass eine Ausweitung des Modells nicht realistisch sei. Der Bericht bleibt aber schuldig, warum dies nicht realistisch sei. Wir teilen diese Einschätzung nicht. Wir sind im Gegenteil davon überzeugt, dass gerade der Ausbau dieses Ansatzes wesentlich zielführender ist als die Einführung einer Meldepflicht zusammen mit Sanktionsandrohungen. Aus dem Bereich der Nonproliferation kennt die Bundesverwaltung bereits seit

vielen Jahren etablierte Zusammenarbeiten mit der Industrie, die der Sensibilisierung dienen, allen voran seien hier das Programm des SECO im Bereich Exportkontrolle sowie PROPHYLAX der fedpol zu nennen. Diese Programme dienen vor allem auch dem Aufbau von Vertrauen zwischen Industrie, Verwaltung und Vollzugsbehörden, dem gegenseitigen Verständnis und der Sicherstellung, dass die Kommunikation zwischen Unternehmen und Verwaltung in beide Richtungen funktioniert. Eine Meldepflicht mit Sanktionsandrohung führt für einen solchen, auf Kooperation zwischen den Partnern angewiesenen Sicherheitsbereich zu mehr Schaden als Nutzen.

Weiter ist zu berücksichtigen, dass bei Schweizer Unternehmen, die Niederlassungen ausländischer Firmen sind, respektive ihrerseits Niederlassungen im Ausland unterhalten, die relevanten IT-Abteilungen, die zu Gunsten der ganzen Unternehmung arbeiten, häufig nicht in der Schweiz angesiedelt sind. Das hat zur Konsequenz, dass die Schweizer Unternehmensbereiche häufig gar nicht über erfolgte Cyberangriffe informiert sind. Entsprechend können sie keine Informationen weiterreichen. Dazu kommt, dass die im Ausland angesiedelten IT-Abteilungen den lokalen gesetzlichen Verpflichtungen entsprechen müssen und somit die Schweizerische Gesetzgebung nicht umsetzen müssen. Eine Meldepflicht kann also dazu führen, dass sich eine Firma also entweder dem Bruch von Datenschutzgesetzen im Sitzstaat oder der Widerhandlung gegen die Meldepflicht in der Schweiz verstösst. Dementsprechend kommt so ein Unternehmen unabhängig davon wie es sich verhält, in eine juristisch problematische Situation. Wir erachten dies als äusserst schädlich.

Sollte an einer Meldepflicht festgehalten werden, so ist für eine erfolgsversprechende Umsetzung zwingend zu berücksichtigen, dass:

- die Meldepflicht den betroffenen Unternehmen und der Volkswirtschaft letztlich mehr bringen muss, als sie kostet.
- sie einen verhältnismässigen, subsidiären, risikobasierten Ansatz verfolgen muss, der administrative und finanzielle Aufwände auf ein Minimum reduziert.
- sie einer kooperativen Grundeinstellung bedarf, da sowohl die Behörden als auch die Unternehmen an einem bestmöglichen Schutz vor Cyber-Angriffen interessiert sind.
- aus dem vorstehenden Argument bei der Durchsetzung der neu angedachten Pflichten prinzipiell auf Strafbestimmungen verzichtet wird.

Es muss überdies sichergestellt werden, dass Überschneidungen mit anderen, sektoriellen Meldepflichten im Bereich Cyber-Sicherheit nicht zu einem Mehraufwand für die Unternehmen führen.

Bemerkungen zu den Artikeln

2. Abschnitt: Pflicht zur Meldung von Cyberangriffen auf kritische Infrastrukturen

---

Art. 74a Meldepflicht

> Die Betreiberinnen von kritischen Infrastrukturen ~~müssen~~ melden dem NCSC Cyberangriffe nach deren Entdeckung so rasch als möglich ~~melden~~, damit das NCSC Angriffsmuster frühzeitig erkennen, mögliche Betroffene warnen und ihnen geeignete Präventions- und Abwehrmassnahmen empfehlen kann.

Wir beantragen die obenstehende, gelb markierte Anpassung des Textes. Ausserdem ist zu definieren, was unter dem Begriff "so rasch als möglich" zu verstehen ist.

Begründung
Die Formulierung "so rasch als möglich" ist unpräzise. Beispiel: Alle Veterinärfirmen sind kleine KMUs mit max. 20-40 Mitarbeitern, selbst im Fall der Tochterfirmen grösserer pharmazeutischer Unternehmen. Im Falle einer Cyberattacke werden die internen Ressourcen extrem gefordert sein. Oberste Priorität hat dann die Lösung des Problems und die Eindämmung des möglichen Schadens. Die Meldung an das NCSC wird in dieser Phase wahrscheinlich nicht die oberste Priorität haben, weshalb hier auch ein Augenmass mit Bezug auf die zeitliche Abwicklung von Meldungen angezeigt ist. Offenbar ist diesbezüglich eigenes Ermessen vorgesehen, dazu gibt es allerdings im Gesetz keine präzisen Angaben, an welchen sich Unternehmen orientieren könnten, was insbesondere dann eine nicht mehr akzeptable Verzögerung bedeuten würde.

Art. 74b Bereiche

Die Meldepflicht gilt für

…

i. Unternehmen, die für die Herstellung, das Inverkehrbringen und die Einfuhr von Arzneimitteln eine Bewilligung nach dem Heilmittelgesetz vom 15. Dezember 200012 (HMG) haben oder Medizinprodukte nach Artikel 4 Absatz 1 Buchstabe b HMG herstellen oder vertreiben;

…

r. Unternehmen, die die Bevölkerung mit unentbehrlichen Gütern des täglichen Bedarfs versorgen;

Wir beantragen eine exakte Definition und unternehmensspezifische Bezeichnung der Betriebe, die unter die Definition fallen, wenn nicht hier direkt im Gesetz, was für uns nachvollziehbar ist, so doch auf Stufen einer Ausführungsverordnung, auf die hier explizit zu verweisen ist.

Begründung:
In Anbetracht der Unklarheit darüber, was als kritische Infrastruktur zu betrachten ist, ist nicht klar, wer durch eine Meldepflicht letztlich erfasst würde. Der Bund hat verschiedene Publikationen mit unterschiedlichen Definitionen, was kritische Infrastrukturen letztlich umfasst. Aus unserer Sicht es es unzumutbar, , dass nun unzählige Unternehmen diese unterschiedliche Publikationen studieren und abwägen müssen, ob sie unter die jeweilige Definition fallen oder nicht. Wir stellen hier klar eine Rechtsunsicherheit fest. Gerade die Corona-Pandemie hat exemplarisch aufgezeigt, dass unter dem Begriff "untentbehrliche Güter des täglichen Bedarfs" schon innerhalb der Bevölkerung kaum ein Konsens besteht und sehr unterschiedlich interpretiert wird. Die Bereitstellung unentbehrlicher Güter des täglichen Bedarfs für die Bevölkerung ist aufgrund internationaler Lieferketten komplexer, als das Politik und Verwaltung annehmen. Denn hinter der Bereitstellung dieser Produkte für die Bevölkerung stehen Produktions- und Lieferketten, die auf den ersten Blick nicht kritisch erscheinen, aber bei Ausfall die Bereitstellung dennoch be- oder sogar verhindern.

Art. 74d Zu meldende Cyberangriffe

1 Ein Cyberangriff auf eine kritische Infrastruktur muss gemeldet werden, wenn Anzeichen dafür bestehen, dass:

…

~~b. ein fremder Staat ihn ausgeführt oder veranlasst hat;~~

…

2 Ein Cyberangriff auf eine kritische Infrastruktur muss immer gemeldet werden, wenn er mit Erpressung, Drohung oder Nötigung gegenüber der Betreiberin einer kritischen Infrastruktur oder ihren Mitarbeitenden verbunden ist.

Wir beantragen die Klärung der Frage der Reichweite der Pflicht. Die Meldepflicht muss auf Angriffe auf Anlagen in der Schweiz beschränkt sein. Ausländische Standorte, selbst wenn kritisch für die Versorgung in der Schweiz, unterstehen nicht dem Schweizer Gesetz.
Art. 74d. Abs. 1.b. ist ersatzlos zu streichen.
Art. 74d. Abs. 2. Die Meldepflicht ist auf Erpressung, Drohung oder Nötigung dahingehend zu beschränken, dass sie nur bei Vorliegen eines Bezuges zur Geschäftstätigkeit wirksam wird.

Begründung
Viele unserer Mitglieder sind Tochterunternehmen ausländischer Firmen, respektive sind Schweizer Unternehmen mit Tochterfirmen im Ausland. Viele von ihnen sind dadurch bereits heute nicht nur exponiert, sondern sehen sich ständig mit Cyber-kriminellen Aktionen konfrontiert. Das geht je nach Unternehmen in Grössenordnungen von einigen Hundert Attacken pro Tag, wovon die meisten bereits durch einfache Sicherheitsmassnahmen wie eine gute Firewall bewältigen lassen. Aber nicht in jedem Fall ist klar, wo ein Angriff seinen Ursprung hat.

Art. 74d. Abs. 1.b. ist deshalb ersatzlos zu streichen, da eine derartige Zuweisung fast nie, und wenn, dann nicht zeitgerecht erfolgen kann.

Art. 74e Inhalt der Meldung

1 Die Meldung muss Informationen zur kritischen Infrastruktur, zur Art und Ausführung des Cyberangriffs, zu seinen Auswirkungen und zum geplanten weiteren Vorgehen der Betreiberin der kritischen Infrastruktur enthalten.

Wir beantragen, dass sich die Meldepflicht auf die Bereitstellung sogenannter IOCs (Indicator of Compromises) fokussiert. Ausserdem ist zu berücksichtigen, dass seitens des NCSC davon ausgegangen werden muss, dass die verschiedenen Unternehmen sich in unterschiedlichsten Stadien der Abwehrbereitschaft sowie Informationslieferfähigkeiten befinden.

Art. 74e Inhalt der Meldung

3 Benötigt eine Stelle oder Behörde Informationen, die über Art. 74e hinausgehen, kann die Betreiberin diese über das System direkt an die betreffende Stelle oder Behörde übermitteln.

Und

Art. 74g Auskunftspflicht

Die Betreiberin der kritischen Infrastruktur ~~muss~~ erteilt, wenn möglich, dem NCSC ergänzende Auskünfte zu den Inhalten der Meldung nach Artikel 74e ~~erteilen~~, die es zur Erfüllung seiner Aufgaben in Bezug auf die Abwehr weiterer Cyberangriffe auf kritische Infrastrukturen benötigt.

Wir beantragen die obenstehende, gelb markierte Anpassung des Textes. Ausserdem ist zu definieren, welche Art der Informationen damit gemeint ist und wie die Begründung für solche zusätzlichen Informationsbegehren auszusehen hat.

Begründung:
Ein betroffenes Unternehmen kann Informationen nur zugänglich machen, wenn dies in seinen Fähigkeiten liegt. Allerdings sind die Spielregeln klar zu definieren, welche Informationen das NCSC noch zusätzlich einzuholen überhaupt berechtigt ist. Insbesondere bei multinationalen Firmen, bei denen für deren ausländischen Firmensitze auch ausländisches Recht tangiert wird, muss seitens des Schweizer Gesetzgebers hier ein Höchstmass an Genauigkeit und Transparenz geschaffen werden, wenn in einem Eintretensfall nicht Zeit durch nachträglich notwendig werdende juristische Abklärungen verloren gehen soll.

Art. 74h Verletzung der Melde- oder Auskunftspflicht

Und

Art. 74i Widerhandlungen gegen Verfügungen des NCSC

Wir beantragen die ersatzlos zu Streichung von Art. 74h und Art 74i.
Eventualiter ist eine Busse auf ein Prozentsatz des Ertrages, jedoch maximal CHF 100'000 zu beschränken.

Begründung
Durch die Formulierungen von Art. 74h und 74i wird bei den Unternehmen unweigerlich ein Fokus auf die Beherrschung der möglichen juristischen Risiken bezüglich Meldung von Cyberangriffen gelegt werden. Damit werden unnötigerweise in einem Bereich, bei dem gleichgerichtete Interessen bestehen und es keinerlei Sanktionsgründe gibt, Ressourcen für die Absicherung gegen die Sanktionsrisiken gebunden, die dadurch einer wirksamen Abwehr und Bewältigung ebensolcher Cyberrisiken entzogen werden.

Darüber hinaus wird durch die Höhe der angesetzten Maximalbussen neben dem potenziell existenzbedrohenden Cyberrisiko auch noch administrativ eine existenzielle Gefahr durch übertrieben hohe Bussandrohung geschaffen.
Eine Busse von CHF 100'000 ist speziell für kleine und mittlere Unternehmen unzumutbar und unverhältnismässig.

3. Abschnitt: Datenschutz und Informationsaustausch

Art. 75 Bearbeitung von Personendaten

Hier ist zu berücksichtigen, dass bei Ereignissen, die Personen ausserhalb der Schweiz (mit-)betreffen, die Weitergabe persönlicher Daten Konflikte mit der Datenschutzgesetzgebung in deren Jurisdiktion hervorrufen können.

Art. 76 Zusammenarbeit im Inland

Absätze 1 und 2
Scienceindustries steht der Weitergabe von vertraulichen Daten, insbesondere auch Personendaten, kritisch gegenüber.
Zumindest ist in den Absätzen 1 und 2 einschränkend vorzusehen, dass die Weitergabe solcher Informationen, speziell an Wettbewerber in ähnlichen Märkten nicht ohne Zustimmung des Dateninhabers erfolgen darf.

Art. 77 Internationale Zusammenarbeit

Scienceindustries steht der Weitergabe von vertraulichen Daten, insbesondere auch Personendaten, kritisch gegenüber.
Zumindest ist mit Gültigkeit für die Absätze 1, 2 und 3 einschränkend vorzusehen, dass die Weitergabe solcher Informationen nicht ohne Zustimmung des Dateninhabers erfolgen darf.

Abschliessend bedanken wir uns im Namen unserer Mitglieder für die Möglichkeit der Mitwirkung.

Wir stehen Ihnen bei allfälligen Fragen zu unserer Stellungnahme gerne zur Verfügung.

Mit freundlichen Grüssen

Dr. Michael Matthes
Stv. Direktor

Dominique Werner
Leiter Chemikalienrecht

SGB | USS
www.sgb.ch | www.uss.ch
Schweizerischer Gewerkschaftsbund
Union syndicale suisse
Unione sindacale svizzera

Eidgenössisches Finanzdepartement EFD
Herr Bundesrat Ueli Maurer
3003 Bern

per Mail an:
ncsc@gs-efd.admin.ch

Bern, 30. März 2022

Vernehmlassung zur Einführung einer Meldepflicht von BetreiberInnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrter Herr Bundesrat

Besten Dank für die Einladung zur oben erwähnten Vernehmlassung.

Der SGB begrüsst die Einführung einer Meldepflicht für Angriffe auf die Informationstechnik kritischer Infrastrukturen. Die vorgeschlagenen Änderungen des Informationssicherheitsgesetzes erscheinen uns bezüglich der notwendigerweise breit gewählten Definition der kritischen Infrastrukturen – darunter sollen nicht nur die Behörden sämtlicher Staatsebenen sowie öffentlich-rechtliche Unternehmungen fallen, sondern auch sämtliche Unternehmen fundamentaler Versorgungsbereiche – als sehr sinnvoll. Auch die vorgesehene Durchsetzung der Meldepflicht mittels "Zuckerbrot" (technische Einschätzung und Unterstützung durch das NCSC bei der Bewältigung eines erfolgten Angriffs auf die Informationstechnik) und "Peitsche" (mögliche Bussen im Fall einer Missachtung der Meldepflicht) ist zielführend ausgestaltet.

Wir teilen selbstredend die Einschätzung, dass die Einführung dieser Meldepflicht nur ein kleines Element einer dringend nötigen Offensive zur allgemeinen Erhöhung der IKT-Resilienz ist. Die Schweiz steht heute im internationalen Vergleich bezüglich Informationssicherheit sehr schlecht da: im aktuellen "Global Cyber Security Index" der Internationalen Fernmeldeunion rangiert sie unter 182 bewerteten Nationen gerade mal auf Platz 42. Dies ist auch aufgrund ihrer gleichzeitig starken Exponiertheit – man denke beispielsweise an das Zuger "Krypto-Valley" oder das kürzlich in die Schlagzeilen gekommene Swift-Rechenzentrum im Kanton Thurgau – umso besorgniserregender.

Für die Berücksichtigung unserer Stellungnahme danken wir Ihnen im Voraus herzlich.

Freundliche Grüsse

SCHWEIZERISCHER GEWERKSCHAFTSBUND

Pierre-Yves Maillard
Präsident

Reto Wyss
Zentralsekretär

Monbijoustrasse 61, 3007 Bern, www.sgb.ch
031 377 01 01, Fax 031 377 01 02, info@sgb.ch
123 RW/vf

Dachorganisation der Schweizer KMU
Organisation faîtière des PME suisses
Organizzazione mantello delle PMI svizzere
Umbrella organization of Swiss SME

Département fédéral des finances
Bundesgasse 3
3003 Berne

ncsc@gs-efd.admin.ch

Berne, le 30 mars 2022 usam-MH/cp

Réponse à la consultation
Obligation de signaler les cyberattaques contre des infrastructures critiques

Monsieur le Conseiller fédéral Maurer,
Madame, Monsieur,

Plus grande organisation faîtière de l'économie suisse, l'Union suisse des arts et métiers usam représente plus de 230 associations et quelque 500 000 PME, soit 99,8% des entreprises de notre pays. La plus grande organisation faîtière de l'économie suisse s'engage sans répit pour l'aménagement d'un environnement économique et politique favorable au développement des petites et moyennes entreprises.

L'usam est d'avis que des mesures rapides et efficaces sont nécessaires pour réduire les multiplications des cyberattaques notamment contre les infrastructures critiques, mais aussi contre les PME. Après une cyberattaque leur existence est menacée. Raison pour laquelle l'usam ne s'oppose pas à soutenir la possibilité de signaler des cyberattaques contre des infrastructures critiques. L'avant-projet manque toutefois de clarté pour la définition des domaines concernés sous l'expression « infrastructures critiques ».

I. Point de situation

Les cyberattaques sur les PME représentent un thème important pour l'usam. Les PME devraient également avoir la liberté d'annoncer les cyberattaques auprès du centre national pour la cybersécurité de la Confédération et d'être prises en considération. De fait, la Confédération pourrait mieux estimer l'étendue du problème et proposer des solutions et des campagnes de sensibilisation pour assurer la sécurité sur les réseaux Internet.

La numérisation progresse rapidement et des processus entiers sont aujourd'hui numérisés. Si une cyberattaque se produit et que les données ne peuvent pas être récupérées, l'existence d'une PME peut être menacée. C'est pourquoi la possibilité d'annonce est nécessaire, également dans l'optique de l'exigence selon laquelle d'autres PME doivent être informées et sensibilisées aux cyberattaques. Les PME restent une cible privilégiée des cyberattaques, les effets néfastes augmenter également largement et risquent, à long terme, de péjorer l'ensemble de l'économie. Les cyberattaques sur les

infrastructures critiques sont plus évidentes, car elles touchent à des points névralgiques de notre société et économie. Il est urgent pour l'usam que la Confédération veille tout particulièrement à instaurer des mesures de protections et de préventions des infrastructures critiques et des PME.

II. Appréciation générale

L'usam est d'avis que pour travailler raisonnablement et efficacement avec l'économie privée, il faudrait instaurer une coopération entre les autorités publiques et les entreprises privées représentant ou comportant des infrastructures critiques. Il n'y a aucune raison d'imposer une obligation de plus aux entreprises. Celles-ci sont responsables de leurs affaires et savent parfaitement à quel moment demander de l'aide aux autorités publiques en cas de cyberattaque. La coopération est importante pour que cet outil de détection précoce puisse fonctionner au niveau national.

La signalisation des cyberattaques contre les infrastructures critiques ne devrait également représenter aucune charge administrative inutile pour les PME. Les entreprises aimeraient y trouver un service qui peut aider dans le cas de cyberattaque et non une charge administrative supplémentaire.

L'usam demande à clarifier ce qui est sous-entendu par « infrastructures critiques ». Dans les termes présentés, il est fort probable qu'on veuille imposer une signalisation des cyberattaques à des secteurs de l'économie qui ignorent encore être concernés. La définition « infrastructures critiques » ne doit pas faire laisser planer de doutes pour les entreprises impliquées.

Autant l'obligation est exagérée, autant la menace de sanction est totalement déplacée. Les entreprises privées sont responsables de leurs affaires. Dans le domaine de la numérisation et de l'IT, la culture de l'erreur possible est indispensable pour développer de nouveaux modèles d'affaires. Raison pour laquelle, l'introduction d'une culture de la sanction dans ce domaine serait absolument contre-productive. L'usam s'oppose fermement à toute sanction ou mesure de contrainte envers l'économie privée.

Si le signalement des cyberattaques peut se faire sur une base de coopération, l'usam demande que le signalement des cyberattaques puisse se faire très simplement, de manière *user-friendly*. La signalisation de ces attaques doit être faite en ligne avec un concept clair et une procédure *user-friendly* qui soit pensée comme une procédure d'accompagnement des entreprises victimes et non comme une punition administrative.

III. Conclusion

L'usam constate que le projet impose trop de restrictions à l'économie privée. Une possibilité d'annoncer suffirait, et cela devrait aussi être ouvert aux PME. En revanche, il est hors de questions d'imposer des obligations accompagnées de sanctions dans le domaine de la signalisation des cyberattaques contre les infrastructures critiques. La Confédération devrait développer un service d'accompagnement des entreprises victimes de cyberattaques sans en faire une énième procédure administrative contraignante pour des entreprises d'ores-et-déjà fragilisées.

Nous vous remercions de l'attention portée à notre prise de position et vous présentons, Monsieur le Conseiller fédéral Maurer, Madame, Monsieur, nos respectueuses salutations.

Union suisse des arts et métiers usam

Hans-Ulrich Bigler
Directeur

Mikael Huber
Responsable du dossier

Schweizerischer Städteverband
Union des villes suisses
Unione delle città svizzere

Eidgenössisches Finanzdepartement EFD
3003 Bern

Per Mail: ncsc@gs-efd.admin.ch

Bern, 31. März 2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe
Vernehmlassung

Sehr geehrter Herr Bundesrat Maurer
Sehr geehrte Damen und Herren

Wir danken Ihnen bestens für die Gelegenheit, zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe Stellung nehmen zu können. Der Schweizerische Städteverband vertritt die Städte, städtischen Gemeinden und Agglomerationen in der Schweiz und damit gut drei Viertel der Schweizer Bevölkerung.

Allgemeine Einschätzung

Cyberangriffe und Cybersicherheit sind wichtige und hochaktuelle Themen für die Schweizer Städte. Sie befürworten die vorgesehene Einführung einer gesetzlichen Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe. Diese erlaubt eine koordinierte Aufarbeitung von Cyberangriffen als wichtiges Element in der Prävention und Abwehr solcher Ereignisse. Die Mitglieder des Städteverbands sind überzeugt, dass die Meldepflicht den Schutz der kritischen Infrastrukturen der Schweiz nachhaltig verbessern wird. Die Kompetenzen des Nationalen Zentrums für Cybersicherheit (NCSC) werden in angemessener und sinnvoller Weise erweitert.

Der Städteverband legt besonderen Wert darauf, dass die Meldung in einfacher Form erfolgen kann. Es soll kein unnötiger bürokratischer Aufwand entstehen in einer Situation, in der eine betroffene Betreiberin mit vitalen Funktionen bereits stark ausgelastet sein kann, um die Situation zu bewältigen. Die Aufarbeitung im Nachhinein scheint den Städten hingegen wesentlich, um Best Practices zu fördern und die Resilienz aller Beteiligten zu erhöhen.

Monbijoustrasse 8, Postfach, 3001 Bern
Telefon +41 31 356 32 32
info@staedteverband.ch, www.staedteverband.ch

Anmerkungen zu einzelnen Bestimmungen

Art. 73b Abs. 3 E-ISG

Eine voreilige Veröffentlichung der Schwachstelle unter Angabe der betroffenen Soft- oder Hardware könnte die meldende Instanz zusätzlich gefährden. Die Voraussetzungen einer Veröffentlichung sind zu konkretisieren.

Art. 74 Abs. 1, 2 E-ISG

Die gewählte Formulierung lässt offen, inwiefern die Städte technische Mittel zur Erkennung und Identifizierung von Cyberangriffen zwingend implementieren müssen. Ferner sollte die Frage geklärt werden, ob die genannten Hilfsmittel des NCSC von den Städten finanziert bzw. mitfinanziert werden müssen.

Art. 74b lit. b E-ISG

Die Städte sehen aufgrund des vorliegenden Entwurfs Klärungsbedarf bei der Zuständigkeit für die Meldepflicht von Gemeindebehörden. Konkret soll die Verantwortung für die Meldung in Fällen geklärt werden, in denen sowohl öffentliche Organisationen als auch externe IT-Dienstleister den Betrieb digitaler Infrastrukturen (wie z.B. Software as a Service, Plattform as a Service oder Infrastructure as a Service) verantworten.

Art. 74b lit. s E-ISG

Gemäss Entwurf soll die Meldepflicht für Hersteller von Hard- und Software gelten, deren Produkte von kritischen Infrastrukturen genutzt werden. Dies unter der Voraussetzung, dass die Hard- oder Software einen Fernwartungszugang hat oder zu einem der im Entwurf genannten Zwecke eingesetzt wird, darunter der Betrieb von Medizinprodukten oder die Gewährleistung der öffentlichen Sicherheit.

Hier stellen sich dem Städteverband Fragen der Umsetzbarkeit. Zahlreiche Hersteller von Hard- und Software sind nicht in der Schweiz ansässig. Wir gehen davon aus, dass nicht jeder Hersteller weiss, wo seine Produkte überall eingesetzt werden. Steht dann der Lieferant oder Zwischenhändler in der Pflicht und wie soll die Meldung hier erfolgen?

Art. 74d Abs. 2 E-ISG

Die abschliessend formulierte Aufzählung wirft die Frage auf, ob die Meldepflicht nicht auch dann gelten soll, wenn ein Cyberangriff mit Erpressung, Drohung oder Nötigung gegenüber *Kunden und Kundinnen oder Patienten und Patientinnen* einer Betreiberin verbunden ist.

Art. 75 E-ISG

Hier stellen sich den Städten Fragen des Datenschutzes: Fällt die in diesem Artikel beschriebene Bearbeitung von Personendaten unter die Datenbearbeitung durch einen Dritten gemäss Art. 10a DSG? Ist eine Vereinbarung über die Bearbeitung von Personendaten zwischen den Städten und dem NCSC notwendig?

Schweizerischer Städteverband
Union des villes suisses
Unione delle città svizzere

Anträge

Wir beantragen deshalb folgende Änderung:

► **Art. 74d Abs. 1 lit. d E-ISG:** Ein Cyberangriff auf eine kritische Infrastruktur muss gemeldet werden, wenn Anzeichen dafür bestehen, dass

…

d. er ~~länger als 30 Tage~~ über einen längeren Zeitraum unentdeckt blieb.

Mit der Fixierung auf 30 Tage entstünde eine terminorientierte Verpflichtung, auf ein Ereignis zu reagieren, von dem man keine Kenntnis hat und von dem man unter Umständen nicht nachvollziehen kann, wann genau es stattgefunden hat.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen.

Freundliche Grüsse

Schweizerischer Städteverband

Präsident	Direktor
	
Kurt Fluri, Nationalrat	Martin Flügel

Kopie Schweizerischer Gemeindeverband

SUISSEDIGITAL

per E-Mail an ncsc@gs-efd.admin.ch

Generalsekretariat EFD
Eidgenössisches Finanzdepartement
Manuel Suter, NCSC / Angelika Spiess, GS-EFD
Bundesgasse 3
CH-3003 Bern

Bern, 07. April 2022

Stellungnahme zur Einführung einer Meldepflicht bei Cyberangriffen

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Mit Schreiben vom 12. Januar 2022 haben Sie interessierte Kreise eingeladen, bis zum 14. April 2022 zu den geplanten Änderungen des Informationssicherheitsgesetz (nachfolgend „E-ISG") betreffend die Einführung einer Meldepflicht von Betreiberinnen kritischer Infrastrukturen bei Cyberangriffen, Stellung zu nehmen. Wir danken Ihnen für diese Möglichkeit der Meinungsäusserung, die für unsere Mitglieder und uns sehr wichtig ist, weil für Anbieterinnen von Fernmeldediensten (FDA) neu eine strafbewehrte Melde*pflicht* an das Nationale Zentrum für Cybersicherheit (NCSC) bei Cyberangriffen auf eine kritische Infrastruktur eingeführt werden soll und damit zusätzliche administrative Aufwände verursacht werden sollen. Die vorliegende Stellungnahme erfolgt innert Frist und äussert sich zu Themen, die unsere Mitglieder in ihrer Geschäftstätigkeit direkt betreffen.

SUISSEDIGITAL ist der Dachverband der Schweizer Telekommunikationsnetzunternehmen und vertritt die Interessen von ca. 180 privatrechtlich oder öffentlich-rechtlich organisierten Unternehmen verschiedener Grösse, die lokal, regional oder landesweit Telekommunikationsinfrastrukturen (Fest- und Mobilfunknetze) betreiben und darüber verschiedene Fernmelde- inklusive Radio- und Fernsehdienste erbringen. Die Bereitstellung dieser Fernmeldedienste erfolgt in arbeitsteiligen Prozessen, wobei je nach Grösse der Unternehmen in unterschiedlichem Ausmass und unterschiedlicher Organisation auf Vorleistungsprodukte von dritten Technologielieferanten zurückgegriffen wird. Unterschiedlich ausgestaltet sind deshalb auch die Diagnose- und Zugriffsmöglichkeiten der Mitglieder auf die einzelnen operativen Netzkomponenten.

1. Einleitung

Das Thema der Sicherheit von Informationen und Fernmeldeinfrastrukturen bildet bei SUISSEDIGITAL ein zentrales strategisches Verbandsthema. Wir beschäftigen uns schon seit längerem intensiv damit und begrüssen Massnahmen, welche bei Telekommunikationsinfrastrukturen zusätzliche Resilienz und Robustheit schafft. Dazu gehört auch der Informationsaustausch zu Methoden und Mustern von aktuellen Cyberattacken, welche die Errichtung eines Abwehrdispositivs und eines Frühwarnsystems ermöglichen. Wir gehen davon aus, dass

einige Mitglieder bereits auf freiwilliger Basis Informationen mit der Melde- und Analysestelle Informationssicherung Melani und nun mit dem NCSC austauschen. Die Mitglieder sind an einer guten Kooperation mit dem NCSC interessiert und anerkennen den Wert eines funktionierenden Zentrums für Cybersicherheit zur Eindämmung von Cyberbedrohungen für sie selbst, aber auch für die gesamte Wirtschaft und die Zivilgesellschaft in der Schweiz. Die Interessen der Schweizer Behörden und Unternehmen sind im Bereich der Abwehr von Cyberangriffen identisch. Wir begrüssen deshalb die gesetzliche Erfassung des NCSC im E-ISG und dessen Betrauung mit Aufgaben zum Schutze der Schweiz vor Cyberrisiken. Auch begrüssen wir die nun im Gesetzesentwurf ausdrücklich vorgesehene Möglichkeit der technischen Unterstützung und Erstanalyse im konkreten Einzelfall durch das NCSC als erste Hilfe bei der Bewältigung eines Angriffs aus dem Cyberraum. Gerade für kleinere Unternehmen kann dies sehr hilfreich sein und wir unterstützen diese Anpassungen des Gesetzes (vgl. Art. 73a, 73b Abs. 1 und 74 E-ISG).

Soll nun aber neu, wie im Revisionsentwurf zum Informationssicherheitsgesetz (E-ISG) vorgesehen, eine *Pflicht* zur Meldung von Cyberangriffen eingeführt werden, welche bei Missachtung sogar zu einer strafrechtlichen Verurteilung der im Unternehmen zuständigen Person führen kann, was wir ablehnen, müsste im Gesetz klar bezeichnet werden, welche Unternehmen in der kommunikationstechnischen Lieferkette unter dieses Obligatorium fallen und wann eine Meldung zwingend an das NCSC zu machen ist. Diesem Anspruch wird der Gesetzesentwurf noch nicht gerecht, die persönlichen und sachlichen Merkmale der Meldepflicht sind noch zu wenig klar und eindeutig bestimmt.

Wir werden nachfolgend einige Punkte in der Vorlage ansprechen, welche unseres Erachtens noch zu wenig präzise ausgearbeitet sind. Auch wenn dazu im erläuternden Bericht u.a. auf die noch zu erlassenden Ausführungsbestimmungen der Verordnung verwiesen wird, sollte der Geltungsbereich der vorgeschlagenen Meldepflicht bereits auf Gesetzesebene genügend eingegrenzt sein. Dies folgt aus dem strafrechtlichen Bestimmtheitsgebot, welches schon in der Gesetzesgrundlage zu berücksichtigen ist, wobei diesbezüglich unerheblich ist, dass das NCSC, wie vorgesehen, vor Erlass der konkreten Meldeverfügung den vermeintlich Meldepflichtigen zuerst in einem ersten Schritt aufzuklären hat, bevor dann die «umzusetzenden Pflichten» durch das NCSC verfügt werden (vgl. Art. 74h E-ISG).

Keine Kommentare haben wir zu den Themen Änderung des Zweckartikels, Ergänzung der Begriffsdefinitionen, Bearbeitungsgrundsätze inkl. Weitergabe der Informationen und Möglichkeit der strafrechtlichen Anzeige gegen den Angreifer sowie Vorgaben zum Datenschutz und Informationsaustausch.

2. Neue Meldepflicht nach E-ISG

Adressaten der Meldepflicht

Mit Art. 74a E-ISG sollen neu Betreiberinnen von kritischen Infrastrukturen einer Melde*pflicht* bei Cyberangriffen unterstellt werden, wobei die nachfolgenden Artikel 74b – 74d E-ISG diese Meldepflicht in persönlicher und sachlicher Hinsicht eingrenzen. Laut dem erläuternden Bericht bilden Betreiberinnen kritischer Infrastrukturen, die in bestimmten Bereichen tätig sind, die Adressaten der Meldepflicht[1]. Diese Tätigkeitsbereiche sind in Art. 74b E-ISG aufgelistet, die Auflistung ist abschliessend[2], was im Gesetz so angeführt werden sollte.

Im Bereich der Informations- und Kommunikationsinfrastrukturen (Begriffsdefinition kritische Infrastrukturen gemäss Art. 5c EIG) sollen sämtliche Anbieterinnen von Fernmeldediensten nach Art. 3 lit. b Fernmeldegesetz (FMG) unter die Meldepflicht fallen (Art. 74b lit. k E-ISG). Laut erläuterndem Bericht sollen auch Over the Top

[1] Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens vom 12.01.2022, Ziff. 3.3.1, S. 10

[2] a.a.O. Ziff. 4 zu Art. 74b, S. 17: «Art. 74b listet deshalb konkret auf, für welche Unternehmen und Organisationen die Meldepflicht gelten soll.»

(OTT)-Dienste als fernmeldetechnische Übertragungen gelten mithin deren Anbieterinnen als FDA[3]. Das Bundesgericht hat jedoch im Entscheid 2C_544/2020 vom 29.04.2020 festgestellt, dass es sich bei Anbieterinnen von OTT-Diensten nicht um Anbieterinnen von Fernmeldediensten i.S. von Art. 3 lit. b FMG handelt[4]. Internetdienste, wie Skype, Threema, etc. fallen demnach entgegen der Aufzählung im erläuternden Bericht nicht unter den Begriff der Fernmeldedienste nach FMG. Sollten die Anbieterinnen dieser Dienste im E-ISG nacherfasst werden, gilt es zudem zu bedenken, dass diese Anbieterinnen oft nicht in der Schweiz domiziliert sind und damit von einer innerstaatlichen Regelung nicht erfasst wären.

Weiter gilt es anzumerken, dass das FMG laut dessen Art. 2 auch für die Übertragung von Radio- und Fernsehprogrammen gilt, soweit das BG über Radio und Fernsehen (RTVG) keine abweichenden Bestimmungen enthält. Auch reine Radio- und Fernsehanbieterinnen gelten demnach als FDA und sollten schon auf Gesetzesstufe beim Adressatenkreis der Meldepflichtigen ausgenommen werden, da es sich bei Radio- und Fernsehnetzen sicher nicht um kritische Infrastrukturen handelt.

Zusammenfassend fordern wir, dass bereits auf Gesetzesstufe der Adressatenkreis der Meldepflicht bei Informations- und Kommunikationsinfrastrukturen mit Bezug auf die Kritikalität der betriebenen Netze und Dienste präziser ausgearbeitet und abgegrenzt wird. Gewisse Kategorien von FDA können bspw. von vornherein ausgeklammert werden. Übrigens auch in anderen Bereichen drängt sich eine präzisere Abgrenzung, meist aber eine Eingrenzung auf, da die Bereiche zu weitläufig umrissen sind. So bspw. auch der Bereich der Anbieterinnen von Online-Markplätzen etc. (Art. 74b lit. f E-ISG) oder die Hersteller von Hard- und Software (Art. 74b lit. s E-ISG). Auch ist, wie oben angesprochene, die Frage des Auslandsbezugs zu klären, viele der potenziellen Adressaten gemäss Entwurf haben keinen Firmensitz in der Schweiz.

Ausnahmen

Art. 74c E-ISG sieht nun Ausnahmen vom Adressatenkreis der Meldepflicht vor, die später in den Ausführungsbestimmungen weiter bestimmt werden sollen. Diese Ausnahmen auf Gesetzesstufe sind jedoch sehr offen formuliert und lassen einen grossen Interpretationsspielraum zu. Es ist deshalb völlig unklar, welche Unternehmen schliesslich von der vorgesehenen Meldepflicht betroffen sein werden. Dies sollte jedoch bereits auf Gesetzesstufe näher konkretisiert werden; wie oben angeführt, sollten bereits auf Gesetzesstufe entweder via engerem Adressatenkreis oder präziseren Ausnahmen bestimmte Anbieterinnen ausgenommen werden.

Insgesamt und unter Berücksichtigung der noch auszuformulierenden Ausführungsbestimmungen sollten die Ausnahmen im persönlichen Geltungsbereich so präzise beschrieben und abgegrenzt sein, dass die Subsumtion nur in ganz wenigen Fällen Anlass zu Diskussionen und Abwägung im Einzelfall geben. Gerade von kleineren FDA, die Opfer eines Cyberangriffs werden, kann nicht verlangt werden, dass sie in diesen ausserordentlichen Situation noch zu prüfen haben, ob eine Meldung an das NCSC für sie obligatorisch ist. Auch kann nicht von ihnen verlangt werden, dass sie Infrastrukturkomponenten überwachen, welche sie in der kommunikationstechnischen Lieferkette nicht selbst betreuen und betreiben. Für all diese Fälle wäre u.E. vor allem auf die freiwillige Kooperation zu setzen und diese mit entsprechender Öffentlichkeits- und Aufklärungsarbeit durch das NSCS zu fördern. Kurz, im Sinne der Sache wäre eher eine grosszügig abgegrenzte Ausnahmeregelung vorzusehen und stattdessen auf die Freiwilligkeit zur Kooperation zu setzen, was sicher auch vertrauensbildender wäre, als eine strafbewehrte Meldepflicht und einen Kooperationszwang vorzusehen.

Auslöser

Auch die definierten Auslösungsfälle für die zwingende Meldung ans NCSC in Art. 74d E-ISG d.h. die sachlichen Merkmale, sind in unseren Augen zu vage beschrieben, um verlässlich im Voraus abzugrenzen zu können,

[3] a.a.O., Ziff. 4 zu Art. 74b lit. k E-ISG, S. 19
[4] BGE 2C_544/2020, Ziff. 5.5.

wann eine Meldung ans NCSC zu ergehen hat und wann nicht. Bei der Implementation des NCSC-Meldeprozesses in die Unternehmensorganisation werden aber klare Kriterien benötigt, wann eine Meldung durch die zuständige Person an das NCSC zwingend ist. Der Wortlaut von Art. 74d Abs. 1 E-ISG weist zudem darauf hin, dass im vornherein nur Angriffe auf die *kritische* Infrastruktur zu melden sind, was umgekehrt bedeutet, dass auch Unternehmen im persönlichen Geltungsbereich der Meldepflicht (Art. 74b und 74c E-ISG) nur dann einen Angriff zu melden haben, falls die kritische Infrastruktur betroffen ist, Angriffe auf andere Infrastrukturbestandteile dann hinsichtlich Meldepflicht unbeachtlich wären. Das Gesetz lässt aber offen, was *kritische* Infrastrukturen sind. Mit Blick auf das Bestimmtheitsgebot für strafrechtliche Sanktionen im Falle einer Missachtung der Meldepflicht, ist es jedoch nicht zulässig, den Begriff der «kritischen Infrastruktur» nur ansatzweise zu definieren.

Weiter kann von den betroffenen Anbieterinnen nicht verlangt werden, dass sie Nachforschungen anstellen zur Frage, ob ein Merkmal der in Art. 74d E-ISG aufgeführten Auslösungsfällen vorliegt. Wie soll bspw. abgeklärt werden, ob ein fremder Staat hinter einem Angriff steckt (Art. 74d Abs. 1 lit. b E-ISG), diese Informationen werden kaum einfach ersichtlich sein. Schliesslich sollte klargestellt werden, dass Angriffe auf Endkundinnen und Endkunden bzw. deren Endgeräte und eigene Infrastrukturbestandteile (bspw. Heimvernetzung) keine Meldepflicht auslöst. Die FDA haben nicht zwingend Kenntnis von solchen Vorfällen.

Persönliche Strafbarkeit

Wir lehnen die in Art. 74i E-ISG vorgesehene persönliche Strafbarkeit der im Unternehmen zuständigen Person bei Missachtung der mit Verfügung des NCSC bestätigten Meldepflichten als ultima ratio -Massnahme ab, eine mögliche Busse des Unternehmens in einem solchen Fall erachten wir als ausreicheichenden Anreiz für die Unternehmen, die Meldepflicht einzuhalten. Der erläuternde Bericht geht an verschiedenen Stellen auf den kollaborativen Ansatz zwischen Behörden und privaten Unternehmen und den diesbezüglichen gemeinsamen Interessen bei der Abwehr von Cyberbedrohungen ein und anerkennt das Potential eines partnerschaftlichen Verhältnisses. Das Ziel sollte also eine freiwillige vertrauensvolle Zusammenarbeit sein, welche aus Sicht der Unternehmen nützlich ist. Die Möglichkeit der strafrechtlichen Verurteilung einzelner Mitarbeiter widerspricht dieser allgemeinen Stossrichtung. Der massgebliche Fachkräfte-Stellenmarkt steht zurzeit eh schon unter Druck und eine solche Regelung würde dies nur noch verstärken, weil die Bereitschaft naturgemäss klein ist, einen Verantwortung mit persönlicher Strafbarkeit im Unternehmen zu übernehmen.

3. Meldepflichten in Ausnahmesituationen an verschiedene Behörden

Wir erachten es als problematisch, wenn in ausserordentlichen Situationen, bspw. bei Netz- und Systemausfällen, die vielleicht auch auf einen Cyberangriff zurückgehen, verschiedene Meldepflichten gegenüber Behörden erfüllt werden müssen. Denn gerade in diesen Momenten sind die Ressourcen der Unternehmen durch die interne Problemlösung gebunden und entsprechend kontraproduktiv wäre es, gleichzeitig den administrativen Aufwand der betroffenen Unternehmen in solchen Fällen zu vergrössern. So sollten die Unternehmen bspw. bei einem Sicherheitsvorfall nicht mehrere Amtsstellen informieren müssen, vielmehr sollte eine zentrale Anlaufstelle, je nach Bedarf, automatisch weitere Stellen informieren («one stop shop»). Wie dies im vorliegenden Gesetzesprojekt mit den Meldungen nach Art. 24 des revidierten Datenschutzgesetzes vorgesehen ist, sollten gleiche Abstimmungen und Harmonisierungen auch mit anderen sektoriellen Anlaufstellen vorgenommen werden. Bspw. haben FDA nach Art. 96 der Verordnung über Fernmeldedienste das BAKOM oder neu nach dem Revisionsentwurf die Nationale Alarmzentrale zu verständigen, wenn ein qualifizierter Netzausfall vorliegt. Ein solcher Netzausfall kann auch auf einen Cyberangriff zurückgehen, weshalb auch hier eine entsprechende Harmonisierung vorgenommen werden sollte.

***

Wir danken Ihnen im Voraus, dass Sie unsere Bemerkungen und Argumente in die weitere Ausarbeitung der E-FDV einbeziehen und unsere Anträge berücksichtigen. Für Fragen dazu stehen wir Ihnen jederzeit gerne zur Verfügung.

Mit freundlichen Grüssen

SUISSEDIGITAL – Verband für Kommunikationsnetze

Dr. Simon Osterwalder, Rechtsanwalt
Geschäftsführer

Stefan Flück, Fürsprecher LL.M.
Leiter Rechtsdienst

Schweizerischer Verein des Gas- und Wasserfaches SVGW
Société Suisse de l'Industrie du Gaz et des Eaux SSIGE
Società Svizzera dell'Industria del Gas e delle Acque SSIGA

Grütlistrasse 44 | Postfach | 8027 Zürich
Tel: +41 44 288 33 33 | info@svgw.ch
www.svgw.ch

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit
Schwarztorstrasse 59
CH-3003 Bern

Kontakt Martin Sager
E-Mail m.sager@svgw.ch
Telefon +41 44 288 33 47
Abteilung Direktion

Zürich, 12. April 2022

Stellungnahme des Schweizerischen Vereins des Gas- und Wasserfaches SVGW

Sehr geehrte Damen und Herren

Im Januar 2022 wurde das Vernehmlassungsverfahren zur Änderung des Bundesgesetzes über die Informationssicherheit eröffnet. Wir bedanken uns für die Möglichkeit zur Stellungnahme und für die Berücksichtigung unserer Anliegen. Der SVGW vertritt als Fachverband die Interessen von über 650 Wasserversorgern und über 100 Gas- und Fernwärmeversorgern in der Schweiz. Unsere Mitglieder versorgen mit ihren Produkten und Dienstleistungen einen Grossteil der Bevölkerung mit Wasser, Gas und Wärme.

Die in der Vernehmlassung unterbreitete Meldepflicht soll es dem Nationalen Zentrum für Cybersicherheit (NCSC) ermöglichen, eine verbesserte Übersicht über Cyberangriffe in der Schweiz zu gewinnen, Betroffene bei der Bewältigung von Angriffen zu unterstützen und alle anderen Betreiber kritischer Infrastrukturen zu warnen.

Der SVGW **begrüsst** daher die Meldepflicht bei Cyberangriffen auf kritische Infrastrukturen und wir versprechen uns mehr Transparenz sowie eine frühere und vollständigere Erkennung von Cyberangriffen. Durch die Kooperation und die Rückmeldungen des NCSC wird die Branche früher und umfassender zu aktuellen Bedrohungen informiert, womit sie sich besser gegen die Angriffe schützen und damit die Resilienz weiter verbessern kann.

Freundliche Grüsse

Schweizerischer Verein des Gas- und Wasserfaches SVGW

Martin Sager
Direktor

Rolf Meier
Vizedirektor, Bereichsleiter Wasser

ASA | SVV

Schweizerischer Versicherungsverband
Association Suisse d'Assurances
Associazione Svizzera d'Assicurazioni
Swiss Insurance Association

Eidgenössisches Finanzdepartement
Bundesgasse 3
CH-3003 Bern
Versand per E-Mail an: ncsc@gs-efd.admin.ch

Zürich, 31. März 2022

Vernehmlassung Revision Informationssicherheitsgesetz: Meldepflicht für Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Vernehmlassung zur Revision des Informationssicherheitsgesetzes (ISG). Gerne nimmt der Schweizerische Versicherungsverband SVV die Gelegenheit zur Stellungnahme wahr:

Im Rahmen der geplanten Revision soll für Betreiberinnen kritischer Infrastrukturen eine Meldepflicht für Cyberangriffe im ISG eingeführt werden. Diese neue Meldepflicht soll dazu dienen, Angriffsmuster frühzeitig zu erkennen und mögliche Betroffene zu warnen (siehe Art. 74a VE-ISG). Die Versicherungsunternehmen sind von dieser Revision direkt betroffen, da sie gemäss Vernehmlassungsentwurf als Betreiberinnen von kritischer Infrastruktur qualifiziert und der Meldepflicht des ISG unterstellt werden (siehe Art. 74a und 74b Bst. e VE-ISG).

Mit der fortschreitenden Digitalisierung sehen sich Staat und Wirtschaft zunehmend mit Cyberangriffen konfrontiert. Der SVV begrüsst deshalb das Etablieren eines diesbezüglichen Frühwarnsystems, wozu entsprechende Meldepflichten einen Beitrag leisten können. Er hat deshalb auch die einschlägigen, erst 2020 erlassenen bzw. verabschiedeten Meldepflichten gemäss Finanzmarktaufsichtsrecht sowie gemäss totalrevidierten Datenschutzgesetz unterstützt (siehe FINMA-Aufsichtsmitteilung 05/2020 Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG vom 7.5.2020 und Art. 24 nDSG vom 25.9.2020). Zumal die Assekuranz auch als Anbieter von Cyberversicherungen an Meldungen von Cybervorfällen interessiert ist, um das Risiko «Cyber» besser verstehen und kalkulieren zu können.

In Anbetracht dessen, dass die Versicherungsbranche staatlich beaufsichtigt ist und bereits einschlägigen Meldepflichten untersteht (gegenüber Aufsichtsbehörde/FINMA sowie künftig auch EDÖB), erachtet der SVV für einen Einbezug der Versicherungsbranche in den Geltungsbereich des ISG folgende Rahmenbedingungen als zwingend:

- Der Einbezug in das ISG darf nicht in einer unübersichtlichen Dreifachregulierung von Meldepflichten münden (Finanzmarktaufsichts-, Datenschutz- und Informationssicherheitsrecht). Aktuell (Stand Vernehmlas-

Schweizerischer Versicherungsverband SVV
Conrad-Ferdinand-Meyer-Strasse 14 – Postfach – CH-8022 Zürich – Zentrale +41 44 208 28 28 – svv.ch
Franziska Streich – franziska.streich@svv.ch – Direktwahl +41 44 208 28 63

sungsentwurf ISG) beinhaltet der Einbezug in das ISG für die Assekuranz ein nicht harmonisiertes Nebeneinander von Meldepflichten gegenüber verschiedenen Behörden (FINMA, EDÖB, NCSC), zumal diese bezüglich zu meldender Vorfälle, Inhalt, Meldefrist und Sanktionierung stark divergieren. Die neu vorgesehene ISG-Meldepflicht belastet so Versicherungsunternehmen zusätzlich im Falle eines Cyberangriffes im kritischsten Moment und blockiert in den betroffenen Unternehmen Ressourcen, die besser zur Bewältigung des Cybervorfalls investiert werden.

- Die Meldepflicht für Cyberangriffe sollte deshalb für Versicherungsunternehmen an sämtliche Stellen (FINMA, EDÖB, NCSC) mit einer Meldung erfolgen können (One-Stop-Shop-Ansatz für alle Meldepflichten), um so den Meldeaufwand für die Unternehmen in der ausserordentlich schwierigen Situation eines Cyberangriffs in Grenzen zu halten und die Unternehmen nicht mit drei verschiedenen Meldeverfahren zu belasten.
- Aus Sicht des SVV ist der Bund hier in der Pflicht, eine optimale Koordination bezüglich der Meldestelle, zu meldender Vorfälle, Inhalt und Meldefrist sicherzustellen, damit statt der verschiedenen staatlichen Meldestellen und Regulierungen eine einzige Anlaufstelle und eine harmonisierte Meldepflicht geschaffen wird. Diesem Anliegen wird der Vernehmlassungsentwurf nicht gerecht und ist daher entsprechend nachzubessern.
- Es ist von Strafbestimmungen abzusehen. Der SVV erkennt keinen Sinn darin, die Meldepflicht gemäss ISG mit Strafbestimmungen durchzusetzen und lehnt diese ab. Für betroffene Unternehmen darf eine ausserordentlich schwierige Situation eines Cyberangriffs nicht noch unnötig mit einer Strafdrohung belastet werden.

Im Übrigen verweisen wir auch auf die Stellungnahme von economiesuisse, die wir unterstützen. Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme bei der weiteren Behandlung der Vorlage. Gerne stehen wir Ihnen für Rückfragen zur Verfügung.

Freundliche Grüsse
Schweizerischer Versicherungsverband SVV

Sandra Kurmann
Leiterin Ressort Rahmenbedingungen

Franziska Streich
Fachverantwortliche Recht

Swico
Lagerstrasse 33
CH-8004 Zürich

Tel. +41 44 446 90 94
www.swico.ch
info@swicorecycling.ch

Herr Bundesrat Ueli Maurer
Eidgenössisches Finanzdepartement EFD
Geschäftsstelle Nationales Zentrum für
Cybersicherheit NCSC

Ausschliesslich per E-Mail an:
ncsc@gs-efd.admin.ch

Zürich, 13. April 2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrter Herr Bundesrat Maurer
Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit, zu oben genanntem Geschäft Stellung zu beziehen und nehmen diese gerne innerhalb der angesetzten Frist wahr.

Swico ist der Wirtschaftsverband der Digitalisierer und vertritt die Interessen etablierter Unternehmen sowie auch Start-ups in Politik, Wirtschaft und Gesellschaft. Swico zählt über 700 Mitglieder aus der ICT- und Online-Branche. Diese Unternehmen beschäftigen 56'000 Mitarbeitende und erwirtschaften jährlich einen Umsatz von 40 Milliarden Franken. Neben Interessenvertretung betreibt Swico das nationale Rücknahmesystem «Swico Recycling» für Elektronik-Altgeräte. Mit unserer Interessengruppe Information Security verfügen wir über ein Fachgremium mit besonders einschlägigen Kenntnissen, das wir vorliegend einbezogen haben.

Aus Sicht von Swico ist eine Meldepflicht im Kontext der kritischen Infrastruktur grundsätzlich zu begrüssen, sofern sie gewisse Voraussetzungen erfüllt. So soll diese mit Augenmass umgesetzt werden und für die betroffenen Unternehmen einen deutlichen Mehrwert bringen. Besonders wichtig sind eine klare Definition des Betroffenenkreises, sowie die Berücksichtigung von bereits bestehenden Meldepflichten.

1 Übergeordnete Bemerkungen

1.1 Definition des Betroffenenkreises

Die im Gesetzesentwurf erwähnten Branchen und Bereiche lassen auf einen sehr umfassenden Geltungsbereich schliessen. Das führt zu einer grossen Verunsicherung im Kreis unserer Mitglieder, ob sie von der Meldepflicht erfasst sind. Es braucht Klarheit darüber,

welche Akteure unter die Meldepflicht fallen. Für detaillierte Bemerkungen hierzu verweisen wir gerne auf die Ausführungen in Art. 74b E-ISG weiter hinten.

1.2 Kosten-Nutzen Verhältnis

Die Meldepflicht muss den betroffenen Unternehmen und der Gesamtwirtschaft einen messbaren Mehrwert bringen. Die Meldepflicht ist deshalb mit Augenmass umzusetzen und soll sich auf schwerwiegende Cybervorfälle fokussieren. Sie muss einen risikobasierten Ansatz verfolgen, der administrative und finanzielle Aufwände auf ein Minimum reduziert.

1.3 Andere, bestehende Meldepflichten

Es bestehen bereits zahlreiche Meldepflichten im Bereich Cybersicherheit oder weiteren Bereichen. Es erscheint uns deshalb wichtig, etablierte Instrumente nicht zu schwächen, sondern eine Angleichung anzustreben. In den nachfolgenden Ausführungen werden diese Meldepflichten und deren Verhältnis zum E-ISG an spezifischen Stellen vermerkt, weshalb wir für detaillierte Ausführungen gerne darauf verweisen (s. Art. 74a, 74b, 74e, 74f und 76 E-ISG).

2 Detailbemerkungen

- *Art. 1 Abs. 1 lit. b E-ISG, Zweck*

Im neuen lit. b wird als Zweck des Gesetzes die Erhöhung der Widerstandsfähigkeit der Schweiz gegenüber Cyberrisiken festgehalten. Wie bereits einleitend genannt, fehlt es jedoch vielfach an definitorischen Rahmenbedingungen. So ist auch an dieser Stelle unklar, was die offizielle Definition von «Cyber» und «Cyberrisko» ist. Wir befürworten deshalb eine Anlehnung dieser Begrifflichkeiten an die Verordnung über den Schutz vor Cyberrisiken der Bundesverwaltung (CyRV).

- *Art. 5 lit. d-e E-ISG, Begriffe*

In lit. e wird der Begriff «Cyberangriff» definiert als Cybervorfall, der von Unbefugten absichtlich ausgelöst wurde. Dabei muss präzisiert werden, ob es sich bei den «Unbefugten» um Interne, Externe oder beides handelt.

Die im Art. 5 E-ISG vorgenommene Differenzierung zwischen Schwachstelle, Cybervorfall (lit. d) und Cyberangriff (lit. e) ist sinnvoll, da dies die Motivation für Meldepflichtige erhöhen könnte, indem nicht jeder Vorfall absolut gemeldet werden muss, sondern nur der Cyberangriff auf kritische Infrastrukturen meldepflichtig ist (während Cybervorfälle und Schwachstellen freiwillig von jeder Person gemeldet werden können). Diese Klarstellung ist wichtig, da im Gegensatz hierzu gemäss CyRV Bundes-intern Schwachstellen und Cybervorfälle gemeldet werden müssen.

Jedoch ist die vorgeschlagene Definition von «Cybervorfall» in der bestehenden Form kaum anwendbar, weil sie mit der blossen – auch theoretischen – Möglichkeit der Beeinträchtigung der Schutzziele operiert. Eine blosse Möglichkeit kann in der Praxis nicht ausgeschlossen werden. Eine Lösungsoption ist, den Begriff an Art. 4 Ziff. 7 NIS-Richtlinie anzulehnen. Diese definiert einen Sicherheitsvorfall als «alle Ereignisse, die tatsächlich eine nachteilige Auswirkung auf die Sicherheit von Netz- und Informationssystemen haben». Die Anpassung könnte vorliegend somit lauten:

Art. 5 lit. d E-ISG

«Cybervorfall: Ereignis beim Betrieb von Informatikmitteln, das tatsächlich dazu führt, dass…»

- *5. Kapitel: Massnahmen des Bundes zum Schutz der Schweiz vor Cyberrisiken (Änderung Gliederungstitel)*

Eine Regelung der Aufgaben des NCSC auf Stufe Gesetz ist zu begrüssen, insbesondere mit ausgebauten Fähigkeiten im Bereich Schwachstellenmanagement (Anerkennung als «CVE Numbering Authority» durch MITRE).

- *73b E-ISG, Bearbeitung von Meldungen zu Cybervorfällen und Schwachstellen*

Diese Bestimmung präzisiert, dass das NCSC als Anlaufstelle für Cyberrisiken (gemäss Art. 12 Abs. 1 lit. a CyRV) neben Meldungen zu Cybervorfällen auch solche zu Schwachstellen entgegennimmt. Abs. 3 dieses Artikels hält fest, dass das NCSC bei Meldung einer Schwachstelle umgehend den Hersteller informiert und ihm eine angemessene Frist zwecks Behebung setzt. Behebt der Hersteller die Schwachstelle nicht innert dieser Frist, so kann das NCSC die Schwachstelle unter Angabe der betroffenen Soft- oder Hardware veröffentlichen, sofern dies zielführend ist. Gemäss vorgeschlagenem Gesetzeswortlaut könnten unter den Begriff «Hersteller von Hard- und Software» auch Anbieter von SaaS- und Cloud-Lösungen fallen. Dies ist jedoch systematisch und inhaltlich unrichtig, weil die Meldepflicht der Cloudbetreiber in Art. 74b lit. f E-ISG richtigerweise separat geregelt wird. Der Klarheit halber sollte deshalb ausdrücklich festgehalten werden, dass der Begriff «Hersteller von Hard- und Software» im ISG jeweils nur Hersteller umfasst, deren Produkte der Kunde auf eigener Infrastruktur betreibt. Dafür bieten sich die Erläuterungen oder auch der Vernehmlassungsbericht an.

- *Art. 73c E-ISG, Weiterleitung von Informationen (neu)*

Dieser Artikel definiert in Abs. 1 und 2 die Voraussetzungen, unter welchen es dem NCSC erlaubt ist, gewisse Informationen, die in einer Meldung enthalten sind, an den NDB oder die Strafverfolgungsbehörden weiterzuleiten. Diese neu vorgesehene Möglichkeit dürfte zu Widerstand und Kritik auf Betroffenenseite führen, weshalb ein besonderes Augenmerk auf die künftige Auslegung zu richten ist. Für die Betroffenen könnte eine solche Weitergabe namentlich öffentliche Berichterstattung, Strafverfolgung oder Monitoring durch den NDB nach sich ziehen. Aus diesem Grund sind wir der Ansicht, dass die Weitergabe der Information neutral auszugestalten ist (d.h. ohne Möglichkeit des Rückschlusses auf eine bestimmte Organisation). Ist dies nicht möglich, so sollte zwingend das Einverständnis der betroffenen Organisation eingeholt werden, sofern keine anderen, gesetzlichen Bestimmungen eine zu einer Weitergabe verpflichten. Dies gilt auch für die Voraussetzung der Weiterleitung von Informationen über strafrechtlich geschützte Geheimnisse gemäss Abs. 4 dieser Bestimmung.

- *Art. 74 E-ISG, Unterstützung von Betreiberinnen von kritischen Infrastrukturen beim Schutz vor Cyberrisiken*

Ergänzend zu seinen allgemeinen Aufgaben erbringt das NCSC gemäss dieser Bestimmung weitergehende Leistungen. Abs. 3 sieht die Unterstützung von Betreiberinnen kritischer Infrastrukturen mit technischer Beratung vor. In der Botschaft wird die Subsidiarität dieser Massnahme zu privaten IT-Dienstleistungen, die auf dem Markt sind, genannt. Zusätzlich soll diese Unterstützung durch das NCSC nur erfolgen, wenn sie zeitkritisch ist und ein erheblicher Schaden droht. Dies birgt das Risiko, dass Betreiberinnen auf Eigenleistungen verzichten und sich im Ernstfall auf das NCSC abstützen, um kostspielige Prävention einzusparen. Eine angemessene Lösung für dieses Problem könnte der Verweis durch das NCSC auf bestehende Best Practice sein, verbunden mit unverbindlichen Umsetzungsempfehlungen, die sich

wiederum auf einen bestimmten Umsetzungsgrad beziehen. Dies bringt jedoch gleichzeitig die Gefahr mit sich, dass das NCSC sich in Bezug auf den angeratenen Umsetzungsgrad haftbar macht. Deshalb erscheint schliesslich ein Verweis auf die zahlreichen, vorhandenen Best Practice mit dem Vermerk, dass diese angemessen umgesetzt werden sollen, als sachgerechte Lösung.

- *Art. 74a E-ISG, Meldepflicht (neu)*

Dieser Artikel definiert die Meldepflicht in den Grundzügen. Es wird festgehalten, dass Betreiberinnen von kritischen Infrastrukturen im Falle von Cyberangriffen der Meldepflicht unterstellt sind und dass die Meldung «so rasch als möglich» nach Entdeckung des Angriffs dem NCSC zu berichten ist. Dabei sollte eine Meldung nur als verspätet betrachtet werden, wenn der meldepflichtige Betreiber eine mögliche Meldung unbegründet und ungerechtfertigt verzögert hat. Dadurch entsteht auch ein Gleichlauf mit anderen Meldepflichten, etwa jenen nach Art. 29 Abs. 2 FINMAG oder nach Art. 24 des revidierten Datenschutzgesetzes.

Nicht definiert wird im Gesetz, wer «Betreiber oder Betreiberin» einer kritischen Infrastruktur ist. Nach der NIS-Richtlinie ist dies die Einrichtung (d.h. diejenige juristische Person), die den vom Cyberangriff betroffenen Dienst «bereitstellt». Dies deutet darauf hin, dass «Betreiber oder Betreiberin» ist, wer einen Dienst nach aussen anbietet und i.d.R. auch als Vertragspartnerin der Dienstbezüger auftritt. Wenn eine kritische Infrastruktur arbeitsteilig betrieben wird, haben die entsprechenden juristischen Personen aber einen gewissen Ermessensspielraum bei der Bestimmung der rechtlichen Betreiberin. Dementsprechend hat eine Meldung durch eine von gegebenenfalls mehreren, beteiligten juristischen Personen zu genügen. Der Bund soll hierzu eine Formulierung wählen, die sicherstellt, dass beispielsweise Meldungen von Tochtergesellschaften auch der Muttergesellschaft zugerechnet werden.

Das Ereignis, welches die Meldeflicht auslöst, sollte an dieser Stelle der Klarstellung halber allenfalls nochmals explizit aufgenommen werden (gemäss Art. 5 lit. d E-ISG vorne). Andernfalls könnte der Anwendungsbereich der vorliegenden Bestimmung zu breit ausgelegt werden und zu «alarm fatigue» führen.

- *Art. 74b Bereiche (neu)*

Der erläuternde Bericht hält richtigerweise fest, dass die Definition kritischer Infrastrukturen nach Art. 5 (Begriffe) E-ISG zu breit gefasst ist. Art. 74b nimmt deshalb eine Konkretisierung vor, welche Unternehmen oder Organisationen als kritische Infrastruktur gelten und darum unter die Meldepflicht fallen. Dazu soll auf bestehende gesetzliche Grundlagen zurückgegriffen werden und – wo keine solchen bestehen – der betroffene Bereich möglichst genau bezeichnet werden. Die Konkretisierung des Begriffs ist aus Sicht von Swico unbedingt notwendig. Jedoch wird der vorliegende Versuch voraussichtlich zu Diskussionsbedarf führen, insbesondere auch für Bereiche, wo kein Verweis auf bestehende Gesetzesgrundlagen möglich ist. Es erscheint uns sinnvoll, eine Arbeitsgruppe oder ein Expertengremium einzusetzen, die sich dem Thema annehmen und eine Definition erarbeiten.

In lit. a bis lit. s werden einzelne Bereiche konkret genannt. Dabei behandelt lit. e Banken, Versicherungen und Finanzmarktinfrastrukturen. Der erläuternde Bericht hält fest, dass die bereits bestehende Meldepflicht für Cyberangriffe gegenüber der FINMA parallel bestehen bleibt und FINMA und NCSC sich so abgleichen werden, dass der Aufwand für die Meldepflichtigen so gering wie möglich ausfällt. Grundsätzlich ist dieses Bestreben zu begrüssen: Die Ausgestaltung hat so zu erfolgen, dass eine Meldung keinen übermässigen

Aufwand verursacht. Gleichzeitig darf hoher Aufwand ohne weitere Differenzierung nicht als generelle Abwehr gegen Meldungen angesehen werden.

Lit. s nennt Hersteller von Hard- und Software, deren Produkte von kritischen Infrastrukturen genutzt werden, sofern die Hard- oder Software einen Fernwartungszugang hat oder zu einem der in Ziff. 1-4 beschriebenen Zwecke eingesetzt wird. Ziff. 4 nennt als solchen Zweck «IT-Sicherheit, Verschlüsselung, Identifikation, Zugriffs- und Zutrittsberechtigung». Aus unserer Sicht kann insbesondere Ziff. 4 sehr breit ausgelegt werden. Es erscheint deshalb sinnvoll, Ziff. 1-4 ersatzlos zu streichen und stattdessen den Begriff des Fernwartungszugangs zu definieren, da eine klare, abschliessende Umschreibung des Einsatzzecks kaum möglich ist. Damit würde auch die Problematik des unklaren Einbezugs der Supply Chain in die Meldepflicht gelöst, da die KI-Betreiber selbst in der Verantwortung stehen würden, ihre Lieferanten je nach Einsatzzweck der Hard- und Software in die Pflicht zu nehmen.

Zum Begriff der Hard- und Software verweisen wir zudem auf die bereits gemachten Ausführungen im Rahmen von Art. 73b Abs. 3 E-ISG weiter vorne.

- *Art. 74c E-ISG, Ausnahmen von der Meldepflicht (neu)*

Lit. a bis c. dieser Bestimmung stellen Kriterien auf, um bestimmte Kategorien von Betreiberinnen kritischer Infrastrukturen von der Meldepflicht auszunehmen. Wir sind der Ansicht, dass die vorgeschlagenen Kriterien in der Praxis schwierig zu ermitteln sein werden. Deshalb schlagen wir vor, stärker auf den möglichen Einfluss eines Schadens als Kriterium abzustellen. Im Falle einer Organisation, deren Einfluss vernachlässigbar ist (bzw. der Schaden aus dem Ereignis), könnte entsprechend auf eine Meldung verzichtet werden.

Auf der anderen Seite fehlt bei den Kategorien, die zum Ausschluss führen, folgende Ergänzung:
«...
c. [neu] weil mitigierende Massnahmen solche Cyberangriffe unschädlich machen. »

- *Art. 74d E-ISG, zu meldende Cyberangriffe (neu)*

Diese Bestimmung zählt die Kriterien auf, unter denen ein Cyberangriff meldepflichtig ist, wobei die Erfüllung eines der Kriterien ausreichend ist. Der Artikel sieht keinen Hinweis auf das für eine Meldung minimal notwendige Schadenspotenzial vor und lässt vor allem in lit. c einen breiten Auslegungsspielraum offen. Der erläuternde Bericht hält in Bezug auf diese Bestimmung hingegen fest, dass die Meldepflicht nur für Cyberangriffe gelten soll, die ein gewisses Schadenspotenzial aufweisen.

Um die Meldung trivialer Vorfälle auszuschliessen, schlagen wir folgende Ergänzung vor:

«...
c. er zu einem Abfluss oder zur Manipulation von Informationen geführt hat oder führen könnte, die für die Funktionsfähigkeit der betroffenen kritischen Infrastruktur oder einer anderen kritischen Infrastruktur relevant sind; oder»

Wir stellen bei der Aufzählung in diesem Artikel zudem fest, dass ein starker Fokus auf Ransomware gelegt wird. Mit Blick auf die Zukunftssicherheit bei einer rasch verändernden Lage erscheint uns dies fraglich. Eine rasche Anpassungsmöglichkeit ist gemäss erläuterndem Bericht auf Verordnungsstufe möglich, was wir in diesem Zusammenhang als zweckdienlich erachten.

- *Art. 74e E-ISG, Inhalt der Meldung (neu)*

Dieser Artikel hält die wesentlichen Angaben, die für die Erfüllung der Meldepflicht notwendig sind, gesetzlich fest. Aus unserer Sicht fehlt dabei die Berücksichtigung des bereits heute gut etablierten Austausches von technischen Informationen (Threat Intelligence) zwischen GovCERT und den Betreibern von KI. Dieses bestehende Instrument sollte nicht gefährdet, sondern allenfalls als weiterer Kanal für die Meldung von Cyberangriffen etabliert werden.

- *Art. 74f E-ISG, Übermittlung der Meldung (neu)*

Mit dieser Bestimmung wird das NCSC verpflichtet, zwecks Erfüllung der Meldepflicht ein sicheres, elektronisches Meldeformular zur Verfügung zu stellen. Der erläuternde Bericht konkretisiert, dass es jedoch in jedem Fall weiterhin zulässig bleibt, das NCSC auf andere Weise (beispielsweise E-Mail, Telefon) über einen Cyberangriff in Kenntnis zu setzen. Vom Grundgedanken her ist es sehr begrüssenswert, wenn eine Meldung ausserhalb des Meldeformulars zugelassen wird, jedoch muss die Sicherheit des Meldevorgangs und -inhalts auf anderen Wegen gewährleistet sein. Insgesamt sollte der Meldemechanismus so frei wie möglich gestaltet werden, um beispielsweise automatische Meldungen durch RSS Feeds oder API zu erlauben oder auch via den bestehenden Austausch von Daten via das System MISP, das viele KI-Betreiber bereits im Einsatz haben.

Abs. 2 hält fest, dass das System der Betreiberin einer kritischen Infrastruktur ermöglichen muss, die Meldung an weitere Behördenstellen weiterzuleiten. Dabei ist vor allem die Kombination mit einer Meldung nach revDSG sinnvoll.

- *Art. 74i E-ISG, Widerhandlungen gegen Verfügungen des NCSC (neu)*

Gemäss dieser Bestimmung macht sich diejenige Person strafbar, die innerhalb der kritischen Infrastruktur hätte dafür sorgen müssen, dass der Verfügung des NCSC gemäss Art. 74i i.V.m. Art. 74h Abs. 2 Folge geleistet wird. Das Adressieren der Leitungsebene von Unternehmen wird gemäss erläuterndem Bericht dabei als Möglichkeit der sachgerechten Zuordnung angesehen. In Anbetracht der Unbestimmtheit der meldepflichtigen Ereignisse/ Vorfälle gemäss Ausführungen weiter vorne, stehen Bussenandrohungen in der vorgesehenen Höhe von CHF 100'000 jedoch dem Legalitätsprinzip entgegen. Zudem widerspricht das vorgesehene Vollzugsregime mit abschreckenden Anreizen der Tatsache, dass es sich bei Cybersecurity um eine Querschnittsaufgabe handelt: Den Gefahren kann nur mittels eines partnerschaftlichen und kooperativen Ansatzes zwischen Staat und Wirtschaft erfolgsversprechend begegnet werden. Wir beantragen deshalb die ersatzlose Streichung von Art. 74i (i.V.m. der notwendigen Anpassung in Art. 74h Abs. 2 E-ISG).

Eventualiter beantragen wir, die Bussenschwellen nach ISG und revDSG gleichzusetzen und von der Verfolgung von natürlichen Personen gänzlich abzusehen (mit Ausnahme von direktvorsätzlichen Fällen).

- *Art. 76 E-ISG, Zusammenarbeit im Inland*

Dieser Artikel bildet die gesetzliche Grundlage für den Informationsaustausch zwischen dem NCSC und den Betreiberinnen von kritischen Infrastrukturen (Abs. 1 und 2) sowie zwischen dem NCSC und den Fernmeldedienstanbieterinnen (Abs. 3 und 4). Wie bereits weiter vorne vermerkt, muss aus unserer Sicht unbedingt der bereits bestehende und gut etablierte Austausch von technischen Informationen (Threat Intelligence) zwischen NCSC, den Betreiberinnen und Betreibern von KI und weiteren Parteien berücksichtigt und nicht gefährdet werden. Insbesondere die international etablierten Protokolle zum Teilen von Informationen (TLP-Protokoll) sollten nicht untergraben, sondern rechtlich präziser umschrieben werden.

Wir bedanken uns bestens für die Berücksichtigung unserer Anliegen und stehen Ihnen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse
Swico

Ivette Djonova
Head Legal & Public Affairs

Andreas Knöpfli
Präsident

Eidgenössisches Finanzdepartement EFD
Herr Bundesrat
Ueli Maurer
Bundesgasse 3, 3003 Bern

Einreichung per Mail an: ncsc@gs-efd.admin.ch

Zürich, 14. April 2022

Vernehmlassung zur Revision des Informationssicherheitsgesetzes (ISG)

Stellungnahme von swissICT zur laufenden Vernehmlassung

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

swissICT bedankt sich für die Möglichkeit, an der Vernehmlassung der Regelungen zur Einführung einer Meldepflicht für Cybersecurity-Vorfälle im Rahmen der Revision des Informationssicherheitsgesetzes (ISG) teilnehmen und eine entsprechende Stellungnahme einreichen zu können.

swissICT

swissICT ist mit über 2'500 Mitgliedern der grösste Fachverband des ICT Werkplatzes Schweiz und verbindet als einziger Verband ICT-Anbieter, Anwender und Fachkräfte in der Schweiz. Der Verband sorgt sich um das Image der Schweizer ICT-Branche, setzt sich für gute Rahmenbedingungen ein und fördert den Austausch und das Fach-Know-how seiner Mitglieder.

Generelle Bemerkungen

swissICT begrüsst generell die Revision und die darin eingeschlagene Stossrichtung zur Einführung einer Meldepflicht von Cyberangriffen für Betreiber kritischer Infrastrukturen. Wir vertreten jedoch die Auffassung, dass der Vorentwurf in verschiedener Hinsicht über das Ziel hinausschiesst und für die betroffenen Unternehmen zusätzliche administrative Bürden ohne erkennbaren Nutzen schafft. Im Wesentlichen richtet sich unsere Kritik auf folgende Punkte:

- Der Kreis meldepflichtiger Betreiber kritischer Infrastrukturen wird nach unserem Dafürhalten zu weit gefasst. Einzelne Kategorien sollten weggelassen oder zumindest herabgestuft werden.
- Die im Gesetz vorgesehene Einschränkung meldepflichtiger Angriffe wird in der Praxis kaum je zum Tragen kommen. Faktisch sind nahezu alle Angriffe zu melden, was kritisch hinterfragt werden sollte.

- Die Modalitäten der Meldepflicht sind mit bestehenden Normen (z.B. Datenschutzgesetzgebung, Meldepflichten für Finanzinstitute) abzustimmen, um Widersprüche (z.B. hinsichtlich Meldefristen) zu vermeiden.
- Die umfassenden und fortdauernden Meldepflichten nehmen erhebliche Ressourcen in Anspruch, die bei einem Cyberangriff nicht für dessen zielgerichtete Abwehr eingesetzt werden können.
- Der Entwurf der Bestimmungen über die Meldepflicht enthält keine konkrete Pflicht des NCSC, Erkenntnisse der Analysen mit Betroffenen zu teilen. Dies ist im Gesetz zu ergänzen.

Spezifische Bemerkungen zu einzelnen Bestimmungen

1.1. Art. 73a E-ISG

Diese Grundsatzbestimmung zu den Aufgaben des nationalen Zentrums für Cybersicherheit (NCSC) ist ausreichend breit gefasst.

1.2. Art. 73b E-ISG

Keine Anmerkungen.

1.3. Art. 73c E-ISG

Zentral ist hier Abs. 3, wonach Informationen, die von einer Person im Rahmen einer Meldung dem NCSC bekanntgegeben wurden, in einem Strafverfahren gegen diese Person nur mit deren Einverständnis verwendet werden dürfen. Wie auch in anderen Gesetzen sind möglicherweise zur persönlichen Strafbarkeit der Verantwortlichen führende Strafbestimmungen zu vermeiden, denn sie schaden der Compliance der Unternehmen mehr, als dass sie ihr helfen würden: IT-Sicherheit ist ein Gebiet, in dem immer wieder mal Fehler passieren. Wer bei einer Meldung trotz sorgsamer Vorkehrungen in der IT-Sicherheit mit einer Strafe für Verfehlungen rechnen muss, wird meist auf eine Meldung verzichten. Obwohl der aktuelle Wortlaut des Entwurfs von Art. 73c E-ISG diesem Dilemma bereits Rechnung trägt, erscheint die folgende Präzisierung im Licht des Selbstbelastungszwangsverbots bei Cybervorfällen angebracht: *"Soweit eine Person im Rahmen einer Meldung dem NCSC möglicherweise die Person belastende Informationen mitteilt, können diese Informationen in einem Strafverfahren gegen die Person nur mit deren Einverständnis verwendet werden."*

1.4. Art. 74 E-ISG

Bemerkenswert ist hier Abs. 4, wonach das NCSC zur Analyse eines Cybervorfalls mit dem Einverständnis der betroffenen Betreiberin auf deren Informationen und Informatikmittel zugreifen kann. Das Einverständnis kann unabhängig von allfälligen Geheimhaltungspflichten gewährt werden.

Da die vorgesehene Meldepflicht offenbar sehr breit sein soll und fast die ganze Palette von Branchen im schweizerischen Wirtschaftsleben umfasst (siehe die Ausführungen unten zu Art. 74b E-ISG), ist dafür zu sorgen, dass bei einer Meldung keine Rechte Dritter gefährdet oder gar verletzt werden, d.h. das NCSC muss die Geheimhaltungsbedürfnisse Dritter schützen und entsprechende Geheimhaltungspflichten beachten.

1.5. Art. 74a E-ISG

Keine Anmerkungen.

1.6. Art. 74b E-ISG

Hier werden zahlreiche Branchen genannt – ein wesentlicher Teil des schweizerischen Wirtschaftslebens. Nicht ganz klar scheint, ob die – sehr umfangreiche – Liste der Betreiberinnen kritischer Infrastrukturen abschliessend ist

oder nicht. Der Umfang der Liste reflektiert jedenfalls die arbeitsteiligen Abläufe in der heutigen Wirtschaft. Die Meldepflicht wird zurecht auf die ganzen (Zu-)Lieferketten ausgedehnt, was in der unternehmerischen Praxis jedoch oft auf eine organisatorisch bzw. administrative Herausforderung hinauslaufen wird. Beim Anblick der Liste fragt man sich jedenfalls unweigerlich, ob bei insgesamt 19 (!) Kategorien kritischer Infrastrukturen angesichts der damit verbundenen und durchaus auch belastenden Auflagen im Bereich der Meldepflicht nicht zumindest diskutiert werden müsste, ob man eine qualitative Gewichtung in z.B. "hochkritisch" bzw. "kritisch" vornehmen und die 19 Kategorien dann in folgende zwei Gruppen einteilen könnte: "Kritische Infrastruktur der Kategorie 1" und "Kritische Infrastruktur der Kategorie 2". Die "hochkritischen" Infrastrukturen hätten dann strengere Auflagen im Zusammenhang mit der Meldepflicht zu erfüllen, als die bloss "kritischen" Infrastrukturen. In beiden Kategorien ist klar zu kommunizieren, wer wem was wie wann zu melden hat. Weiter könnte man eine Kategorisierung nach Art und Gefährdungspotential des jeweiligen Vorfalls vorsehen. Auf diese Weise liesse sich verhindern, dass weite Teile der Wirtschaft mit neuen organisatorisch-administrativen Auflagen belastet würden – insbesondere für KMU wäre dies eine willkommene Entlastung.

Was die 19 Kategorien angeht, so ist vorab lit. s bemerkenswert: Cyberangreifer manipulieren oft die Hard- und Software bereits vor der Auslieferung an die Endkunden, damit sie später Zugriff auf die Systeme erhalten. Besonders relevant sind Cyberangriffe auf Hersteller von Software, wenn diese über Fernwartungszugänge verfügen. Angreifer können versuchen, über solche legitimen Zugänge direkt in die Systeme der kritischen Infrastrukturen einzudringen. Neben dem Kriterium des Fernwartungszugangs sind Hersteller von Hard- und Software dann meldepflichtig, wenn ihre Produkte in besonders heiklen Bereichen zum Einsatz kommen. Zurecht zählt der Entwurf in diesem Zusammenhang vier relevante Gruppen auf. Es wird aber leider versäumt klarzustellen, dass die Anbieterinnen von Software as a Service (SaaS) keine kritischen Infrastrukturen betreiben, da bei diesen Dienstleistungen den Endkunden keine Software überlassen wird; vielmehr erhalten die Endkunden bloss Zugang zu den Funktionalitäten der Software.

Lit. f schliesslich definiert drei alternative Bedingungen, bei denen Anbieterinnen von Online-Marktplätzen, Cloudcomputing und weiteren digitalen Diensten unter die Meldepflicht fallen, nämlich (i) eine grosse Zahl von Nutzern, (ii) eine hohe Bedeutung für die digitale Wirtschaft, und (iii) das Anbieten von Sicherheits- und Vertrauensdiensten. Alle Bedingungen sind unklar und lassen übermässig viel Spielraum für individuelle Interpretationen. Es wäre wünschenswert, wenn entweder das Gesetz oder dann aber die Verordnung klare Definitionen aufwiesen.

1.7. Art. 74c E-ISG

Keine Anmerkungen.

1.8. Art. 74d E-ISG

Art. 74d E-ISG legt fest, welche Cyberangriffe auf kritische Infrastrukturen dem NCSC zu melden sind. Hierbei werden im ersten Absatz vier alternative Fallgruppen definiert, welche die Meldepflicht auslösen. Für den Eintritt der Meldepflicht muss sich keine dieser Fallgruppen bereits verwirklicht haben; vielmehr greift die Meldepflicht schon dann, wenn Anzeichen für das Bestehen einer dieser Fallgruppen existieren, was die Meldepflicht in ein frühes Stadium vorverlagert.

Von den vier Fallgruppen wird insbesondere die dritte Kategorie (Anzeichen, dass ein Cyberangriff "zu einem Abfluss oder zur Manipulation von Informationen geführt hat oder führen könnte") in der Praxis sehr häufig erfüllt sein, weil sich ein solcher Abfluss bzw. eine solche Manipulation innerhalb der Meldefrist ("so rasch als möglich"; vgl. Art. 74a E-ISG) kaum je mit hinreichender Sicherheit ausschliessen lässt. In Kombination mit den weiteren Fallgruppen gemäss Absatz 1 sind kaum Fälle denkbar, wo die Meldepflicht nicht zum Tragen kommt.

Sollten die Voraussetzungen von Absatz 1 im Einzelfall ausnahmsweise dennoch nicht erfüllt sein, kann eine Meldepflicht immer noch aufgrund des zweiten Absatzes bestehen, nämlich wenn der Cyberangriff "mit Erpressung, Drohung oder Nötigung gegenüber der Betreiberin einer kritischen Infrastruktur oder ihren

Mitarbeitenden verbunden ist." Erfasst werden hier also beispielsweise die klassischen und in der Realität überaus häufigen Ransomware-Attacken, bei denen ein Lösegeld für die Entschlüsselung von Daten gefordert und/oder mit der Offenlegung von Daten gedroht wird.

Im Ergebnis bleiben aufgrund der vielfältigen und offenen Kriterien für meldepflichtige Cyberangriffe eigentlich nur harmlose, nicht von einem fremden Staat ausgeführte oder veranlasste, innerhalb von längstens 30 Tagen entdeckte Angriffe ohne Abfluss oder Manipulation von Informationen und ohne erpresserische, drohende oder nötigende Elemente übrig. Solche Cyberangriffe (nicht Cybervorfälle) sind in der Realität kaum vorstellbar. Zu melden ist somit praktisch jeder Cyberangriff. Dies mag aus Sicht des mit der Meldepflicht verfolgten Zwecks (Früherkennung, Warnung, Empfehlung geeigneter Präventions- und Abwehrmassnahmen; vgl. Art. 74a E-ISG) gewollt sein, macht jedoch die vermeintliche Eingrenzung meldepflichtiger Cyberangriffe in Art. 74d E-ISG weitgehend obsolet. Auf die Bestimmung kann schmerzfrei verzichtet werden. Dies wäre auch im Einklang mit der EU NIS-Richtlinie, die ebenfalls keine solche Regelung kennt.

1.9. Art. 74e E-ISG

Gemäss Art. 74e E-ISG hat die Betreiberin einer kritischen Infrastruktur Cyberangriffe zu melden und mit der Meldung bestimmte Informationen mitzuliefern. Wie diese Informationen jedoch genau aussehen und inwiefern sie mit Anforderungen an die Angaben anderer Behörden übereinstimmen, ist (noch) nicht ersichtlich. Es ist für die betroffenen Unternehmen, Behörden oder Anstalten jedoch von hoher Bedeutung, die Anstrengungen im Bereich Cybersecurity zu bündeln und die Informationen nicht in unterschiedlicher Tiefe und Breite an verschiedene Behörden (gleichzeitig) herausgeben zu müssen. Die in Art. 74e E-ISG geforderten Informationen sollten deshalb präziser beschrieben und mit anderen Behörden (z.B. FINMA) abgestimmt werden. Betrachtet man gleichzeitig die gesetzten Fristen für die Meldepflicht (24 Stunden Meldepflicht gegenüber FINMA, so rasch als möglich Meldung gegenüber NCSC), so sollte dies harmonisiert und die Inhalte abgestimmt werden.

Die weiterzugebende Information bezüglich der nächsten Schritte kann höchstens im Sinne von «best efforts» weitergegeben werden, was im Gesetzestext aufgenommen werden sollte. Zum Zeitpunkt eines Angriffs haben die Verantwortlichen meist sehr viel zu tun und sind kaum in der Lage, vertiefte Informationen an Behörden aufzubereiten und weiterzuleiten.

1.10. Art. 74f E-ISG

Die in Art. 74f E-ISG statuierte Schnittstellenthematik zur Weiterleitung der Information nebst dem NCSC an weitere Behörden ist eine Pflicht für die Behörden, nicht die Unternehmen. Die Kompatibilität ist auf alle Fälle zu gewährleisten resp. die einfache Handhabung.

1.11. Art. 74g E-ISG

Die festgelegten Mitwirkungspflichten machen im operativen Bereich zwar Sinn, dürfen die Unternehmen und Anstalten, Behörden und Gemeinden aber in einer schwierigen Zeit noch mehr belasten. Es ist deshalb wichtig zu ergänzen, dass diese Informationen nur dann während der Krise eingeholt werden dürfen, wenn dies zwingend notwendig ist für die Sicherheit der jeweiligen Versorgung.

1.12. Art. 74i E-ISG

Art. 74i Abs. 3 sieht eine Obergrenze des voraussichtlichen Bussenbetrags vor, der es erlaubt, anstelle einer natürlichen Person den Geschäftsbetrieb zu belasten. Dieser Betrag sollte von CHF 20’000 auf CHF 50’000 erhöht werden. Der höhere Betrag erlaubt zum einen besser, unverhältnismässigen Untersuchungsaufwand in Bagatellfällen zu vermeiden. Zum anderen entsteht dadurch ein Gleichlauf mit Art. 64 Abs. 2 des revidierten Datenschutzgesetzes (revDSG). Dieser Gleichlauf erleichtert die Orientierung und ist sachlich gerechtfertigt, weil kein Grund für eine Abweichung besteht.

Ergänzend zu unseren detaillierten Rückmeldungen unterstützen wir auch die Rückmeldungen von asut, digitalswitzerland und ISSS.

Wir danken Ihnen im Namen unserer Mitglieder im Voraus dafür, dass Sie unsere Anregungen in geeigneter Weise bei der weiteren Umsetzung berücksichtigen.

Gerne stehen wir Ihnen für Rückfragen und weitere Diskussionen zur Verfügung.

Freundliche Grüsse

Kathy Riklin
Vorstand swissICT
Alt-Nationalrätin
Leiterin swissICT Politikkommission

Christian Hunziker
Geschäftsführer swissICT
Delegierter des Verwaltungsrates 3L Informatik AG

Eidgenössisches Finanzdepartement
Nationales Zentrum für Cybersicherheit NCSC

ncsc@gs-efd.admin.ch

Digitalisierung und Innovation

Robert Rudolph
Bereichsleiter

Pfingstweidstrasse 102
Postfach
CH-8037 Zürich
Tel. +41 44 384 48 44
Fax +41 44 384 48 43
www.swissmem.ch
r.rudolph@swissmem.ch

Zürich, 28. März 2022

Stellungnahme im Vernehmlassungsverfahren zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrte Damen und Herren

Wir beziehen uns auf das vom Vorsteher des Eidgenössischen Finanzdepartements EFD am 12. Januar 2022 eröffnete Vernehmlassungsverfahren zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe und nehmen die Möglichkeit der Stellungnahme gerne wahr.

Swissmem ist der führende Verband für KMU und Grossunternehmen der schweizerischen Maschinen-, Elektro- und Metall-Industrie (MEM-Industrie) und verwandter technologieorientierter Branchen. Swissmem fördert die nationale und die internationale Wettbewerbsfähigkeit ihrer 1'250 Mitgliedsfirmen durch eine wirkungsvolle Interessenvertretung, bedarfsgerechte Dienstleistungen, eine gezielte Vernetzung sowie eine arbeitsmarktgerechte Aus- und Weiterbildung der Mitarbeiterinnen und Mitarbeiter der MEM-Industrie.

Die Schweizer MEM-Industrie ist eine facettenreiche und innovative Hightech-Branche, die in sämtlichen Lebens- und Wirtschaftsbereichen leistungsstarke Lösungen anbietet. Sie erwirtschaftet ca. 7% des Bruttoinlandproduktes (2021) und nimmt damit in der schweizerischen Volkswirtschaft eine Schlüsselstellung ein. Die Branche ist mit rund 320'000 Beschäftigten die grösste industrielle Arbeitgeberin der Schweiz und leistet mit Ausfuhren im Wert von CHF 68.5 Milliarden rund 27% der gesamten Güterexporte. 57% der ausgeführten Güter der MEM-Industrie werden in die EU exportiert.

Mit ihren Lösungen beliefert die MEM-Industrie auch die Betreiberinnen von kritischen Infrastrukturen in der Schweiz und im Ausland. Neben Komponenten und Systemen gehören dazu auch Dienstleistungen unterschiedlicher Art. Aus diesen Geschäftsbeziehungen ergibt sich eine Betroffenheit der Branche bei den Änderungen im Informationssicherheitsgesetz (ISG) im Zusammenhang mit der vorgesehenen Meldepflicht.

A. Allgemeine Bemerkungen

Die Überführung der freiwilligen Meldung von Cyberangriffen in eine Pflicht für die Betreiberinnen von kritischen Infrastrukturen begrüssen wir. Als wesentlicher Akteur der Schweizer Wirtschaft unterstützen wir die zugrundeliegende Begründung gemäss dem erläuternden Bericht. Wir erkennen den Nutzen dieser Meldepflicht nicht nur für die Betreiberinnen selbst, sondern für die gesamte Schweiz, einschliesslich der Bevölkerung und Wirtschaft. Deshalb ermutigen wir unsere Mitglieder, die selbst erfahrenen Cyberangriffe zu melden und damit einen Beitrag zur Erhöhung der Cybersicherheit der Schweiz zu leisten.

Die Einbettung der Meldepflicht in das ISG erachten wir als passend und zielführend. Die damit einhergehende Gliederung in Abschnitte erhöht die Übersichtlichkeit über die Bestimmungen. Die neuen Bestimmungen im 1. Abschnitt sind zweckdienlich. Mit Blick auf den folgenden Abschnitt weisen wir darauf hin, dass die grundsätzliche Pflicht zum Schutz der Informatikmittel durch die Betreiberinnen in Art. 6, Ziff. 3 ISG festgehalten ist und diese Pflicht auch in die Zusammenarbeit mit Dritten (Art. 9 ISG) zu übertragen ist.

Im gesamten 5. Kapitel des geänderten ISG werden durchgehend, entsprechend der Absicht der Meldepflicht, die Betreiberinnen von kritischen Infrastrukturen angesprochen. Jedoch wird dieses Prinzip in Abschnitt 2, konkret bei den meldepflichtigen Bereichen (Art. 74b), aufgebrochen, indem einerseits Anbieter von Online-Marktplätzen (lit. f) und Hersteller von Hard- und Software (lit. s) aufgenommen werden. Bei Art. 74b, lit. f wird durch die aufgeführten Kriterien der Kreis der betroffenen Betreiber eingeschränkt. Obwohl dennoch die Abgrenzung zwischen einem Betreiber oder Anbieter eines Dienstes und dem Anbieter einer Dateninfrastruktur (Clouddienste) nicht immer eindeutig ist, kann dieser Bestimmung zugestimmt werden. Mit der Erweiterung durch Art. 74b, lit. s jedoch wird aus unserer Sicht eine Büchse der Pandora aufgemacht, welche eine Umsetzung sowohl für das NCSC wie auch für die Hersteller unklar und aufwändig macht. Im folgenden Abschnitt nehmen wir dazu Stellung.

Die weiteren Bestimmungen im 2. und 3. Abschnitt halten wir für passend und zweckdienlich.

B. Zu den einzelnen Bestimmungen

2. Abschnitt: Pflicht zur Meldung von Cyberangriffen auf kritische Infrastrukturen

Art. 74b Bereiche

Mit lit. s werden auch Hersteller von Soft- und Hardware, deren Produkte in kritischen Infrastrukturen eingesetzt werden, unter die Unternehmen und Organisationen eingereiht, welche der Meldepflicht unterstehen. Diese Kategorie wird zwar auf bestimmte Einsatzzwecke reduziert bzw. mit dem Fernwartungszugang eine technische Eigenheit der Lösung vorausgesetzt. Dennoch entsteht damit einerseits eine Kategorie, welche sich fundamental von den anderen unterscheidet, weil sie nicht selbst Betreiberin ist. Andererseits kommen technische Dimensionen ins Spiel, welche komplexer sind, als sie im Er-

läuternden Bericht beschrieben sind und in den entsprechenden Bestimmungen abgebildet werden können.

Die im Erläuternden Bericht beschriebenen Gefahrensituationen können wir durchaus bestätigen. Wir weisen jedoch darauf hin, dass bei Betreiberinnen von kritischen Infrastrukturen wie Trinkwasser- und Energieversorger (lit. c und d), Transportunternehmen (lit. o) oder Zivilluftfahrtunternehmen (lit. p) der Einsatz von Informatikmittel über die klassischen Datenhaltung und – verarbeitung hinausgehen. Dabei kommen unter anderem Steuerungen, Sensoren und verschiedenste elektromechanische und elektronische Aktuatoren zum Einsatz. Übergeordnet können verschiedene Softwaresysteme zum Einsatz kommen, die miteinander verknüpft sind und Abhängigkeiten aufweisen. So können beispielsweise in Kraftwerken, Unterstationen, Trinkwasseraufbereitungen oder Zugsteuerungs- und sicherungssystemen ganze Netzwerke von Kommunikations- und Datenverbindungen entstehen, zu denen verschiedene Hersteller, sowie wiederum deren Zulieferer beitragen. Eine Zuordnung von Verantwortungen seitens der Hard- und Software ist sehr schwierig zu realisieren. Ausserdem verfügt innerhalb solcher Systeme nicht jede Komponente einen eigenen Fernwartungszugang sondern Komponenten teilen sich Kommunikationskanäle. Weiter ist zu beachten, dass Betreiberinnen Wartungsverträge auch mit anderen Dienstleistern als den ursprünglichen Herstellern abschliessen können, wodurch die Unklarheiten der Verantwortungen und Rollen weiter zunehmen.

Wie bereits erwähnt, passen die Firmen gemäss lit. s nicht in die Aufzählung der weiteren Unternehmen und Organisationen, welche der Meldepflicht unterliegen. Alle anderen sind Betreiberinnen von Infrastrukturen und passen damit in die durchgängige Terminologie von Art. 74ff. Es wird durchgängig von «Betreiberinnen von kritischen Infrastrukturen» gesprochen, von der Unterstützung durch das NCSC, über die Festlegung der Meldepflicht in Art 74a, den Ausnahmen in Art. 74c bis zu den Sanktionen in Art. 74h und 74i. Beispielsweise kann nur ein Betreiber gemäss Art. 74c von der Meldepflicht ausgenommen werden, nicht jedoch ein Hersteller, dessen Lösungen in unterschiedlichen Konstellationen eingesetzt werden können. Damit kann ein Ausfall oder eine Fehlfunktion der gelieferten Lösungen nicht nach Wahrscheinlichkeit oder Wirkung (lit. a und b) beurteilt werden. Insbesondere verfügt ein Hersteller auch nicht über das notwendige Wissen über das gesamte System des jeweiligen Betreibers, um über eine Meldung nach Art. 74d entscheiden zu können. Die Hersteller von Hard- und Software als Zulieferer passen nicht in diese Systematik der Meldepflicht, welche auf Betreiberinnen ausgerichtet ist.

Mit diesen Feststellungen wollen sich die Hersteller jedoch nicht aus der Verantwortung ziehen. Die Betreiberinnen von kritischen Infrastrukturen müssen jedoch in die Pflicht genommen werden, den Schutz des gesamten, durch sie zu verantwortenden Systems sicherzustellen. Diese Pflicht ist in Art. 6 Ziff. 3 ISG festgehalten. Falls die Betreiberinnen der kritischen Infrastrukturen für ihre Systeme Lösungen von Dritten, wie Herstellern von Hard- und Software beziehen, sind sie gemäss Art. 9 verpflichtet, dass die Schutzanforderungen an ihr System auch durch die Zulieferer eingehalten werden. Für die Hersteller aus der MEM-Industrie gehören die entsprechenden vertraglichen Vereinbarungen zum Standard, nicht nur bei kritischen Infrastrukturen. Auch eine Überprüfung gemäss Art. 9 Ziff.2 sind sich die Hersteller gewohnt, beispielsweise im Rahmen eines Vendor Risk Managements der Betreiberinnen. In diesem vertraglichen Lieferantenverhältnis tragen die Hersteller bereits heute proaktiv ihren Teil für sichere Infrastrukturen bei. Mit diesem Verständnis der Verantwortung der Betreiberinnen sind insbesondere auch ausländische Hersteller ins Sicherheitskonzept eingebunden.

Antrag

Art. 74b lit. s ist zu löschen.

Art. 74d: zu meldende Cyberangriffe

Die Kriterien für eine Meldung erachten wir als zweckdienlich und durch die Betreiberinnen im Rahmen eines Risiko- und Sicherheitsmanagements umsetzbar. Wir empfehlen jedoch, die Formulierung unter lit. a zu verschärfen. Damit können «alltägliche» Angriffe ausgefiltert und die Qualität der gemeldeten Angriffe für die Auswertung und Interventionen durch das NCSC verbessert werden.

Antrag

Art. 74d lit. a

«die Funktionsfähigkeit der betroffenen kritischen Infrastruktur oder einer anderen kritischen Infrastruktur **wesentlich** gefährdet ist;»

Für die Berücksichtigung unserer Anliegen sowie für die Möglichkeit zur Stellungnahme danken wir Ihnen bestens.

Freundliche Grüsse

Stefan Brupbacher
Direktor

Robert Rudolph
Bereichsleiter

Envoi électronique
ncsc@gs-efd.admin.ch

swissuniversities

Comité de swissuniversities

Martina Weiss
Secrétaire générale
T +41 31 355 07 68
weiss@swissuniversities.ch

swissuniversities
Effingerstrasse 15, Case Postale
3001 Berne
www.swissuniversities.ch

3001 Berne, le 30 mars 2022

Prise de position de swissuniversities concernant l'obligation de signaler les cyberattaques contre des infrastructures critiques

Madame, Monsieur,

Nous vous remercions de la possibilité qui nous est offerte de prendre position sur l'avant-projet de modification de la loi sur la sécurité de l'information (LSI) relatif à l'introduction d'une obligation de signaler les cyberattaques contre les infrastructures critiques.

swissuniversities est favorable à l'annonce des cyberattaques pertinentes aux autorités mais s'oppose à l'introduction d'une obligation large d'annonce de toutes les cyberattaques.

Ce type de menaces allant en augmentant, la promotion de la prévention et de la réaction est cruciale afin d'améliorer le niveau de sécurité des infrastructures critiques. L'introduction d'une obligation large d'annonce est cependant perçue avec scepticisme par nos membres.

En effet, l'introduction d'une obligation pourrait s'avérer contre-productive. Le Centre national pour la cybersécurité (NCSC) reçoit déjà plus de 300 annonces par semaine sur une base volontaire. L'introduction d'une obligation juridique en la matière pourrait pousser les entités concernées et leurs services juridiques à privilégier le respect formel de l'obligation. Ceci aurait pour conséquence de retarder les annonces et d'en réduire la transparence ainsi que le niveau de détails, compliquant ainsi la tâche du NCSC.

De plus, l'art. 24 al. 1 de la nouvelle loi fédérale sur la protection des données (nLPD) prévoit déjà une obligation d'annonce, auprès du Préposé fédéral à la protection des données et à la transparence (PFPDT), des cas entraînant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Or, il est prévu dans le cadre de la révision en cours de compléter cet art. 24 par un al. 5bis prévoyant que le PFPDT puisse transmettre au NCSC le signalement d'une violation de la sécurité des données. Cette obligation d'annonce liée à la protection des données apparaît ainsi comme suffisante pour garantir la sécurité de l'information.

Si une obligation devait néanmoins être introduite dans la LSI, son champ d'application au sens des art. 74a et b de l'avant-projet devrait être précisé. L'objectif du législateur ne peut

être que toutes les cyberattaques soient annoncées sans discrimination. Cela n'est ni praticable pour les exploitants des infrastructures ni dans l'intérêt du NCSC. Toute obligation d'annonce devrait ainsi être limitée aux infrastructures véritablement critiques et ne saurait s'appliquer à l'ensemble de l'infrastructure d'un domaine. En effet, toutes les composantes de l'infrastructure d'une haute école ne sont pas critiques au sens de l'art. 5 let. c LSI.

swissuniversities

Dans tous les cas, il est primordial, afin de limiter la charge administrative pour les hautes écoles comme pour le NCSC, de prévoir un processus d'annonce simplifié et de limiter au strict nécessaire les informations à transmettre.

Enfin, l'échange et la coordination dans ce domaine doivent constituer la priorité. Au-delà des annonces, la collaboration entre les hautes écoles et entre les hautes écoles et le NCSC ainsi que le soutien mutuel que ceux-ci pourront s'apporter suite à des attaques sont essentiels.

Nous vous remercions par avance de la prise en compte de notre position, nous tenons bien volontiers à disposition pour toute précision et vous prions d'agréer, Madame, Monsieur, nos salutations les meilleures.

Prof. Dr. Yves Flückiger
Président

Vereinigung Schweizerischer Assetmanagement- und Vermögensverwaltungsbanken
Association de Banques Suisses de Gestion
Associazione di Banche Svizzere di Gestione Patrimoniale ed Istituzionale
Association of Swiss Asset and Wealth Management Banks

Eidgenössisches Finanzdepartement (EFD)
Nationales Zentrum für Cybersicherheit NCSC
Schwarztorstrasse 59
3003 Bern
per E-Mail an: ncsc@gs-efd.admin.ch

Zürich, 14. April 2022

Stellungnahme der VAV zur Meldepflicht von Betreiber/-innen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrte Damen und Herren

Wir danken für die Möglichkeit zur Stellungnahme im Rahmen der Vernehmlassung zur Revision des Informationsgesetzes (ISG) betr. Einführung einer Meldepflicht für Betreiber/-innen kritischer Infrastrukturen bei Cyberangriffen. Unsere Antwort beschränkt sich auf grundsätzliche Bemerkungen. Im Übrigen möchten wir uns der Stellungnahme der Schweizerischen Bankiervereinigung, an deren Ausarbeitung wir mitgewirkt haben, anschliessen.

Die VAV begrüsst grundsätzlich die Verankerung der Aufgaben des Nationalen Zentrums für Cybersicherheit (NCSC). Die Einführung einer Pflicht für Betreiberinnen kritischer Infrastrukturen, Cyberangriffe den Behörden zu melden, unterstützen wir allerdings nur, sofern umständliche Mehrfachmeldungen an verschiedene Behörden vermieden werden können. So sind unsere Mitglieder bereits heute verpflichtet, der FINMA unverzüglich Vorkommnisse zu melden, die für die Aufsicht von wesentlicher Bedeutung sind. Dazu gehören auch Cyberangriffe. Es gilt daher zu verhindern, dass unterschiedliche Meldungen sowohl dem NCSC als auch der FINMA erstattet werden müssen. Um dies zu gewährleisten, muss das Meldeformular zwingend so konzipiert sein, dass es parallel und ohne zusätzlichen Aufwand auch weiteren Behörden geschickt werden kann. Zudem müssen Rückfragen involvierter Behörden über das Formular und den dafür zu schaffenden Kanal beantwortet werden können.

Für die Kenntnisnahme und wohlwollende Prüfung unserer Ausführungen möchten wir Ihnen danken. Gerne stehen wir Ihnen für Rückfragen zur Verfügung.

Freundliche Grüsse

Michael Meli

Vorsitzender VAV-Expertengruppe
Cyber Security

Simon Binder

Public Policy Director

VUD Verein Unternehmens-Datenschutz

Sehr geehrter Herr Bundesrat Maurer,
Sehr geehrte Damen und Herren,

Bezugnehmend auf die Medienmitteilung vom 12. Januar 2022 danken wir Ihnen für die Gelegenheit, uns zur Einführung einer Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen zu äussern. Wir freuen uns, Ihnen nachfolgend die Stellungnahme des Vereins Unternehmens-Datenschutz (VUD) zu unterbreiten.

Zum Verein Unternehmens-Datenschutz (VUD)

Im Verein Unternehmens-Datenschutz (VUD) schliessen sich juristische Personen, andere Organisationen und natürliche Personen zusammen, die sich mit der Umsetzung des Datenschutzes in ihrer eigenen betrieblichen Praxis befassen. Der VUD fördert den fachlichen Austausch unter seinen aktuell ca. 80 Mitgliedern und ist der selbständigen wie auch unabhängigen Meinungsbildung im Bereich Datenschutz verpflichtet. Zu seinen statutarischen Zwecken gehört auch, sich zu Entwicklungen des Datenschutzes öffentlich vernehmen zu lassen.

Stellungnahme

Allgemeine Bemerkungen

Die im Informationssicherheitsgesetz vom 18. Dezember 2020 (ISG) vorgesehenen Änderungen werfen aus Sicht des VUD eine Vielzahl von Fragen auf.

Besonders kritisch beurteilt der VUD die gesetzgeberische Lösung, den Kreis der von der Meldepflicht erfassten Ereignisse (Art. 5 Bst. d-e ISG) und Unternehmen bzw. Organisationen (Art. 74b ISG) extrem weit zu fassen, um ihn dann über zwei Ausnahmeregelungen (Art. 74c und 74d ISG) wieder einzuschränken. Diese Lösung führt zu Rechtsunsicherheit und unnötigem Aufwand bei den betroffenen Unternehmen und Organisationen. Der VUD schlägt deshalb vor, die Meldepflicht von vornherein auf Cyberangriffe zu begrenzen, die kritische Infrastrukturen im Sinne von Art. 5 Bst. c ISG erheblich gefährden und deshalb von nationalem Interesse sind.

Darüber hinaus empfiehlt der VUD, unklare bzw. widersprüchliche Bestimmungen (insbesondere Art. 74c, 74d und 74g ISG) zu konkretisieren bzw. zu präzisieren, um Rechtsunsicherheiten auf ein Minimum zu reduzieren. Eine deutliche Verbesserung der relevanten Bestimmungen erscheint auch deshalb zwingend, weil die Verletzung von Melde- und Auskunftspflichten strafbar ist (Art. 74h i.V.m. Art. 74i ISG).

Schliesslich ist der VUD der Ansicht, dass die Bekanntgabe von Informationen durch das NCSC (Art. 73c und 76) ausschliesslich auf anonymer Basis erfolgen sollte. Die von den meldepflichtigen Unternehmen und Organisationen an das NCSC gelieferten Informationen werden in der Praxis hochsensibel sein und bedürfen deshalb eines besonderen Schutzes. Die Bekanntgabe dieser Informationen ohne Anonymisierung und Kontrolle durch die betroffenen Unternehmen und Organisationen kann diesen nicht zugemutet werden.

Der VUD ist überzeugt, dass die zielgerichtete, klare und effiziente Regelung der Meldepflicht im Sinne der nachfolgenden Bemerkungen sich auf die Wirksamkeit und Akzeptanz der Meldepflicht sehr positiv auswirken wird.

Bemerkungen zu einzelnen Bestimmungen

Bemerkung zu Art. 5 Bst. d-e ISG

Der Begriff des Cybervorfalls ist zu weit gefasst. In der täglichen Praxis können mit dem Internet verbundene Informatikmittel einer extrem grossen Zahl von (automatisierten) Angriffen ausgesetzt sein. Jeder dieser Angriffe kann – zumindest theoretisch – eine Beeinträchtigung der Vertraulichkeit, Integrität oder Verfügbarkeit zur Folge haben und wäre gemäss Art. 74a ISG dem nationalen Zentrum für Cybersicherheit (NCSC) zu melden, sofern er absichtlich ausgelöst wurde. Indem die blosse Möglichkeit einer Beeinträchtigung für die Begründung einer Meldepflicht im Einzelfall ausreicht, müssten dem NCSC bei konsequenter Auslegung der gesetzlichen Bestimmungen eine extrem grosse Zahl von Cyberangriffen gemeldet werden, selbst wenn diese Angriffe aufgrund von bestehenden Sicherheitsmassnahmen keine unerwünschte Wirkung erzielen. Diese Konsequenz läuft den in Art. 1 Abs. 1 ISG formulierten Zielen zuwider, weil das NCSC mit unnötigen Meldungen überflutet würde. Zudem wäre der mit den Meldungen verbundene Aufwand für die meldepflichtigen Betreiberinnen unverhältnismässig. Jede Meldung zieht einen erheblichen Aufwand nach sich, indem die geforderten Informationen zusammengetragen und in eine kommunizierbare Form gebracht werden müssen. Je mehr Meldungen abzusetzen sind, desto höher ist der Aufwand.

Der VUD schlägt deshalb vor, die Begriffe in Art. 5 Bst. d-e ISG mit Blick auf das Risiko bzw. den Erfolg von Cybervorfällen und -angriffen zu definieren. Von nationalem Interesse sind jene Ereignisse, welche den Betrieb von kritischen Infrastrukturen ernsthaft gefährden. Nur diese sollten meldepflichtig sein. Dadurch wird auch sichergestellt, dass das NCSC seine Ressourcen dort einsetzen kann, wo sie dem Sinn und Zweck des Gesetzes gerecht werden.

Eine Einschränkung von Art. 5 Bst. d-e ISG ist auch dadurch gerechtfertigt, dass das NCSC vor allem aus statistischen Gründen an Informationen über Cybervorfälle interessiert ist. Art. 74 Abs. 3 ISG macht nämlich deutlich, dass das NCSC die betroffenen Unternehmen und Organisationen bei der Bewältigung von Vorfällen nur dann berät und unterstützt, wenn diese ein hohes Mass an Kritikalität aufweisen und eine rechtzeitige private Unterstützung nicht möglich ist. Durch diese weitgehenden Einschränkungen wird Art. 74 Abs. 3 ISG in der Praxis kaum je Anwendung finden.

Bemerkung zu Art. 73a ISG

Das NCSC kann gemäss Bst. b und c dieser Bestimmung vor Cyberrisiken und Schwachstellen von Informatikmitteln warnen und bestimmte Informationen veröffentlichen (siehe auch Art. 73b Abs. 2, erster Halbsatz). Hier ist zu beachten, dass durch die Veröffentlichung von Schwachstelleninformationen die Gefahr von Cyberangriffen auch erhöht werden kann, indem potenziellen Angreifer ebenfalls von einer Schwachstelle und deren Eigenheiten erfahren. Die Erfahrung zeigt, dass es in der Praxis mehrere Monate dauern kann, bis eine neu erkannte Schwachstelle durch die Betreiberinnen von betroffenen Informatikmitteln beseitigt wird. Bis dahin besteht ein erhöhtes Risiko von erfolgreichen Cyberangriffen. Aus unserer Sicht müssen sämtliche Informationen und Kommunikationsmassnahmen des NCSC deshalb unter dem gesetzlichen Vorbehalt stehen, dass Cyberangriffe dadurch nicht gefördert oder erleichtert werden.

Bemerkungen zu Art. 73b ISG

Das NCSC wird in Erfüllung seiner gesetzlichen Aufgaben eine Fülle von Informationen über die in der Schweiz betriebenen Informatikmittel und deren Schwachstellen erhalten. Diese Informationen stehen interessierten Parteien über das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung vom 14. Dezember 2004 (BGÖ) zur Verfügung. Die ausgesprochen öffentlichkeitsfreundliche Anwen-

dung des BGÖ durch Verwaltungsbehörden und Bundesgericht führt dazu, dass gestützt auf ein Öffentlichkeitsgesuch selbst äusserst sensible Informationen über kritische Infrastrukturen und ihre Schwachstellen in die Öffentlichkeit oder sogar in die Hände von potenziellen Angreifern gelangen können. Auch kann eine Offenlegung von Cybervorfällen mit Beteiligung von privaten Unternehmen oder Organisationen deren Ruf nachhaltig schädigen. Die gesetzlichen Einschränkungen der Öffentlichkeit gemäss Art. 7 Abs. 1 BGÖ erweisen sich als kaum wirksam, weil sie in der behördlichen bzw. gerichtlichen Praxis überaus restriktiv ausgelegt werden und kaum je erfolgreich angerufen werden können – selbst Vertraulichkeitszusagen werden in der Praxis erfahrungsgemäss nicht respektiert. Diese Konsequenz widerspricht dem gesetzgeberischen Ziel, die Widerstandsfähigkeit der Schweiz gegenüber Cyberrisiken zu erhöhen (Art. 1 Abs. 1 ISG). Sie widerspricht auch den Interessen der Betreiberinnen sowie den nationalen Interessen. Die Angst vor einer nachträglichen Offenlegung wird dazu führen, dass Informationen dem NCSC im Zweifel nicht offengelegt werden. Der VUD schlägt deshalb vor, Informationen in Bezug auf einzelne kritische Infrastrukturen und deren Schwachstellen und Cybervorfälle, einschliesslich deren Meldungen, im ISG vom Anwendungsbereich des BGÖ ausdrücklich auszunehmen.

Bemerkungen zu Art. 73c ISG

Die Weiterleitung von Informationen zu Cybervorfällen an den NDB gemäss Art. 7c Abs. 1 ISG wirft rechtsstaatliche Bedenken auf. Mit der Weiterleitung an den NDB werden die Informationen potenziell zweckentfremdet. Während das NCSC einen klar definierten gesetzlichen Auftrag erfüllt, liegt es in der Natur der Sache, dass eine nachrichtendienstliche Verarbeitung der Informationen nicht transparent sein kann. Es besteht das Risiko, dass die vom NDB erhaltenen Informationen auf für Zwecke verwendet werden, die ausserhalb des ISG stehen. Wie die betreffenden Informationen vom NDB verarbeitet werden, wird für die betroffenen Unternehmen und Organisationen kaum je erkennbar bzw. kontrollierbar sein. Dies ist umso stossender, als die von den Unternehmen und Organisationen gelieferten Informationen regelmässig sehr sensitiv sein werden. Art. 7c Abs. 4 ISG bietet für die betroffenen Unternehmen und Organisationen in diesem Zusammenhang kaum Schutz. Die Weiterleitung von Informationen gemäss Art. 73c ISG darf daher nur anonymisiert erfolgen. Die Anonymisierung der Informationen vor Weiterleitung an den NBD behindert den Zweck der Weiterleitung (*"Beurteilung von Bedrohungslage oder für die nachrichtendienstliche Früherkennung zum Schutz von kritischen Infrastrukturen"*) nicht.

Die Einverständnispflicht gemäss Art. 73c ISG muss auf alle Mitarbeitenden und Organe eines meldenden Unternehmens bzw. einer meldenden Organisation ausgeweitet werden. In der Praxis werden bei einem Cybervorfall regelmässig eine Vielzahl von Mitarbeitenden und Organen beteiligt bzw. mitverantwortlich sein. Dies gilt sowohl im Vorfeld eines Cybervorfalls (z.B. Ursachen des Vorfalls) wie auch bei der Vorbereitung einer Meldung. Es ist unter diesen Umständen nicht einzusehen, weshalb nur jene Person in die Verwendung der Informationen im Strafverfahren einwilligen muss, welche die Informationen tatsächlich bekanntgegeben hat. Diese Lösung ist willkürlich und wird der Realität der Arbeitsteilung im Unternehmen nicht gerecht. Dies umso mehr, als diese Person, welche die Informationen bekannt gibt, diese vielleicht nur aufgrund einer bestimmten Funktion im Unternehmen bzw. in der Organisation bekanntgibt. Der strafrechtlich fundamentale Grundsatz, wonach sich niemand selbst bezichtigen muss, muss zwingend auf alle Personen in einem Unternehmen oder einer Organisation ausgeweitet werden, welche direkt oder indirekt am Cybervorfall und dessen Meldung beteiligt bzw. dafür verantwortlich sind. Nur auf dieser Grundlage lässt sich eine gesetzliche Meldepflicht mit potenziell strafrechtlichen Konsequenzen rechtsstaatlich rechtfertigen.

Bemerkungen zu Art. 74 ISG

Art. 74 Abs. 4 ISG sieht vor, dass das NCSC auf Informationen der betroffenen Betreiberin zugreifen kann. Diese Regelung ist zu unbestimmt. Insbesondere der Begriff des Zugriffs ist sowohl in technischer wie auch in rechtlicher Hinsicht unklar. Technisch wird in der Informatik unter *"Zugriff"* normalerweise die Möglichkeit verstanden, über einen technischen Zugang auf ein Speichermedium zuzugreifen (z.B. Remote-Zugriff). Das ist mit der gesetzlichen Regelung vermutlich aber nicht gemeint. Rechtlich lässt sich der Begriff nicht gut einordnen. Das schweizerische Recht kennt eine Vielzahl von Möglichkeiten, wie Behörden Informationen proaktiv beschaffen können. Die Bandbreite reicht von Informationsanfragen und Auskunftsrechten bis zu Hausdurchsuchungen und Beschlagnahmungen. Unter welche Kategorie der bisher gesetzlich geregelten Informationsrechte das Zugriffsrecht von Art. 74 Abs. 4 ISG fällt, ist nicht ersichtlich. Der VUD schlägt vor, die Art der Informationsbeschaffung gemäss Art. 74 Abs. 4 ISG mit einem Recht auf Information oder Auskunft zu ersetzen. Das Informationsrecht ist angesichts des Fokus des NCSC auf statistische Auswertungen und der besonderen Kritikalität der Informationen angemessen zu begrenzen. Das Verhältnismässigkeitsprinzip muss auch in diesem Punkt konsequent angewendet werden.

Bemerkungen zu Art. 74a ISG

Die Meldepflicht gemäss Art. 74a ISG schafft eine besondere Dringlichkeit (*"so rasch wie möglich"*), auch wenn diese nicht konkret bemessen wird. Ob diese zeitliche Dringlichkeit angemessen ist, muss in Frage gestellt werden. Wird die Meldepflicht unter dem ISG wie oben (siehe Bemerkung zu Art. 5 Bst. d-e ISG) auf Cybervorfälle begrenzt, die den Betrieb von kritischen Infrastrukturen ernsthaft gefährden, so ist zu bedenken, dass die von einem solchen Vorfall betroffenen Unternehmen oder Organisationen in der ersten Phase damit beschäftigt sind, den Vorfall und dessen Folgen abzuwehren bzw. zu beseitigen. Jede Aktivität, welche diesen Zielen nicht dient, muss unter diesen Umständen zurückstehen. Eine dringliche Meldung an das NCSC ist nur dann angezeigt, wenn der Cybervorfall innert kürzester Zeit und aller Voraussicht nach auch andere Unternehmen und Organisationen treffen kann. Denn nur dann wird das NCSC andere Unternehmen und Organisationen warnen. In allen anderen Fällen kann die Meldung an das NCSC später erfolgen. Der VUD schlägt deshalb vor, in Art. 74a ISG eine angemessene Frist vorzusehen.

Bemerkungen zu Art. 74b ISG

Die Liste der meldepflichtigen Unternehmen und Organisationen gemäss Art. 74b ISG ist unverhältnismässig. In Verbindung mit den extensiven Begriffen von Art. 5 Bst. d-e ISG wird das NCSC mit Meldungen überflutet werden (siehe dazu Bemerkung zu Art. 5 Bst. d-e ISG oben). Wenn man zusätzlich bedenkt, dass die überwiegende Mehrheit von Cyberangriffen nicht von nationalem Interesse sein werden und deshalb nur in die Statistik des NCSC eingehen, so ist der Aufwand, der durch Art. 74b ISG bei den betroffenen Unternehmen und Organisationen bewirkt wird, nicht zu rechtfertigen. Die Einhaltung der aktuell vorgesehenen Meldepflicht lässt sich in der Unternehmenspraxis nur gewährleisten, wenn die meldepflichtigen Unternehmen eine entsprechende Organisation mit den erforderlichen Schlüsselrollen (z.B. Cyber-Team mit Betriebs-, Sicherheits- und Rechtspezialist:innen) und geeignete Prozesse implementieren. Dazu müssen die erforderlichen Budgets bereitgestellt, entsprechende Ressourcen aufgebaut und Schlüsselpersonen geschult werden. Dieser Aufwand lässt sich nur rechtfertigen, wenn der einzelne Cybervorfall für sich von nationalem Interesse ist. In allen anderen Fällen müssen die Unternehmen und Organisationen von jeglichem Aufwand entlastet werden. Aus diesem Grund ist die gesetzgeberische Lösung, wonach die zu meldenden Ereignisse (Art. 5 Bst. d-e ISG) und die meldepflichtigen Unternehmen und Organisationen (Art. 74b ISG) möglichst breit gefasst werden, die Meldepflicht aber begrenzt wird (Art. 74d ISG), abzulehnen. Der grosse Aufwand für die betroffenen Unternehmen und Organisationen entsteht bereits bei den erforderlichen Vorbereitungsarbeiten

zur Gewährleistung der Meldepflicht (Organisation, Prozesse, Schulung). Diese Investitionen sind nur gerechtfertigt, wenn die betroffenen Unternehmen und Organisationen tatsächlich kritische Infrastrukturen im Sinne von Art. 5 Bst. c ISG betreiben.

Dies ist bei vielen der in Art. 74b ISG aufgelisteten Unternehmen und Organisationen nicht der Fall. Nicht jede noch so kleine Privatbank betreibt eine kritische Infrastruktur und ist deshalb staatstragend. Und Ärzt:innen, die nebenbei auch noch ein kleines Labor für ihre Patient:innen betreiben, sind es auch nicht. Man könnte die Beispiele von Unternehmen und Organisationen, die von Art. 74b ISG erfasst sind, aus nationaler Sicht aber keine kritischen Infrastrukturen betreiben, beliebig verlängern. Es ist absehbar, dass nur der kleinste Teil der von Art. 74b ISG erfassten Unternehmen und Organisationen (in der Mehrheit KMU) aus nationaler Sicht tatsächlich kritische Infrastrukturen betreiben. Dies umso mehr, als Art. 74b ISG einzig für digitale Dienste Grössenschwellen für eine Unterstellung vorsieht, andere Unternehmen hingegen ungeachtet jeglicher Grössenschwellen der Meldepflicht unterstellt. Ohne solche Grössenschwellen würde jeder Quartierladen und jeder Marktstand der Meldepflicht unterstehen, da er die Bevölkerung mit Gütern des täglichen Bedarfs versorgt. Nimmt man diese Unternehmen vom Anwendungsbereich von Art. 74b ISG aber nicht aus, so müssen diese die mit der Gewährleistung der Meldepflicht verbundenen Investitionen leisten, obwohl sie von der Meldung eines Cyberangriffs gemäss Art. 74c ISG ausgenommen wären, weil sie keine kritischen Infrastrukturen im Sinne von Art. 5 Bst. c ISG betreiben.

Der VUD deshalb schlägt vor, die Meldepflicht von vornherein auf Cyberangriffe zu begrenzen, welche kritische Infrastrukturen im Sinne von Art. 5 Bst. c ISG erheblich gefährden und deshalb von nationalem Interesse sind. Für eine Meldepflicht kann nur die Kritikalität eines Cyberangriffs aus nationaler Sicht massgebend sein. Dies würde zunächst bedeuten, dass nur jene Unternehmen und Organisationen der Meldepflicht unterliegen würden, welche für solche kritischen Infrastrukturen und deren Betrieb tatsächlich verantwortlich sind. Die Meldepflicht auf bestimmte Arten von Unternehmen und Organisationen auszurichten, ist nicht zielführend, weil sie aufgrund von zahlreichen unklaren Rechtsbegriffen erhebliche Rechtsunsicherheiten schafft und nicht jede der von diesen Unternehmen und Organisationen betriebenen Infrastruktur kritisch ist. Ebenfalls nicht sachgerecht ist es, die Meldepflicht auf jegliche Infrastruktur auszuweiten, die angegriffen werden können, denn nicht jede Infrastruktur ist aus nationaler Sicht kritisch. Schliesslich ist bei der Ausgestaltung von Art. 74b ISG auch darauf zu achten, dass die Meldepflicht in persönlicher Hinsicht klar zugewiesen wird. Die Wertschöpfungskette im Bereich der Informationstechnologie ist komplex und erfasst meist eine Vielzahl von Akteuren (z.B. Auftraggeber, Auftragnehmer, Unterauftragnehmer) auf unterschiedlichen Ebenen (Netzwerk, Infrastruktur, Applikation, User Interface). Ohne klare Bezeichnung der meldepflichtigen Unternehmen und Organisationen droht ein Verantwortlichkeits- und Informationschaos. Der Fokus auf Unternehmen und Organisationen, Infrastrukturen und Cybervorfälle von nationaler Bedeutung erlaubt demgegenüber den allseitig effizienten Einsatz von (begrenzten) Ressourcen und erhöht die Wirksamkeit und Akzeptanz der Meldepflicht.

Bemerkungen zu Art. 74c ISG

Die vom Gesetzgeber vorgeschlagene Lösung mit einer langen Liste von meldepflichtigen Unternehmen bzw. Organisationen (Art. 74b ISG) und deren Begrenzung gemäss Art. 74c ISG ist unnötig und schafft Rechtsunsicherheiten. Es ist ferner nicht ersichtlich, weshalb die Konkretisierung von Art. 74c Bst. b ISG gemäss Ingress von Art. 74c ISG nur auf "bestimmte Kategorien von Betreiberinnen" anwendbar sein soll. Wenn ein Cyberangriff die Voraussetzungen von Art. 74c Bst. b ISG erfüllt, so sollte er unabhängig von der Unternehmensbranche nicht meldepflichtig sein. Massgebend kann nur die Frage sein, ob ein Cyberangriff die nationale Sicherheit erheblich beeinträchtigt. Ist dies nicht der Fall, so ist von einer Meldepflicht abzusehen.

Die Bestimmungen von Art. 74c Bst. a und b ISG sind widersprüchlich bzw. unklar. So können *"ausgelöste"* Funktionsausfälle oder Fehlfunktion nicht "unwahrscheinlich" sein, denn sie wurden nach dem Wortlaut ja bereits ausgelöst. Die Frage der Wahrscheinlichkeit stellt sich somit nicht mehr. Unklar ist, was mit *"einer geringen Abhängigkeit von Informatikmitteln"* (Art. 74c Bst. a ISG) gemeint ist. Unklar ist auch, wann ein Cybervorfall *"nur geringe Auswicklungen auf das Funktionieren der Wirtschaft oder das Wohlergehen der Schweiz"* hat. Ebenso ist nicht klar, wann eine Personenzahl *"gering"* ist oder wann die Auswirkungen *"von anderen kritischen Infrastrukturen"* aufgefangen werden. Durch solche Formulierungen entstehen bei der Rechtsanwendung erhebliche Rechtsunsicherheiten.

Der VUD schlägt vor, die Meldepflicht generell auf Cyberangriffe zu begrenzen, die kritische Infrastrukturen im Sinne von Art. 5 Bst. c ISG erheblich gefährden und deshalb von nationalem Interesse sind. Der VUD empfiehlt zudem, die unklaren bzw. widersprüchlichen Regelungen zu präzisieren. Dies umso mehr, als die Verletzung der Meldepflicht gemäss Art. 74h i.V.m. 74i ISG strafbar ist. Es ist den meldepflichtigen Unternehmen und Organisationen nicht zuzumuten, unklare Rechtsbegriffe auslegen zu müssen, wenn der Verzicht auf eine Meldung aufgrund einer sich nachträglich als falsch erweisende Auslegung mit Strafe bedroht ist. Es ist Aufgabe des Gesetzgebers, die gesetzlichen Anforderungen an die Unternehmen und Organisationen so klar zu formulieren, dass diese ohne Auslegungsrisiko eingehalten werden können.

Bemerkungen Art. 74d ISG

Die gesetzgeberische Lösung, wonach die zu meldenden Ereignisse möglichst breit gefasst werden (Art. 5 Bst. d-e ISG), nur um die Meldepflicht danach wieder zu begrenzen (Art. 74d ISG), ist abzulehnen. Diese Lösung verursacht unnötigen Aufwand bei den betroffenen Unternehmen und Organisationen (siehe dazu Bemerkungen zu Art. 74b ISG oben).

Will der Gesetzgeber an dieser Lösung festhalten, so sollte Art. 74d Bst. a ISG nach Ansicht des VUD nur greifen, wenn die Gefährdung erheblich ist. Eine noch so kleine Gefährdung lässt sich in der Praxis nie ganz ausschliessen, weshalb ein Cyberangriff nach dieser Bestimmung immer gemeldet werden muss. Diese Konsequenz entspricht nicht der in Art. 74d ISG verfolgten Absicht.

Die Konkretisierung in Art. 74d ISG dürfte in der Praxis ins Leere laufen, weil die Beteiligung eines fremden Staates an einem Cyberangriff kaum je eruiert werden kann. Diese Bestimmung dürfte kaum je relevant werden, weshalb sie ersatzlos gestrichen werden kann.

Art. 74d ISG ist nach Ansicht des VUD ersatzlos zu streichen. Wie lange ein Cyberangriff nicht entdeckt wurde, ist für dessen Kritikalität nicht entscheidend, solange die damit verbundene Gefährdung nicht erheblich ist.

Bemerkung zu Art. 74g ISG

Diese Bestimmung ist zu ungenau und sollte ersatzlos gestrichen werden. Der Inhalt der Meldung wird durch Art. 74e ISG erschöpfend geregelt. Welche Informationen das NCSC sonst noch brauchen könnte, die in Art. 74e ISG nicht vorgesehen sind, ist nicht erkennbar. Eine Pflicht der meldepflichtigen Unternehmen und Organisationen zur Auskunftserteilung über Art. 74e ISG hinaus ist ohne weitere Konkretisierung und Begrenzung der zu leistenden Auskunft aus rechtsstaatlichen Gründen abzulehnen. Das Informationsbedürfnis des NCSC muss gesetzlich konkretisiert werden und lässt sich nicht mit einem pauschalen Hinweis auf den gesetzlichen Auftrag rechtfertigen. Dies umso mehr, als sich die Meldepflicht auf einen hochsensiblen Bereich der betroffenen Unternehmen und Organisationen richtet und die Widerhandlung gegen eine Verfügung des NCSC gemäss Art. 74h ISG strafbar ist.

Bemerkungen zu Art. 77 ISG

Der Austausch von Informationen mit ausländischen Behörden gemäss Art. 77 ISG darf nur anonymisiert erfolgen. Die von den betroffenen Unternehmen und Organisationen an das NCSC gelieferten Informationen werden sehr sensitiv sein. In welchem Umfang und zu welchen Zwecken die Informationen ausgetauscht werden, wird für die betroffenen Unternehmen und Organisationen kaum je erkennbar bzw. kontrollierbar sein. Der Austausch von Informationen gemäss Art. 77 ISG darf daher zum Schutz der beteiligen Unternehmen und Organisationen nur anonymisiert erfolgen.

* * * * * * *

Der guten Ordnung halber weisen wir darauf hin, dass die in dieser Stellungnahme vorgetragenen Ansichten und Anregungen nicht in jedem Fall der Meinung aller VUD-Mitglieder entspricht. Wir danken für die wohlwollende Aufnahme und verbleiben

Mit freundlichen Grüssen

Heribert Grab
Präsident VUD

Dr. Nicolas Passadelis
Vorstandsmitglied

Verband Schweizerischer Elektrizitätsunternehmen
Association des entreprises électriques suisses
Associazione delle aziende elettriche svizzere

Eidgenössisches Finanzdepartement
Nationales Zentrum für Cybersicherheit (NCSC)
3003 Bern

Elektronisch an: ncsc@gs-efd.admin.ch

28. März 2022

Markus Riner, Direktwahl +41 62 825 25 27, markus.riner@strom.ch

Stellungnahme zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrte Damen und Herren

Der Verband Schweizerischer Elektrizitätsunternehmen (VSE) dankt Ihnen für die Möglichkeit, sich zur Einführung einer Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe zu äussern. Er nimmt diese Gelegenheit gern wahr.

Der VSE vertritt als Dachverband die Interessen der schweizerischen Elektrizitätswirtschaft entlang der gesamten Wertschöpfungskette von der Produktion über den Handel bis zur Übertragung und Endverteilung von Strom. Eine sichere Stromversorgung ist für eine funktionierende Gesellschaft und Wirtschaft lebensnotwendig. Die Infrastrukturen der Strombranche gehören daher eindeutig mit zu den wichtigsten kritischen Versorgungsinfrastrukturen. Um diese möglichst effektiv vor den zunehmenden Cyberbedrohungen zu schützen, engagiert sich der VSE stark durch die Erarbeitung von Branchendokumenten und unterstützt die Branchenunternehmen in Belangen der Cybersicherheit. Der VSE hat sich ebenfalls aktiv und konstruktiv in die Grundlagenarbeiten für die vorliegende Gesetzesrevision des Informationssicherheitsgesetzes ISG eingebracht.

Betreffend die Änderungen des ISG unterstützt der VSE die vorgeschlagene gestärkte Positionierung des NCSC als zentrale Anlaufstelle des Bundes für die Wirtschaft, einschliesslich der Energiewirtschaft, bei Cyberfragen und als Unterstützerin bei der Bewältigung von Cyberangriffen. Dies entspricht den Erwartungen der Branche insbesondere zur gemeinsamen Verbesserung der Cybersicherheit im Rahmen der Meldepflicht.

Grundsätzlich erwartet der VSE vom NCSC im Ernstfall eines Cyberangriffs schnell verfügbare CERT Dienstleistungen zur Unterstützung bei der Analyse und präzisen Erfassung der Lage sowie bei der Initiierung der nötigen Schritte zur schnellen Abwehr und zur Bewältigung eines Vorfalls.

Der VSE begrüsst die Bestrebung, durch die Leistungen des NCSC die privatwirtschaftlichen Angebote nicht zu konkurrenzieren. Die zu erwartenden Unterstützungsleistungen des NCSC gemäss Art. 73a und Art. 74 Abs. 3 ISG sowie das Zusammenspiel zwischen dem NCSC als CERT für kritische Infrastrukturen und privaten Anbietern von CERT Dienstleistungen sind jedoch im Rahmen der Verordnung präziser festzulegen und

an die Erfordernisse für den Schutz kritischer Infrastrukturen anzupassen. Der VSE beantragt, dass das NCSC als GovCERT einen Schirm über die privatwirtschaftlichen CERTs bildet und diese bei der Krisenbewältigung je nach Situation und Bedarf unterstützt.

Art. 74 Abs. 3 ISG unterscheidet hinsichtlich des Zugangs zu Unterstützungsleistungen durch das NCSC zwischen privaten und nicht privaten Institutionen. Der Erläuternde Bericht schafft indes nicht hinreichend Klarheit über die sachlichen Beweggründe und Folgen dieser Unterscheidung. Verschiedene Betreiberinnen kritischer Infrastrukturen in der Strombranche sind Teil der öffentlichen Verwaltung, andere sind privatwirtschaftlich organisiert; sie weisen indes keine unterschiedlichen Gefährdungspotenziale auf. Die Trägerschaft oder Eigentumsverhältnisse sind somit als Unterscheidungskriterium nicht relevant und widersprechen dem Grundsatz, dass das NCSC nach Art. 73a Bst. f ISG alle Betreiberinnen von kritischen Infrastrukturen unterstützt.

Antrag:

Art. 74 Unterstützung von Betreiberinnen von kritischen Infrastrukturen

3 Es berät und unterstützt sie bei der Bewältigung von Cybervorfällen und der Behebung von Schwachstellen, wenn für die kritische Infrastruktur ein unmittelbares Risiko von gravierenden Auswirkungen besteht ~~und, sofern es sich um private Betreiberinnen handelt, die Beschaffung gleichwertiger Unterstützung auf dem Markt nicht rechtzeitig möglich ist~~.

Der Bundesrat unterstreicht in den Erläuterungen, dass auf Verordnungsebene zu präzisieren sei, aufgrund welcher Kriterien die Vorfälle nach Art. 74d ISG zu melden sind. Der VSE erachtet dies ebenfalls als notwendig. Insbesondere die Zuordnung nach Bst. b, ob ein fremder Staat einen Cyberangriff ausgeführt oder veranlasst hat, dürfte durch den Betroffenen nur schwer bis gar nicht durchführbar sein. Bezüglich Bst. d ist nicht klar, ob bereits das Auftreten früherer, möglicherweise gestoppter oder nicht erfolgreicher Angriffskomponenten meldepflichtig sind, oder nur solche, die direkt und unmittelbar für das Ziel des Cyberangriffs eingeführt wurden.

Nach Art. 73b Abs. 2 ISG können Informationen zu Cybervorfällen veröffentlicht oder an interessierte Behörden und Organisationen weitergeleitet werden, sofern dies dazu dient, Cyberangriffe zu verhindern oder zu bekämpfen. Der VSE anerkennt, dass solche Informationen hilfreich sein können, unterstreicht jedoch, dass Personendaten und Daten juristischer Personen nur mit ausdrücklicher und vorhergehender Zustimmung veröffentlicht werden sollen. In der Verordnung sollte zudem näher definiert werden, zu welchem Zeitpunkt Informationen veröffentlicht werden: Dies sollte ausschliessen, dass Betroffene, die verwundbar sind, durch Rückschlüsse für weitere Angriffe oder Straftaten exponiert werden.

Schliesslich weist der VSE darauf hin, dass Art. 24 revDSG für Vorfälle bezüglich Personendaten (mit hohem Risiko) eine Meldepflicht an den EDÖB vorsieht. Für denselben Vorfall kann es somit zu Meldungen an mindestens zwei verschiedene Behörden kommen. Betroffene Unternehmen sollten jedoch über den gleichen, vom NCSC koordinierten Kanal an den EDÖB melden können, sollte sich dies je nach Art des Angriffs als notwendig erweisen. Eine Doppelspurigkeit würde hingegen zu zusätzlichem Aufwand und schwierigen Abgrenzungsfragen führen.

Betreffend die Änderungen des StromVG begrüsst der VSE, dass sich der Bundesrat gemäss Erläuterndem Bericht beim allfälligen Erlass von Vorgaben für kritische Infrastrukturen der Strombranche auf Verordnungs-

stufe an den subsidiären Branchenregelungen orientieren will. Der VSE erachtet es als sinnvoll, wenn der Bundesrat die einschlägigen Branchennormen für anwendbar erklärt, da dies eine rasche Anpassung an die dynamische Entwicklung möglicher Bedrohungslagen und -szenarien ermöglicht. Beim allfälligen Erlass von Verordnungsbestimmungen muss das Gefährdungspotenzial im Hinblick auf die Versorgungssicherheit bei der Definition der einzuhaltenden Vorgaben und der Bezeichnung der verpflichteten Akteure berücksichtigt werden. Bei den Verordnungsbestimmungen ist sicherzustellen, dass ein pragmatischer Umgang mit der Meldepflicht gewählt wird, sodass auch kleineren und mittleren Unternehmen eine einfache und unkomplizierte Handhabung ermöglicht wird.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und unterstützen das NCSC gerne bei der weiteren Festlegung des effizienten Zusammenspiels von Akteuren im Ernstfall eines Cyberangriffs.

Für allfällige Rückfragen oder zur Diskussion stehen wir Ihnen gern zur Verfügung.

Freundliche Grüsse

Michael Frank
Direktor

Michael Paulus
Leiter Netze und Berufsbildung

VÖV UTP
Verband öffentlicher Verkehr
Union des transports publics
Unione dei trasporti pubblici

Nationales Zentrum für Cybersicherheit
z.H. Manuel Suter, Geschäftsstelle NCSC
3003 Bern

elektronisch eingereicht bei:
ncsc@gs-efd.admin.ch

Bern, 05.04.2022
bettina.meury@voev.ch

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrte Damen und Herren

Wir bedanken uns für die Gelegenheit, im Rahmen der Vernehmlassung über die Einführung einer Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen Stellung nehmen zu können.

Da die Risiken von Cyberangriffen seit Jahren kontinuierlich zunehmen, sehen wir das Bedürfnis des NCSC eine bessere Übersicht über die aktuelle Cyber-Lage zu erhalten und dadurch eine Lücke im Dispositiv der Cybersicherheit der Schweiz zu schliessen. Eines der Ziele aus den Meldungen sollte sein, den Organisationen, die Opfer von Cyberangriffen geworden sind, schnell und unkompliziert Hilfeleistungen zur Unterstützung anzubieten.

Die Bahnbranche leistet gerne einen Beitrag zur Optimierung dieses Sicherheitsdispositivs.

Der aktuelle Gesetzesentwurf lässt allerdings zur vollständigen Beurteilung an einigen Stellen Interpretationen zu, so dass aus unserer Sicht den konkreten Ausführungsbestimmungen eine grosse Bedeutung zukommt.

Folgende Punkte möchten wir zur Beachtung hervorheben:

- Der Aufwand für die Erstellung von Meldungen muss verhältnismässig sein und auch für die Betreiberinnen einen Mehrwert bringen.
- Öffentliche Publikationen von Schwachstellen sollten erst nach einer Risiko- bzw. Güterabwägung durch das NCSC erfolgen, um nicht dadurch das Risiko für die Betreiberinnen weiter zu erhöhen.

Anmerkungen und Details zu den einzelnen Bestimmungen finden Sie im Anhang.

Wir bedanken uns für die Berücksichtigung unserer Anliegen. Für Fragen zu den Rückmeldungen stehen wir Ihnen sehr gerne zur Verfügung.

Freundliche Grüsse,

Thomas Küchler
Vorsitzender der GL SOB
Präsident Kommission Infrastruktur

Ueli Stückelberger
Direktor VöV

Dählhölzliweg 12
www.voev.ch
CH-3000 Bern 6
info@voev.ch

Anhang: Anmerkungen zu den einzelnen Bestimmungen

5. Kapitel: Massnahmen des Bundes zum Schutz der Schweiz vor Cyberrisiken

1. Abschnitt: Allgemeine Bestimmungen

Art. 73b Bearbeitung von Meldungen zu Cybervorfällen und Schwachstellen

Art. 73b Abs. 2: Konkretisierung des Vorgehens bei der Weitergabe der Daten. Die Einwilligung der Betroffenen soll verdeutlicht werden (Schriftlichkeit und vorgängige Erwähnung im Gesetzestext).

Antrag: Diese Informationen dürfen Personendaten und Daten juristischer Personen enthalten, sofern es sich um missbräuchlich verwendete Identifikationsmerkmale und Adressierungselemente handelt und die betroffene **natürliche oder juristische** Person **schriftlich** einwilligt.

Art. 73b Abs. 3: Schwachstellen müssen nicht ausschliesslich auf den Produkten bzw. deren Implementation durch die Hersteller begründet sein, sondern auch in den Normen und/oder Standards, welche verpflichtend anzuwenden sind.
Responsible Disclosure kann, wenn durch die Betreiberin einer kritischen Infrastruktur gemeldet, zu einer Verletzung eines bestehenden Vertragsverhältnisses führen, wenn beispielsweise ein Non Disclosure Agreement zwischen der Betreiberin und einem Lieferanten besteht.
Die Veröffentlichung der Schwachstelle (gerade durch ein Bundesorgan) kann zu einem offenen Angriffsvektor bei den Betreiberinnen der kritischen Infrastrukturen führen und damit die Sichtbarkeit der Angriffsfläche deutlich erhöhen. Man kann den Absatz so interpretieren, dass das NCSC nach einer gewissen Frist **veröffentlichen muss.** Eine vorzeitige Veröffentlichung (bevor entsprechende Schutzmassnahmen umgesetzt wurden) könnte dazu führen, dass danach die Schwachstelle (auch durch nicht professionelle Hacker) tatsächlich vermehrt ausgenutzt wird.

Antrag: Werden dem NCSC Schwachstellen gemeldet, so informiert es ***nach erfolgter rechtlicher Klärung mit der meldenden Stelle*** umgehend den Hersteller und setzt ihm zur Behebung der Schwachstelle eine angemessene Frist. Behebt der Hersteller die Schwachstelle nicht innert dieser Frist, so ***kann*** das NCSC die Schwachstelle unter Angabe der betroffenen Soft- oder Hardware ***und einer Risiko- bzw. Güterabwägung veröffentlichen***, sofern dies zum Schutz vor Cyberrisiken beiträgt.

2. Abschnitt: Pflicht zur Meldung von Cyberangriffen auf kritische Infrastrukturen

Art. 74d Zu meldende Cyberangriffe

Art. 74d Abs. 1, Bst. b: Als Betreiberin einer kritischen Infrastruktur sind wir nicht in der Lage eine solche Fragestellung abschliessend zu beantworten.

Antrag: Art. 74d Abs. 1 Bst. b: ersatzlos streichen.

Art. 74g Auskunftspflicht

Es gibt keine Aufbewahrungs- bzw. Sammelpflicht, im Gegenzug kann das NCSC für sie benötige Auskünfte verlangen. Präzisierung, dass die vorhandenen Daten ausreichend sind.

Antrag Die Betreiberin der kritischen Infrastruktur muss dem NCSC ergänzende Auskünfte zu den Inhalten der Meldung nach Artikel 74e erteilen, die es zur Erfüllung seiner Aufgaben in Bezug auf die Abwehr weiterer Cyberangriffe auf kritische Infrastrukturen benötigt, ***sofern diese bei der Betreiberin der kritischen Infrastruktur vorhanden sind***.

Art. 74i Widerhandlungen gegen Verfügungen des NCSC

Grundsätzlich sind Bussen mit einem Strafrahmen von bis zu CHF 10'000 gemäss Schweizer Strafgesetzbuch (StGB) vorgesehen. Eine Verzehnfachung dieses Bussenrahmens erscheint in Anbetracht der betroffenen Rechtsgüter wie auch der geringen, wenn nicht gar vollkommen fehlenden kriminellen Energie nicht begründbar. Es geht hier nicht um die Verursacher der Cyberangriffe, sondern um von Cyberangriffen betroffene Betreiberinnen.
Persönliche Bussen von bis zu CHF 100'000 aufgrund einer unterlassenen resp. gemäss einer nach Ansicht der Behörde nicht gehörig wahrgenommenen Melde- oder Auskunftspflicht sind auch als *ultima ratio* unverhältnismässig. Die persönliche Busse ist – wenn in dieser Form überhaupt notwendig – gemäss den gesetzlichen Vorgaben auf CHF 10'000 zu beschränken, ebenfalls sind dementsprechend die Verweise auf das Verwaltungsstrafrecht anzupassen.
Es erscheint uns insgesamt wesentlich sinnvoller, dass juristische Personen in die Verantwortung gezogen werden, d.h. die Unternehmen und nicht direkt die Arbeitnehmer/innen zu büssen, sollten sie ihren Pflichten nicht nachkommen.

Antrag im Minimum zu Art. 74i Abs. 1: Mit Busse bis zu ***10 000*** Franken wird bestraft, ….

Antrag im Minimum zu Art. 74i Abs. 3: Fällt eine Busse von höchstens ***5000*** Franken in Betracht ….

3. Abschnitt: Datenschutz und Informationsaustausch

Art. 76 Zusammenarbeit im Inland

Das Verhältnis der Bestimmungen Art. 76 Abs. 1 zu Art. 73b Abs. 2 sowie Art. 73c ist unklar. Eine Weiterleitung von Informationen sollte unter den Voraussetzungen von Art. 73b Abs. 2 und Art. 73c stehen.

Antrag: Art. 76a Abs. 1: Das NCSC kann Betreiberinnen von kritischen Infrastrukturen ***unter den Voraussetzungen von Art. 73b und Art. 73c*** Personendaten bekanntgeben, sofern dies zum Schutz von kritischen Infrastrukturen vor Cyberrisiken erforderlich ist.

Art. 76a Unterstützung für Behörden

Da gemäss erläuterndem Bericht eine Weiterleitung von Informationen zu den Betroffenen nur in Ausnahmefällen erfolgt und an die Bedingungen nach Artikel 73c Absatz 1 und 2 gebunden sind, sind die Absätze 2 und 3 dahingehend zu konkretisieren, dass ausschliesslich Personendaten, die Aufschluss über die Identität und Vorgehensweise der Verursacher von Cyberangriffen geben, mittels Abrufverfahren bekanntgeben werden können. Weitergehende Personendatenbekanntgaben (z.B. Personendaten von Betreiberinnen) dürfen davon nicht

umfasst sein. Die Behörde hat die Abrufverfahren nach dem Grundsatz des “privacy by design” entsprechend zu gestalten.

Antrag Art. 76a Abs. 2 Es gewährt dem NDB Zugriff auf Informationen im Abrufverfahren, die ***ausschliesslich*** Aufschluss über die Identität und die Vorgehensweise der Verursacherinnen und Verursacher von Cyberangriffen geben.

Antrag Art. 76a Abs. 3: Es gewährt den Strafverfolgungsbehörden Zugriff auf Informationen im Abrufverfahren, die ***ausschliesslich*** Aufschluss über die Identität und die Vorgehensweise der Verursacherinnen und Verursacher von Cyberangriffen geben.

Art. 77 Internationale Zusammenarbeit

Das Verhältnis der Bestimmungen Art. 77 Abs. 1 zu Art. 73b Abs. 2 sowie Art. 73c ist unklar. Eine Weiterleitung von Informationen sollte unter den Voraussetzungen von Art. 73b Abs. 2 und Art. 73c stehen.

Antrag Art. 77 Abs. 1, zweiter Satz: Umfasst der Informationsaustausch auch Personendaten nach Art. 75, ~~ist~~ ***sind Artikel 73b Abs. 2 und 73c sowie*** Artikel 6 DSG zu beachten

Art. 79 Datenaufbewahrung und -archivierung

Es ist nicht genau definiert, was unter “*letzten Verwendung*” der Personendaten zu verstehen ist: Der Abschluss der Vorfallmeldung? Was lässt diese Frist (5 Jahre resp. 2 Jahre) immer wieder unterbrechen? Was sind die Voraussetzungen für eine gültige “*letzte Verwendung*”?

Antrag Art. 79 Abs. 1 ist zu konkretisieren.

2. Datenschutzgesetz vom 25. September 2020

Es ist im Gesetz zu verdeutlichen, dass eine Weitergabe ausschliesslich mit dem Einverständnis des meldepflichtigen Verantwortlichen überhaupt möglich ist und Art. 24 Abs. 6 revDSG (entsprechend den Erläuterungen) vorbehalten bleibt.

Antrag Art. 24 Abs. 5bis. Der EDÖB kann die Meldung ***ausschliesslich*** mit dem Einverständnis des meldepflichtigen Verantwortlichen zur Analyse des Vorfalls an das Nationale Zentrum für Cybersicherheit weiterleiten. ***Art. 24 Abs. 6 bleibt vorbehalten.***

Hallo NCSC

Abraxas hat die Vernehmlassungsvorlage studiert und unterstützt sowohl die formulierten Ziele wie auch die Massnahmen. Als Betreiberin kritischer Infrastrukturen sind wir uns der Bedeutung der Thematik voll bewusst, und wir sind auch der Meinung, dass der mit der Meldepflicht verbundene Informationsaustausch ein wesentlicher Mehrwert für die Bekämpfung von Angriffen darstellt.

Beste Grüsse
Peter Gassmann

--
Peter Gassmann
Leiter Solution Engineering
Mitglied der Geschäftsleitung

Abraxas Informatik AG

The Circle 68 | CH-8058 Zürich-Flughafen
Direkt +41 58 660 21 55
peter.gassmann@abraxas.ch | www.abraxas.ch

Für die digitale Schweiz.
Mit Sicherheit.

abraxas

Axpo Services AG | Parkstrasse 23 | 5401 Baden | Switzerland

Per E-Mail
ncsc@gs-efd.admin.ch

Ihr Kontakt Thomas Porchet, Leiter Energiepolitik Schwiez
E-Mail thomas.porchet@axpo.com
Direktwahl T +41 56 200 31 45
Datum 7. April 2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe: Stellungnahme Axpo Group

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Möglichkeit im Rahmen des Vernehmlassungsverfahrens zur Änderung des Informationssicherheitsgesetzes (ISG) und zur Einführung einer Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe Stellung nehmen zu können.

Allgemeine Bemerkungen

Axpo ist die grösste Schweizer Produzentin von erneuerbarer Energie und international führend im Energiehandel sowie in der Vermarktung von Solar- und Windkraft. Rund 5000 Mitarbeitende verbinden Erfahrung und Expertise und entwickeln für Kunden in 30 Ländern in Europa, Nordamerika und Asien innovative Energielösungen auf Basis modernster Technologie. Axpo ist zu 100% im Eigentum der Nordostschweizer Kantone und Kantonswerke.

Als grösste Produzentin von erneuerbarer Energien in der Schweiz sind wir Eigentümerin von oder halten Beteiligungen an rund 60 Wasserkraftanlagen. Zudem betreiben wir das Kernkraftwerk Beznau I und II und sind an den Kernkraftwerken Leibstadt und Gösgen beteiligt. Schliesslich betreiben und unterhalten wir ein mehrere tausend Kilometer umspannendes Leitungsnetz auf den Netzebenen 3 und 5. Damit sind wir von der Vorlage, die zur Definition von Betreiberinnen kritischer Infrastruktur ausdrücklich auf Art. 6 Abs. 1 EnG abstellt, direkt angesprochen.

Zur Vorlage

Art. 74d Abs. 1 Bst. b

Antrag:
Streichen.

Begründung:
Art. 74d Abs. 1 Bst. b hält fest, dass Cyberangriffe auf kritische Infrastrukturen gemeldet werden müssen, wenn sie von einem fremden Staat ausgeführt oder veranlasst worden sind. Dieser Bestimmung können Betreiberinnen kritischer Infrastrukturen kaum in allen gebotenen Fällen nachkommen, da oftmals nicht zu bestimmen ist, welche Personen oder Organisationen einen Angriff ausgeführt – geschweige denn veranlasst – haben. Zumindest ist Bestimmung zur Regelung von Ausnahmen vorzusehen.

Art. 74e

Antrag:
Art. 74e ist dahingehend zu präzisieren, dass eine Meldung unmittelbar, nachdem ein Angriff festgestellt worden ist, gemacht werden muss – unabhängig vom Umfang der vorliegenden Informationen.

Begründung:
Das Sammeln von Informationen über einen festgestellten Angriff kann sich sehr zeitintensiv gestalten. Im Sinn der Gefahrenabwehr scheint es zielführender, Angriffe unverzüglich zu melden, und weitere Informationen nachzuliefern, sobald sie verfügbar sind.

Schliesslich weisen wir darauf hin, dass die Kernkraftwerke bereits heute in mit der Vorlage vergleichbarem Rahmen gegenüber dem ENSI meldepflichtig sind. Wir beantragen deshalb auch, dass sich die verschiedenen Bundesbehörden untereinander koordinieren, um Doppelspurigkeiten zu vermeiden. Eine Lösung könnte vorsehen, dass auf eine Meldepflicht von Betreiberinnen kritischer Infrastrukturen ans NCSC in denjenigen Bereichen verzichtet wird, in denen sie bereits gegenüber anderen Behörden meldepflichtig sind. Die entsprechenden Behörden hätten aber alle erhaltenden Informationen mit dem NCSC zu teilen.

Für die Berücksichtigung unserer Anliegen danken wir Ihnen.

Freundliche Grüsse

Christoph Brand
CEO

Lukas Schürch
Head Corporate Public Affairs

Bundesanwaltschaft
Ministère public de la Confédération
Ministero pubblico della Confederazione
Procura publica federala

CH-3003 Bern, BA

Per E-Mail an
ncsc@gs-efd.admin.ch

Eidgenössisches Finanzdepartement EFD
Herr Bundesrat Ueli Maurer
Bundesgasse 3
3003 Bern

Referenz: RD.22.0021
Bern, 13. April 2022

Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen
Änderung des Bundesgesetzes über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) vom 18. Dezember 2020
Vernehmlassung der Bundesanwaltschaft (BA)

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Mit Bezugnahme auf Ihre Einladung zur Vernehmlassung vom 12. Januar 2022 nimmt die BA als fachlich und organisatorisch von Bundesrat und Bundesverwaltung unabhängige Behörde Stellung zu Aspekten der Vorlage, welche sie betreffen bzw. betreffen könnten.

Zu den folgenden Bestimmungen der Vorlage äussert sich die BA wie folgt:

Art. 73c ISG – Weiterleitung von Informationen

Die BA nimmt von der Regelung in Art. 73c ISG Kenntnis und stellt fest, dass der Schwerpunkt auf der Melde- und Auskunftspflicht der betroffenen Behörden und Unternehmen liegt, die der Meldepflicht unterstellt werden, und dass es insbesondere in der Verantwortung des Nationalen Zentrums für Cybersicherheit (NCSC) liegen wird, darüber zu entscheiden, ob und gegebenenfalls zu welchem Zeitpunkt eine Weiterleitung der Meldung an die Strafverfolgungsbehörden angebracht ist.

Bundesanwaltschaft
Nicole Vontobel
Guisanplatz 1
3003 Bern
www.bundesanwaltschaft.ch

Art. 74d Abs. 2 ISG – Zu meldende Cyberangriffe

Die BA regt an, den Begriff «Cyberangriff» in diesem Kontext präziser zu definieren. Ansonsten könnte die Definition von Art. 5 lit. e ISG [Cyberangriff: Cybervorfall, der von Unbefugten absichtlich ausgelöst wurde.] dazu führen, dass bspw. bereits ein personalisiertes Spam E-Mail mit erpresserischem Inhalt (wie sie heute relativ häufig vorkommen) meldepflichtig würde.

Abs. 77 Abs. 3 ISG – Internationale Zusammenarbeit / Verwendung von Informationen für ein rechtliches Verfahren im Ausland

Diese Bestimmung schafft neue Möglichkeiten der internationalen Zusammenarbeit bei der Bekämpfung von Cyber-Phänomenen, die Gegenstand der vorliegenden Gesetzesänderung sind. Um die Wirksamkeit dieser neuen Möglichkeiten sicherzustellen, sollten sie sich in den Rahmen der bereits bestehenden Bestimmungen zur internationalen Zusammenarbeit – insbesondere im Bereich der Rechtshilfe – einfügen.

Art. 77 Abs. 3 ISG beschränkt sich darauf, die Bestimmungen über die Amts- und Rechtshilfe vorzubehalten, ohne einen Koordinierungsmechanismus vorzusehen. Sowohl die schweizerischen als auch die ausländischen Behörden müssen wissen, wie weit sie die übermittelten Daten verwenden dürfen. Es sollte Klarheit darüber bestehen, ob die ausländische Partnerbehörde des NCSC die erhaltenen Daten einer Drittbehörde in ihrem Land weitergeben darf, zum Beispiel an eine Strafverfolgungsbehörde, damit diese anschliessend ein Rechtshilfeersuchen an die Schweiz richten kann. Es wäre nicht zielführend, Daten mit ausländischen Behörden auszutauschen, ohne das Vorgehen zu definieren, das es ihnen ermöglicht, die erhaltenen Informationen gerichtlich zu verwerten. Solche Koordinierungsnormen existieren bereits im Schweizer Recht (sh. z.B. Art. 30 Abs. 4 lit. a Ziff. 2 GwG).

Daher schlagen wir vor, Abs. 3 zumindest wie folgt zu ergänzen:

> [3] Werden die Informationen für ein rechtliches Verfahren im Ausland benötigt, so gelten die Bestimmungen über die Amts- und Rechtshilfe. *Die übermittelten Informationen können zur Substantiierung eines Rechts- oder Amtshilfeersuchens verwendet werden.*

Die BA bedankt sich für die Berücksichtigung der vorliegenden Vernehmlassung.

Freundliche Grüsse

Bundesanwaltschaft BA

Stefan Blättler
Bundesanwalt

Beat Lehman
lic.iur. Fürsprech
Acting Counsel Alcan Holdings Switzerland AG
Kongoweg 9 (Home Office)
5034 Suhr

Fetnetz 062 842 49 52
Mobil-Tf 079 500 82 32
e-mail b.lehmann-aarau@bluewin.ch

Suhr, 14. April 2022

Elektronisch übermittelt an ncsc@gs-efd.admin.ch

Herr Bundesrat Ueli Maurer
Eidgenössisches Finanzdepartement EFD

Frau Bundesrätin Viola Amherd
Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS)

Geschäftsstelle Nationales Zentrum für Cybersicherheit NCSC

Stellungnahme

Zur Ergänzung des Bundesgesetzes über die Informationssicherheit beim Bund ("ISG") durch Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen

Der Unterzeichnende* stellt Ihnen gestützt auf Art. 4 Abs. 1 und Art. 7 Abs. 3 Bst. c) VlG iVm Art. 1, Art. 5 und Art. 20 Abs. 3 VwVG folgende

Anträge

1. Das in den Jahren 2018-2019 in Angriff genommene Vorhaben der Ergänzung des ISG durch Einführung einer hybriden Meldepflicht für Cyberangriffe sowohl privater als auch öffentlich-rechtlicher Organisationen als Betreiberinnen kritischer Infrastrukturen gemäss der am 12. Januar publizierten Vernehmlassungsvorlage sei aufgrund der seit dem 24. Februar 2022 und namentlich seit dem 9. März 2022 **wesentlich veränderten Umstände und Bedrohungslage nicht weiterzuführen**.

2. Dafür sei auf dem Weg der durch die Bundesverfassung vorgesehenen Weges der **Rechtsetzung bei Dringlichkeit** (Art. 163, 165 und 173 Abs.1 Bst. a) BV bzw Art. 185 Abs. 1 BV) gestützt auf Art. 2 Abs. 1 BV iVm Art. 57 und Art. 58 BV eine wirkungsvolle **Rechtgrundlage für die Koordination, Integration und Bündelung der bestehenden und künftigen Massnahmen unseres Landes zur Abwehr von Cyberangriffen professionell agierender Täter auf kritische Infrastrukturen** zu schaffen.

---

* aufgrund von mehr als 2'000 Diensttagen im militärischen Nachrichtendienst, zuletzt als Leitender Nof einer Heereseinheit (Feld Div 5); Rechtskonsulent IBM Schweiz und Europa in Zürich und Paris; hierauf Angehöriger Konzernstab Recht der Alusuisse Lonza Gruppe sowie der Alcan Holdings Switzerland; Mitglied der Expertenkommission des Bundes zur Schaffung des geltenden Datenschutzgesetzes von 1992; langjähriger Lehrbeauftragter für Datenschutz- und Informatikrecht an ETHZ / Universität Zürich und FHNW Campus Brugg; Mitwirkung in Vorstand Beirat von Fachorganisationen wie SWISSMEM, VUD, SWICO, ISSS, S-I; 1994-2020 Mitglied des Verwaltungsrats / VR Präsident eines mittelständischen Chemie-Unternehmens

Begründung

1. Bedrohungssituation bei der Ausarbeitung der Vernehmlassungsvorlage

1.1 Der Gegenstand der heutigen Vernehmlassung wurde den Adressaten **am 12. Januar 2022** vorgelegt https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/dl/proj/2021/70/cons_1/doc_1/de/pdf-a/fedlex-data-admin-ch-eli-dl-proj-2021-70-cons_1-doc_1-de-pdf-a.pdf

1.2 Die Vorlage beruht auf den Vorarbeiten und Forderungen aus der Mitte des Parlaments während der Periode **2019 und 2020** für die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/dl/proj/2021/70/cons_1/doc_2/de/pdf-a/fedlex-data-admin-ch-eli-dl-proj-2021-70-cons_1-doc_2-de-pdf-a.pdf

1.3 In jener Zeit durften sich Gesellschaft, Wirtschaft und Politik noch der behaglichen Existenz unseres Landes auf einer **"**F r i e d e n s i n s e l**"** wähnen, umgeben von der trügerischen Idee der Nachbarschaft mit befreundeten Nationen.

1.4 Dabei hatte der autokratische Päsident Russlands nach den Kiewer Maidan Unruhen ab dem 21. November 2013 und der Flucht des von Russland unterstützten Präsidenten Janukowytsch nach Moskau am 27. Februar 2014 im März 2014 mit der völkerrechtswidrigen Besetzung der Krim und der Unterwanderung des Donbas (Oblaste Donezk und Lugansk) reagiert und eine acht Jahre anhaltende Krise ausgelöst. In diesem Zusammenhang hatte die Schweiz Konten des geflüchteten Präsidenten Wiktor Janukowytsch und Mitglieder seiner Regierung gesperrt. Euromaidan https://de.wikipedia.org/wiki/Euromaidan

2. Grundlegende Veränderung der Bedrohungslage

2.1 Seit der sog. "**Zeitenwende**" des 24. Februar 2022 (gemäss dem von Bundeskanzler Olaf Scholz in seinen Ausführungen am 27. Februar 2022 vor dem deutschen Bundestag geprägten Begriff) d.h. seit dem völkerrechtswidrigen **Einfall russischer Truppen** in die Ukraine haben sich nach hier vertretener Auffassung auch in unserem Land die **Randbedingungen der Gesetzgebung für Cyber-Risiken tiefgreifen verändert** https://polen.diplo.de/pl-de/04-news/04-2-Aktuelles/-/2515474 2709758.html .

2.2 Der Schweizerische Bundesrat hat am 4. und 25. März 2022 gestützt auf Art. 2 des Embargo-Gesetzes (SR 946.231) die **S a n k t i o n e n** der wichtigsten demokratischen Länder der Welt, insbesondere der OECD und unserer Nachbarstaaten, gegenüber dem völkerrechtlichen Aggressor, der russischen Föderation, und deren Präsidenten als deren faktischen Alleinherrscher sowie einflussreichen Personen aus seiner Entourage, die sog. "Silowiki", übernommen https://www.fedlex.admin.ch/eli/cc/2022/151/de#fn-d6e35.

2.3 Als Reaktion auf diesen Schritt wurde unser Land am 9. März 2022 durch den Ukas des russischen Präsidenten Wladimir Wladimirowitsch Putin auf die Liste "**U n f r e u n d l i c h e r S t a a t e n**" gesetzt Russian government approves list of unfriendly countries and territories - Russian Politics & Diplomacy - TASS https://de.wikipedia.org/wiki/Liste_unfreundlicher_Staaten .

2.4 Damit hat der russische Präsident von der ihm durch das "***Law on Counter-Sanctions against Unfriendly Countries***" von Mai-Juni 2018 eingeräumten Kompetenz Gebrauch gemacht, "Unfreundliche Staaten " –

und damit seiner Ansicht nach eben auch die Schweiz - mit angemessenen **Vergeltungs-Massnahmen** zu belegen https://tass.com/politics/1007868 https://tass.com/politics/1007192

1.5 Die "Vergeltungs-Massnahmen" sind im erwähnten Gesetz **nicht abschliessend definiert** und gewähren dem russischen Präsidenten einen **erheblichen Ermessens-Spielraum**.

3. Cyberangriffe Russlands

3.1 Es ist bekannt, dass in Russland (aber auch anderen Staaten mit einer autoritären Herrschaftsstruktur wie Belarus, China und Nord-Korea) verschiedene von der Regierung, bzw. im vorliegenden Fall den russischen Sicherheits- und Geheimdiensten betriebene oder stillschweigend tolerierte Organisationen des "*Dark Net*" tätig sind https://en.wikipedia.org/wiki/List_of_cyber_warfare_forces,

3.2 Diese Organisationen haben in der Vergangenheit eine ganze Anzahl von **Aktionen gegen die IT Infrastruktur ausländischer Nationen** durchgeführt. Vgl. dazu auch den recht allgemein und abstrakt gehaltenen Bericht 21.070 des Bundesrates zur Sicherheitspolitik Ziff. 2.3.1, vor allem aber die Aufstellung in Wikipedia "**Cyberwar by Russia**" https://en.wikipedia.org/wiki/Cyberwarfare_by_Russia

3.3 Besondere hellseherische Fähigkeiten müssen daher nicht vorausgesetzt werden, um davon ausgehen zu können, dass im Rahmen der vom russischen Präsidenten angeordneten "Vergeltungs-Massnahmen" gemäss vorstehender Ziff. 1.4 und 1.5 früher oder später Cyberangriffe gegen kritische Infrastrukturen unseres Landes ausgelöst werden können.

3.4 /1 Nach hier vertretener Auffassung handelt es sich bei den in der Statistik des NCSC publizierten Cyberangriffen https://www.ncsc.admin.ch/ncsc/de/home/aktuell/aktuelle-zahlen.html vor allem um Delikte von **Wirtschafts-Kriminellen** [z.B. Verwertung unbefugt beschaffter Daten im Sinn von Art. 143 StGB; Erpressung von Lösegeld unter Einsatz sog. "*Ransomware*" gemäss Art. 144bis StGB iVm Art. 156 StGB].

/2 Die betreffenden Straftaten richteten sich gegen wenig geschützte Angriffsziele wie KMU, Altersheime, Regionalspitäler https://www.it-markt.ch/cybersecurity/2021-09-21/ransomware-attacke-auf-genfer-pflegeheim https://www.inside-it.ch/post/immer-mehr-ransomware-attacken-auf-krankenhaeuser-20210217

/3 Dagegen ist bei der Analyse der heutigen und künftigen Bedrohungslage davon auszugehen, dass im Rahmen von "Vergeltungs-Massnahmen gegen unfreundliche Nationen" durch **professionelle staatliche oder halbstaatliche Organisationen** der russischen Föderation oder deren Verbündeten gezielte Angriffe gegen kritische Infrastrukturen unseres Landes unternommen werden.

/4 Wenn sie nicht abgewehrt werden können derartige Angriffe längerfristige, tiefgreifende Wirkungen entfalten und eine **elementare Bedrohung** für Wirtschaft und Gesellschaft darstellen.

3.5 /1 Cyberangriffe auf kritische Infrastrukturen unseres Landes unter dem Titel "Vergeltungmassnahmen" können **jederzeit** ausgeführt werden. Die personellen und materiellen Voraussetzungen zur Auslösung von Angriffen sind vorhanden; sie sind einsatzbereit und wurden auch bereits wiederholt eingesetzt. Aus diesem Grunde wird an dieser Stelle aufgrund der **veränderten Bedrohungslage** die Schaffung einer Rechtsgrundlage für die wirkungsvolle Integration, Koordination und Bündelung der in unserem Land vorhandenen Mittel zur Abwehr von Cyberangriffen auf dem Weg des von der Verfassung vorgesehenen **Dringlichkeitsverfahren** vorgeschlagen.

/2 Derartige Aktionen sind auch an **keine Landesgrenzen** gebunden. Daher greift leider die von vielen Verantwortlichen getroffene Annahme ins Leere, wenn in optimistischem Unterton vorgegeben wird, die Schweiz sei zur Zeit nicht bedroht, weil wir ja von einem einfachen oder sogar doppelten "Cordon Sanitaire" befreundeter Nationen umgeben seien, welche Angriffe gegen unser Land abfangen und unsere Verteidigung übernehmen würden.

/3 Befreundete Nachbarn oder das von der NATO um unsere Grenzen aufgebaute Schutzdispositiv nach der Beistandsklausel von Art. 5 des NATO Vertrages https://de.wikipedia.org/wiki/Nordatlantikvertrag bieten für ein neutrales Land wie die Schweiz jedoch keinen Schutz vor Cyberangriffen.

/3 Vielmehr müssen Cyberangriffe auf kritische Infrastrukturen nach hier vertretener Meinung als geradezu klassisches Mittel von Vergeltungsmassnahmen für die von "unfreundlichen" bündnisfreien Nationen wie der neutralen und unabhängigen Schweiz ergriffenen Sanktionen betrachtet werden.

/4 Andererseits ist denkbar, dass "Vergeltungsmassnahmen" gegen die Schweiz und unsere ebenfalls in die Liste unfreundlicher Nationen aufgenommenen Nachbarländer in einem konzentrierten Angriff ausgelöst werden. Daher ist zu empfehlen, dass die Schweiz Vorkehrungen trifft, um bei der Abwehr von Cyberangriffen **mit unseren Nachbarländern zusammenarbeiten** zu können, z.B. durch Austausch von Informationen über erkannte Bedrohungen, Auftauchen neuartiger Formen von "Malware" und deren Verbreitung über sog. "Bot-Netze" https://de.wikipedia.org/wiki/Botnet , estgestellte Eindringversuche usw.

4. Aktuelle Bedrohungsanalyse

4.1 Für die Schweiz stehen nach hier vertretener Auffassung Cyberangriffe auf die elektronische Steuerung folgender im Inventar des Bundes gemäss Art. 8 BGZ aufgenommenen kritischer Infrastrukturen als besonders gefährliche Attacken im Vordergrund gegen

a. die **Stromversorgung** in unseren grossen Energiezeugungsanlagen, den Kernkraftwerken, deren Betreiber sowie insbesondere unsere nationale Netzgesellschaft **Swissgrid** in Aarau und Prilly für die Betrieb des schweizerischen Höchstspannungsnetzes https://de.wikipedia.org/wiki/Swissgrid weil ein "**Blackout**" für grössere Teile unseres Landes und über längere Zeit unabsehbare Folgen für Wirtschaft und Gesellschaft hätte https://energieclub.ch/de/home

b. das europäische Operation Center (OPC) der Organisation **SWIFT** zur Abwicklung des grenzüberschreitenden Zahlungsverkehrs https://de.wikipedia.org/wiki/SWIFT in Diessenhofen [Das SWIFT OPC Diessenhofen wird zur Zeit von der Kantonspolizei Thurgau bewacht; es gibt im Internet allerdings eine Serie von 26 Luftaufnahmen des OPC aus verschiedenen Winkeln, welche die gedeckten Annäherungsmöglichkeiten an die Anlage bei Tag und Nacht für interessierte "Besucher" abbilden https://www.reportair.ch/archiv/index.php?q=Kanton_Thurgau%2FDiessenhofen%2FDiessenhofen_Swift_Datenzentrum%2F1 https://www.fm1today.ch/ostschweiz/thurgau/sabotage-moeglich-polizei-schuetzt-swift-rechenzentrum-145661864; Es wird jedoch an dieser Stelle davon ausgegangen, dass man - hoffentlich - Vorsorge getroffen hat, Cyber Attacken professionell zu begegnen].

c. Die für die Geld- und Währungspolitik unseres Landes, die Bargeldversorgung und die Abwicklung des bargeldlosen Zahlungsverkehrs verantwortliche **Schweizerische Nationalbank** (SNB) https://de.wikipedia.org/wiki/Schweizerische_Nationalbank

4.2 Darüber hinaus ist nach den Erfahrungen im Ausland - in nicht abschliessender Aufzählung - zu rechnen mit Attacken von meist anonymen professionellen Hackern aus dem Gebiet der russischen Föderation, Belarus oder anderen mit Russland "befreundeten Nationen" wie China oder Nordkorea, insbesondere gegen die **elektronische Infrastruktur für den Einsatz folgender Organisationen**:

a. Versorgung / Entsorgung mit Wasser und Lebensmitteln

b. Kantonsspitäler, grosse Regionalspitäler und medizinische Laboratorien

c. Chemische Fabriken und pharmazeutische Unternehmen

d. Betrieb der Mobilitäts-Infrastruktur (Bahnen und Flugplätze und Strassen-Transportdienste)

e. Informatik-Abteilungen der Hochschulen mit Cyber Security Spezialisten

f. zivile und militärische Luftraumüberwachung

g. die beiden "systemrelevanten" sowie bedeutende Kantonal- und Genossenschafts-Banken

h. Telekommunikation (Swisscom) und Medien: Radio, TV

i. Post und Possfinance,

j. Bundesorgane wobei vor allem das VBS mit Armee und Zivilschutz im Vordergrund stehen, sowie das EDA für die Kooperation mit ausländischen Cyber Abwehrorganisationen

k. Organe von Kantonen und grösseren Gemeinden, insbesondere die kantonalen Führungsstäbe sowie Polizei und Feuerwehr

5. Verantwortung für Schutzvorkehrungen und Abwehrmassnahmen

5.1 Nach hier vertretener Auffassung sind für die Organisation von **Abwehrmassnahmen gegen Cyber Attacken primär die privaten oder öffentlich-rechtlichen Betreiber** verantwortlich, doch wird das NCSC dazu Information, Aufklärung, technische und organisatorische Unterstützung leisten, jedoch auch eine Aufgabe der Überwachung und Kontrolle zu übernehmen haben.

5.2 Es ist davon auszugehen dass bei einem Cyber-Angriff auf eine kritische Infrastruktur (z.B. die Verkehrs-Infrastruktur) mehrere Bereiche von Wirtschaft und Gesellschaft betroffen sein können: Es sollten somit Voraussetzungen für die **Kooperation und Koordination** der mit der Abwehr von Cyberangriffen betrauten Stellen und Organisationen unseres Landes geschaffen werden.

5.3 In diesem Zusammenhang wird nach hier vertretener Auffassung der **IKT Branche** bei der Organisation der Verteidigung gegen Cyber-Attacken **besondere Bedeutung** zukommen: National und international tätige IKT Unternehmen gehören zur "*First Line of Cyber Defence*", weil sie den Anwendern sicherheitsgeprüfte Geräte, Netzwerklösungen und virenfreie Betriebs- und Anwendungsprogramme vermitteln, Cloud-Dienstleistungen in sicherer Umgebung betreiben, bei der Analyse von Unterbrüchen und der Überwindung der Auswirkungen von Cyber-Attacken mitwirken, eingeschleuste Schadprogramme erkennen und eliminieren, bei einem Systemausfall Back-up Services anbieten und damit zur **Resilienz der Anwender** beitragen Daher sollten die IKT Unternehmen angehalten werden, nicht nur ihren Kunden, sondern durch Zusammenarbeit mit dem NCSC der Gesamtheit der Anwender ihre Kenntnisse und Erfahrungen zur Abwehr von Cyberangriffen in geeigneter Art und Weise verfügbar zu machen.

Ideen und Vorschläge zur Umsetzung

Folgende Regeln könnten in nicht abschliessender Aufzählung in die zur Festigung der Abwehr von Cyber-Attacken unseres Landes im Dringlichkeitsverfahren zu erlassende Rechtsgrundlage aufgenommen werden:

1. Für das NCSC ist durch Rechtssatz eine **geeignete Organisation** für seine anspruchsvolle Aufgabe durch Einordnung in die Bundesverwaltung festzulegen.

2. Regelung von Auftrag, Schnittstellen und Kompetenzen des NCSC für die **Bündelung von Massnahmen auf dem Gebiet der Cyber-Defence** tätigen Stellen und Organisationen wie

- Cyber Defence von Armee (Cyber Bataillon 42) und Armasuisse
- Zivil- und Bevölkerungsschutz
- Nachrichtendienst des Bundes
- IKT (Dienstleistungs-) Anbieter
- Kantonale Führungsstäbe
- Polizei; Strafverfolgungsbehörden
- EDA - Diplomatische Vertretungen

3. Das NCSC ist mit den erforderlichen **personellen und materiellen Mitteln** zur Erfüllung seiner Aufgaben auszustatten.

4. Das NCSC **bezeichnet** [analog Art. 8 BZG] **die einzelnen** - durch einen **nicht rückführbaren Code g**ekennzeichneten - im Bereich der Cyber Defence kritischer Infrastrukturen gemäss vorstehender Ziff. 4.2 tätigen **meldepflichtigen Organisationen** und führt darüber eine **geheime und verschlüsselte Liste.**

5. Der **Meldepflicht** sollen auch bezeichnete qualifizierte **IKT Anbieter** für die bei ihrer Tätigkeit festgestellten Anzeichen von Cyberangriffen unterstellt werden.

6. Es sollte ein **elektronisches Meldeformular** geschaffen werden, auf welchem Meldungen der durch ihren **Code gekennzeichneten Organisationen** von Sicherheits-Vorfällen über s**ichere, redundante Kommunikationsmittel verschlüsselt** an das NCSC übermittelt werden können.

7. **Voraussetzungen** und **Inhalt** der der zu erstattenden Meldungen sollte definiert werden.

8. Es sollte eine **abhörsichere Kommunikation** zwischen dem NCSC und den gemäss Ziff. 4 im Bereich kritischer Infrastrukturen tätigen und den gemäss Ziff. 5 meldepflichtigen Organisationen vorhanden sein.

9. Die erhaltenen Meldungen und die vom NCSC bearbeiteten Daten sind gestützt auf eine Spezialbestimmung im Sinne von Art. 4 BGÖ von der **öffentlichen Einsichtnahme gemäss BGÖ ausdrücklich auszunehmen**; das Auskunftsrecht betroffener Personen sollte sich nach dem DSG richten.

10. Die **Kontrolle der Tätigkeit des NCSC** wird durch eine zur Verschwiegenheit verpflichteten unabhängigen Aufsichtsbehörde im Sinn von Art. 76 ff NDG wahrgenommen, mit Oberaufsicht des Parlamentes.

11. Das NSCS sollte beauftragt und ermächtigt werden, die von den Betreibern kritischer Infrastrukturen getroffenen **Sicherheitsmassnahmen zu überprüfen** und zusätzliche **Verbesserungen anzuordnen**.

12. Die Anordnungen und Verfügungen des NCSC gemäss vorstehender Ziff. 11 sollten **keine aufschiebende Wirkung haben**; ihre **Nichteinhaltung** sollte **sanktioniert** sein, im Extremfall durch polizeilich durchsetzbare **Einstellung des Betriebs** der betreffenden kritischen Infrastruktur.

13. Es wird eine **besondere Strafnorm** mit einem **angemessen abschreckenden Strafmass** im StGB für Cyberangriffe auf kritische Infrastrukturen und die vorsätzliche Verletzung der Meldepflicht (für eingeschleuste Malware!) geschaffen.

14. Die Verfolgung dieser Delikte soll der **Bundesgerichtsbarkeit** obliegen.

15. Es soll eine Möglichkeit **für Gegenmassnahmen gegen einen Cyberangriff** auf kritische Infrastrukturen geschaffen werden.

16. Das NCSC darf und soll für die Erfüllung seiner Aufgaben mit **spezialisierten privatrechtlichen Organisationen und der wissenschaftlichen Forschung** im Bereich von Leistungen für die IKT Sicherheit zusammenarbeiten [auch mit talentierten "ethischen Hackern" aus dem Kreis des Chaos Computer Club]

17. Das NSCS muss zur **Zusammenarbeit mit ausländischen Organisationen** zur Bekämpfung von Cyberangriffen beauftragt und ermächtigt werden; denn die Abwehr gegen Cyber-Attacken professioneller ausländischer Agenten kann nur im internationalen Verbund wirkungsvoll realisiert werden.

Der Unterzeichnende ist sich selbstverständlich bewusst, dass die in dieser Stellungnahe enthaltenen Anträge und Vorschläge als **Ideen und Anregungen** zu verstehen sind, welche unserem Land angesichts der aktuellen veränderten Bedrohungslage die erfolgreiche Abwehr von Cyberangriffen professioneller Organisationen aus einem der Schweiz nicht freundlich gesinnten Land erleichtern sollen.

Beat Lehmann

Schlussbemerkung

Aufgrund der von einer üblichen Stellungnahme zu einem Gesetzgebungsvorschlag abweichenden Anträgen werde ich mir erlauben, den Inhalt des Dokumentes den Entscheidungsträgern politischer Parteien und Organisationen zugänglich zu machen

per E-Mail an: ncsc@gs-efd.admin.ch

Eidgenössisches Finanzdepartement
Bundesgasse 3
3003 Bern

13. April 2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe; Vernehmlassung

Sehr geehrter Herr Bundesrat Maurer
Sehr geehrte Damen und Herren

Die Coop-Gruppe (nachfolgend «Coop») bedankt sich für die Gelegenheit, zur Einführung einer Meldepflicht für Betreiberinnen kritischer Infrastrukturen für Cyberangriffe Stellung nehmen zu können.

Coop anerkennt grundsätzlich, dass die Schaffung einer Meldepflicht für kritische Infrastrukturen eine adäquate Schutzmassnahme gegen Cyberangriffe darstellt. Als Unternehmensgruppe, die in verschiedenen Bereichen tätig ist, ist der vorliegende Gesetzesentwurf jedoch mit zu vielen Unklarheiten verbunden und führt zu grosser Rechtsunsicherheit. Aus Sicht von Coop sind die Definitionen von kritischen Infrastrukturen sowie zu meldender Sachverhalte im Entwurf zu umfassend und unklar. Es ist hierbei eine Regulierung mit Augenmass anzustreben, welche ein positives Kosten/Nutzen-Verhältnis aufweist.

Grundhaltung Coop: Rechtssicherheit zentral – Definitionen zu umfassend

- Die Liste der Bereiche, welche als kritische Infrastrukturen angesehen werden sollen, ist zu umfassend. Zudem ist die Rechtssicherheit nicht gegeben, da es für viele Unternehmen nicht klar ist, ob man unter die Definition fällt. Es ist eine klare und abschliessende Bezeichnung zu wählen.
- Die pauschale Unterstellung ganzer Unternehmen unter die Meldepflicht ist abzulehnen. Nur die Unternehmensbereiche, bei welchen es sich um kritische Infrastrukturen handelt, sind der Meldepflicht zu unterstellen.
- Die Definition der zu meldenden Sachverhalte ist zu breit und zu unklar, was wiederum zu Rechtsunsicherheit führt. Es ist auch hier eine klare und abschliessende Definition zu wählen.
- Bussen sind abzulehnen, da sie zu Fehlanreizen führen.
- Doppelspurigkeiten bei Meldungen sind zu vermeiden.

Coop Genossenschaft
Wirtschaftspolitik
Hauptsitz

Thiersteinerallee 12
Postfach 2550
4002 Basel
Schweiz

Tel. +41 61 336 72 04
Fax +41 61 336 60 40
CHE-116.311.185 MWST

Damian.Misteli@coop.ch
www.coop.ch

Zu den einzelnen Punkten

Definition kritische Infrastrukturen zu umfassend

Generell sind wir der Ansicht, dass nicht primär das Medium alleine, über das ein Dienst bzw. eine Tätigkeit ausgeführt wird, ausschlaggebend für die Einstufung als kritische Infrastruktur ist, sondern der konkrete Inhalt/Gegenstand eines Dienstes bzw. einer Tätigkeit sowie seine Bedeutung für das Funktionieren der Wirtschaft bzw. das Wohlergehen der Bevölkerung.

Die Meldepflicht ist also auf als kritisch erachtete Tätigkeiten innerhalb des Unternehmens zu beschränken. Nicht das gesamte Unternehmen bzw. die Unternehmensgruppe soll pauschal der Meldepflicht unterstellt werden, sondern die relevanten Unternehmensbereiche. Zur Coop-Gruppe gehören nebst Lebensmittelgeschäften u.a. auch Parfümerie- und Schmuckgeschäfte. Diese auch einer Meldepflicht zu unterstellen, wäre unverhältnismässig. Eine Meldepflicht ist daher auf diejenigen Bereiche zu beschränken, deren Ausfall oder Beeinträchtigung zu nachhaltig wirkenden Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen führen würde.

Weiter vermissen wir eine risikobasierte Regelung, wonach die Betreiberin von kritischen Infrastrukturen anhand einer Risikoabwägung im Einzelfall von einer Meldepflicht absehen kann, da z.B. erkennbar - und auch entsprechend dokumentiert - keine oder nur geringe Schadensereignisse eingetreten sind.

Definition zu meldender Sachverhalte zu breit

Die vorgeschlagene Definition ist zu generisch und zu breit (Art. 5 E-ISG). Es gibt keine klare Differenzierung zwischen Vorfällen, welche keinen oder nur einen unwesentlichen Einfluss auf die Geschäftsprozesse haben und solchen, die das Betreiben kritischer Infrastrukturen direkt betreffen oder ein hohes Risiko bergen.

Nach momentanem Wortlaut des Entwurfes müssten ausserdem sowohl erfolgreiche als auch nicht erfolgreiche Cyber-Angriffe dem NCSC gemeldet werden. Aufgrund der vorhandenen Informationen müssen wir davon ausgehen, dass bereits lediglich Anzeichen auf einen Angriff zur Meldepflicht führen könnten. Ausnahmen von der Meldepflicht sind nur für bestimmte Kategorien von Betreiberinnen nach Art. 74c E-ISG, nicht aber für bestimmte Arten von Angriffen geplant. Art. 74d E-ISG, welcher die zu meldenden Cyberangriffe definiert, ist deshalb zwingend zu überarbeiten. Die Kriterien sind zu weit gefasst und für die Unternehmen kaum greif- oder umsetzbar. Zielführender wäre es, eine eingeschränktere (Positiv-)liste der zu meldenden Vorfälle zur Verfügung zu stellen und die Meldepflicht generell nur auf erfolgreiche oder besonders schwerwiegende Versuche zu begrenzen.

Dass z.B. Cyberangriffe, welche länger als 30 Tage unentdeckt blieben, gemeldet werden müssen (vor allem in Kombination mit der ebenfalls abzulehnenden Strafbarkeit), ist nicht sinnvoll und scheint auch für die Zielsetzung der Einführung einer Meldepflicht nicht relevant.

Ebenso schwierig ist das Kriterium der Involvierung eines fremden Staates. Je nachdem kann ein Unternehmen dies zum Zeitpunkt der Entdeckung gar nicht wissen.

Das Ziel einer Meldepflicht soll es sein, dass ein Unternehmen in bestimmten und klar definierten Fällen mit den Behörden in den Dialog tritt. In diesem Dialog können dann weitere Fragen geklärt werden, wie zum Beispiel auch der Absender. Die Anforderungen an die Meldung an sich müssen jedoch einfach gehalten werden, um die Hürden für die Unternehmen tief zu halten.

Bussen kontraproduktiv
Coop erkennt wenig Sinn, die neuen Pflichten mit Bussen durchzusetzen. Dies kann zu Fehlanreizen führen und bspw. die Bereitschaft der zuständigen Personen reduzieren, in Sachen Cyber-Security Verantwortung zu übernehmen. Gerade die im Cyber-Bereich so wichtige Fehlerkultur wird damit untergraben. Art. 74i ist daher zu streichen.

Doppelspurigkeiten bei Meldungen sind zu vermeiden
Es ist essenziell, dass Unternehmen in Stresssituationen sich nicht zusätzlich darum kümmern müssen, mehrere, sich überschneidende Meldepflichten wahrzunehmen. Hierbei ist aus unserer Sicht der Bund in der Pflicht, eine optimale Koordination sicherzustellen.

Wir danken für die Kenntnisnahme und für die Berücksichtigung unserer Anmerkungen.

Freundliche Grüsse

Coop

Reto Conrad
Mitglied der Geschäftsleitung
Leiter Direktion Informatik / Produktion / Services

Damian Misteli
Mitglied des Fachmanagements
Stv. Leiter Wirtschaftspolitik

Flughafen Zürich

Eidgenössisches Finanzdepartement EFD
Bundeshaus West
CH-3003 Bern

Per Email an
ncsc@gs-efd.admin.ch

Zürich-Flughafen, 4. April 2022

Vernehmlassung zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe – Stellungnahme Flughafen Zürich AG

Sehr geehrte Damen und Herren

Mit Schreiben vom 12 Januar 2022 hat Herr Bundesrat Ueli Maurer interessierte Kreise zur Teilnahme an der erwähnten Vernehmlassung eingeladen. Gerne nehmen wir die Gelegenheit wahr, unsere Anliegen zur geplanten Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe zu äussern. Die Flughafen Zürich AG ist Eigentümerin und Betreiberin des grössten Landesflughafen mit über 30 Millionen Passagieren im Jahr. Nach unserem Verständnis und der vom Bundesrat definierten nationalen Strategie «Spektrum der kritischen Infrastrukturen» fällt auch der Flughafen Zürich unter die Definition einer kritischen Infrastruktur. Mit Verweis auf Art. 74b lit p könnte jedoch angenommen werden, dass lediglich Fluggesellschaften mit Bewilligung des Bundesamtes für Zivilluftfahrt (BAZL) von der Meldepflicht betroffen wären. Hier wäre eine Präzisierung im Sinne der Rechtssicherheit erwünscht, ob auch die Landesflughäfen betroffen sind – für die Flughafen Zürich AG ist das Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK) die Konzessionsgebende Behörde.

Die Flughafen Zürich AG anerkennt, dass Cyberrisiken zu einer wichtigen Bedrohung für die Schweiz und für Unternehmen geworden sind. Dazu gehören namentlich auch die Betreiberinnen von kritischen Infrastrukturen. Bereits heute findet innerhalb der Closed Usergroups des NCSC ein ständiger Austausch zwischen den Unternehmen statt, der insbesondere die Meldepflicht bei erfolgreichen Cyberattacken umfasst. Dazu gibt es eine lose Interessengruppe bestehend aus Flughäfen im deutschsprachigen Raum. Die Flughafen Zürich AG ist als Konzessionärin des Bundes bereits heute für Vorfälle meldepflichtig, die potenzielle Auswirkungen auf die Sicherheit haben. Das beinhaltet die Meldung von erfolgreichen Cyber-Angriffen an das BAZL. Zusätzlich nimmt unser Unternehmen am freiwilligen Austausch über Cybervorfälle via NCSC teil. Eine Harmonisierung und Koordination der Meldepflicht auf Bundesebene und damit

andrew.karim@zurich-airport.com | T +41 43 816 71 29 | M +41 77 529 13 93
Flughafen Zürich AG | Postfach | CH-8058 Zürich-Flughafen | flughafen-zuerich.ch

die Förderung des Informationsaustauschs zwischen den Sektoren ist daher grundsätzlich begrüssenswert. Dass die Meldepflicht wie im erläuternden Bericht dargelegt «einen möglichst geringen Mehraufwand» bedeuten soll, wird unterstützt. Mittelfristig ist eine Harmonisierung der Meldepflichten anzustreben, sodass Unternehmen lediglich an einer Stelle einen Angriff melden müssen.

Mit der Vernehmlassungsvorlage sollen ebenfalls die rechtlichen Grundlagen geschaffen werden, um die Informationen ohne Einverständnis der Betreiberinnen weiterzuleiten. Dies wird unterstützt, sofern es nur die Weiterleitung der Information betrifft und keine Forensik über die Ursachen des Vorfalls betrieben bzw. die Berichterstattung vorgeschrieben wird. Insbesondere ist es wichtig, dass durch Melde- und Aufklärungspflichten die Wiederherstellung der Systeme und das Aufrechterhalten des Betriebs nicht tangiert werden. Dies könnte ansonsten zu massiven wirtschaftlichen Einbussen führen.

Allerdings ist es unerlässlich, eine Präzisierung im vorgeschlagenen Gesetzestext vorzunehmen und lediglich erfolgreiche Cyberangriffe der Meldepflicht zu unterstellen. Für erfolgreiche Cyberattacken ist eine Informations- und Meldepflicht für alle Betreiberinnen von kritischen Infrastrukturen unbestritten und bereits heute zu einem gewissen Grad etabliert. Damit können der Informationsaustausch und der Schutz der anderen Infrastrukturen sichergestellt werden. Unverhältnismässig ist es jedoch, jeden versuchten Cyberangriff (gemäss Entwurf «Cybervorfall») der Meldepflicht zu unterstellen. Dies widerspricht auch dem erläuternden Bericht, wonach «die Meldepflicht nur für Cyberangriffe gelten [soll], die ein gewisses Schadenspotential aufweisen».

Art. 74a könnte in Verbindung mit Art. 5 Bst. lit e dahingehend interpretiert werden, dass jeder Cyberangriff der Meldepflicht unterstehen soll. Dies kann bei Rechtsanwendern zu Missverständnissen bzw. Unsicherheiten führen und darüber hinwegtäuschen, dass es letztlich Art. 74d ist, der kumulativ aufführt, wann ein Angriff auf eine kritische Infrastruktur zu melden ist. Hier wäre eine Präzisierung wünschenswert, mit der klargestellt wird, dass lediglich Cyberangriffe im Sinne von Art. 74d der Meldepflicht unterstehen sollen. Die Lösung könnte bspw. darin bestehen, dass in Art. 74a ausdrücklich auf die Regelung von Art. 74d verwiesen wird.

Antrag 1: Ergänzung Art. 74a

Die Betreiberinnen von kritischen Infrastrukturen müssen dem NCSC Cyberangriffe *im Sinne von Art. 74d* nach deren Entdeckung so rasch als möglich melden, damit das NCSC Angriffsmuster frühzeitig erkennen, mögliche Betroffene warnen und ihnen geeignete Präventions- und Abwehrmassnahmen empfehlen kann.

Neben der oben vorgeschlagenen Anpassung gilt es auch die Definition der zu meldenden Cyberangriffe zu überarbeiten. Die Auflistung von Kriterien wie sie Art. 74d vorsieht ist hinsichtlich der Klarheit der Auslegung des Gesetzes positiv zu werten. Aber auch hier ist ein verhältnismässiger Ansatz zu wählen, der den betriebswirtschaftlichen und operationellen Möglichkeiten von Unternehmen Rechnung trägt. Mit dem Ziel des Gesetzes und der Meldepflicht soll vornehmlich ein Informationsaustausch mit dem Bund in der Hauptrolle gefördert werden. Dieses Ziel kann bereits erreicht werden, wenn erfolgreiche Cyberangriffe

auf die eigene Infrastruktur dem Bund gemeldet werden. Art. 74a regelt bereits, dass das NCSC «mögliche Betroffene warnen und ihnen geeignete Präventions- und Abwehrmassnahmen empfehlen kann».

Im Falle eines Angriffes auf die eigene Infrastruktur wird ein Unternehmen die volle Aufmerksamkeit darauf richten, den Angriff abzuwehren bzw. die Systeme wieder herzustellen. Es sollte deshalb beim Bund und nicht beim betroffenen Unternehmen liegen, zu überprüfen, inwiefern andere kritische Infrastrukturen gefährdet sind. Diese Aufgabe darf nicht auf die Unternehmen abgewälzt werden, insbesondere nicht in einer allfälligen eigenen Notsituation.

Im Weiteren ist es das Ziel des Gesetzes, den Strafbehörden und dem Nachrichtendienst durch die Meldepflicht Informationen zu Cyberangriffen zur Unterstützung zur Verfügung zu stellen. Diese polizeilichen Aufgaben sollten ausschliessen von spezialisierten Behörden erfüllt und nicht auf private Unternehmen abgewälzt werden. Diese verfügen nicht über die nötigen Informationsgrundlagen noch das Wissen, um eine qualifizierte Aussage darüber zu treffen, ob ein fremder Staat in den Angriff involviert ist. Es kann daher nicht Aufgabe von Privaten sein, zu untersuchen, inwiefern ein fremder Staat einen erfolgreichen Cyberangriff ausgeführt oder veranlasst hat.

Art. 74d lit c zielt auch auf schützenswerte Daten gemäss Datenschutzgesetz ab. Diese sind bereits dem Datenschutzbeauftragten des Bundes zu melden. Im Sinne der Vermeidung von Doppelspurigkeiten ist in der Verordnung darauf zu achten, dass nicht eine zweifache Meldepflichte entsteht, sondern im Fall eines Verlusts von Personendaten diese vom NCSC direkt beim Datenschutzbeauftragten abzuholen sind.

Es ist zu beobachten, dass sogenannte stille Cyberangriffe (Art. 74d ISG) zunehmen und viel kritischer für die Sicherheit geworden sind. Da direkte Angriffe oftmals schneller entdeckt werden, können stille Angriffe über Tage, Wochen oder sogar Monate unbemerkt bleiben. Hier ist nicht zwingend die Dauer des Angriffs entscheidend, sondern vielmehr der Schweregrad des Angriffs bzw. ob andere Unternehmen von der Meldung profitieren könnten.

Antrag 2: Art. 74d ISG ist anzupassen, dass Unternehmen im Falle eines erfolgreichen Angriffs lediglich eine Meldepflicht haben und keine polizeilichen oder Sicherheits-Aufgaben übernehmen sowie dass die Meldepflicht zeitunabhängig auf den Schweregrad abgestützt wird.

1 Ein *erfolgreicher* Cyberangriff auf eine kritische Infrastruktur muss gemeldet werden, wenn Anzeichen dafür bestehen, dass:

a. die Funktionsfähigkeit der betroffenen kritischen Infrastruktur ~~oder einer anderen kritischen Infrastruktur~~ gefährdet ist;

b. ~~ein fremder Staat ihn ausgeführt oder veranlasst hat~~;

c. er zu einem Abfluss oder zur Manipulation von Informationen geführt hat oder führen könnte; oder

d. ~~er länger als 30 Tage unentdeckt blieb~~. *wenn er trotz technischer Mittel unentdeckt blieb und andere von der Entdeckung profitieren würden.*

2 Ein Cyberangriff auf eine kritische Infrastruktur muss immer gemeldet werden, wenn er mit Erpressung, Drohung oder Nötigung gegenüber der Betreiberin einer kritischen Infrastruktur oder ihren Mitarbeitenden verbunden ist.

Gemäss erläuterndem Bericht sollen durch die angedachte Meldepflicht andere Betreiberinnen kritischer Infrastrukturen rechtzeitig gewarnt werden. Zur Erhöhung der Cybersicherheit in der Schweiz sieht der Bericht vor, den heute freiwilligen Informationsaustausch unter Wahrung der «Kultur der Zusammenarbeit und des gegenseitigen Vertrauens» auszubauen. Ebenso soll den Unternehmen durch die Einführung ein Mehrwert entstehen. Die in Art. 74h vorgeschlagenen Sanktionen stehen im Widerspruch zu den aufgeführten Zielen der Vorlage. Sollen der Austausch und ein kooperatives Verhalten gefördert werden, so sind andere Mittel zu wählen als eine Sanktion. Zielführender ist es, den Aufruf zur Zusammenarbeit durch Unterstützungsleistungen, Hilfe zur Bekämpfung von Cyberangriffen, gegenseitige Schulungen und Informationsaustausch zu bewerkstelligen, die einen Mehrwert für den Schutz der kritischen Infrastruktur bieten. Anstelle einer finanziellen Strafe ist eine Zugangsbeschränkung zu diesen Hilfeleistungen vorzusehen. Damit wird die freiwillige Kooperationsbereitschaft gestärkt.

Antrag 3: Art 74h ist wie folgt anzupassen

2 Kommt die Betreiberin trotz dieser Information ihrer Pflicht nicht nach, so erlässt das NCSC eine Verfügung über die umzusetzenden Pflichten, setzt ihr darin eine Frist und verweist auf ~~die Bussandrohung~~ *den Ausschluss* nach Artikel 74i.

Der heute stattfindende aktive Austausch mit dem NCSC ist zufriedenstellend. Hauptreiber ist das Eigeninteresse der Betreiberinnen von kritischen Infrastrukturen. Es ist deshalb entscheidend, dass das NCSC den Unternehmen weiterhin diesen Mehrwert bietet, damit der Austausch weiter genutzt wird. Eigeninteresse ist der beste Treiber, insbesondere im Zusammenhang mit Cyberrisiken. Sanktionen verhindern aber gerade diese Freiwilligkeit und limitieren oftmals den Austausch. Aus diesem Grund gilt es, auf finanzielle Sanktionen zu verzichten und stattdessen eine Sanktionierung durch Ausschluss aus der Austauschgruppe zu wählen.

Demzufolge ist auch Art. 74i anzupassen, um den Gedanken der freiwilligen Zusammenarbeit zu fördern und den Mehrwert des Austauschs aufzuzeigen. Betreiberinnen von kritischen Infrastrukturen sollen von Unterstützungsleistungen, Hilfeleistungen, Schulungen und Informationsaustausch ausgeschlossen werden, wenn sie ihrer Meldepflicht nicht nachkommen. Mit einer freiwilligen Teilnahme wird – analog zur Luftfahrt – eine positive Fehlerkultur gestärkt, die dazu führt, dass gemeinsam aus Fehlern gelernt wird, Prozesse verbessert werden und letztlich die Sicherheit erhöht werden kann. Alle Teilnehmer profitieren von einem Dialog und offenen Austausch untereinander sowohl zur Bekämpfung von Schadensfällen als auch in der Prävention vor Cyberangriffen.

Antrag 4: Art. 74i ist gänzlich zu streichen und wie folgt anzupassen

Mit Ausschluss von Unterstützungsleistungen, Hilfe zur Bekämpfung von Cyberangriffen, Schulungen und Informationsaustausch und weiterer Angebote des NCSC wird bestraft, wer einer vom NCSC unter Hinweis auf diesen Artikel erlassenen rechtskräftigen Verfügung vorsätzlich nicht Folge leistet.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Michael Hofmeier
Leiter Information & Communication Technology

Andrew Karim
Stv. Leiter Public Affairs

Politische Gemeinde
Gachnang
Neues Schloss
Islikonerstrasse 7
8547 Gachnang

Energiestadt
european energy award

Schweizerische Eidgenossenschaft
Finanzdepartement
Herr Bundesrat Ueli Maurer
Per E-Mail: ncsc@gs-efd.admin.ch

GEMEINDERATSKANZLEI
Telefon 058 346 28 09
Telefax 058 346 28 00
E-Mail manuela.haas@gachnang.ch
Webseite www.gachnang.ch

Gachnang, 9. Februar 2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe - Vernehmlassung

Sehr geehrter Herr Bundesrat

Wir danken Ihnen für die Möglichkeit zur Stellungnahme zum Vernehmlassungsentwurf zur Einführung einer Meldepflicht für Cyberangriffe.

Wir begrüssen die Einführung einer Meldepflicht für Cyberangriffe und die definierten Aufgaben für das NCSC, welches als zentrale Meldestelle für Cyberangriffe vorgesehen ist.

Gerne nehmen wir zu folgenden Punkten Stellung:

Generell

Antrag: Das NCSC muss in seiner Arbeit auch regelmäßig überprüft werden. Eine Revision/ein Audit sollte daher im Gesetz vermerkt werden. Zudem soll geregelt sein, dass bei Bedarf die nötigen Ressourcen (personell, technisch etc.) bezogen werden können.

Begründung: Das NCSC soll effizient das Richtige tun und es nachweisen können. Revisionen/Audits können dazu dienen, dies nachzuweisen. Zudem können Revisionen nötige Maßnahmen erkennen und an die richtige Stelle weitertragen. Auch soll der Datenschutz überprüft werden. Wird z. B. Art. 79 Abs. 1, Bewahren von Personendaten im Sinne des Gesetzes getätigt? Werden infolge außerordentlicher Beobachtungen/Vorkommnissen personelle und/oder technische Ressourcen benötigt, sollten diese verfügbar sein. Auf die Gefahr, die aus Cyberangriffen entstehen kann, soll durch eine bestmögliche Vorbereitung entgegengewirkt werden können.

Artikel 5- Begriffe

Antrag: In die Begriffsdefinition soll der Begriff „Cyber" aufgenommen werden.

Begründung: „Cyber" ist ein Wortverbindungselement, welches heute eine virtuelle Computer-Scheinwelt bezeichnet. Der Rahmen dieses Gesetztes und die Zuständigkeit werden dank der Definition klarer.

Politische Gemeinde
Gachnang
Neues Schloss
Islikonerstrasse 7
8547 Gachnang

Energiestadt
european energy award

Antrag: In die Begriffsdefinition soll der Begriff „Betreiberin" aufgenommen werden.

Begründung: Die Definition stellt klar, wer an die Auskunftspflicht gebunden ist. Dies ergänzend zu Art. 74a und b.

Artikel 73a – Grundsatz

Antrag: Ergänzung der Aufgaben sinngemäß mit Lit. g: Regelmäßiges Reporting an (z. B. jährlich an den zuständigen Bundesrat) zwecks Qualitätssicherung und Erfolgskontrolle.

Begründung: Das NCSC soll seine Arbeiten (Ausblick: Risiken, Maßnahmen etc. Rückblick: Erfolge/Misserfolge etc.) der richtigen Stelle darlegen können. Ziel: Das NCSC soll das „Richtige" tun und regelmäßig sachlich-kritisch geprüft werden und sich den aktuellen Gegebenheiten anpassen.

Artikel 74 Abs. 3 – Unterstützung von Betreiberinnen von kritischen Infrastrukturen

Antrag: *Ergänzung mit „und öffentliche"*, wie folgt: ...besteht und, sofern es sich um private *und öffentliche* Betreiberinnen handelt, die Beschaffung... Zudem sollte der lange Satz in Teilsätze aufgeteilt werden.

Begründung: Nebst den privaten Betreiberinnen gibt es auch öffentlich-rechtliche Betreiberinnen, die auf Unterstützung angewiesen sein könnten, wenn auf dem privaten Markt keine Unterstützung vorliegt. Der aufgeteilte Satz wird in Teilsätzen verständlicher.

Besten Dank für die Entgegennahme und die kritisch-sachliche Prüfung unserer Anträge. Wir würden uns freuen, wenn wir mit unseren Anträgen der Sache dienen könnten.

Freundliche Grüsse

POLITISCHE GEMEINDE GACHNANG

Roger Jung
Gemeindepräsident

Manuela Haas
Gemeindeschreiberin

GENÈVE
AÉROPORT

DIRECTEUR GÉNÉRAL

GPO

Par courriel
Département fédéral des finances
Monsieur Ueli Maurer
Conseiller fédéral
Bundesgasse 3
3003 Berne

ncsc@gs-efd.admin.ch

Genève, le 24 février 2022

Procédure de consultation relative à l'obligation de signaler les cyberattaques contre des infrastructures critiques

Monsieur le Conseiller fédéral,

Nous nous référons à l'affaire visée en marge, et vous remercions de l'invitation à prendre position. Conformément à la classification établie par l'Office fédéral de la protection de la population (OFPP), les aéroports nationaux constituent des infrastructures critiques de sorte que la révision législative mise en consultation concerne l'aéroport de Genève.

Nous saluons la volonté de la Confédération de renforcer la protection de la Suisse contre les cyberrisques qui tendent à se multiplier, notamment à l'égard du transport aérien comme la presse s'en est récemment faite l'écho. L'aviation civile étant largement réglementée à l'échelle internationale, toute cyberattaque doit déjà être rapportée à l'Office fédéral de l'aviation civile (OFAC) en tant qu'autorité de régulation. Dans ce contexte, nous sommes d'avis que cette voie de report existante doit être identifiée dans la loi pour assurer autant que possible une cohérence à l'égard de l'ensemble du système.

À la lecture du message qui accompagne la révision, nous avons pris bonne note du fait qu'une attaque cyber doit faire l'objet d'une annonce obligatoire, tandis que celle-ci n'est que facultative en cas de cyberincidents (comme le *phishing* par exemple). Cette distinction nous semble appropriée car une obligation d'annonce pour de tels incidents entrainerait une charge non négligeable de travail qui prétériterait l'utilisation de ressources (humaines et financières) à meilleur escient notamment en cas d'attaque. Il conviendrait dès lors que le projet d'article 73b relève expressément le caractère non-contraignant de l'avis pour des incidents, si cela ne figure pas ailleurs dans la loi existante.

S'agissant de la proposition d'art. 74b let. p, il nous apparait que la formulation retenue manque de précision puisque les aéroports nationaux désignés comme infrastructures critiques disposent d'une concession fédérale octroyée par le DETEC, et non d'une simple autorisation délivrée par l'OFAC. À ce propos, il convient encore de préciser que l'aéroport binational de Bâle-Mulhouse bénéfice d'un régime conventionnel particulier convenu entre la Suisse et la France auquel il faudrait se reporter.

GENÈVE
AÉROPORT

Il importe encore de noter que le projet d'art. 74d al. 1 let. a fait référence à « d'autre infrastructure critique » (seconde partie de la phrase), sans que le message apporte réellement d'explication. Nous proposons dès lors de biffer ce passage.

Enfin, nous nous interrogeons sur la pertinence du projet d'articles 74h et 74i, tant leur caractère coercitif nous semble excessif au regard de l'esprit de collaboration qui devrait prévaloir dans ce genre de cas. Contraindre un exploitant d'aéroport de la sorte, avec menace d'amende, nous semble peu propice à la résolution aussi rapide que possible de l'attaque dont un opérateur aurait fait l'objet. Une formulation plus pragmatique nous semblerait opportune.

En vous remerciant par avance de bien vouloir tenir compte de ce qui précède, nous vous prions de croire, Monsieur le Conseiller fédéral, à l'assurance de notre parfaite considération.

André Schneider
Directeur général

Copie :

- Interne : ccb, mgt, ctt, gru, aam
- Flughafen Zürich AG, M. David Karrer, responsable des affaires publiques

einfach. klar. helvetia.
Ihre Schweizer Versicherung

Helvetia Versicherungen
Hauptsitz
St. Alban-Anlage 26
4002 Basel

T 058 280 10 00 (24 h)

www.helvetia.ch

Dr. Martin Jara, 058 280 19 24
martin.jara@helvetia.ch

Eidgenössisches Finanzdepartement
Bundesgasse 3
CH-3003 Bern
Versand per E-Mail an: ncsc@gs-efd.admin.ch

Basel, 13. April 2022

Vernehmlassung Revision Informationssicherheitsgesetz: Meldepflicht für Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrter Herr Bundesrat Maurer
Sehr geehrte Damen und Herren

Wir danken für die Gelegenheit, im Zuge der Vernehmlassung Revision des Informationssicherheitsgesetzes (ISG) Stellung zu nehmen und äussern uns gerne wie folgt.

Im Rahmen der geplanten Revision soll für Betreiber:innen kritischer Infrastrukturen eine Meldepflicht für Cyberangriffe im ISG eingeführt werden. Diese neue Meldepflicht soll dazu dienen, Angriffsmuster frühzeitig zu erkennen und mögliche Betroffene zu warnen (siehe Art. 74a VE-ISG). Als Helvetia Versicherungen (im folgenden «Helvetia») sind wir von dieser Revision direkt betroffen, da wir gemäss Vernehmlassungsentwurf als Betreiberin von kritischer Infrastruktur qualifiziert und der Meldepflicht des ISG unterstellt werden (siehe Art. 74a und 74b Bst. e VE-ISG).

Mit der breit gefassten Meldepflicht ist jedoch auch eine Vielzahl unserer Kundinnen und Kunden von der Meldepflicht betroffen. Nach Art 74a VE-ISG sind alle unter Art. 74b VE-ISG aufgelisteten Bereiche kritische Infrastrukturen. Gemäss dieser Auflistung gelten beispielsweise bereits Hersteller:innen von Steuerungstechnik einzelner Komponenten kritischer Infrastruktur als von der geplanten Meldepflicht betroffen, unabhängig der Grösse dieser Unternehmen. Insbesondere bei kleineren KMU stellt sich die Frage, ob die Meldepflicht gegenüber dem beabsichtigten Nutzen im richtigen Verhältnis steht und ob angesichts dieser breiten Betroffenheit nicht ein abgestufter Ansatz zu verfolgen wäre.

Mit der fortschreitenden Digitalisierung sehen sich Staat und Wirtschaft zunehmend mit Cyberangriffen konfrontiert. Helvetia begrüsst deshalb die Etablierung eines diesbezüglichen Frühwarnsystems, wozu entsprechende Meldepflichten einen Beitrag leisten können. Wir haben im Rahmen unserer Mitgliedschaft im Schweizerischen Versicherungsverband (SVV) deshalb auch

die einschlägigen, erst 2020 erlassenen bzw. verabschiedeten Meldepflichten gemäss Finanzmarktaufsichtsrecht sowie gemäss totalrevidierten Datenschutzgesetz unterstützt.[1] Zumal wir auch als Anbieterin von Cyberversicherungen an Meldungen von Cybervorfällen interessiert sind, um das Cyberrisiken besser verstehen und kalkulieren zu können.

In Anbetracht dessen, dass die Versicherungsbranche staatlich beaufsichtigt ist und bereits einschlägigen Meldepflichten untersteht (gegenüber Aufsichtsbehörde/FINMA sowie künftig auch EDÖB), erachten wir für einen Einbezug als dem Versicherungsaufsichts- und dem Finanzmarktinfrastrukturgesetz unterstehendes Unternehmen in den Geltungsbereich des ISG folgende Rahmenbedingungen als zwingend:

- Der Einbezug in das ISG darf nicht in einer unübersichtlichen Dreifachregulierung von Meldepflichten münden (Finanzmarktaufsichts-, Datenschutz- und Informationssicherheitsrecht). Aktuell (Stand Vernehmlassungsentwurf ISG) enthält der Einbezug in das ISG für uns als Unternehmen ein nicht harmonisiertes Nebeneinander von Meldepflichten gegenüber verschiedenen Behörden (FINMA, EDÖB, NCSC), zumal diese bezüglich zu meldender Vorfälle, Inhalt, Meldefrist und Sanktionierung stark divergieren. Die neu vorgesehene ISG-Meldepflicht belastet so Versicherungsunternehmen zusätzlich im Falle eines Cyberangriffes im kritischsten Moment und blockiert in den betroffenen Unternehmen Ressourcen, die besser zur Bewältigung des Cybervorfalls investiert werden.
- Die Meldepflicht für Cyberangriffe sollte deshalb für uns als Versicherer an sämtliche Stellen (FINMA, EDÖB, NCSC) mit einer Meldung erfolgen können (One-Stop-Shop-Ansatz für alle Meldepflichten), um so den Meldeaufwand in der ausserordentlich schwierigen Situation eines Cyberangriffs in Grenzen zu halten und unsere Unternehmen nicht mit drei verschiedenen Meldeverfahren zu belasten.
- Aus unserer Sicht ist der Bund hier in der Pflicht, eine optimale Koordination bezüglich der Meldestelle, zu meldender Vorfälle, Inhalt und Meldefrist sicherzustellen. Statt der verschiedenen staatlichen Meldestellen und Regulierungen sind eine einzige Anlaufstelle und eine harmonisierte Meldepflicht für alle davon erfassten Unternehmen zu schaffen. Zudem müssen die konkreten Meldeinhalte mit dem Fokus auf schlanke und effiziente Prozesse festgelegt werden. Diesem Anliegen wird der Vernehmlassungsentwurf nicht gerecht und ist daher entsprechend nachzubessern.
- Es ist von Strafbestimmungen abzusehen. Wir erkennen keinen Sinn darin, die Meldepflicht gemäss ISG mit Strafbestimmungen durchzusetzen und lehnen diese prinzipiell ab. Für betroffene Unternehmen darf eine ausserordentlich schwierige Situation eines Cyberangriffs nicht noch unnötig mit einer Strafdrohung belastet werden – insbesondere im Sinne einer Fehlerkultur. Wenn es gelingt, mit der Meldepflicht einen konkreten Nutzen hinsichtlich partnerschaftlicher Stossrichtung von privatwirtschaftlichen Unternehmen und Staat gegen Cyberrisiken zu genieren, dann sind keinerlei Strafbestimmungen nötig.

Die obigen Erörterungen sehen wir ebenso im Sinne unserer Geschäftskunden im Bereich Cybersicherheit. Gerade für KMU und kleinere Betreiber:innen kritischer Infrastrukturen bzw. deren

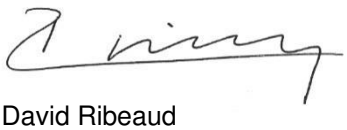
[1] siehe FINMA-Aufsichtsmitteilung 05/2020 Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG vom 7. Mai 2020 und Art. 24 neues DSG vom 25. September 2020

Zulieferer muss zudem konkret aufgezeigt werden, welchen Mehrwert die beabsichtigten Unterstützungsleistungen im Zuge einer Meldepflicht aufweisen, beziehungsweise in welchem sinnvollen Verhältnis die Meldepflichten zu einem möglichen Ertrag stehen. Damit würde das Vertrauen der Unternehmen in den Nutzen hinsichtlich dem zu etablierenden Frühwarnsystem deutlich gestärkt.

Weiter verweisen wir auf die Stellungnahmen des SVV und economiesuisse, die wir unterstützen. Für die Berücksichtigung unserer Stellungnahme bei der weiteren Behandlung der Vorlage danken wir Ihnen und stehen für Rückfragen zur Verfügung.

Freundliche Grüsse

Dr. Martin Jara
CEO Schweiz



David Ribeaud
CEO Specialty Markets

HÄRTING

HÄRTING Rechtsanwälte AG

Landis + Gyr-Strasse 1
6300 Zug
+41 41 710 28 50
office@haerting.ch
www.haerting.ch

Generalsekretariat des Eidgenössischen
Finanzdepartements
Nationales Zentrum für Cybersicherheit (NCSC)
3003 Bern

Per E-Mail an: ncsc@gs-efd-admin.ch

BETREFF

Stellungnahme zum Entwurf des Bundesgesetzes über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG)

DATUM

14. März 2022

Sehr geehrter Herr Bundesrat Maurer,
sehr geehrte Damen und Herren,

Wir bedanken uns für die Möglichkeit zum rubrizierten Geschäft Stellung zu beziehen und nehmen diese gerne fristgerecht wahr.

HÄRTING Rechtsanwälte AG ist eine national und international tätige, auf Informations-, Kommunikations- und Technologierecht (ICT) spezialisierte Wirtschaftsanwaltskanzlei mit Sitz in Zug. Wir beraten KMU, börsenkotierte Unternehmen als auch Kantone und Bundesbehörden.

Gerne schlagen wir Ihnen die nachfolgenden Änderungen bzw. Ergänzungen vor:

1. Informationsschutzgesetz (ISG)

Art. 1 - Ergänzung

[1] Dieses Gesetz soll:

a. die sichere Bearbeitung der Informationen, für die der Bund zuständig ist, sowie den sicheren Einsatz der Informatikmittel des Bundes gewährleisten, es sei denn eine Spezialgesetzgebung sehe eine gesonderte Zuständigkeit vor;

Begründung

Es sollte explizit erwähnt werden, dass eventuelle Spezialgesetzgebungen vorgehen können.

Art. 2 – Präzisierung

[5] Für Organisationen des öffentlichen und privaten Rechts, die kritische Infrastrukturen gemäss Artikel 74b betreiben, die aber nicht unter die Absätze 1–3 fallen, gelten die Artikel 73a–79. Die Spezialgesetzgebung kann weitere Teile dieses Gesetzes für anwendbar erklären.

Begründung

Es sollte klar sein, dass man die kritischen Infrastrukturen gemäss der Definition im ISG meint.

Art. 5 Bst. f-g - Ergänzung

Hinzufügen von lit. f mit der Definition von Cyberrisiko.

Hinzufügen von lit. g mit der Definition von Schwachstellen von Informatikmitteln

Begründung

Beide Begrifflichkeiten werden in Art. 73a ff. ISG erwähnt, jedoch erscheint deren Unterscheidung nicht geläufig. Deren Abgrenzung ist für die Erfüllung der Meldepflicht jedoch von grosser Bedeutung, weswegen wir empfehlen, die beiden Begriffe in Art. 5 ISG zu definieren.

Zudem sollten Begrifflichkeiten gesetzesübergreifend definiert und mit dem revDSG abgeglichen werden. Art. 5 Abs. 1 lit. h. revDSG spricht von Verletzung der Datensicherheit. Eine Verletzung der Datensicherheit liegt vor, wenn eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden.

Art. 73a Grundsatz Ergänzung

f. Subsidiäre Unterstützung von Betreiberinnen von kritischen Infrastrukturen.

Begründung

Da die Subsidiarität auch im erläuternder Bericht aufgewiesen wird, sollte diese auch im Gesetzestext statuiert werden. Das NCSC soll nur unterstützen, wenn die freie Wirtschaft dazu nicht in der Lage ist, weil es sich z.B. um einen Fall nationaler Bedeutung handelt.

Art. 73b Bearbeitung von Meldungen zu Cybervorfällen und Schwachstellen - Ergänzung

[2] Das NCSC kann Informationen zu Cybervorfällen veröffentlichen oder an interessierte Behörden und Organisationen weiterleiten, sofern der Geheimhaltungs- und Datenschutz sichergestellt ist und sofern dies dazu dient, Cyberangriffe zu verhindern oder zu bekämpfen. Diese Informationen dürfen Personendaten und Daten juristischer Personen enthalten, sofern es sich um missbräuchlich verwendete Identifikationsmerkmale und Adressierungselemente handelt und die betroffene Person einwilligt. Gleiches gilt für Immaterialgüterrechte im weitesten Sinne.

[3] Werden dem NCSC Schwachstellen gemeldet, so informiert es umgehend den Hersteller und setzt ihm zur Behebung der Schwachstelle eine angemessene Frist. Behebt der Hersteller die Schwachstelle nicht innert dieser Frist, so veröffentlicht das NCSC die Schwachstelle unter Angabe der betroffenen Soft- oder Hardware und des Herstellers, sofern dies zum Schutz vor Cyberrisiken beiträgt. Diese Meldungen werden vom Öffentlichkeitsprinzip ausgeschlossen.

Begründung

Betr. Abs. 1: Es muss präziser geregelt werden, welche Schwachstellen vom NCSC den Herstellern gemeldet werden müssen. Auch sollte aufgezeigt werden, ob diese Meldung lediglich optional erfolgen kann. Ebenfalls muss diese Meldung mit anderen Meldungen koordiniert werden, sodass Doppelspurigkeiten vermieden werden.

Betr. Abs. 2: Da die Bekanntgabe von Cybervorfällen negative Konsequenzen für die Reputation des angegriffenen Unternehmens nach sich ziehen kann, sollte präziser geregelt werden, unter welchen Umständen der Cybervorfall unter Nennung welcher Angaben veröffentlicht werden soll. Idealerweise ist mit dem betroffenen Unternehmen die Kommunikation sogar abzustimmen. Zudem muss der Daten- und Geheimhaltungsschutz von vertraulichen Informationen gewährleistet sein, es sei denn die betroffene Person hat zugestimmt Wenn eine Kommunikation eine Firma, Marke oder dergleichen einer Firma beinhaltet, so gilt die Zustimmung auch für diese Immaterialgüterrechte.

Betr. Abs. 3: Da auch der erläuternde Bericht die Angabe des Herstellers erwähnt, empfehlen wir auch eine explizite Nennung des Herstellers im Gesetzestext.

Art. 74 Unterstützung von Betreiberinnen von kritischer Infrastruktur - Ergänzung

[2] Es stellt ihnen dazu insbesondere folgende Hilfsmittel zur Verfügung:

a. ein Kommunikationssystem für den sicheren Informationsaustausch sowie eine sichere Datenablage;

[3] Es berät und unterstützt sie bei der Bewältigung von Cybervorfällen und der Behebung von Schwachstellen in subsidiärer Weise zu IT-Dienstleistungen, die auf dem Markt erhältlich sind, wenn für die kritische Infrastruktur ein unmittelbares Risiko von gravierenden Auswirkungen besteht und, sofern es sich um private Betreiberinnen handelt, die Beschaffung gleichwertiger Unterstützung auf dem Markt nicht rechtzeitig möglich ist.

[4] Es kann zur Analyse eines Cybervorfalls mit dem Einverständnis der betroffenen Betreiberin auf deren Informationen und Informatikmittel zugreifen. Der Zugriff kann gewährt werden ohne allfällige Geheimhaltungspflichten zu verletzen.

Begründung

Betr. lit. a: Es sollte explizit auch erwähnt werden, dass der NCSC eine sichere Datenablage gewährleistet.

Betr. lit. c: Was ist unter technischen Hilfsmittel zu verstehen?

Betr. Abs. 2: Da die Subsidiarität auch im erläuternder Bericht aufgewiesen wird, sollte diese auch im Gesetzestext statuiert werden.

Art. 74a Meldepflicht - Präzisierung

Die Betreiberinnen von kritischen Infrastrukturen müssen dem NCSC Cyberangriffe und -vorfälle nach deren Entdeckung so rasch als möglich melden, damit das NCSC Angriffsmuster frühzeitig erkennen, mögliche Betroffene warnen und ihnen geeignete Präventions- und Abwehrmassnahmen empfehlen kann.

Begründung

Bereits Cybervorfälle sollen gemeldet werden. Auch Schwachstellen sollte man freiwillig melden können, damit das NCSC Hersteller darauf hinweisen kann.

Art. 74b Bereiche - Ergänzung

r. Unternehmen, die die Bevölkerung mit unentbehrlichen Gütern des täglichen Bedarfs versorgen. Der Bundesrat bezeichnet die betroffenen Unternehmen.

Oder alternativ ganz streichen und eine gesetzliche Grundlage schaffen, um dies auf Verordnungsstufe zu definieren.

Begründung

Da der erläuternde Bericht die Präzisierung durch den Bundesrat auf dem Verordnungsweg explizit erwähnt, sollte dies auch im Gesetzestext aufgenommen werden. Es fragt sich, ob nicht die gesamte Definition der Kritischen Infrastrukturbetreiber durch den Bundesrat erfolgen soll.

Art. 74d Zu meldende Cyberangriffe – und Vorfälle– Ergänzung und Löschung

[1] Ein Cyberangriff oder ein Cybervorfall auf eine kritische Infrastruktur muss gemeldet werden, wenn die ernsten Befürchtungen bestehen, dass:

Streichung von lit. b.

Begründung

Die Ausführungen in lit. a-d verdeutlichen, dass Bagatellfälle nicht gemeldet werden sollen, sondern lediglich, wenn der Cyberangriff weitgehende Konsequenzen beinhalten kann und somit schweizweit zum Tragen kommt. Dass bereits Anzeichen der Meldepflicht gemäss Art. 74d unterliegen, widerspricht demnach der ratio legis. Lit. b ist zu streichen, da in der Regel oft nicht belegt werden kann, dass ein fremder Staat einen Cyberangriff tätigt. Lit. d ist auch zu streichen.

Art. 74e Inhalt der Meldung – Ergänzung + Bemerkung

[1] Die Meldung muss Informationen zur kritischen Infrastruktur, zur Art und Ausführung des Cyberangriffs, des Cybervorfalles, zu seinen Auswirkungen und zum geplanten weiteren Vorgehen der Betreiberin der kritischen Infrastruktur enthalten.

Begründung

Der Inhalt der Meldung sollte präziser formuliert werden, auch im Hinblick auf die Gefahr von Bussgeldern. Vorstellbar wäre die Präzisierung auch auf Stufe der Verordnung vorzunehmen.

Auch sollte der Inhalt der Meldung mit anderen Meldungspflichten an anderen Behörden abgestimmt werden, um Doppelspurigkeiten zu vermeiden.

Art. 74f Übermittlung der Meldung – Bemerkung + Streichung

[1] Für die elektronische Meldung von Cyberangriffen stellt das NCSC ein sicheres System zur Übermittlung der Meldung an das NCSC zur Verfügung.

[2] Das System muss der Betreiberin einer kritischen Infrastruktur ermöglichen, die Meldung des Cyberangriffs oder seiner Auswirkungen gesamthaft oder in Teilen an weitere Stellen und Behörden zu übermitteln.

Neuer Vorschlag

Abs. 3 ist zu streichen.

Begründung

Es kann nicht angehen, dass hier Meldungen an das NCSC und an die Datenschutzbehörde, BAKOM oder FINMA vermischt wird. Es ist sicherzustellen, dass andere «Stelle» und Behörden, nur den Umfang an Information erhalten, zu dem sie gesetzlich berechtigt sind oder im Rahmen des Zweckes der zugrundeliegenden Gesetzgebung eine Rechtfertigung besteht.

Abs. 3 ist zu streichen oder sonst ist eine klare Governance-Regelung aufzunehmen, welche es der betroffenen Infrastruktur ermöglicht zu erkennen, an welche andere(n) Behörde, Stelle oder Dritten die Informationen über ihren Cybervorfall oder -angriff mitgeteilt wurden. Das Transparenzgebot staatlichen Handelns gebietet dies.

Art. 74g Auskunftspflicht - Ergänzung

Es ist festzulegen, wie weit eine Auskunftspflicht gehen kann.

Begründung

Mit der Meldung sollte die Pflicht der kritischen Infrastrukturanbieter erfüllt sein. U.U. müsste man sich überlegen, ob man die Meldepflicht detaillierter in einer Verordnung fasst. Ausserdem ist mit der Erteilung der ergänzenden Auskünfte die Meldepflicht erfüllt. Auch die ergänzenden Auskünfte dürfen nicht zu einer Belastung in einem Strafverfahren führen und sie können nicht endlos sein.

Art. 74i Widerhandlungen gegen Verfügungen des NCSC

Neuer Vorschlag

Komplett streichen

Begründung

Die Verletzung der Meldepflicht wie auch die nachträgliche Auskunft soll nicht unter Strafe gestellt werden. Dies ist kontraproduktiv und verhindert freiwillige Meldungen, die über die reine Pflicht hinausgehen.

4. Abschnitt: Datenschutz und Informationsaustausch

Art. 77 Internationale Zusammenarbeit

[1]Das NCSC kann mit ausländischen und internationalen Stellen, die für die Cybersicherheit zuständig sind, Informationen austauschen, wenn sie diese zur Erfüllung von Aufgaben benötigen, die denjenigen des NCSC entsprechen. Umfasst der Informationsaustausch auch Personendaten nach Artikel 75, ist Artikel 6 und Art. 10a DSG zu beachten.

[2] Der Informationsaustausch nach Absatz 1 ist nur dann zulässig, wenn die ausländischen und internationalen Stellen die bestimmungsgemässe datenschutzkonforme Verwendung gewährleisten.

Begründung

Der Transfer von Personendaten hat sich an die allgemeinen datenschutzrechtlichen Grundsätze zu halten, insbesondere auch Art. 10a DSG.

Art. 79 Abs. 1

[1] Das NCSC bewahrt Personendaten nur so lange auf, wie dies zur Abwehr von Gefahren oder zur Erkennung von Vorfällen zweckmässig ist, höchstens jedoch ein Jahr ab der letzten Verwendung; bei besonders schützenswerten Personendaten beträgt die Frist 6 Monate. In anonymisierter Form sowie als erkannte Muster dürfen die aus Personendaten gewonnen Erkenntnisse unbefristet aufbewahrt werden.

Begründung

Das Verhältnissmässigkeitsprinzip im Datenschutz gebietet, dass Daten nur so lange aufbewahrt bleiben, wie sie für die Zweckerfüllung benötigt werden. Aus den Personendaten können anonymisierte Muster generiert werden.

II. Die nachstehenden Erlasse werden wie folgt geändert:

2. Datenschutzgesetz vom 25. September 2020

Art. 24 Abs. 5bis

Streichen.

Begründung

Sofern eine zentrale Stelle zu schaffen wäre, welche sämtlichen Meldungen aufnimmt, erübrigt sich diese Ergänzung.

Nach dem Gesagten danken wir Ihnen, sehr geehrter Herr Bundesrat Maurer, sehr geehrte Damen und Herren, bestens für die Berücksichtigung unserer Anliegen und stehen Ihnen für allfällige Rückfragen gerne zur Verfügung.

Freundliche Grüsse

N. Beranek Zanon

Nicole Beranek Zanon

C. Boccali

Olivia Boccali

Migros-Genossenschafts-Bund

Eidgenössischen Finanzdepartements EFD
Per E-Mail an: ncsc@gs-efd.admin.ch

Ort/Datum Zürich, 14.4.2022

Betreff **Stellungnahme zu der Vernehmlassung:**
Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrte Damen und Herren

Vielen Dank, dass Sie uns die Möglichkeit einräumen, zum Vorentwurf Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe Stellung zu nehmen.

Die Migros engagiert sich im Verein Unternehmens-Datenschutz VUD, der ebenfalls eine Stellungnahme zum Informationssicherheitsgesetz E-ISG eingereicht hat. Diese geht in eine vergleichbare Stossrichtung wie die Unsrige ebenso wie auch die Stellungnahme des Swico, dem Wirtschaftsverband der Digitalisierer.

Allgemeine Anmerkungen

Die Migros begrüsst den Vernehmlassungsentwurf zum E-ISG grundsätzlich. Vergleichbare Regelungen gibt es bereits in anderen Ländern. Es ist nachvollziehbar und sinnvoll, dass die Schweiz hier nachzieht.

Für eine Unternehmensgruppe wie die Migros, die in verschiedenen Bereichen tätig ist, ist der vorliegende Gesetzesentwurf jedoch mit zu vielen Unklarheiten verbunden und führt zu grosser Rechtsunsicherheit. Aus Sicht der Migros sind die Definitionen von kritischen Infrastrukturen sowie zu meldender Sachverhalte im Entwurf zu umfassend und unklar. Auch stellen wir unterschiedliche Detaillierungsgrade in Bezug auf Anforderungen für unterschiedliche Industrien fest, die nicht nachvollziehbar sind. Es ist eine praktikable Regulierung mit einem positiven Kosten-/Nutzen-Verhältnis für die Unternehmung anzustreben.

Grundhaltung Migros: Rechtssicherheit und praktikable Definitionen sind zwingend

- Die Liste der Bereiche, die als kritische Infrastrukturen angesehen werden sollen, ist zu umfassend. Auch ist Rechtssicherheit nicht gegeben, da unklar ist, welche Unternehmen unter die Definition fallen. Die Migros empfiehlt, die Definition der bestehenden Liste der kritischen Infrastrukturen des Bundesamtes für Bevölkerungsschutz zu übernehmen.
- Die pauschale Unterstellung ganzer Unternehmen unter die Meldepflicht ist abzulehnen. Nur jene Unternehmensbereiche, bei welchen es sich um kritische Infrastrukturen handelt,

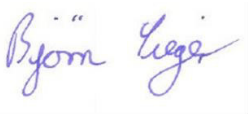
sind der Meldepflicht zu unterstellen.

- Die Definition der zu meldenden Sachverhalte ist zu breit und zu unklar, was wiederum zu Rechtsunsicherheit führt. Es ist auch hier eine klare und abschliessende Definition zu wählen.
- Insgesamt sollten Definitionen, Grenzwerten etc. auf bestehenden Regelungen basieren und nicht explizit für diese Gesetzesvorlage neu entwickelt werden.

Unsere detaillierten Bemerkungen zu den einzelnen Artikeln finden Sie in der nachfolgenden Tabelle. Für die Berücksichtigung unserer Anliegen danken wir Ihnen.

Bei Fragen stehen wir Ihnen sehr gerne zur Verfügung.
Freundliche Grüsse

Migros-Genossenschafts-Bund



Björn Sieger
Stv.Group CISO Migros

Jürg Maurer
Stv. Leiter Direktion Wirtschaftspolitik

Migros-Genossenschafts-Bund

Artikel, Absatz gemäss Vernehmlassung	Antrag Migros	Begründung / Bemerkung
Art. 1 Abs. 1	Ergänzen mit einer Regelung über den räumlichen Geltungsbereich	
Art. 5 Bst. d–e	Eingrenzen bzw. definieren des Begriffs «Betrieb» Eingrenzen bzw. definieren der Wahrscheinlichkeit des Eintretens («dazu führen kann…») Schärfung der Begrifflichkeit «Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist»	Die vorgeschlagene Definition ist zu generisch und zu breit. Es gibt keine klare Differenzierung zwischen Vorfällen, die keinen oder nur einen unwesentlichen Einfluss auf die Geschäftsprozesse haben und solchen, die das Betreiben kritischer Infrastrukturen direkt betreffen oder ein hohes Risiko bergen. Ohne genauere Definitionen bzw. Eingrenzungen besteht ein zu grosser Interpretationsspielraum. Zudem wäre der mit den Meldungen verbundene Aufwand für die meldepflichtigen Betreiberinnen unverhältnismässig, da jede Meldung einen erheblichen Aufwand nach sich zieht.
Art. 73a		Zu begrüssen wäre eine Skizzierung der möglichen Unterstützungsmöglichkeiten bereits auf Gesetzesstufe, z.B. mittels beispielhafter, nicht abschliessender Aufzählungen.
Art. 73b		Es ist sicherzustellen, dass der Zustimmungsvorbehalt von juristischen Personen auch nach dem Inkrafttreten des revidierten Datenschutzgesetzes bestehen bleibt. Nach dem revidierten Datenschutzgesetz sind Daten von juristischen Personen nicht mehr im Anwendungsbereich des Datenschutzgesetzes. Wir erachten es als wichtig, dass Unternehmen Kontrolle bzw. ein Mitspracherecht in Bezug auf die Veröffentlichung bzw. Kommunikation der sie betreffenden Cyberangriffe haben.
Art. 74b		Der Kreis der betroffenen Unternehmen und Organisationen ist deutlich zu gross angesetzt und nicht klar definiert bezüglich der Zielgruppen. Zudem ist die Meldepflicht auf die als kritisch erachtete Tätigkeit innerhalb des Unternehmens zu begrenzen. Nicht das gesamte Unternehmen soll pauschal der Meldepflicht unterstellt werden, sondern nur jene Tätigkeiten des Unternehmens, die als kritische Infrastruktur im Sinne von Art. 74b gelten. Beispielsweise betreiben die Migros Genossenschaften auch Erholungsparks («Park im Grünen») oder Kultureinrichtungen (z.B. Migros Museum für Gegenwartskunst). Cyberangriffe auf diese Unternehmensbereiche auch der Meldepflicht zu unterstellen, ist nicht zielführend. Die unterschiedlichen Detaillierungsgrade in Bezug auf Anforderungen für unterschiedliche Industrien sind für uns nicht nachvollziehbar.

Migros-Genossenschafts-Bund

Artikel, Absatz gemäss Vernehmlassung	Antrag Migros	Begründung / Bemerkung
Art. 74b Buchstabe f	Die Bestimmung ist technologieneutral zu formulieren. Dies wäre kohärent mit den weiteren in Art. 74b E-ISG genannten Bereichen, die allesamt auch digitale Dienste erbringen können, bspw. Banken oder Behörden. Sofern am Anwendungsbereich Digitale Dienste festgehalten wird, ist der Begriff bereits auf Gesetzesstufe klarer zu definieren und abzugrenzen. Andernfalls besteht die Gefahr, dass ein Grossteil der digitalen Wirtschaft undifferenziert der Meldepflicht unterstellt wird.	Aus unserer Sicht ist nicht primär das Medium allein, über das ein Dienst oder eine Tätigkeit ausgeführt wird, ausschlaggebend für die Kritikalität, sondern der konkrete Inhalt/Gegenstand eines Dienstes/einer Tätigkeit sowie seine Bedeutung für das Funktionieren der Wirtschaft bzw. das Wohlergehen der Bevölkerung. Wir erachten es deshalb als nicht zielführend, digitale Dienste pauschal einer Meldepflicht zu unterstellen. Ferner ist mit Bezug auf «Online-Marktplätze» festzuhalten, dass hierunter nur Marktplätze im engeren Sinne zu verstehen sind, die zwischen Marktgegenseiten (z.B. Käufer und Verkäufer) vermitteln, und nicht eigene Dienstleistungen oder Produkte verkaufen.
Art. 74b Buchstabe r	Einführung von Grenzwerten (Grössenschwellen) In Betracht zu ziehen sind einfach messbare Kriterien wie beispielsweise die Mitarbeitenden-Anzahl oder der Umsatz, für die gewisse Erleichterungen oder Ausnahmen direkt im Gesetz eingeräumt werden.	Ohne Einführung von Grössenschwellen würde jeder Marktstand und jeder Lebensmittel-Quartierladen der Meldepflicht unterstehen, was nicht im Sinne des Gesetzes sein kann. Es ist nicht nachvollziehbar, warum der Gesetzesentwurf für digitale Dienste Grössenschwellen definiert, mit Bezug auf Anbieter von Gütern des täglichen Bedarfs hingegen auf solche Grössenschwellen verzichtet.
Art. 74c Buchstabe b		Die Ausnahmeregelung nach lit. b ist unseres Erachtens nicht praktikabel. Es ist unklar, wie potenzielle Auffanginfrastrukturen zu bestimmen sind und wer diese Bestimmung vornimmt. Ferner ist die Definition des geringen volkswirtschaftlichen Schadenspotenzials unklar: Ist dies bzw. muss dies finanziell quantifizierbar sein und anhand welcher Kriterien wird dies bestimmt? Diese Fragen sind zumindest auf der Verordnungsstufe aufzugreifen bzw. zu definieren. Auch vermissen wir eine risikobasierte Regelung, wonach die Betreiberin von kritischen Infrastrukturen anhand einer Risikoabwägung im Einzelfall von einer Meldepflicht absehen kann, da beispielsweise erkennbar - und auch entsprechend dokumentiert - keine oder nur geringe Schadensereignisse eingetreten sind.
Art. 74d	Formulierung anpassen: Streichen: ~~«Anzeichen bestehen»~~ NEU: «überwiegende Wahrscheinlichkeit» oder «voraussicht-	Siehe auch Antrag/Anmerkung zu Art. 74b lit. f Es ist essenziell, die kritische Infrastruktur in Art. 74b E-ISG klar zu definieren und die Meldepflicht auf die als kritisch erachtete Tätigkeit innerhalb des Unternehmens zu begrenzen. Eine

Artikel, Absatz gemäss Vernehmlassung	Antrag Migros	Begründung / Bemerkung
	lich»	pauschale Meldepflicht, die auch nicht kritische Tätigkeiten umfasst, erachten wir als nicht zielführend. Zudem verursacht dies administrative Zusatzkosten. Weiterhin ist die Formulierung «Anzeichen besteht» sehr vage. Wir empfehlen eine Formulierung wie «überwiegende Wahrscheinlichkeit» oder «voraussichtlich» zu verwenden.
Art. 74d *Buchstabe d*		Eine Zeitspanne für die «Nicht-Entdeckung» sollte kein Einzel-Kriterium für eine Meldung darstellen. Insbesondere im Zusammenspiel mit der vagen Formulierung der «Anzeichen» würde dies der Meldepflicht einen sehr weiten Anwendungsbereich eröffnen.
Art. 75 *Abs. 3*		Diese Regelung ist in Einklang mit den datenschutzrechtlichen Vorgaben des revidierten Datenschutzgesetzes (Art. 24 Abs. 4 revDSG) zu bringen. Es ist für uns nicht ersichtlich, weshalb es nach revDSG und E-ISG unterschiedliche Schwellen geben soll, die eine Information an die betroffene Person auslösen. Dies führt in der Unternehmenspraxis zu ungewollten Unsicherheiten. Die Botschaft zum revDSG hält fest, dass eine betroffene Person grundsätzlich nicht zu benachrichtigen ist. Ausgenommen sind Fälle, in denen eine Information zum Schutz der betroffenen Person erforderlich ist oder der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte dies verlangt. Demnach besteht ein gewisser Ermessensspielraum (BBl 2017 6941 ff., 7065). Das E-ISG sollte ebenfalls auf diese Kriterien abstellen und damit dem NCSC einen Ermessensspielraum schaffen. Auf eine starre und pauschale Informationspflicht ist zu verzichten.
Art. 79 Abs. 1	Definition des Begriffs «Verwendung»	Mit dieser Formulierung der letzten Verwendung kann das NCSC die Aufbewahrung theoretisch beliebig lang gestalten. Dies widerspricht gängigen Datenschutzgrundsätzen und ist daher anzupassen. Möglich wäre unseres Erachtens die Speicherdauer an den Abschluss einer Untersuchung oder eines Verfahrens zu knüpfen. Geht man vom datenschutzrechtlichen Begriff der Bearbeitung aus, würde auch die Speicherung einer Verwendung entsprechen und damit die Aufbewahrungsdauer fortlaufend verlängern. Die vorgeschlagene Formulierung bzw. der Begriff ist daher anzupassen.

UZH / UNIL

Consultation 2021/70 : obligation de signaler les cyberattaques contre des infrastructures critiques

Dans ce rapport, des membres du projet *L'éthique et le droit pour promouvoir la confiance en la cybersécurité* (projet PNR 77 n°197425) transmettent leur prise de position concernant la consultation 2021/70 relative à l'introduction d'une obligation de signaler les cyberattaques. Le projet fait partie du programme national de recherche 77 *transformation numérique*. Le texte est disponible en français.

Dieser Bericht beinhaltet die Überlegungen des Teams des Projekts *Mit Ethik und Recht das Vertrauen in die Cybersicherheit fördern* (Projekt NFP 77 Nr°197425) zur Vernehmlassung 2021/70 «Einführung einer Meldepflicht für Cyberangriffe». Das Projekt ist Teil des Nationalen Forschungsprogramms 77 *Digitale Transformation*. Der Text liegt auf Französisch vor.

Version: Version 3 du 15 mars 2022 (version finale).

Auteurs : Sylvain Métille et Pauline Meyer

Distribution : Département fédéral des finances DFF / Par courriel : ncsc@gs-efd.admin.ch

Prise de position

Tout d'abord, l'introduction d'une obligation de signaler les cyberattaques contre des infrastructures critiques est bienvenue et utile. En effet, les cyberattaques visant ces services essentiels comportent des risques importants pour la société dans son ensemble, raison pour laquelle il nous paraît important de mettre en place les mécanismes s'imposant pour protéger et défendre efficacement ces biens.

Ensuite, le champ d'application de la loi soulève des questions :

- Art. 2 al. 5 AP-LSI : les exploitants d'infrastructures critiques doivent être soumis aux art. 6 à 10 LSI en plus des art. 74 à 80 afin de disposer de standards minimaux, prévus légalement, en matière de cybersécurité, tout en permettant aux différents secteurs d'adopter ensuite d'autres exigences plus précises et adaptées à leurs spécificités. L'avant-projet prévoit par ailleurs une modification de la LApEl mais pas d'autres lois, dans la mesure où seul le secteur de l'approvisionnement en électricité a été examiné. Nous ne pensons pas qu'il soit nécessaire d'attendre qu'un tel examen ait été entrepris dans tous les autres secteurs critiques pour affirmer le besoin de légiférer en la matière.
- La définition des infrastructures n'est pas claire entre l'art. 5 let. c et l'art. 74b LSI. Est-ce que l'art. 74b précise la notion des infrastructures considérées comme critiques et donc étend le champ d'application de la loi (contrairement à l'art. 2s. notamment) ou s'agit-il d'une autre notion d'infrastructures critiques visant seulement celles soumises à l'obligation de signaler mais pas au reste de la LSI ? Dans le second cas, il serait regrettable que les institutions soumises à l'obligation d'annonce ne puissent pas bénéficier du soutien du NCSC conformément à l'art. 74 AP-LSI.

- Il serait utile de prévoir la possibilité de saisir le NCSC pour constater si un exploitant est ou non soumis à la loi ou à l'obligation de signaler, à la manière de ce qui est prévu dans la LSCPT par exemple (voir notamment l'art. 51 OSCPT).
- Art. 74a AP-LSI : l'obligation de signaler ne doit pas se limiter aux cyberattaques mais inclure également les cyberincidents importants (au sens de l'art. 74d al. 1 let. a, c ou d) car un incident peut avoir graves conséquences même s'il n'est pas d'origine malveillante. On peut ici se poser la question de la pertinence de certains critères de l'art. 74d al. 1, en particulier le soutien d'un État étranger ou le fait qu'elle soit passée inaperçue pendant trente jours. Le premier critère sera difficile, voire impossible, à évaluer par l'institution attaquée. De plus, une attaque réalisée par une mafia ou une organisation terroriste ne remplirait pas le critère mais n'en serait pas moins dangereuse. Le second n'est à notre avis pas relevant en termes de gravité.
- Art. 74b let. f et k AP-LSI : il y a un aspect extraterritorial, raison pour laquelle il faudrait prévoir l'application du droit suisse (voir p. ex. la théorie des effets de l'art. 3 nLPD). En outre, la let. f introduit de nouvelles notions qu'il faudrait harmoniser avec les autres lois du secteur (LTC, LSCPT, ODI) et préciser si les fournisseurs de services de télécommunication dérivés sont également concernés.
- Art. 74b let. s AP-LSI: il est plus logique et réalisable d'intégrer les fabricants aux fournisseurs de l'art. 74b let. f AP-LSI.
- Le statut du NCSC mérite d'être éclairci, notamment en lien avec la décision d'annoncer ; est-il une autorité de surveillance ou a-t-il vocation à le devenir ?

Finalement, nous vous faisons part de quelques autres observations portant sur l'avant-projet soumis à consultation :

- Art. 5 let. d AP-LSI : nous apprécions la définition du cyberincident figurant dans l'AP-LSI, mais insistons sur le fait qu'elle ne reprend pas la définition prévue à l'art. 3 let. b OPCy et qu'une harmonisation serait souhaitable. En outre, la formulation « lors de l'exploitation de moyens informatiques » n'est pas optimale, dans la mesure où elle pourrait être considérée comme trop restrictive en excluant tout comportement passif.
- Art. 73b al. 1 AP-LSI : d'une part, la formulation « pour autant que la situation ne nécessite pas d'analyses ou de clarifications supplémentaires » n'est pas claire. D'autre part, nous préconiserions une formulation plus large telle que « lorsque des cyberincidents ou des vulnérabilités sont portés à la connaissance du NCSC » afin de ne pas se limiter à un signalement que l'on pourrait confondre avec le signalement de cyberattaques par la personne concernée.
- Art. 73b al. 2 1ère phrase AP-LSI : il convient d'opter pour une formulation plus large que « si cela permet de prévenir ou de combattre les cyberattaques », comme « si cela permet la protection contre les cyberrisques ». Une telle formulation permettrait de ne pas limiter trop restrictivement l'application de cette disposition. En outre, le consentement à requérir devrait être celui de la personne partageant les données et non pas celui des personnes concernées, dans la mesure où l'obtention du consentement de toutes les personnes concernées pourrait requérir des efforts disproportionnés.
- Art. 73b al. 3 AP-LSI : il serait préférable de prévoir une obligation pour le fabricant, sous menace d'une peine, de remédier à la vulnérabilité. Les utilisateurs de certains produits risquent de perdre des certifications s'ils modifient des dispositifs (notamment dans le cadre de l'Ordonnance sur les dispositifs médicaux).

- Art. 73c al. 4 AP-LSI : la disposition ne semble pas avoir de portée propre.
- Art. 74 al. 2 let. b AP-LSI : l'alinéa ne doit pas se limiter aux recommandations sur des « mesures de prévention » uniquement.
- Art. 74 al. 3 AP-LSI : les conséquences graves ne doivent pas uniquement viser « l'infrastructure critique » mais que la disposition devrait élargir les conséquences dommageables à ses collaborateurs, bénéficiaires, prestations ainsi qu'à (une partie de) la société.
- Art. 74 al. 4 AP-LSI : la disposition doit être reformulée en prévoyant que le NCSC assure la confidentialité et que l'exploitant ne viole pas de secret en transmettant des informations et en lui fournissant l'accès à ses moyens informatiques pour analyser un incident.
- Art. 74a AP-LSI : tout d'abord, le terme « détection » semble plus correct à la lumière de la pratique que le terme « découverte ». Ensuite, la formulation « celui-ci » manque de clarté quant à la question de savoir si c'est le NCSC ou l'exploitant qui doit informer les potentielles victimes (contrairement à la version allemande qui prévoit expressément qu'il s'agit du NCSC ainsi qu'à la version italienne qui utilise la formulation « ce dernier », plus claire également). Finalement, il semble à la lecture du projet que le NCSC va uniquement fournir des recommandations aux potentielles victimes ; il faut qu'il fournisse un réel soutien aux exploitants d'infrastructures critiques également.
- Art. 74b let. g AP-LSI : le renvoi doit être effectué à l'art. 39 (al. 1 let. e) LAMal et non pas à l'art. 9 LAMal.
- Art. 74c AP-LSI : l'exception devrait davantage porter sur les cyberattaques.
- Art. 74d al. 1 let. b AP-LSI : une formulation telle que « exécuté par un État étranger, à son instigation ou avec son concours » permettrait de couvrir plus de cas de figure en empêchant les États de passer entre les mailles.
- Art. 74d al. 2 AP-LSI : il semblerait que seuls les cas accompagnés d'infractions contre la liberté devraient systématiquement être signalés, alors que le rapport prévoit, à juste titre, une obligation de signaler dès que « des actes pénalement répréhensibles » seraient commis. Partant, l'art. 74d al. 2 AP-LSI doit être modifié en fonction. À noter également que la limitation des menaces faites à l'exploitant ou à ses collaborateurs paraît trop restrictive, dans la mesure où d'autres groupements de personnes pourraient être visés par ces menaces.
- Art. 74e al. 1 AP-LSI : la formulation « ainsi que les mesures prises ou prévues » est plus complète.
- Art. 74f AP-LSI : il faut préciser que les autorités n'ont pas accès aux informations à destination d'autres services.
- Art. 74f al. 2 AP-LSI : le rapport mentionne à sa p. 22 que le NCSC peut transmettre à d'autres autorités des informations dans les cas de l'art. 73c al. 1 et 2. Cela ne ressortant pas expressément de la loi, il est nécessaire modifier l'art. 73c de la sorte afin de prévoir un renvoi exprès s'il existe effectivement une volonté d'application l'art. 73c al. 1, 2 et 3 AP-LSI aux communications sur les cyberattaques signalées.
- Art. 74h al. 2 AP-LSI : dans la mesure où il s'agit d'une violation administrative, il faut régler la procédure au moins en renvoyant à la PA et s'assurer du respect du droit d'être entendu.
- Art. 74i AP-LSI : on peut douter du caractère réellement dissuasif d'une sanction de 100 000 CHF et renvoyons à ce titre aux critiques énoncées dans le cadre de la révision de la LPD, alors

que l'amende prévue dans la LPD constitue plus du double de ce montant. La LPD semble imposer plus d'obligations aux responsables du traitement que ce que ne le fait la LSI avec les exploitants d'infrastructure critique et l'argument selon lequel le niveau de sécurité n'est pas le même dans chaque secteur devrait justement motiver à fixer un montant dissuasif.

- Art. 76 al. 1 AP-LSI : il faut non seulement que les données personnelles soient « utiles » mais « nécessaires à la protection des infrastructures critiques contre les cyberrisques ».
- Art. 76 al. 4 AP-LSI : bien qu'il nous semble cohérent que le NCSC n'ait pas besoin de fournir d'autres données personnelles que des ressources d'adressage aux fournisseurs de services de télécommunications, ces derniers pourraient potentiellement être susceptibles de détenir d'autres informations utiles pour les tâches du NCSC. Une formulation plus large, comme ce qui est prévu à l'art. 75 al. 1 AP-LSI, serait donc à préconiser (en précisant p. ex. que « les fournisseurs de services de télécommunication peuvent communiquer au NCSC des données personnelles, y compris des ressources d'adressage »).
- En lien avec l'art. 76a AP-LSI : il s'agit d'une procédure d'appel pour laquelle il faut prévoir les conditions dans la loi ; il faut prévoir quelles informations le NCSC peut transmettre à quelle autorité et selon quelles conditions. En outre, il conviendrait peut-être de mettre à jour les différentes législations pour prévoir un accès ou des communications au NCSC et assurer de la sorte une certaine réciprocité dans l'assistance entre autorités ?
- Art. 79 al. 1 AP-LSI : les durées de conservation prévues à l'art. 79 AP-LSI sont raisonnables mais que la notion d'utilisation devrait être précisée au moins dans le Message.
- Art. 24 al. 5bis LPD : nous soulevons quelques questions concernant la terminologie utilisée à l'art 24 al. 5bis LPD. Nous conseillons de conserver la notion de l'art. 24 LPD, à savoir « personne tenue d'annoncer » (au lieu de « responsable tenu à l'obligation de signalement ») et « annonce » (au lieu de « signalement »). En outre, il serait possible en pratique que l'annonce contienne d'autres données sensibles concernant des tiers (p. ex. des potentiels auteurs) et d'autres catégories de données sensibles. Partant, toutes les données sensibles doivent pouvoir être transmises et pas seulement certaines. Nous tenons aussi à préciser qu'il conviendra de régler le sort de l'art. 42 AP-OLPD. Finalement, l'art. 51 al. 3 let. f LPD doit se limiter à la violation de l'annonce selon l'art. 24 al. 1 et 4 LPD.
- La coordination entre la LSI et l'entrée en vigueur de la nLPD devra être assurée. En outre et dans la mesure où l'OPCy ne va pas survivre à la LSI, il faudra veiller à l'intégrer à la loi et à ses ordonnances.

Herr Manuel Sauter
Geschäftsstelle NCSC
Schwarztorstrasse 59
3003 Bern

Zürich, 13.04.2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe - Vernehmlassungsantwort der Operation Libero

Sehr geehrte Damen und Herren

Für die Möglichkeit zur oben genannten Vorlage Stellung zu beziehen danken wir Ihnen. Gerne geben wir Ihnen im Folgenden von unserer Position Kenntnis.

Cybersicherheit wurde von Wirtschaft und Politik zu lange auf die leichte Schulter genommen. Mit der Erschaffung des NCSC hat der Bund einen wichtigen und richtigen Schritt getätigt. Doch neben neuen Institutionen benötigt es auch neue Prozesse und eine Kultur in Politik und Wirtschaft, die Cybersicherheit ernst nimmt. Eine bessere Übersicht über die Bedrohungslage ist hierfür ein wichtiger Schritt, weshalb wir den vorliegenden Gesetzesentwurf sehr begrüssen. Die im Gesetz vorgesehene Anreizstruktur dürfte einen nachhaltigen Beitrag zur Verbesserung der Cybersicherheit in der Schweiz leisten und folgt liberalen Grundsätzen. Diesen ist auch bei der konkreten Umsetzung der Verordnung Rechnung zu tragen, um bürokratischen Aufwand durch effiziente Abläufe und somit die Kosten für die Umsetzung auch in kleinen Betrieben möglichst tief zu halten.

Dennoch würde Operation Libero die folgenden Anpassungen begrüssen:
Klarere Definition der Meldefrist: Cyberangriffe sind “nach deren Entdeckung so rasch als möglich” zu melden. Eine schärfere Definition wäre begrüssenswert, etwa indem man diese um Verdachtsfälle erweitert. So heisst es im erläuternden Bericht, dass bei Cyberangriffen oft “längere Zeit” unklar sei, wie gravierend ein Angriff ist und eine Meldung erst bei “ausreichendem Kenntnisstand” verlangt werde. Dies könnte aber dazu führen, dass Angriffe mit Verweis auf diese Definition erst verzögert gemeldet werden, weil die Informationen “unvollständig” seien bzw. es sich erst um einen noch nicht bestätigten Verdacht handelt. Zudem ist der Schaden meistens grösser, wenn ein gravierender Angriff zu lange nicht gemeldet wird, als wenn ein weniger gravierender Angriff (unnötigerweise) gemeldet wird.

Weisungen zur Behebung der Schwachstellen verschärfen: Fristen zur Behebung von Schwachstellen (Art 73b, lit. 3) sollen nicht nur für Hersteller, sondern auch für Betreiber gesetzt werden können. Nur so ist sichergestellt, dass ein Sicherheitsupdate nicht nur

von Herstellern entwickelt, sondern von kritischen Infrastrukturen auch tatsächlich eingespielt wird.

Einschränkung der Ausnahmen der Meldepflicht: Art. 74c Abs. a ist nicht zeitgemäss und sollte gestrichen werden. Angesichts der Durchdringung von IT-Mitteln trifft es nicht (mehr) zu, dass Cyberangriffe auf gewisse kritische Infrastrukturen “unwahrscheinlich sind, insbesondere wegen der geringen Abhängigkeit von Informatikmitteln”. Es ist nicht ersichtlich, bei welchen der unter Art. 74b aufgeführten kritischen Infrastrukturen Störungen an Informatikmitteln keine gravierenden Auswirkungen zur Folge hätten. Selbst eine tiefe Zahl oder ältere Informatikmittel schützen nicht vor Angriffen oder Zwischenfällen. Während Art. 74c Abs. a besonders problematisch erscheint, wäre es begrüssenswert, Ausnahmen generell auszuschliessen (d.h. Streichung gesamter Artikel Art. 74c).

Zu überlegen wäre die Ergänzung eines Passus zur kontinuierlichen Anpassung des Gesetzes um mit der sich weiterentwickelnden Bedrohungslage Schritt zu halten und technische Realitäten angemessen zu reflektieren.

Transparenz über Schwachstellen: Auf Basis der zwingenden Meldungen an das NCSC sollte dieses mindestens jährlich in aggregierter Form über Schwachstellen bei kritischen Infrastrukturen berichten (in einer Form, die Angreifern keine spezifischen verwertbaren Informationen zur Verfügung stellt). Diese Praxis - analog der Sicherheitskultur im Flugverkehr (siehe SUST) - schärft das Problembewusstsein und ermöglicht schnelleres Handeln bei Schwachstellen.

Automatisierte Meldungen: Neben manuellen Meldungen soll eine IT-Schnittstelle (API) auch automatisierte Meldungen an das NCSC erlauben. So können Cyber-Überwachungssysteme von kritischen Infrastrukturen etwa automatisch verdächtige Signale an das Zentrum weiterleiten. Die Datengrundlage des NCSC wird damit umfassender und zeitnaher als bei rein manuellen Eingaben nach grösseren Vorfällen. Allerdings ist hierbei und im Allgemeinen zu betonen, dass ein Meldesystem selbst ein lukratives Angriffsziel ist und entsprechend geschützt werden sollte. Wie funktioniert der Meldefluss bei Sicherheitsproblemen im Meldesystem selbst?

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und für die Berücksichtigung unserer Überlegungen.

Mit freundlichen Grüssen

Nicolas Zahn, Co-Lead Digitalisierung
Operation Libero

Die Schweizerische Post AG
Stab CEO
Wankdorfallee 4
3030 Bern

Telefon +41 58 341 15 64
Fax +41 58 667 33 73
www.post.ch

Stab CEO, Wankdorfallee 4, 3030 Bern

Eidg. Finanzdepartement
3003 Bern

Als PDF/Word an: ncsc@gs-efd.admin.ch

Datum 6. April 2022
Kontaktperson Kim Pfister
E-Mail kim.pfister@post.ch
Direktwahl +41 58 386 66 65

Stellungnahme der Schweizerischen Post zur Meldepflicht für Cyberangriffe

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Wir danken Ihnen bestens für die Gelegenheit, im Rahmen der Vernehmlassung zur Meldepflicht für Cyberangriffe für Betreiberinnen von kritischen Infrastrukturen, die im künftigen Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz ISG) vorgesehen ist, Stellung nehmen zu können.

a) Ausgangslage für die Schweizerische Post

Die Post sieht in der digitalen Transformation eine Notwendigkeit für die Schweiz und will sie mit ihren Kompetenzen fördern. Sie versteht sich als Motor für eine moderne Schweiz und will heutige und zukünftige Bedürfnisse ihrer Kundinnen und Kunden erfüllen, ganz gleich ob physisch oder digital. IT ist seit Langem Teil des Postalltags: einerseits ermöglichen die sicheren und stabilen digitalen Systeme den reibungslosen Ablauf des physischen Kerngeschäfts. Andererseits schaffen sie die Voraussetzung dafür, dass die Post ihre Kernkompetenz, sensible Informationen sicher und vertrauensvoll zu transportieren, auch in der digitalen Welt umsetzen kann.

Die Post hat in den letzten Jahren ihre Kompetenzen und Ressourcen in der IT ausgebaut. Wir wollen das bewährte Prinzip des Briefgeheimnisses auch in der digitalen Welt sicherstellen. Informationssicherheit hat bei der Post höchsten Stellenwert, denn das Vertrauen der Kundinnen und Kunden in die Post ist von zentraler Bedeutung. Es ist unser Auftrag, die Daten, Informationssysteme und Dienstleistungen angemessen und verantwortungsvoll zu schützen. Transparenz und eine offene Kommunikation sind für die Post Voraussetzungen für einen nachhaltigen Vertrauensaufbau – auch im digitalen Bereich.

Cybervorfälle haben in den letzten Jahren stark zugenommen. Die Post selbst ist ebenfalls regelmässig Ziel von Angriffsversuchen. Und obwohl wir in Bezug auf Cybersicherheit sehr gut aufgestellt sind, verstehen wir Sicherheit nicht als Zustand, sondern als kontinuierlichen Verbesserungsprozess. Wir suchen gezielt nach neuen Methoden und Technologien, um die Sicherheit zu verbessern. Wir

analysieren laufend technologische Entwicklungen und Cyberbedrohungen. Schwachstellen erkennen wir dank einem mehrstufigen Verteidigungssystem frühzeitig und reagieren schnell - noch bevor eine Gefahr für die gespeicherten Daten entsteht.

Bereits heute pflegen wir eine enge Zusammenarbeit mit den entsprechenden Behörden, namentlich dem NCSC. Der zwischen der Post und den Fachstellen des Bundes etablierte, informelle Austausch betreffend Informationssicherheit ist eng, wertvoll und stellt eine wichtige Massnahme bei der Bekämpfung von Cyberrisiken dar.

Die Post und einzelne ihrer Konzerngesellschaften sind durch die geplanten Neuerungen betroffen als Anbieterin von Postdiensten (Art. 74b Buchstabe n E-ISG) insbesondere aber auch als Bank (Bst. e), als Anbieterin digitaler Vertrauensdienste (Bst. f), als Transportunternehmen im ÖV (Bst. o) und als Herstellerin von Hard- und Software (Bst. s). In den einzelnen Tätigkeitsbereichen sind teils separate Regulierungen bei Informationssicherheitsthemen einzuhalten. Wir verweisen auf entsprechende Vorgaben der FINMA[1] sowie Spezialvorschriften für Vertrauensdienste wie E-Health[2] oder E-Voting[3]. Hinzu kommen künftig generelle, datenschutzrechtliche Meldeverpflichtungen bei Datensicherheitsverletzungen[4].

b) Grundsätzliches zum Entwurf der Vorlage

Vor dem Hintergrund der dargestellten Ausgangslage begrüssen wir die geplanten Ergänzungen zum Informationssicherheitsgesetz. Die Beauftragung des NCSC als zentrale Meldestelle und die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen halten wir für geeignete Massnahmen, um die Widerstandsfähigkeit der Schweiz gegenüber Cyberrisiken zu erhöhen. Die Post hat bereits früher eine Meldepflicht für Cybervorfälle an eine zentrale Meldestelle angeregt. Diese Massnahmen, die primär der zentralen Koordination der Akteure in Gesellschaft, Wirtschaft und Staat dienen, stehen jedoch nicht für sich alleine. Sie stehen neben vielen anderen Massnahmen der Informationssicherheit, die von den genannten Akteuren in eigener Verantwortung unter hohem Ressourceneinsatz umgesetzt werden. Die im ISG geplanten neuen Massnahmen sind somit ein Element unter vielen, die dazu beitragen, die Ziele des ISG zu erreichen.

Die im ISG geplanten Neuerungen insb. die Meldepflichten müssen mit bereits bestehenden Regulierungen abgestimmt sein (Grundsatz der «Harmonie der Rechtsordnung»). Durch eine Zentralisierung der Meldewege lassen sich die Schutzziele des ISG und der anderen Regulierungen effizienter erreichen und es kann eine höhere Akzeptanz, Wirksamkeit und Compliance erzielt werden. Das ISG bietet die Chance, Meldevorgaben zu zentralisieren oder zumindest zu harmonisieren.

Folgende Punkte möchten wir insbesondere hervorheben:

1. **Klare Definition von Gegenstand und Umfang einer Meldung:**
   Die Meldepflicht von Art. 74a ist gegen unten nicht abgegrenzt, so dass unklar ist, ob auch **Vorfälle mit tiefem Schweregrad** oder Bagatellvorfälle zu melden sind. Firewalls und Spamfilter wehren täglich sehr hohe Mengen von Portscans, Phishingversuchen und virenverseuchten E-Mails ab. Inhaltlich soll die Meldepflicht gemäss Vorlage nur für Cyberangriffe gelten, die ein hohes Schadenspotential aufweisen. Aus unserer Sicht bedarf es einer Detaillierung der Begriffsdefinitionen, damit zukünftig nicht auch Bagatellvorfälle der Meldepflicht unterstehen und somit unnötigen Aufwand generieren würden. Die FINMA stellt bei der

[1] Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG.

[2] Meldepflicht von sicherheitsrelevant eingestuften Vorfällen gemäss Art. 12 Abs. 3 EPDV.

[3] Grundsatz des offenen Austauschs zwischen Bund, Kantonen und Systemanbieter bei Sicherheitsereignissen und –schwächen (vgl. Bundeskanzlei BK, Erläuternder Bericht zur Vernehmlassung vom 28. April 2021 betreffend Teilrevision VPR und Totalrevision VEleS).

[4] Pflicht zur Meldung von Verletzungen der Datensicherheit gemäss Art. 24 nDSG.

Meldepflicht basierend auf dem formellen Gesetz (Art. 29 FINMAG) auf die Wesentlichkeit des Vorkommnisses für die Aufsicht ab. Sie setzt in den Ausführungsbestimmungen auf anerkannte Kriterien für die konkrete Ermittlung des Schweregrades von Angriffen. Dieser Ansatz sollte auch beim ISG verfolgt werden und nur mittel oder höher klassierte Vorfälle meldepflichtig sein.
Zudem kommt in der Vorlage der **Unterschied zwischen «Cybervorfall» und «Schwachstelle»** zu wenig deutlich hervor. Der Begriff «Schwachstelle» sollte in Art. 5 in Abgrenzung vom Begriff «Cybervorfall» definiert werden. Im Ergebnis muss klar sein, dass die Meldepflicht für Cybervorfälle nicht aber für Schwachstellen gilt.
Ein weiterer essenzieller Bestandteil ist der **Inhalt einer Meldung**, der auf ein notwendiges Minimum zur effektiven Aufgabenerfüllung des NCSC beschränkt werden muss.
Es muss sichergestellt werden, dass nur zwingend notwendige oder auch validierte Informationen zugestellt werden müssen, ansonsten werden unnötig Ressourcen gebunden, die in der Folge zur Bearbeitung des Cybervorfalls fehlen. Eine kontinuierliche Berichterstattung über einen Cybervorfall erachten wir ferner als nicht zielführend. Sie bindet in erheblichem Masse unnötig Ressourcen. Wir schlagen vor, die kontinuierliche Berichterstattung zu ersetzen durch Ursachenberichte nach Abschluss der Bearbeitung des Vorfalls in Abhängigkeit zur Schwere des Vorfalls (analog FINMA-Prozess).

2. **Vermeidung von Doppelspurigkeiten:** Die Post und PostFinance melden heute schon Vorfälle nach definierten Kriterien je nach Situation an FINMA, EDÖB, BAG und ggf. anderen Aufsichtsstellen. Die Meldungen sind aber oftmals äusserst umfangreich und aufwändig zu tätigen. Wir begrüssen es daher, wenn mit der neuen zentralen Meldestelle beim NCSC konsequent Synergien genutzt werden, um Doppelspurigkeiten zu verhindern. Gerade bei Cybervorfällen sind diese besonders hinderlich. Ein Nebeneinander von Meldestellen bei unterschiedlichen Behörden, unterschiedliche Meldeschwellen und inhaltlichen Meldevorgaben, gilt es zu verhindern. Zielführend ist hingegen, dass sämtliche Meldepflichten über eine einzige zentrale Stelle laufen - nach genau definierten Kriterien.

3. **Definition des Meldeprozesses bis zur Publikation einer Meldung:**
Der Umgang mit vertraulichen Informationen muss präziser geregelt werden. Um den Schutz der meldepflichtigen Stellen sicherzustellen, sind die Daten durch das NCSC an einem sicheren Ort zu erfassen und zu halten. Die Vertraulichkeit der Meldungen muss sichergestellt sein. Von Offenlegungen gegenüber Dritten und Veröffentlichungen, die nicht direkt der Verhinderung oder Bekämpfung von Cyberangriffen dienen, ist strikte abzusehen. Wenn es Veröffentlichungen von Cybervorfällen gibt, müssen sie zwischen NCSC und Hersteller zeitlich und inhaltlich abgestimmt und durch diese vorgenommen werden. Durch eine Anpassung des Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung (BGÖ) sind Meldungen über Cybervorfälle und Schwachstellen vom Geltungsbereich des BGÖ auszunehmen. Dem legitimen Interesse der Öffentlichkeit können regelmässige, für die Öffentlichkeit aufbereitete Transparenzberichte des NCSC dienen.
Sodann ist aus unserer Sicht der konkrete Meldeprozess und der inhaltliche Umfang der Meldungen aktuell zu wenig präzise formuliert. Insbesondere erscheint als unklar, zu welchem Zeitpunkt welche Informationen an Dritte weitergeleitet werden dürften.

4. **Aktiver Einbezug der betroffenen Kreise bei der Ausarbeitung des Verordnungsrechts:**
Wie im erläuternden Bericht ausgeführt, werden die Aufgaben des NCSC und die Zusammenarbeit mit weiteren Stellen auf Verordnungsstufe geregelt werden. Wer, wann welche Cyberangriffe über welche Verfahren zu melden hat, werde in der Verordnung genauer umschrieben und präzisiert. Die Post ist bereit, bei diesen Arbeiten einen aktiven Beitrag zu leisten, und bietet ihre Mitarbeit an.

a) Im Einzelnen

Wir erlauben uns, konkret zu einzelnen Artikeln Stellung zu nehmen.

Artikel	Stellungnahme
Art. 5 Bst. d-e ISG – Begriffe	Teilweise wird von Cyberrisiken und Schwachstellen zusammen gesprochen und teilweise nur von Cyberrisiken allein. Die Begrifflichkeiten Cybervorfall, Cyberrisiko und Schwachstellen sind für die Abgrenzung der Meldepflicht essenziell, jedoch nicht klar definiert. Wir empfehlen die einzelnen Begrifflichkeiten unter Art. 5 aufzuführen und sich an internationale Definitionen wie z.B. den Standard CVSS (Common Vulnerabilities Scoring System) zu halten. Die Post und viele andere Akteure arbeiten bereits nach diesem international akzeptierten Standard.
Art. 73a ISG – Grundsatz	Die Aufgaben des NCSC sind umfangreich sowie für eine effektive Bearbeitung sehr ressourcenintensiv. Das NCSC bedarf genügend Ressourcen, um alle vorgesehenen Aufgaben zu erfüllen. Namentlich muss eine effektive und kompetente Zusammenarbeit mit den Meldepflichtigen jederzeit gewährleistet sein.
Art. 73b Abs. 2 ISG - Bearbeitung von Meldungen von Cybervorfällen und Schwachstellen	Die Veröffentlichung und Weiterleitung von Informationen über Cybervorfälle können negative Konsequenzen für das angegriffene Unternehmen und die zu schützenden Güter haben. Bei der Bearbeitung muss die Vertraulichkeit sichergestellt werden. Meldungen von Cybervorfällen und Schwachstellen müssen vom Geltungsbereich des BGÖ ausdrücklich ausgenommen werden. Im Falle einer Weiterleitung sind die interessierten bzw. empfangenden Stellen aufzuführen, zur Vertraulichkeit zu verpflichten sowie für konkrete Informationen entsprechende Sperrfrist zu definieren. Zusätzlich soll im ISG geklärt werden, dass die meldende Stelle betreffend die Meldeinhalte (Cybervorfälle und Schwachstellen) gegenüber dem NCSC von vertraglichen und gesetzlichen Geheimhaltungsverpflichtungen enthoben ist.
Art. 73b Abs. 3 ISG - Bearbeitung von Meldungen zu Cybervorfällen und Schwachstellen	Die Bearbeitung von Meldungen zu Schwachstellen ist nicht präzise genug geregelt. Aktuell werden identifizierte Schwachstellen von Informatikmitteln, die in kritischen Infrastrukturen eingesetzt werden («kritische Systeme»), direkt dem Hersteller gemeldet, mit der Aufforderung zur Behebung. Die neuen Vorschriften müssen dahingehend klar sein, dass auch künftig jegliche Schwachstellen dem NCSC gemeldet werden dürfen, aber nicht müssen. Davon ausgenommen sind Schwachstellen, die bei einem meldepflichtigen Cybervorfall gemäss "root-cause Analyse" relevant sind. Wir

	empfehlen, in Bezug auf Schwachstellen in kritischen Systemen zu präzisieren, dass in Abwesenheit eines Cybervorfalls ein Melderecht aber keine Meldepflicht besteht. Betreiber von kritischen Infrastrukturen können durch freiwillige Meldung von Schwachstellen sicherstellen, dass die Meldungen und deren Bearbeitung beim Hersteller durch das NCSC koordiniert werden und somit Mehrfachmeldungen vermeiden. Umso mehr als deren Meldung freiwillig ist, müssen Schwachstellenmeldungen strikte vertraulich behandelt werden und namentlich vom Geltungsbereich des BGÖ ausgenommen werden. Wir begrüssen sehr, dass das ISG bei der Veröffentlichung von Schwachstellen auf eine «Coordinated Disclosure» setzt, d.h. dem Hersteller vor Veröffentlichung erlaubt, die Schwachstelle zu schliessen. Damit wird eine "best practice" kodifiziert, die bei der Post seit Jahren und bei Schwachstellenmeldungen und Bug Bounties mit Pioniercharakter umgesetzt wird. In diesem Zusammenhang stellt sich die Frage, ob für Meldende bei Einhaltung der Fristen für die koordinierte Veröffentlichung Straffreiheit in Aussicht gestellt werden soll, sofern eine für die Meldung kausale Handlung strafrechtlich relevant war. Ein solcher "Legal Safe Harbor" kann ein Bedürfnis für ethische Hacker sein und die Meldebereitschaft einerseits und andererseits die koordinierte Veröffentlichung im Interesse der Gesamtziele des ISG begünstigen.
Art. 74 Abs. 2 lit. a ISG - Unterstützung von Betreiberinnen von kritischen Infrastrukturen	Nebst der Bereitstellung eines Kommunikationssystems für den sicheren Informationsaustausch muss der NCSC eine sichere Ablage der Daten sicherstellen. Wir empfehlen, die Anforderung einer sicheren Datenablage, explizit ins ISG aufzunehmen. Zu prüfen ist, ob das betreffende System seinerseits als kritische Infrastruktur zu gelten hat. Sämtliche Meldungen und Angaben über deren Bearbeitung müssen ferner vom Geltungsbereich des BGÖ ausgenommen werden.
Art. 74 Abs. 2 lit. e ISG - Unterstützung von Betreiberinnen von kritischen Infrastrukturen	Unter den technischen Instrumenten verstehen wir die Installation von Sonden in unserer Systemlandschaft, die bei der Erkennung von Cybervorfällen unterstützen. Die Formulierung muss zweifelsfrei sicherstellen, dass der Einsatz solcher technischen Hilfsmittel zwar empfohlen, aber letztlich freiwillig und nicht verpflichtend ist. Die aktuelle Formulierung ist u.E. nicht klar genug. Die Betreiberinnen müssen in jedem Fall die Möglichkeit haben, die Hilfsmittel vor ihrem Einsatz selbst zu testen und über den Einsatz zu entschei-

	den, dies um die Sicherheit und Stabilität ihrer Infrastruktur nicht durch nicht abgestimmte Fremdkörper zu gefährden. Die Betreiberinnen sind für den Einsatz solcher Hilfsmittel angemessen zu entschädigen.
Art. 74 Abs. 3 ISG Unterstützung von Betreiberinnen von kritischen Infrastrukturen	Gemäss dem Artikel unterstützt der NCSC bei der Bewältigung von Cybervorfällen und der Behebung von Schwachstellen, wenn für die kritische Infrastruktur ein unmittelbares Risiko von gravierenden Auswirkungen besteht. Wir empfehlen, zu präzisieren, wann ein unmittelbares Risiko sowie gravierende Auswirkungen angenommen werden.
Art. 74a ISG Meldepflicht	Nur das Melden von Cybervorfällen ist geregelt. Bei Schwachstellen soll die Meldung freiwillig sein und sich auf kritische Schwachstellen beschränken, bei denen der Nachdruck beim Hersteller über NSCS die grössere Hebelwirkung auf die Behebung erzielen kann.
Art. 74d ISG - Zu meldende Cyberangriffe	Die Meldepflicht von Art. 74a ist gegen unten nicht abgegrenzt, so dass unklar ist, ob auch **Vorfälle mit mittlerem und tiefem Schweregrad** oder Bagatellvorfälle zu melden sind. Firewalls und Spamfilter wehren täglich sehr hohe Mengen von Portscans, Phishingversuchen und virenverseuchte E-Mails ab. Inhaltlich soll die Meldepflicht gemäss Vorlage nur für Cyberangriffe gelten, die ein gewisses Schadenspotential aufweisen. Aus unserer Sicht bedarf es einer Detaillierung der Begriffsdefinitionen, damit nicht zukünftig auch Bagatellvorfälle der Meldepflicht unterstehen und somit unnötigen Aufwand generieren würden. Die FINMA stellt bei der Meldepflicht basierend auf dem formellen Gesetz (Art. 29 FINMAG) auf die Wesentlichkeit des Vorkommnisses für die Aufsicht ab. Sie setzt in den Ausführungsbestimmungen auf anerkannte Kriterien für die konkrete Ermittlung des Schweregrades von Angriffen. Dieser Ansatz sollte auch beim ISG verfolgt werden und nur als mittel oder höher klassierte Vorfälle meldepflichtig sein.
Art. 74e ISG - Inhalt der Meldung	Es muss sichergestellt werden, dass die Inhalte der Meldungen mit den Inhalten anderer gesetzlichen Meldepflichten abgestimmt sind. Nur so können Synergien genutzt werden. Das Ziel muss sein, dass eine zentrale Meldung an den NCSC für alle regulierten Meldungen genügt.
Art. 74f ISG - *Übermittlung der Meldung*	Nebst der Bereitstellung eines Kommunikationssystems für den sicheren Informationsaustausch muss der NCSC eine sichere Ablage der Daten sicherstellen. Wir empfehlen, die Anforderung einer sicheren Datenablage, explizit ins ISG aufzuneh-

	men. Zu prüfen ist, ob das betreffende System seinerseits als kritische Infrastruktur zu gelten hat. Sämtliche Meldungen und Angaben über deren Bearbeitung müssen ferner vom Geltungsbereich des BGÖ ausgenommen werden.
Art. 74i ISG - *Widerhandlungen gegen Verfügungen des NCSC*	Wir regen an, diesen Artikel ersatzlos zu streichen. Eine Sanktionierung der Meldepflicht ist aus unserer Sicht nicht zielführend und könnte dazu führen, dass weniger Cybervorfälle gemeldet werden.
Art. 75 Abs. 3 ISG - *Bearbeitung von Personendaten*	Unklar ist, wie damit umgegangen wird, wenn die Täterschaft bei einem Identitätsmissbrauch nicht vollständig aufgeklärt ist und eine laufende Untersuchung stattfindet. Insbesondere ist zu klären, ob zugewartet werden soll, bis konkrete Hinweise auf die Person der Täterschaft vorliegen. Der Schutz der betroffenen Personen sollte dabei vorrangig berücksichtigt werden. Somit ist eine frühzeitige Information vorzuziehen, auch wenn die Täterschaft noch nicht bekannt ist.

Wir bedanken uns für Ihre Kenntnisnahme und die Prüfung unserer Anliegen.

Freundliche Grüsse

Die Schweizerische Post AG

Stab CEO

Matthias Dietrich
6. April 2022
Qualified Electronic Signature by SwissID

Matthias Dietrich
Co-Leiter Stab CEO

Die Schweizerische Post AG

Informatik/Technologie

Marcel Zumbühl
April 6, 2022
Qualified Electronic Signature by SwissID

Marcel Zumbühl
CISO Post Group

RAIFFEISEN

Eidgenössisches Finanzdepartement EFD
Herr Bundesrat Ueli Maurer
Bundeshaus West
3003 Bern

Für Sie zuständig:
Cécile Kessler
cecile.kessler@raiffeisen.ch

Vernehmlassung zur Einführung einer Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

14.04.2022

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Mit der Eröffnung der Vernehmlassung vom 12. Januar 2022 laden Sie interessierte Kreise ein, Stellung zu nehmen zu den Ausführungen im erläuternden Bericht und insbesondere zur Umsetzung der vorgeschlagenen Regelungen. Diese Gelegenheit nimmt Raiffeisen gerne wahr.

Allgemeine Beurteilung der Vorlage

Raiffeisen unterstützt die Einführung einer Pflicht der Betreiberinnen kritischer Infrastrukturen, Cyberangriffe dem NCSC zu melden. Nach Ansicht von Raiffeisen muss diese Meldepflicht verhältnismässig und praxisfreundlich ausgestaltet sein. Mehrfache Meldepflichten an verschiedene Behörden gilt es zu vermeiden.

Als beaufsichtigtes Finanzinstitut regt Raiffeisen die Harmonisierung der Vorlage mit der Aufsichtsmitteilung 05/2020 der Eidgenössischen Finanzmarktaufsicht (FINMA) an. Eine Orientierung daran schlägt Raiffeisen insbesondere bei folgenden Themenvor: Bei der Einführung quantitativer Schwellenwerte für meldepflichtige Unternehmen, bei der Präzisierung der Fristen, bei der Definition des Cybervorfalls sowie der gesetzlichen Kriterien für zu meldende Angriffe, bei der Festlegung der vertraulichen Behandlung der weitergegebenen Informationen und bei der Vermeidung von mehrfachen Meldepflichten. Die für diese Themen relevanten Bestimmungen der Vorlage sind mit jenen der Aufsichtsmitteilung in Einklang zu bringen.

Gerne gehen wir im Folgenden detailliert auf einzelne Bestimmungen ein und formulieren dabei konkrete Anpassungsvorschläge für die genannten Themen. Gleichzeitig verweisen wir auf die Stellungnahme der Schweizerischen Bankiervereinigung, an der Raiffeisen mitgewirkt hat. Die darin vorgetragenen zusätzlichen Anliegen unterstützt Raiffeisen vollumfänglich.

Bemerkungen zu den einzelnen Bestimmungen des Entwurfs

Art. 73a Grundsatz

Keine Verbindlichkeit: Raiffeisen geht davon aus, dass die in Art. 73a Bst. c erwähnten «Anleitungen für präventive und reaktive Massnahmen gegen Cyberrisiken» keine Pflicht für die Unternehmen beschreiben, sondern als Grundlage zu freiwilligen Massnahmen in eigener Verantwortung zu verstehen sind. Weil das NCSC die Lage in den Unternehmen nicht detailliert einschätzen kann, wären verbindliche Anweisungen nicht zielführend.

Ermächtigung des NCSC zur Kooperation mit privatrechtlichen Organisationen: Raiffeisen schlägt für den betreffenden Abschnitt die Aufnahme einer ausdrücklichen Ermächtigung des NCSC zur Kooperation mit privatrechtlichen Organisationen der Wirtschaft in einem Art. 73bis vor. Ein Beispiel dafür ist der derzeit im Aufbau befindliche Verein Financial Swiss Sector Cyber Security Centre (Swiss FS-CSC). Durch die ausdrückliche Nennung der Kooperationsmöglichkeit können allfällige künftige Diskussionen um die Zulässigkeit von Public-Private Partnerships vermieden werden. Die entsprechende Bestimmung könnte wie folgt lauten:

«Zusammenarbeit mit Organisationen der Privatwirtschaft
[1] Das NCSC kann im Rahmen seiner Aufgaben gemäss diesem Abschnitt mit Organisationen der Privatwirtschaft, insbesondere Unternehmen und ihren Verbänden, zusammenarbeiten.
[2] Dabei sind die Berufs- und Geschäftsgeheimnisse der betroffenen Unternehmen zu wahren.»

Art 74 Unterstützung von Betreiberinnen von kritischen Infrastrukturen

Freiwillige Nutzung von Hilfsmitteln: Raiffeisen ist der Ansicht, dass die Nutzung der vom NCSC bereitgestellten Hilfsmittel freiwillig bleiben muss und keine Pflicht zur Nutzung der Hilfsmittel etabliert werden soll.

Art. 74a Meldepflicht

Subsidiarität der Meldepflicht: Die neu einzuführende Meldepflicht an das NCSC soll gegenüber Meldepflichten in anderen Gesetzen (z.B. an die FINMA gemäss Art. 29 Abs. 2 FINMAG) subsidiär sein, um mehrfache Meldungen des gleichen Sachverhalts an verschiedene Behörden zu vermeiden. Anstelle dessen ist der von der Branche eingebrachte Vorschlag zu berücksichtigen, das Meldeformular dergestalt zu konzipieren, dass es sich im Sinne einer Parallelmeldung gleichzeitig verschiedenen Behörden zustellen lässt. Damit würde das Meldeformular und der dafür zu schaffende Kanal die verschiedenen durch einen Cyberangriff ausgelösten Meldepflichten gesamtheitlich abdecken und Mehrfachmeldungen vermeiden.

Einschränkung der Meldepflicht: Raiffeisen schlägt im Sinne der Verhältnismässigkeit und in Anlehnung an die FINMA-Aufsichtsmitteilung 05/2020 eine Einschränkung der Meldepflicht vor. Die Meldepflicht soll sich auf erfolgreiche oder teilweise erfolgreiche Cyberangriffe auf kritische Funktionen von Beaufsichtigten beschränken, deren Ausfall oder Fehlfunktion erhebliche Auswirkungen auf die Geschäftstätigkeit hätte und diese stark beeinträchtigen würde (siehe hierzu auch die Bemerkungen zu Art. 74d).

Präzisierung Fristen: Die in Art. 74a genannte Zeitspanne für die Meldepflicht ist zu vage formuliert. Raiffeisen empfiehlt die Übernahme der zweistufigen Fristen aus der Aufsichtsmitteilung 05/2020 der FINMA. Eine klar definierte Frist vereinfacht die vertragliche Verankerung entsprechender Bestimmungen gegenüber Lieferanten.

Art. 74d Zu meldende Cyberangriffe

Klare Kriterien: Herkunft und Auswirkungen eines Cyberangriffs sind zum Zeitpunkt von dessen Erkennung nicht eindeutig feststellbar. Die in Art. 74d genannten Kriterien eignen sich deshalb nicht für die Feststellung der Notwendigkeit der Meldung eines Cyberangriffs. Was genau gemäss Art. 74d als «Anzeichen» und «Drohung» gilt, ist für Raiffeisen nicht erkennbar. Es braucht klar definierte und anwendbare Kriterien für die Unterscheidung wesentlicher Cyberangriffe von unwesentlichen Cyberangriffen. Raiffeisen geht davon aus, dass die aktuelle Formulierung von Art. 74d die Meldung einer Vielzahl von unwesentlichen und nicht geschäftskritischen Ereignissen zur Folge haben wird. Raiffeisen schlägt deshalb die vollständige Ersetzung von Art. 74d durch eine Formulierung vor, die der FINMA-Aufsichtsmitteilung 05/2020 entspricht. Diese Formulierung könnte z.B. wie folgt lauten:

«Zu melden sind Cyberangriffe mit erheblichen Auswirkungen auf die Geschäftstätigkeit des Unternehmens, insbesondere erfolgreiche oder teilweise erfolgreiche Angriffe auf kritische Funktionen, deren Ausfall oder Störung den Schutz der Kundinnen und Kunden oder das Funktionieren der Märkte stark beeinträchtigen würde.»

Freiwillige Meldung: Die Möglichkeit, freiwillig weitere Cybervorfälle und -angriffe zu melden, erwähnt der Gesetzesentwurf nicht ausdrücklich. Im Sinn der Rechtssicherheit schlagen wir eine Bestimmung über die Zulässigkeit freiwilliger Meldungen (Art. 74d Abs. 2) vor, die z.B. so lauten könnte:

> *«[2] Über die Meldepflicht aufgrund von Artikel 74a ff. hinaus darf eine Betreiberin von kritischen Infrastrukturen auch Cybervorfälle und -angriffe melden, welche die Kriterien gemäss Artikel 74d nicht vollständig erfüllen.»*

Mit dieser Bestimmung wird explizit ausgeschlossen, dass eine von der Meldepflicht nicht erfasste aber dennoch erfolgte Meldung als Verletzung des Berufsgeheimnisses missverstanden werden könnte. Rechtsunsicherheit kann damit vorgebeugt werden.

Art. 74f Übermittlung der Meldung

Elektronisches System für Meldungen: Raiffeisen begrüsst die Schaffung eines elektronischen Systems für die Meldung von Cyberangriffen. Um zusätzlichen Aufwand für die Betreiber bei der Übermittlung einer Meldung zu vermeiden, schlägt Raiffeisen vor, Art. 74f folgendermassen zu ergänzen:

> *«Dieses System ist auch von den anderen Bundesbehörden zu verwenden, die Meldepflichten im Zusammenhang von Cyberangriffen etablieren.»*

Art. 74i Widerhandlungen gegen Verfügungen des NCSC

Strafandrohung streichen: Aus Sicht von Raiffeisen ist diese Strafdrohung zu streichen, da sie kontraproduktiv wirkt und der guten Zusammenarbeit aller Involvierten hinderlich ist. Diese Bestimmung ist nicht geeignet, die Verantwortlichen der kritischen Infrastrukturen zu pflichtkonformem Verhalten zu bewegen. Sie schafft im Gegenteil Verunsicherung. Dies zumal die Abgrenzung gegenüber anderen einzuhaltenden Bestimmungen (Einhaltung Datenschutzbestimmungen, Geheimhaltung etc.) im Einzelfall vertiefte rechtliche Abklärungen zur Folge haben kann und die Überprüfung von Verfügungen im ordentlichen Verwaltungsverfahren möglich sein muss. Raiffeisen erachtet es deshalb vielmehr als sachgerecht, bezüglich Durchsetzung der Meldepflicht wie im Erläuterungsbericht unter Ziff. 1.2.3 ausgeführt, anstelle von Sanktionsdrohungen in erster Linie positive Anreize zu setzen. Die Bestimmung erscheint umso mehr redundant, als das NCSC aufgrund der langbewährten Zusammenarbeit mit den kritischen Infrastrukturen selbst davon ausgeht, dass diese Bestimmung weitgehend symbolischen Charakter hätte.

Art. 75 ff Datenschutz und Informationsaustausch

Wahrung der Berufsgeheimnisse: Raiffeisen ist der Auffassung, dass bei Meldungen im Sinn der neuen Regelung Berufsgeheimnisse zu wahren sind. Das betrifft insbesondere auch das Bankkundengeheimnis. Wir bitten Sie, diesem Anliegen bei der Überarbeitung des Gesetzestextes Rechnung zu tragen.

Wir schlagen in diesem Zusammenhang zudem vor, die Regelung mit einem Art. 76 über die Vertraulichkeit der Informationen zu ergänzen, der wie folgt lauten kann:

> *«Weitergegebene Informationen sind durch die Empfängerbehörde vertraulich zu behandeln. Sie dürfen nicht weitergegeben werden, wenn dadurch die Sicherheit des betroffenen Unternehmens oder der betroffenen Personen gefährdet würde.»*

Für die Gelegenheit zur Stellungnahme bedanken wir uns bestens. Wir bitten um Berücksichtigung der Anliegen von Raiffeisen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse

UEX16286

Digitally signed by UEX16286
Date: 2022.04.14 15:12:01 +02'00'

Friedrich Rub
CISO
Raiffeisen Schweiz Genossenschaft

Digitally signed by UEX14132
Date: 2022.04.14 16:13:43 +02'00'

Dr. Christian Hofer
Leiter Public Affairs a.i.
Raiffeisen Schweiz Genossenschaft

Votre contact :
Oscar Prado
Rue de Lausanne 53
1110 Morges
oscar.prado@romande-energie.ch

Romande Energie SA, Rue de Lausanne 53 – CH-1110 Morges

Département fédéral des finances
Centre national pour la cybersécurité (CNCS)
3003 Berne

Par e-mail uniquement : *ncsc@gs-efd.admin.ch*

Références : FIS/mdo

Morges, le 31 mars 2022

Prise de position concernant l'obligation pour les exploitants d'infrastructures critiques de signaler les cyberattaques

Position de Romande Energie SA

Madame, Monsieur,

Par la présente, nous avons l'avantage de vous faire parvenir notre prise de position par rapport aux modifications proposées de la loi sur la sécurité de l'information (LSI), qui introduit l'obligation de signaler des cyberattaques subies par les exploitants d'une infrastructure critique.

Romande Energie SA, en sa qualité de gestionnaire de réseau (électrique) de distribution, exploite une infrastructure critique au sens de la LSI, et nous saluons le renforcement proposé du CNCS et le monitoring plus précis des cyberattaques menées en Suisse. Les récents développements géopolitiques démontrent une nouvelle fois l'importance de ce sujet.

Nous souhaiterions par la présente vous faire part de quelques remarques relatives aux modifications qui permettraient à notre sens de mieux tenir compte de la situation spécifique que nous avons pu constater dans le cadre de notre activité.

Conformément aux définitions contenues à l'art. 5 LSI, seul un cyberincident provoqué par un tiers est qualifié de cyberattaque et par conséquent, uniquement des actions menées par des tiers résultent en une obligation de signalement. Or, nous souhaitons attirer votre attention sur le fait que les menaces peuvent tout à fait venir de l'interne et selon une étude publiée en 2019 par le Software Engineering Institute, elles représentent entre 15% à 25% des incidents. Il en découle qu'une partie importante des cyberincidents ne pourra de fait pas être suivie, et ce sans raison objective.

En ce qui concerne l'obligation de signaler en tant que telle, l'art. 74 b définit les différents secteurs concernés, dont les *« (…) fabricants de matériel et de logiciels informatiques dont les produits sont utilisés par des infrastructures critiques »*. Nous proposons d'élargir cette rubrique au prestataires-intégrateurs de services informatiques qui fournissent des services aux exploitants d'infrastructures critiques, puisque la compromission d'un fournisseur peut largement faciliter la compromission de l'exploitant de l'infrastructure. Dès lors, un monitoring en dehors des obligations de droit privé qui découlent des contrats conclus parait justifié.

De même, l'art. 74 c exempte les petits exploitants de l'obligation de signalement d'une cyberattaque. Nous constatons toutefois que la compromission d'un petit exploitant peut tout à fait, de par ses interconnexions avec d'autres partenaires, souvent plus grand, impliquer un impact sur l'infrastructure qui dépasserait uniquement son champ d'activité restreint. Nous proposons dès lors de supprimer cette exception. Cela permettrait aussi de rendre tous les exploitants attentifs au fait des possibles conséquences d'une cyberattaque.

Finalement, nous relevons que nous comprenons tout à fait la nécessité d'échange d'informations entre services de renseignement, tel qu'il est prévu à l'art. 77, mais nous pensons néanmoins qu'il serait alors judicieux d'informer les exploitant de l'infrastructure, si des données personnelles de leurs clients sont concernées par un tel échange.

En vous remerciant pour l'attention portée à notre prise de position, nous vous prions de croire, Madame, Monsieur, à l'assurance de notre considération distinguée.

Romande Energie SA

Ottilie Morand
Juriste Senior, LL.M.

Oscar Prado
Responsable sécurité IT

Salt.

Salt Mobile SA
Rue du Caudray 4
CH-1020 Renens 1

Generalsekretariat EFD
Eidgenössisches Finanzdepartement
Bundesgasse 3
3003 Bern

Eingereicht als pdf und word per email an: ncsc@gs-efd.admin.ch

Renens, 12. April 2022

Stellungnahme zum Entwurf des Bundesgesetzes über die Informationssicherheit beim Bund (ISG): Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrter Herr Bundesrat, sehr geehrte Damen und Herren

Wir möchten uns für die Möglichkeit zur Anhörung betreffend die Revision des Bundesgesetzes über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) bedanken und nehmen dazu gerne fristgerecht Stellung wie folgt.

Wir verweisen integral auf die Stellungnahme unseres Branchenverbandes asut und unterstützen diese vollends, anbei die Zusammenfassung der asut ihrer Stellungnahme als Auszug. Wir bitten Sie um wohlwollende Aufnahme.

asut unterstützt das Ziel, die Widerstandsfähigkeit der Schweiz gegenüber Cyberrisiken zu erhöhen und begrüsst die vorgeschlagenen Anpassungen des ISG im Grundsatz. asut regt jedoch die Schaffung einer zentralen Meldestelle für sämtliche Cybervorfälle an. Zu präzisieren ist zudem die Meldepflicht (Art. 74a), die ausdrücklich nur bei Cybervorfällen auf die eigene kritische Infrastruktur bestehen soll. Abzulehnen ist zudem Art. 74h bezüglich Strafbestimmungen die zur persönlichen Strafbarkeit der Verantwortlichen führen. In diesem Zusammenhang ist der Grundsatz des Selbstbelastungszwangsverbots bei Cyberangriffen und Cybervorfällen in Art. 73c Abs. 3 zu präzisieren.

Freundliche Grüsse

Felix Weber, Regulatory Affairs Manager, Salt Mobile SA

Stiftung Auffangeinrichtung BVG

Direktion

Stiftung Auffangeinrichtung BVG, Postfach, 8050 Zürich

ncsc@gs-efd.admin.ch
Eidgnössisches Finanzdepartement
Rechtsdienst GS-EFD
Angelika Spiess
Bundesgasse 3
3003 Bern

Stiftung Auffangeinrichtung BVG
Elias-Canetti-Strasse 2
Postfach
8050 Zürich
+41 41 799 75 75 (Tel)
+41 44 468 22 98 (Fax)
www.chaeis.ch
POFICHBEXXX (SWIFT)
CH25 0900 0000 3017 0878 7 (IBAN)
PD Dr. iur. Urs Müller
Rechtsanwalt
+41 44 468 23 85
urs.mueller@aeis.ch

Zürich, 14. März 2022

Vernehmlassungsverfahren: Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe (Informationssicherheitsgesetz)

Sehr geehrte Frau Spiess

Die Geschäftsleitung verzichtet in Abstimmung mit dem Stiftungsratsausschuss auf eine Stellungnahme zur eingangs erwähnten Angelegenheit.

Freundliche Grüsse

Stiftung Auffangeinrichtung BVG
Direktion

Marc Gamba
Geschäftsführer

Urs Müller
Leiter Recht & Compliance

Marcel Huber
Chief Corporate Affairs Officer

Sunrise UPC GmbH
Thurgauerstrasse 101B, 8152 Glattpark (Opfikon)

Mobile: +41 76 777 38 58
Marcel.Huber@sunrise.net
sunrise.ch
upc.ch

Generalsekretariat des Eidgenössischen Finanzdepartements
Nationales Zentrum für Cybersicherheit NCSC

ncsc@gs-efd.admin.ch

Opfikon, 13. April 2022

Stellungnahme zum Entwurf des Bundesgesetzes über die Informationssicherheit beim Bund (ISG)

Sehr geehrter Herr Bundesrat,
sehr geehrte Damen und Herren

Sunrise UPC GmbH erbringt als grösstes privates Telekommunikationsunternehmen der Schweiz führende Mobilfunk-, Internet-, TV- und Festnetzdienste für Privat- und Geschäftskunden. Aktuell beliefert sie rund 2,99 Mio. Mobile-, 1.22 Mio. Breitband- und 1.24 Mio. TV-Kundinnen und -kunden und ist damit die führende Anbieterin von Breitband-Internet in der Schweiz.

Die vorgeschlagene Änderung des ISG ist für Sunrise UPC als Betreiberin einer kritischen Infrastruktur von hoher Relevanz. Wir danken Ihnen deshalb für die Möglichkeit, zum Gesetzesentwurf Stellung nehmen zu können.

Sunrise UPC unterstützt das Ziel, die Widerstandsfähigkeit der Schweiz gegenüber Cyberrisiken zu erhöhen und begrüsst die vorgeschlagenen Anpassungen des ISG im Grundsatz. Sunrise UPC regt jedoch die Schaffung einer zentralen Meldestelle für sämtliche Cybervorfälle[1] an. Zu präzisieren sind zudem die Begrifflichkeiten in Art. 5 sowie die Meldepflicht in Art. 74a, die ausdrücklich nur bei Cybervorfällen auf die eigene kritische Infrastruktur bestehen soll. Abzulehnen ist weiter Art. 74h bezüglich Strafbestimmungen, die

[1] Gemäss Art. 5 Bst. d-e E-ISG ist ein *Cybervorfall* ein Ereignis beim Betrieb von Informatikmitteln, das dazu führen kann, dass die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist. Ein *Cyberangriff* ist ein Cybervorfall, der von Unbefugten absichtlich ausgelöst wurde.

zur persönlichen Strafbarkeit der Verantwortlichen führen. Art. 73c Abs. 3 ist zu präzisieren.

Ausgangslage

- Cyberrisiken sind zu einer der wichtigsten Bedrohungen der Sicherheit und der Wirtschaft der Schweiz geworden.
- Der Bund will mit dieser Vorlage eine Meldepflicht für Betreiberinnen kritischer Infrastrukturen einführen.
- Damit soll das Nationale Zentrum für Cybersicherheit (NCSC) eine verbesserte Übersicht über Cyberangriffe in der Schweiz gewinnen, Betroffene besser bei der Bewältigung von Cyberangriffen unterstützen und alle anderen Betreiberinnen kritischer Infrastrukturen warnen können.

Position von Sunrise UPC

Sunrise UPC begrüsst die vorgeschlagenen Anpassungen des ISG im Grundsatz, schlägt jedoch folgende Anpassungen vor:

NCSC als zentrale Meldestelle definieren

Um das Schadensausmass eines Cybervorfalls zu minimieren, muss dieser unter Umständen rasch gemeldet und ebenso rasch bearbeitet werden können. Die innerbetrieblichen Ressourcen werden in einer ersten Phase jedoch vor allem für die Krisenbewältigung, also für die Abwehr und Schadensbegrenzung eingesetzt. Der bürokratische Aufwand für die Erfüllung der verschiedenen Meldepflichten muss deshalb so gering und der Prozess so einfach wie möglich sein.

Sunrise UPC schlägt vor, *beim Bund eine zentrale Meldestelle für sämtliche Cybervorfälle zu schaffen*, deren Meldung gesetzlich vorgeschrieben ist. Mit einer zentralen Meldestelle könnte die Wirtschaft administrativ entlastet und die Prozesse vereinfacht werden. *Prädestiniert für diese Aufgabe dürfte das NCSC sein.* Statt es den Meldenden zu überlassen, einen Vorfall auch anderen Bundesstellen weiterzuleiten, könnte dies durch die zentrale Meldestelle geschehen. Wo nötig, könnte der Meldepflichtige mit der Meldung auch gleich sein Einverständnis für die Weitergabe der Meldung geben. Im erläuternden Bericht ist ein solcher Prozess angedacht.[2]

Mit der geplanten Revision der FDV sollen Vorfälle (wie z.B. Störungen der Netze, Cyberangriffe und andere böswillige Eingriffe) künftig nicht mehr an das BAKOM, sondern an die Nationale Alarmzentrale (NAZ) erfolgen.[3] Sunrise UPC hat sich in ihrer Stellungnahme

[2] Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens, Seite 11
[3] Vgl. Art. 96 FDV

zur Revision der FDV ebenfalls für das NCSC als zentrale Meldestelle für Störungen in Telekommunikationsnetzwerken ausgesprochen. *Wichtig ist, dass die Revision der FDV und die Anpassung des ISG koordiniert erfolgen*.

Begriff «Cybervorfall» präzisieren

Die im Art. 5 E-ISG vorgenommene Differenzierung zwischen Schwachstelle, Cybervorfall (lit. d) und Cyberangriff (lit. e) ist sinnvoll. Sie könnte die Motivation für Meldepflichtige erhöhen, indem nicht jeder Vorfall, sondern nur der Cyberangriff auf kritische Infrastrukturen meldepflichtig ist (während Cybervorfälle und Schwachstellen freiwillig von jeder Person gemeldet werden können). Diese Klarstellung ist wichtig, da im Gegensatz hierzu gemäss Verordnung über den Schutz vor Cyberrisiken der Bundesverwaltung (CyRV) bundesintern Schwachstellen und Cybervorfälle gemeldet werden müssen.

Jedoch ist *die vorgeschlagene Definition von «Cybervorfall» in der bestehenden Form kaum anwendbar*, weil sie mit der blossen – auch theoretischen – Möglichkeit der Beeinträchtigung der Schutzziele operiert. Eine blosse Möglichkeit kann in der Praxis nicht ausgeschlossen werden. Eine Lösungsoption ist, den Begriff an Art. 4 Ziff. 7 der europäischen Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie) anzulehnen. Diese definiert einen Sicherheitsvorfall als «alle Ereignisse, die tatsächlich eine nachteilige Auswirkung auf die Sicherheit von Netz- und Informationssystemen haben». Die Anpassung könnte vorliegend somit lauten (zu ergänzender Text ist unterstrichen):

Art. 5d	«Cybervorfall: Ereignis beim Betrieb von Informatikmitteln, das tatsächlich dazu führt, dass…»

Meldepflicht präzisieren

Sunrise UPC stellt als «Internet Access Provider» (IAP) anderen kritischen Infrastrukturen den Zugang zum Internet zur Verfügung. Die IAP sind stets bestrebt, bei Cybervorfällen ihre Kunden zu unterstützen. *Ein IAP kann jedoch unmöglich zur Meldung sämtlicher Cyberangriffe verpflichtet werden, die über sein Netzwerk auf Betreiberinnen von kritischen Infrastrukturen erfolgen.* Auch ist unter Umständen eine Meldung durch den IAP aufgrund von Vorgaben des Datenschutzgesetzes[4] oder von vertraglichen Vereinbarungen nicht möglich. Sunrise UPC schlägt darum in Art. 74a E-ISG *folgende präzisierende Ergänzung* vor (zu ergänzender Text ist unterstrichen):

Art. 74a	Die Betreiberinnen von kritischen Infrastrukturen müssen dem NCSC Cyberangriffe auf ihre eigenen Infrastrukturen nach deren Entdeckung so rasch als möglich melden, damit das NCSC Angriffsmuster frühzeitig erkennen, mögliche Betroffene warnen und ihnen geeignete Präventions- und Abwehrmassnahmen empfehlen kann.

[4] Vgl. Art. 24 revDSG

Strafbestimmungen zur persönlichen Strafbarkeit

Trotz der Erkenntnis, dass das heutige Modell des freiwilligen Informationsaustausches an seine Grenzen stösst, basiert die Vernehmlassungsvorlage auf einem partnerschaftlichen Vorgehen zwischen Staat und Wirtschaft bei der Eindämmung von Cyber-Bedrohungen.[5] *Diesem kooperativen Vorgehen widerläuft Art. 74h E-ISG. Der Artikel ist daher zu streichen.* Bestimmungen, die zur persönlichen Strafbarkeit der Verantwortlichen führen, sind für die Bekämpfung von Cyber-Bedrohungen vielmehr schädlich als förderlich, führen zu Fehlanreizen und können insbesondere die Bereitschaft der zuständigen Personen reduzieren, in Fragen der Cyber-Security Verantwortung zu übernehmen.

Art. 74h	ist komplett zu streichen

In diesem Zusammenhang ist zudem der *Grundsatz des Selbstbelastungszwangsverbots* bei Cyberangriffen und Cybervorfällen eminent wichtig. Wir schlagen eine Präzisierung von Art. 73c Abs. 3 vor (zu ergänzender Text ist unterstrichen):

Art. 73c Abs. 3	Informationen, die dem NCSC im Rahmen einer Meldung bekanntgegeben wurden und die meldende Person selbst belasten könnten, dürfen in einem Strafverfahren gegen diese Person nur mit Einverständnis dieser Person verwendet werden.

Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme. Bei Fragen stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse

Marcel Huber
Chief Corporate Affairs Officer

Matthias Forster
Senior Regulatory Affairs Manager

[5] Siehe auch erläuternder Bericht 1.2.1

suva

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC

Per E-Mail (in Word und PDF) an:
ncsc@gs-efd.admin.ch

Suva

Fluhmattstrasse 1
Postfach 4358
6004 Luzern

Telefon 041 419 51 11
Telefax 041 419 58 28
Postkonto 60-700-6
www.suva.ch

Marc Epelbaum, lic. iur.
Direktwahl 041 419 55 00
Direktfax 041 419 61 70
marc.epelbaum@suva.ch

Datum 08.04.2022
Betrifft Vernehmlassung zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Gerne nutzen wir die Gelegenheit, uns zur Einführung einer Meldepflicht für Cyberangriffe und der damit verbundenen Änderungen des Informationssicherheitsgesetzes (ISG) äussern zu dürfen.

Die Schweizerische Unfallversicherungsanstalt Suva mit ihren Rehakliniken in Bellikon und Sion soll als Betreiberin von kritischen Infrastrukturen der Meldepflicht für Cyberangriffe unterstellt werden (Artikel 74b lit. g und j).

Die Suva begrüsst die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen. Der gegenseitige Informationsaustausch ist ein wichtiges Mittel zum Schutz vor Cyberrisiken und kann einen wesentlichen Beitrag zur Erhöhung der Cybersicherheit in der Schweiz leisten.

Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme. Wunschgemäss senden wir Ihnen diese auf elektronischem Weg an die angegebene E-Mail-Adresse (ncsc@gs-efd.admin.ch).

Freundliche Grüsse

Suva

Marc Epelbaum, lic.iur.
Generalsekretär

Ronald Abegglen
Public Affairs – Advisor

Swiss International Air Lines AG
P.O. Box ZRHS/V/ABRO
CH-8058 Zürich-Flughafen
Tel. +41 44 564 21 25
ronald.abegglen@swiss.com

Eidgenössisches Finanzdepartement
Bundesgasse 3
3003 Bern

Per E-Mail an: ncsc@gs-efd.admin.ch

Zürich-Flughafen, 13. April 2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrter Herr Bundesrat,
sehr geehrte Damen und Herren

Danke für die Einladung zur Teilnahme an der Vernehmlassung über die Einführung einer Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe. Gerne nehmen dazu Stellung und übermitteln Ihnen die nachfolgenden Anliegen und Bemerkungen.

Das Thema Cybersecurity geniesst bei Swiss International Air Lines AG (SWISS) grosse Aufmerksamkeit. Unsere Geschäftsprozesse und viele operative Vorgänge sind auf gute und sichere Datenübermittlung angewiesen. Cyberangriffe sind – mit Blick auf das potentielle Schadensausmass – ein grosses Risiko. Die Angriffe auf flugbetriebsnahe Dienstleister wie Swissport oder Gategourmet vor kurzem haben deutlich gemacht, wie stark ein erfolgreicher Cyberangriff die ausgeklügelten und aufeinander abgestimmten Prozesse in der Aviatik stören kann.

Die zuständigen Abteilungen von SWISS sind denn auch regelmässig im Austausch mit der NCSC. Ferner bestehen bereits auf der Grundlage des Nationalen Luftfahrtsicherheitsprogramms der zivilen Luftfahrt (National Aviation Security Programme, NASP) umfassende Meldepflichten für Security und Safety relevante Cybervorfälle an das BAZL.

Mit der nun vorgeschlagenen Änderung des Informationssicherheitsgesetzes (ISG) soll nun eine weitere Meldepflicht für Betreiberinnen von kritischen Infrastrukturen hinzukommen. SWISS steht diesen Ansinnen, zumindest in der vorgeschlagenen Form, kritisch gegenüber, auch wenn wir – wie beschrieben – die Brisanz und Relevanz des Themas anerkennen.

Erstens sind diverse zentrale Begriffe im Entwurf sehr weit gefasst, so dass eine Folgenabschätzung sehr schwierig ist. Besonders unklar ist, wer der Meldepflicht unterliegen soll und was genau gemeldet werden muss. Hier sind unseres Erachtens Präzisierungen nötig. Zweitens erkennen wir im Entwurf keinen wesentlichen Mehrwert einer zusätzlichen Meldepflicht. Diese macht allenfalls dann Sinn, wenn sie komplementär zu bestehenden Meldeverfahren ist und der zusätzliche Aufwand entsprechend verhältnismässig ist. Drittens erachten wir die Absicht, die Pflichten mit Sanktionen durchzusetzen als nicht zielführend. Wenn die Absicht der Vorlage ist, eine bessere Übersicht über Vorfälle zu erlangen und als System zu lernen, dann ist ein «just culture»-Ansatz, wie er in der Aviatik verbreitet ist, deutlich geeigneter, um das Ziel zu erreichen.

1. Begrifflichkeiten

Art. 74a E-ISG verankert die Meldepflicht von Betreiberinnen kritischer Infrastrukturen für «Cyberangriffe». Was einen relevanten Angriff darstellt, ist nicht spezifiziert. Es fehlen sowohl quantitative als auch qualitative Präzisierungen. Sind die Unternehmen und Organisationen, die der Meldepflicht unterliegen sollen, verpflichtet, jeden «Angriff» mit einem Phishing-Mail zu melden? Oder braucht es eine gewisse Systematik/ Organisationsgrad und Intensität, um die Meldepflicht auszulösen. Reicht ein «alltäglicher» Angriff auf ein nicht kritisches System oder muss es eine qualifizierte Attacke auf ein kritisches System sein?

Die nicht abschliessende Liste mit Fragen zum Anwendungsbereich macht deutlich, dass die offene Formulierung der Sache nicht dienlich ist. Wir würden es sehr begrüssen, wenn bereits auf Stufe Bundesgesetz der Begriff eines «Cyberangriffs» präzisiert würde mit qualitativen sowie ggf. quantitativen Definitionen.

Nicht nur die Definition des Auslösers der Meldepflicht, sondern auch der «Betreiberin einer kritischen Infrastruktur» ist sehr weit gefasst. Art. 74b E-ISG enthält eine äusserst umfangreiche Liste von möglichen Unternehmen und Organisationen, die als «Betreiberin einer kritischen Infrastruktur» bezeichnet werden und so unter die Meldepflicht fallen könnten. Diese Definition ist unseres Erachtens zu unpräzis, auch wenn Art. 74c E-ISG dem Bundesrat die Möglichkeit gibt, auf Verordnungsstufe korrigierend einzugreifen.

Problematisch ist unseres Erachtens, dass der Begriff einer kritischen Infrastruktur in anderen Gesetzen bereits besetzt ist. Damit verbunden sind mitunter diverse administrative Pflichten oder gar die Pflicht zu einer kostspieligen Zertifizierung. Für die Meldepflicht gemäss E-ISG ist der Begriff jedoch deutlich weiter gefasst. Gemäss dem «Erläuternden Bericht» umfasst er «jene Prozesse, Systeme und Einrichtungen […], die essenziell für das Funktionieren der Wirtschaft beziehungsweise das Wohlergehen der Bevölkerung sind» (vgl. auch Art. 5 ISG [SR 126]). Übersetzt für den Luftverkehr bedeutet dies gemäss Art. 74b lit. p. E-ISG «Unternehmen der Zivilluftfahrt, die über eine Bewilligung des Bundesamtes für Zivilluftfahrt verfügen». Diese Definition betrifft eine Vielzahl von Unternehmen in der Aviatik, vom Grossflughafen, der internationalen Airline bis zu kleinen Betrieben in einer Nische.

Wir können nachvollziehen, dass der Luftverkehr insgesamt als kritisches System betrachtet wird und im Dispositiv zur Cyberabwehr einen festen Platz haben muss. Allerdings ist der Begriff «Betreiberin einer kritischen Infrastruktur» hier irreführend. Rein semantisch betreibt zum Beispiel ein Unternehmen wie SWISS keine kritische Infrastruktur im engen Sinne. Entsprechend sind wir nicht als solche qualifiziert in anderen Gesetzen. Als solche dürften wohl die Betriebsgesellschaften von Landesflughäfen gelten. Selbstverständlich ist SWISS aber Teil eines kritischen und relevanten Systems für die Wirtschaft und das Wohlergehen der Bevölkerung.

Der langen Rede kurzer Sinn: Wir erachten den Begriff «Betreiberin einer kritischen Infrastruktur» im Kontext mit der extensiven Auslegung der potentiell Betroffenen als nicht geeignet und tendenziell irreführend, da er in anderen Zusammenhängen bereits besetzt und deutlich enger definiert ist. Wir würden es entsprechend begrüssen, wenn im E-ISG ein anderer, nicht besetzter und ggf. offenerer Begriff gewählt würde. Ferner regen wir an, bereits auf Gesetzesstufe Einschränkungen des Anwendungsbereichs vorzusehen.

2. Notwendigkeit einer weiteren Meldepflicht

SWISS unterliegt bereits heute zahlreichen Meldepflichten für Cybervorfälle. Zum Beispiel sind alle Angriffe, die potentiell die Flugsicherheit und Luftsicherheit (Safety und Security) beeinträchtigen könnten, gemäss dem erwähnten NASP meldepflichtig. Auch aus dem Datenschutzrecht ergeben sich entsprechende Pflichten. Schliesslich besteht seit längerem ein guter und etablierter Austausch zwischen der NCSC und unseren Spezialisten im Bereich Cybersecurity. Aus unserer Optik ist eine neue, erweiterte Meldepflicht für Cyberangriffe nicht zwingend notwendig, da wir die für die Sicherheit und die Funktion von SWISS wesentlichen Aspekte bereits von anderen Meldepflichten abgedeckt ist.

Aus dieser Perspektive erwarten wir durch die vorgeschlagene Meldepflicht eher kompliziertere und teurere administrative Prozesse, die in keinem Verhältnis zum allfälligen Mehrwert der Meldepflicht steht. Unseres Erachtens macht eine weitere Meldepflicht für Cyberangriffe nur in jenen Bereichen Sinn, die derzeit noch nicht anderweitigen Meldepflichten unterliegen.

Wir anerkennen das Bedürfnis von NCSC, möglichst umfassend über Cyberangriffe informiert zu sein. Mit Blick auf die Ausführungen oben erachten wir jedoch eine weitere Meldepflicht nicht als das einzige Instrument zum Erreichen dieses Zieles. Eine verstärkte Koordination und Informationsaustausch zwischen den involvierten Behörden und dem NCSC – soweit dies noch nicht etabliert ist – erscheint uns als sachdienlicheres Vorgehen.

3. «Just Culture» statt Sanktionen

Nach unserem Verständnis verfolgt der Gesetzgeber mit der Einführung einer Meldepflicht für Cyberangriffe mehrere Ziele: Attacken sollen frühzeitig erkannt und analysiert werden können, damit andere potentielle Ziele frühzeitig, idealerweise vor dem Ereignis gewarnt werden und entsprechend ihre Abwehr- oder Mitigationsmassnahmen einleiten können. In diesem Sinne soll ein System etabliert werden, das mit jeder Meldung lernt und somit über die Zeit sicherer und resilienter wird.

Wir sehen hier starke Analogien zum Luftverkehr. Auch hier gibt es ein Meldesystem für Fehler, die beispielsweise Piloten während eines Fluges passieren und potentiell die Sicherheit gefährden könnten. Der Fokus dieses Meldesystems liegt auf dem Lerneffekt und allenfalls dem frühzeitigen Erkennen von Verhaltensmustern etc., die der Safety abträglich sein könnten. Um Anreize zu setzen, dass möglichst viele Fehler gemeldet werden, wird explizit der Lerneffekt über eine möglich disziplinarische oder sonstige Sanktionierung gestellt. Dieser «just culture»-Ansatz gewichtet mit Blick auf die systemische Sicherheit den Mehrwert des Lernens deutlich höher als den Effekt einer Sanktion des einzelnen Mitarbeitenden, der einen Fehler gemacht hat. Selbstverständlich greift dieser Ansatz nicht bei strafrechtlich relevanten Ereignissen. Dennoch hat diese Fehlerkultur in den vergangenen Jahrzehnten massiv zur Verbesserung der Flugsicherheit beigetragen und ist heute Teil der DNA im Luftverkehr.

Aus unserer Perspektive sollte dieser Ansatz auch mit Blick auf die Cybersicherheit gewählt werden. Das Ziel sollte sein, möglichst viele Anreize für umfassende Meldungen zu Cyberattacken zu setzen. Die Androhung von Strafen im Falle von Pflichtverletzungen erachten wir als kontraproduktiv.

Besten Dank für die wohlwollende Prüfung unserer Anliegen und Bemerkungen. Gerne stehen wir Ihnen für weitere Gespräche zur Verfügung.

Freundliche Grüsse

Swiss International Air Lines AG

Ronald Abegglen, MLaw
Public Affairs
Advisor to the CEO

Swisscom AG, Konzernrechtsdienst, 3050 Bern

Eidg. Finanzdepartement EFD
Hr. Bundesrat Ueli Maurer
zH Nat. Zentrum für Cybersicherheit (NCSC)
Bundesgasse 3
3003 Bern

Eingabe per E-Mail an: ncsc@gs-efd.admin.ch

Datum	13. April 2022	**Seite**
Ihr Kontakt	Lorenz Inglin / +41 58-223 08 48 / Lorenz.Inglin@swisscom.com	1 von 6
Thema	**Vernehmlassung zur Einführung einer Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen (Revision ISG) / Stellungnahme Swisscom**	

Sehr geehrte Herr Bundesrat,
sehr geehrte Damen und Herren

Bezugnehmend auf die Medienmitteilung des Bundesrates vom 12. Januar 2022 und die diesbezüglich gleichzeitig publizierten Vernehmlassungsunterlagen[1] nimmt Swisscom hiermit die eingeräumte Möglichkeit gerne wahr, sich im Rahmen der nachfolgenden Stellungnahme zum **Vernehmlassungsentwurf des Informationssicherheitsgesetzes**[2] (nachfolgend "*E-ISG*") im Zusammenhang mit der Einführung einer Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe in die Diskussionen einzubringen:

1. Allgemeine Vorbemerkungen sowie Grundposition Swisscom zum Revisionsvorhaben

Swisscom teilt die Wahrnehmung und Einschätzung des Bundesrates, wonach die Bedeutung der Cybersicherheit gerade in der jüngeren Vergangenheit zugenommen hat und von eine deutlich intensivierten Bedrohungslage im Bereich Cyber-Sicherheit ausgegangen werden muss. Cyberangriffe stellen eine ernsthafte Bedrohung der Sicherheit und des Wirtschaftsstandortes Schweiz dar. In Anbetracht dessen scheint ein **gesetzgeberischer Handlungsbedarf grundsätzlich ausgewiesen** mit dem Ziel, die Schweiz bei der Nutzung der Chancen der Digitalisierung angemessen vor Cyberrisiken zu schützen und in diesem Zusammenhang insbesondere die Resilienz der kritischen Infrastrukturen zu stärken und damit gleichzeitig die Widerstandsfähigkeit der Schweiz gegenüber Cyberrisiken zu erhöhen[3]. Die Verankerung einer gesetzlichen Meldepflicht und eine Stärkung des Meldewesens zum Zwecke der Frühwarnung, zur Einschätzung der Cyberbedrohungslage sowie zur frühzeitigen Erkennung aktueller Angriffsmuster scheint unter diesen Vorzeichen und Entwicklungen geboten.

Für die ICT-Branche im Allgemeinen und **Swisscom** als Betreiberin von modernen (leitungsgebundenen und mobilfunkbasierten) Telekommunikationsnetzen im Besonderen sind Cybersecurity-Aspekte von zentraler Bedeutung, weshalb die im Rahmen der ISG-Revisionsvorlage vorgeschlagenen Änderungen von hoher Relevanz sind. Im eigenen Interesse schützt Swisscom bereits seit Jahren die als kritische Infrastrukturen geltenden eigenen ICT-

[1] Vgl. https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-86768.html.

[2] Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) vom 18. Dezember 2020 (BBl 2020 9975 ff.)

[3] Vgl. Art. 1 lit. b E-ISG.

Netzinfrastrukturen sowie die entsprechenden Systeme der Kunden. Sie hat Produkte, das Know-How und die Sicherheitskultur, um im Markt für IT-Security weiter zu wachsen. Swisscom hat dabei den Anspruch, ihre eigene ICT-Infrastruktur nach best industry practices und mit modernen und innovativen Ansätzen zu schützen. Die zentrale Bedeutung sicherheitsrelevanter Aspekte sowie der Thematik Cybersecurity bei Swisscom kommt auch dadurch zum Ausdruck, dass der Bund als Mehrheitseigner im Rahmen der Governance sowie der im Vierjahresrhythmus verabschiedeten strategischen Zielen explizit entsprechende sicherheitsspezifische Erwartungshaltungen an Swisscom adressiert[4].

Bekanntlich fand bereits bisher zwischen Swisscom sowie den Cyber-Security-Fachstellen des Bundes (MELANI; NCSC) regelmässige Kontakte und ein **Informationsaustausch auf freiwilliger Basis** statt. Diese nach Wahrnehmung von Swisscom **etablierte Zusammenarbeit** in einer vertrauensvollen und konstruktiven Atmosphäre und im Bestreben, die Cyber-Bedrohungslage im Sinne eines Frühwarnsystems im allseitigen Interesse zu evaluieren und bei Bedarf im allseitigen Interesse die notwendigen Sicherheitsmassnahmen zur Stärkung der Resilienz der kritischen Infrastrukturen zu gewährleisten, sollte Basis für den Ausbau und die "Offizialisierung" der weiteren Zusammenarbeit bilden. Swisscom erachtet es als entscheidend, dass die über den bisherigen Informationsaustausch entwickelte Kultur der Zusammenarbeit und des gegenseitigen Vertrauens weitergeführt werden kann und auch den Unternehmen durch die Einführung der Meldepflicht ebenfalls ein ausgewiesener Mehrwert entsteht.

Im Lichte der dargestellten Entwicklungen und der stetig zunehmenden Bedrohungslage im Cyber-Raum, scheint das bisher praktizierte Modell der Zusammenarbeit und des Informationsaustausches indessen an seine Grenzen zu gelangen. Die Schaffung entsprechender gesetzlicher Grundlagen für die entsprechenden Tätigkeiten bzw. Zusammenarbeit ist deshalb auch aus **rechtsstaatlicher Sicht** und unter Verweis auf das zentrale **Legalitätsprinzip** zu begrüssen. Da gewisse sicherheitsrelevante Massnahmen zur Gewährleistung der Informationssicherheit zudem Persönlichkeitsrechte sowie weitere Aspekte des Geheimnis- bzw. Datenschutzes tangieren können, sind klare rechtliche Grundlagen hinsichtlich den zulässigen Massnahmen sowie der Rahmenbedingungen hinsichtlich des Informationsaustausches sowie der damit verbundenen Weiterleitung sensitiver Angaben auch mit Blick auf das Postulat der Rechtssicherheit begrüssenswert[5].

Zentral erachtet es Swisscom dabei, dass sich die vorgeschlagenen neuen Bestimmungen des ISG im Allgemeinen und insbesondere die angedachte Regelung im Zusammenhang mit der Meldepflicht für Cyberangriffe auf kritische Infrastrukturen im Besonderen an den Grundsätzen und Leitlinien orientiert, welche mit den **übergeordneten strategischen Vorgaben des Bundes[6]** im Einklang stehen. Ohne Anspruch auf Vollständigkeit erlaubt sich Swisscom, im vorliegenden Kontext folgende Eckpunkte hervorzuheben:

– **Ganzheitlicher, umfassender und risikobasierter Ansatz[7]:** Der Schutz von kritischen Infrastrukturen sowie die Gefahrenabwehr im Cyber-Raum hat einem ganzheitlichen und risikobasierten Ansatz zu folgen. Es sind sämtliche relevanten Verwundbarkeiten und Gefährdungen, die zu einer signifikanten Störung führen können, zu berücksichtigen und miteinander in ein Verhältnis zu setzen. Auch bezüglich Erarbeitung und Umsetzung von Schutzmassnahmen ist ein umfassendes und risikobasiertes Vorgehen zu verfolgen. Aus dem zu verfolgenden risikobasierten Ansatz gleichzeitig, dass ein Ausschluss jeglichen Risikos weder realistisch noch erstrebenswert

[4] Vgl. **Strategische Ziele des Bundesrates für die Swisscom AG 2022–2025** vom 24. November 2021 (BBl 2021 2848 ff.), Ziff. 1.2: "*Die Swisscom sorgt für den Ausbau und Betrieb einer zukunftsgerichteten und zuverlässigen Netz- und Informatikinfrastruktur unter Berücksichtigung der Marktbedürfnisse, der technologischen Entwicklung und der Sicherheit, insbesondere der Cyber-Sicherheit, des Fernmeldegeheimnisses, des Datenschutzes und der ständigen Erreichbarkeit der Notrufzentralen.*"

[5] Dies gilt beispielsweise in Bezug auf Art. 76 E-ISG, wo aus Sicht der Fernmeldedienstanbieterinnen begrüssenswerte Klarstellungen zur Bekanntgabe von Adressierungselementen sowie damit zusammenhängenden Personendaten gemacht werden (vgl. Abs. 3 und Abs. 4)

[6] **Strategie "Digitale Schweiz"** des Bundesrates vom 11. September 2020 (BBl 2020 7593 ff.) (vgl. v.a. Ziff. 3.2. und Ziff. 4.3.1). **Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken 2018 – 2022** (nachfolgend *"Strategie NCS"*) des Bundesrates vom 18. April 2018 (https:// www.ncsc.admin.ch/ncsc/de/home/strategie/strategie-ncss-2018-2022.html). **Nationale Strategie zum Schutz kritischer Infrastrukturen 2018 – 2022** (nachfolgend *"Strategie SKI")* des Bundesrates vom 8. Dezember 2017 (BBl 2018 503 ff).

[7] Vgl. Strategie SKI, BBl 2018 S. 514 ff.

ist und entsprechende Massnahmen bzw. Eingriffe zu Lasten der Wirtschaftsakteure **verhältnismässig**[8] auszugestalten sind. Die gesetzlichen Vorgaben sowie die konkreten Schutz- und Abwehrmassnahmen sollen deshalb ein optimales Verhältnis zwischen Massnahmenkosten und erzieltem Nutzen (Risikoreduktion) aufweisen. Abzulehnen sind insofern mit unverhältnismässig grossem (administrativem) Aufwand verbundene Eingriffe, welche für die Wirtschaft zu einer unnötigen administrativen (Mehr)Belastung führen und nicht durch die Bedrohungslage gerechtfertigt werden können.

- **Cyber-Security als gemeinsame Verantwortung bzw. als Querschnittsthema und -aufgabe:** Der Schutz vor Cyber-Risiken ist eine gemeinsame Verantwortung von Wirtschaft, Gesellschaft und Staat. Aus der gemeinsamen Verantwortung ergibt sich auch die gemeinschaftliche Umsetzung. Bund, Kantone, Wirtschaft und Gesellschaft sollen die notwendigen Massnahmen in enger Kooperation implementieren und dabei ihre jeweiligen Kompetenzen einbringen. Eine möglichst effektive Zusammenarbeit aller kompetenten Stellen und eine systematische internationale Vernetzung sind entscheidend für die Schaffung eines sicheren Umfeldes für die Digitalisierung der Gesellschaft und Wirtschaft[9].

Trotz dieser insgesamt positiven und dem Grundsatze nach befürwortender Grundhaltung zur Vernehmlassungsvorlage, erlaubt sich Swisscom nachfolgend, im Rahmen einer themenspezifischen Gliederung auf einige ausgewählte **Vorbehalte** hinzuweisen und in diesem Zusammenhang **Änderungsanregungen** einzubringen bzw. auf **Optimierungspotential** der Vorlage hinzuweisen.

2. Meldepflicht Betreiberinnen kritischer Infrastrukturen bei Cyberangriffen

2.1. Konzeptioneller Regelungsansatz

Der vorgesehene konzeptionelle Regulierungsansatz, wonach sich die neu vorgesehene **gesetzliche Meldepflicht** gem. Art. 74a E-ISG an **Betreiberinnen von kritischen Infrastrukturen** i.S. von Art. 74b E-ISG richtet und grundsätzlich[10] "**Cyberangriffe"** im Sinne der neuen Legaldefinition (Art. 5 lit. e E-ISG) sowie entsprechend den Kriterien von Art. 74d E-ISG als **meldepflichtige Ereignisse/Vorfälle** gelten, erscheint nach dem Dafürhalten von Swisscom sachgerecht[11]. Daneben bleibt für Cybervorfälle, welche nicht als Cyberangriffe zu qualifizieren sind, sowie für Schwachstellen von Informatikmitteln weiterhin eine freiwillige Meldemöglichkeit bzw. Zusammenarbeit gemäss den Rahmenbedingungen von Art. 73b E-ISG[12].

2.2. Voraussetzungen, Umfang, Inhalt und Ausgestaltungsmodalitäten der Meldepflicht

Auch wenn der konzeptionelle Regelungsansatz grundsätzlich nachvollziehbar und begrüssenswert ist, muss gleichzeitig festgehalten werden, dass aktuell noch wesentliche Unklarheiten bestehen, welche konkreten Konstellationen bzw. Ereignisse nun genau als meldepflichtige Cybervorfälle zu betrachten sind. Die in **Art. 74d E-ISG** definierten **Kriterien** zur Bejahung eines **meldepflichtigen Cyberangriffes** sehr offen und unbestimmt formuliert

---

[8] Vgl. Art. 5 Abs. 2 BV (Grundsätze rechtsstaatlichen Handelns): "*Staatliches Handeln muss im öffentlichen Interesse liegen und verhältnismässig sein.*"

[9] Vgl. Strategie Digitale Schweiz, Ziff. 4.3.1. (BBl 2020, S. 7607), Strategie SKI (BBl 2019, S. 515).

[10] Vgl. Art. 74c E-ISG zu den möglichen Ausnahmen, welche der Bundesrat auf Verordnungsstufe festlegen kann.

[11] Zu den möglichen Varianten, den Rahmenbedingungen sowie der Ausgestaltung der Meldepflichten vgl. u.a. auch Varianten für Meldepflichten von kritischen Infrastrukturen bei schwerwiegenden Sicherheitsvorfällen, Bericht des Bundesrates vom 13. Dezember 2019 in Erfüllung des Postulates 17.3475 Graf-Litscher. Meldepflicht für schwerwiegende Sicherheitsvorfälle bei kritischen Infrastrukturen Rechtliche Grundlagen, Bericht GS-EFD vom 11. Dezember 2020 (https://www.newsd.admin.ch/newsd/message/attachments/64412.pdf). Prüfung einer Meldepflicht bei Sicherheitsvorfällen, Studie von PwC Schweiz im Auftrag des Informatiksteuerungsorgans des Bundes (ISB) vom Oktober 2019 (PwC-Studie).

[12] Vgl. Erläuternder Bericht EFD/NCSC vom 12. Januar 2022, S. 13.

sind. Klare Kriterien, wann nun in der Tat ein schwerwiegender Sicherheitsvorfall bzw. ein Cyberangriff mit "*erheblichem Schadenspotential*"[13] zu bejahen ist, welcher auch vom Sinn und Zweck der Regelung eine Meldepflicht rechtfertigen, fehlen. Problematisch erscheint in diesem Zusammenhang insbesondere, dass für die Bejahung einer Meldepflicht bereits "*Anzeichen*" für gewisse Sachverhaltskonstellationen genügen[14]. Aus Sicht von Swisscom wäre zumindest prüfenswert, ob im Sinne einer graduellen Erhöhung der Meldeschwelle nicht von "*begründeten Verdachtsmomenten*" gesprochen werden sollte, zumal damit ein bei anderen Melde- und Sorgfaltspflichten relevantes Aufgreifkriterium herangezogen würde[15].

Zwecks Gewährleistung der Vollzugstauglichkeit und um die mit der Einführung der Meldepflicht verfolgten Ziele zu erreichen, erachtet es Swisscom deshalb als zentral, dass die auf Gesetzesstufe vorgegebenen Kriterien der zu meldenden Cyberangriffe im Rahmen von **Ausführungsbestimmungen auf Verordnungsstufe** detaillierter vorgegeben und präziser umschrieben werden[16]. Zur Sicherstellung eines effizienten und zielführenden Meldewesens bedarf es klarer Vorgaben und es besteht offensichtlich ein **ausgewiesener Konkretisierungsbedarf** auf Verordnungsstufe, was konkret gemeldet werden muss und welche Kritikalität die meldepflichtigen Ereignisse aufweisen müssen. Die entsprechenden Umsetzungsaspekte sind dabei vorzugsweise unter Einbezug der Fachexpertise der Cybersecurity-Abteilungen der betroffenen Betreiberinnen kritischer Infrastrukturen anzugehen.

2.3. Parallele Meldepflichten / Sektorielle Meldestellen

Der erläuternde Bericht zur Vernehmlassungsvorlage hält fest, dass die vorgeschlagene neue Meldepflicht für Cyberangriffe anderweitig bereits bestehende sektorspezifische Meldepflichten[17] nicht ersetze, sondern lediglich ergänze[18]. Insofern bestehen unter Umständen Überschneidungen durch parallele Meldepflichten[19]. Mit Blick auf die zu gewärtigenden administrativen Mehraufwendungen sowie entsprechender Doppelspurigkeit als suboptimal beurteilt Swisscom die zu gewärtigenden Überschneidungen mit anderen sektoriellen Meldepflichten im Bereich Cyber-Sicherheit oder weiteren Bereichen. Zur Vermeidung von unnötigem bürokratischem Aufwand sowie zur Vereinfachung der Prozesse wäre aus Sicht von Swisscom ein zentralerer Lösungsansatz mit einer einzigen Meldestelle für Cyberangriffe prüfens- und begrüssenswert. Im Zusammenhang mit den sektorspezifische Meldepflichten gestützt auf Art. 48a FMG und der diesbezüglich präsentierten FDV-Revisionsvorlage vom Dezember 2021[20] wird zwar hinsichtlich der vorgeschlagenen neuen Regelungen im Zusammenhang mit Cyberangriffen bzw. Cybervorfällen[21] in koordinativer Hinsicht erwähnt, dass der Vollzug der entsprechenden neuen regulatorischen Vorgaben dem BAKOM in "*Zusammenarbeit mit dem NCSC*" obliege[22]. Weshalb aber nicht gleichzeitig im Zusammenhang mit der angepassten Störungsmeldungspflichten[23] (welche regelmässig auch durch Cybervorfälle ausgelöst werden dürften) neu die Nationale Alarmzentrale und nicht das NCSC vorgesehen ist, wird zumindest aus den öffentlich zugänglichen Informationen prima vista mit keiner nachvollziehbaren Begründung dargelegt.

---

[13] Erläuternder Bericht EFD/NCSC vom 12. Januar 2022, S. 9 und S. 21.

[14] Art. 74d Abs. 1 E-ISG.

[15] Vgl. dazu z.B. Art. 9 GwG (geldwäschereirechtliche Meldepflichten der Finanzintermediäre) oder Art. 5 VSoTr (Sorgfalts- und Berichterstattungspflichten bei begründetem Verdacht auf Kinderarbeit).

[16] Erläuternder Bericht EFD/NCSC vom 12. Januar 2022, S. 10.

[17] Vgl. z.B. Art. 24 nDSG (Meldung von Verletzungen der Datensicherheit) (BBl 2020 7650); Finanzmarktrechtliche Meldepflicht von Cyberattacken gem. Art. 29 Abs. 2 FINMAG (Aufsichtsmitteilung FINMA 05/2020 vom 7. Mai 2020) oder Art. 48a FMG i.V.m. Art. 96 FDV (Mindestanforderungen an Netzsicherheit und -verfügbarkeit; Meldepflicht Betriebsstörungen Telekommunikationsnetze).

[18] Erläuternder Bericht EFD/NCSC vom 12. Januar 2022, S. 5.

[19] Erläuternder Bericht EFD/NCSC vom 12. Januar 2022, S. 11.

[20] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-86234.html.

[21] Art. 96a ff. E-FDV ["unbefugte Manipulation von Fernmeldeanlagen"]), im Rahmen welcher Anbieterinnen von Internetzugängen neu verpflichtet werden, angemessene Cybersicherheits- und Schutzmassnahmen zu ergreifen.

[22] Art. 96c E-FDV.

[23] Art. 96 E-FDV.

Ob insofern das bestehende Koordinations- und das aus Unternehmenssicht wünschbare Zentralisierungs- bzw. Vereinheitlichungspotential vollumfänglich ausgeschöpft wurde, ist insofern zumindest fraglich. Ungeachtet dessen erscheint jedenfalls die prozedurale Ausgestaltung des Meldeprozesses mit der Bereitstellung eines elektronischen Meldeformulars[24], welches bei Bedarf von den Meldenden auch an weitere Behördenstellen verwendet werden kann, im Sinne einer absoluten Minimalvariante als begrüssenswert.

3. Funktion und Aufgaben NCSC sowie Unterstützungsangebote des Bundes

Im Lichte der bereits bisher auf konstruktiv-lösungsorientierter Basis erfolgten Unterstützungsleistungen durch MELANI bzw. das NCSC erachtet es Swisscom als begrüssenswert, dass neben der aus rechtsstaatlicher Sicht wünschenswerten Verankerung der Grundlagen, Aufgaben und Kompetenzen des **nationalen Zentrums für Cybersicherheit ("NCSC")** auf Gesetzesstufe[25] gleichzeitig auch Aufgaben des Bundes bei der **Unterstützung von Wirtschaft und Bevölkerung** (z.B. in Form von technischer Beratung) vorgesehen werden[26]. Dies vor dem Hintergrund, dass Cyber-Security als gemeinsame Verantwortung bzw. als Querschnittsthema zu verstehen ist und sowohl die Behörden als auch die betroffenen Betreiberinnen kritischer Infrastruktur bzw. weitere private Akteure im Sinne einer "Public-Privat-Partnership" bestmöglich von den ausgetauschten und gemeinsam gewonnenen Erkenntnissen profitieren können und bei Bedarf geeignete Sicherheitsmassnahmen zur Beseitigung oder zumindest Minimierung der Cyber-Bedrohungslage initiieren können. Entsprechende Unterstützungs- und Beratungsdienstleistungen bei der Bewältigung von Cybervorfällen oder der Behebung von Schwachstellen dürften wesentlich dazu beitragen, dass sich das Meldewesen im allseitigen Interesse baldmöglichst etabliert und sich auch die weiterhin freiwillige Zusammenarbeit bei nicht meldepflichtigen Cybervorfällen bzw. Schwachstellen in der Wirtschaft gestärkt wird, damit den zunehmenden Cybergefahren gemeinsam und im allseitigen Interesse begegnet werden kann.

4. Vertraulichkeits- und Geheimhaltungsaspekte / Zusammenarbeit NCSC weitere Behörden

Auf Grund der regelmässigen Kritikalität und Sensitivität der im Rahmen der Meldung von Cyberangriffen von den Betreiberinnen kritischer Infrastrukturen zur Verfügung gestellten Informationen erscheint es zentral, dass ein möglichst vertrauensvoller Informationsaustausch gewährleistet bleibt.

Dies setzt einerseits voraus, dass das NCSC entsprechend sensitive Informationen nur mit anderen Behörden austauschen bzw. an diese weiterleiten darf, wenn hierfür eine ausdrückliche gesetzliche Grundlage besteht[27] oder die meldende Betreiberin ihre explizite Einwilligung dazu erteilte. Andererseits ist darauf hinzuweisen, dass die Behörden im Rahmen der bisherigen freiwilligen Zusammenarbeit sowie dem damit einhergehenden Informationsaustausch die Vertraulichkeit einer Meldung explizit zusicherte[28], weshalb unter Verweis auf Art. 7 Abs. 1 lit. h BGÖ[29] eine Offenlegung gestützt auf die Bundesöffentlichkeitsgesetzgebung nicht befürchtet werden musste. In Anbetracht der nun vorgesehenen Einführung einer gesetzlichen Meldepflicht für Cyberangriffe, wird der erwähnte Ausnahmetatbestand nicht mehr Anwendung finden, weshalb die Gefahr besteht, dass Dritte via BGÖ-Zugangsgesuche Zugang zu entsprechend sensitiven und nicht für die Öffentlichkeit bestimmten Informationen gelangen

---

[24] Art. 74f Abs. 1 E-ISG sowie Erläuternder Bericht EFD/NCSC vom 12. Januar 2022, S 9, S. 11 und S. 21.

[25] Vgl. Art. 73a E-ISG.

[26] Vgl. Art. 74 E-ISG.

[27] Vgl. z.B. Art. 76a E-ISG.

[28] Vgl. https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden/scope-and-rules.html": *"Wenn die Schwachstelle innerhalb der vorgegebenen Regeln übermittelt wird, wird NCSC.ch keine rechtlichen Schritte gegen Sie einleiten. Ihre Angaben werden vertraulich behandelt. Sie können uns Ihre Informationen anonym mitteilen."*

[29] Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ) vom 17. Dezember 2004 (SR 152.3), Art. 7 Abs. 1 lit. h BGÖ: *"Der Zugang zu amtlichen Dokumenten wird … verweigert, wenn durch seine Gewährung Informationen vermittelt werden können, die der Behörde von Dritten freiwillig mitgeteilt worden sind und deren Geheimhaltung die Behörde zugesichert hat".*

könnten, zumal andere Ausnahmetatbestände gemäss Art. 7 BGÖ (Geschäftsgeheimnisse; Informationen mit Sicherheitsrelevanz) von den Behörden und Gerichten nur sehr zurückhaltend bejaht werden. Vor diesem Hintergrund und in Anbetracht des ausgewiesenen und überwiegenden öffentlichen Geheimhaltungsinteresse **beantragt Swisscom**, im Rahmen der aktuellen ISG-Revisionsvorlage eine Ausnahmeregelung einzuführen, welche im Sinne einer lex specialis Vorrang vor dem Öffentlichkeitsprinzip gemäss BGÖ beansprucht[30].

5. Sanktionsbestimmungen sowie Durchsetzungsmechanismen bei Verletzung der Meldepflichten

Die vorgesehenen verwaltungsstrafrechtlichen Sanktionsmechanismen sowie der vorgeschlagene Bussenrahmen bei Wiederhandlungen gegen Anordnungen des NCSC (Art. 74h Abs. 2 i.V.m. Art. 74i E-ISG) erachtet Swisscom in mehrfacher Hinsicht als problematisch und deshalb als nicht sachgerecht. In Anbetracht der Unbestimmtheit der meldepflichtigen Ereignisse/Vorfälle[31] stehen Bussenandrohungen in der vorgesehenen Höhe einerseits bereits in einem Spannungsfeld mit dem Legalitätsprinzip. Andererseits scheint ein entsprechendes Umsetzungs- und Vollzugsverständnis mit abschreckenden negativen Anreizen in Form von substanziellen Bussenandrohungen schwer vereinbar mit der Tatsache, dass Cybersecurity eine Querschnittsaufgabe darstellt und den entsprechenden Gefahren nur im Rahmen eines partnerschaftlichen und kooperativen Ansatzes zwischen dem Staat und der Wirtschaft erfolgsversprechend begegnet werden kann. Abgesehen davon ergibt ist auch keine nachvollziehbare Begründung dafür, wieso in der vorliegenden Konstellation von den allgemeinen Zwangsvollstreckungsinstrumentarien abgewichen werden soll[32], zumal eingestanden wird, dass die Regelung ohnehin "*weitgehend symbolischen Charakter*" hat[33]. Swisscom beantragt deshalb, **Art. 74i E-ISG ersatzlos zu streichen** und gleichzeitig im Zusammenhang mit dem Verweis in Art. 74h Abs. 2 E-ISG die insofern notwendigen Anpassungen vorzunehmen.

Für die Kenntnisnahme und Berücksichtigung der Anliegen sowie Überlegungen von Swisscom bedanken wir uns im Voraus bestens.

Mit vorzüglicher Hochachtung

Swisscom AG

Lorenz Inglin
Head of Cyber Defense
12.04.2022
QES Qualified electronic signature
Signed with Swisscom certificate by ajila Blink

Stefan Gilgen
12.04.2022
QES Qualified electronic signature
Signed with Swisscom certificate by ajila Blink

Lorenz Inglin
Head of Cyber Defense

Stefan Gilgen
Senior Counsel

[30] Vgl. Art. 4 BGÖ.

[31] Vgl. dazu im Einzelnen oben Ziff. 2.2.

[32] Vgl. Art. 292 StGB (Ungehorsam gegen amtliche Verfügungen), welche Bussenandrohung bis max. CHF 10'000.—erlaubt (Art. 106 StGB).

[33] Erläuternder Bericht EFD/NCSC vom 12. Januar 2022, S 6.

swissgrid

Swissgrid AG
Bleichemattstrasse 31
Postfach
5001 Aarau
Schweiz

T +41 58 580 21 11
info@swissgrid.ch
www.swissgrid.ch

Ihr Kontakt
Michael Rudolf
T direkt +41 58 580 35 15
michael.rudolf@swissgrid.ch

Nationales Zentrum für Cybersicherheit
Schwarztorstrasse 59
CH-3003 Bern

Per E-Mail an: ncsc@gs-efd.admin.ch

5. April 2022

Swissgrid Stellungnahme zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrte Damen und Herren,

Als nationale Netzgesellschaft sorgt Swissgrid dauernd für einen diskriminierungsfreien, zuverlässigen und leistungsfähigen Betrieb des Übertragungsnetzes als wesentliche Grundlage für die sichere Versorgung der Schweiz (Art. 20 Stromversorgungsgesetz, StromVG). Das Übertragungsnetz bzw. die Stromversorgung ist die kritischste Infrastruktur der Schweiz[1]. Gerne äussern wir uns zum Entwurf einer Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe.

Swissgrid begrüsst die Einführung einer Meldepflicht für Cyberangriffe nach Art. 74a des vorliegenden Entwurfs des Informationssicherheitsgesetzes (ISG). Die bisher auf Freiwilligkeit basierende Regelung in Art. 76 Abs. 3 ISG ist nicht ausreichend. Damit die Schweiz ihre kritischen Infrastrukturen vor Cyberangriffen schützen kann, müssen die dafür zuständigen Stellen beim Bund Kenntnis über Herkunft, Methodik und Ausmass von Cyberangriffen haben. Die vom Bund gesammelten resp. daraus gewonnen Erkenntnisse müssen wiederum mit Betreiberinnen kritischer Infrastrukturen geteilt werden können.

Bei den Bestimmungen des vorliegenden Entwurfs sehen wir an verschiedenen Stellen Präzisierungsbedarf. Zudem besteht unserer Ansicht nach Abstimmungsbedarf mit dem revidierten Datenschutzgesetz (revDSG). Dies betrifft u.a. die Meldepflicht im revDSG bei der Verletzung der Datensicherheit.

[1] Vgl. u.a. Bericht des Bundesamtes für Bevölkerungsschutz BABS (2020) «Katastrophen und Notlagen Schweiz 2020, Bericht zur nationalen Risikoanalyse»

Zu den Bestimmungen haben wir folgende Anmerkungen.

Art. 5 Begriffe

> *In diesem Gesetz bedeuten:*
>
> *d. Cybervorfall: Ereignis beim Betrieb von Informatikmitteln, das dazu führen kann, dass die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist;*
>
> *e. Cyberangriff: Cybervorfall, der von Unbefugten absichtlich ausgelöst wurde.*

Bst. d: Mit der Formulierung «Beeinträchtigung der Nachvollziehbarkeit» unterscheidet sich das ISG von Datenschutzgesetzen, die vor allem die Vertraulichkeit, Integrität und Verfügbarkeit von Personendaten sicherstellen wollen. Will das ISG mit dieser Formulierung absichtlich zur Meldung einer weiteren Form der Beeinträchtigung anregen? Und wenn Ja, an welches Szenario ist bei einer Beeinträchtigung der Nachvollziehbarkeit einer Informations-Bearbeitung zu denken?

Bst. e: Für Swissgrid ist unklar, ob «Unbefugte» auch betriebsinterne Personen miteinschliesst, die absichtlich über ihre Kompetenzen hinaus eine Beeinträchtigung der «Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung» herbeiführen. Weiter ist für Swissgrid unklar, ob Bst. e nur «erfolgreich» durchgeführte Cyberangriffe oder auch versuchte Angriffe («near misses») erfasst. Die Unklarheit ergibt sich für Swissgrid einerseits aus dem Verweis auf Bst. d, wo schon die blosse Möglichkeit einer Beeinträchtigung erfasst ist und andererseits aus Art. 74d Abs. 1 – insbesondere aus Bst. a und c (Anzeichen einer potenziellen Gefährdung/Veränderung des Informationsbestands bereits Auslöser der Meldepflicht). Wir beantragen entsprechende Klarstellungen im Entwurf oder den Erläuterungen.

Art. 73b *Bearbeitung von Meldungen zu Cybervorfällen und Schwachstellen*

> *[2] Das NCSC kann Informationen zu Cybervorfällen veröffentlichen oder an interessierte Behörden und Organisationen weiterleiten, sofern dies dazu dient, Cyberangriffe zu verhindern oder zu bekämpfen. Diese Informationen dürfen Personendaten und Daten juristischer Personen enthalten, sofern es sich um missbräuchlich verwendete Identifikationsmerkmale und Adressierungselemente handelt und die betroffene Person einwilligt.*

Für Swissgrid ist unklar, wie der Einwilligungsprozess ablaufen soll bzw. wer für das Einholen der Einwilligung zuständig ist. Holt das NCSC die Einwilligung der betroffenen Person ein oder ist angedacht, dass dies das meldepflichtige Unternehmen tun muss? In letzterem Fall: Besteht für das meldepflichtige Unternehmen gar eine Mitwirkungspflicht, welche über die Auskunftspflicht in Art. 74g ISG hinausgeht? Swissgrid geht diesbezüglich davon aus, dass die Weitergabe von Personendaten, namentlich die Bekanntgabe von Kontaktdaten zur Ermöglichung der Einholung der Einwilligung durch das NCSC nicht durch die Art. 74e und 74g ISG abgedeckt ist.

Die Weitergabe von Personendaten bedarf nach Ansicht von Swissgrid einer Grundlage im Gesetz (Mitwirkungspflicht).

Art. 73c Weiterleitung von Informationen

> [4] *Informationen, die strafrechtlich geschützte Geheimnisse offenbaren, darf das NCSC nur nach den Vorgaben von Artikel 320 StGB weiterleiten.*

Swissgrid regt an, dass in den Erläuterungen namentlich erwähnt wird, durch welche Behörde sich das NCSC vom Geheimnisschutz entbinden lassen kann.

Art. 74 *Unterstützung von Betreiberinnen von kritischen Infrastrukturen*

Swissgrid begrüsst die in Art. 74 ISG verankerte Unterstützung von Betreiberinnen kritischer Infrastrukturen durch das NCSC. Der bereits heute etablierte Austausch zwischen Betreiberinnen kritischer Infrastrukturen und dem NCSC bzw. ehemals MELANI funktioniert gut. Eine Ausweitung dieses Modells dürfte indes eine Herausforderung darstellen. Swissgrid teilt die Ansicht der Erläuterungen (S. 27), dass dies seitens Bund zusätzliche Aufwände verursachen wird und deshalb beim Ausbau des NCSC zu berücksichtigen ist.

Art. 74a *Meldepflicht*

Sowohl der vorliegende Entwurf (Art. 74a) als auch das revDSG (Art. 24) verlangen, dass Meldungen an das NCSC resp. den EDÖB «so rasch als möglich» erfolgen. Unklar ist, in welchem Verhältnis diese Meldepflichten bzw. die beiden Gesetze zueinanderstehen. Haben die beiden Meldungen gleichzeitig zu erfolgen oder ist die Erwartung, dass die Meldung nach ISG zuerst erfolgt? Swissgrid geht von einem zeitlichen Vorrang der Meldung nach ISG aus, zumal die Formulierung von Art. 74e Abs. 2 ISG explizit die Möglichkeit eröffnet, nach einer ersten so rasch als möglich erfolgten Meldung, gewisse Informationen zu einem späteren Zeitpunkt nachzuliefern. Das revDSG sieht eine solche Möglichkeit nicht explizit vor. Die Frage stellt sich zudem, weil je nach Unternehmen unterschiedliche Funktionen (bzw. Personen) zuständig für die Entgegennahme von Informationen und das Absetzen der jeweiligen Meldungen sein können. Alleine dadurch können sich Verzögerungen der beiden Meldungen ergeben.

Gemäss Art. 74a ISG, ist es Aufgabe des NCSC, mögliche Betroffene zu warnen. Diesbezüglich weisen wir auf Fälle von unter falschem Namen (oder anderen Identifikationsmerkmalen wie bspw. Foto der Person) versendeten Phishing Mails hin. Es stellt sich die Frage, ob die Informierung der Person unter dessen Namen die Phishing Mail verschickt wurde, ebenfalls unter diese Bestimmung fällt, d.h. eine Informationspflicht des NCSC gegenüber dem/der (vermeintlichen) Absender/Absenderin besteht. Zu berücksichtigen ist dabei:

1) Zwischen der Person und dem NCSC besteht womöglich kein bisheriges Kontaktverhältnis. Hingegen kann ein solches mit dem meldepflichtigen Unternehmen bestehen. Ist vorgesehen, dass hier das meldepflichtige Unternehmen wiederum eine Mitwirkungspflicht bei der Informierung hat? Wenn Ja, sollte diese gesetzlich festgehalten werden.

2) Die Person kann zu den Geschädigten gehören oder aber die Täterschaft sein. Somit stellt sich die Frage, zu welchem Zeitpunkt die Informierung dieser Person zu erfolgen hat, bzw. welche allfälligen Abklärungen zuerst durchzuführen sind (um bspw. nicht eine Untersuchung oder Beweissicherung zu tangieren).

Art. 74c *Ausnahmen von der Meldepflicht*

Swissgrid kann den Grundgedanken der vorgesehenen Delegationsnorm an den Bundesrat bzgl. Ausnahmen von der Cybermeldepflicht nachvollziehen. Hinsichtlich Stromnetzbetreibern geben wir zu bedenken, dass ein Grossteil dieser nur wenige oder nur eine einzige Gemeinde versorgen. Die Stromversorgung bzw. das Stromnetz ist jedoch die kritischste Infrastruktur. Sie ist Grundlage für das Funktionieren zahlreicher anderer kritischer Infrastrukturen. Zudem geht Swissgrid von einem relativ hohen Standardisierungsgrad der eingesetzten Applikationen auf den unteren Netzebenen aus. Ist ein Cyberangriff auf einen einzelnen Netzbetreiber erfolgreich, könnte der Angriff auch bei anderen Netzbetreibern erfolgreich sein. Eine Meldepflicht an den Bund mit anschliessender Weiterleitung von Erkenntnissen des Angriffs an weitere Netzbetreiber kann somit entscheidend zur Sicherheit des Gesamtsystems beitragen. Aus Sicht von Swissgrid, ist deshalb von einer allfälligen Anwendung der Ausnahmebestimmungen in Art. 74c ISG im Strombereich abzusehen.

Art. 74d *Zu meldende Cyberangriffe*

> [1] *Ein Cyberangriff auf eine kritische Infrastruktur muss gemeldet werden, wenn Anzeichen dafür bestehen, dass:*
>
> a. *die Funktionsfähigkeit der betroffenen kritischen Infrastruktur oder einer anderen kritischen Infrastruktur gefährdet ist;*
>
> b. *ein fremder Staat ihn ausgeführt oder veranlasst hat;*
>
> c. *er zu einem Abfluss oder zur Manipulation von Informationen geführt hat oder führen könnte*

Art. 74d stellt nach Ansicht von Swissgrid den «Kern» der Vorlage dar. Die Bestimmung erscheint jedoch noch nicht ausgereift und ist zu präzisieren.

Bei Bst. a stellt sich uns die Frage, ab wann eine Gefährdung der Funktionsfähigkeit der betroffenen kritischen Infrastruktur meldungsrelevant ist. Wie stark muss die Beeinträchtigung der Funktionsfähigkeit sein, damit eine Meldepflicht ausgelöst wird?

Auch im Hinblick auf die Gefährdung «einer anderen kritischen Infrastruktur» schafft die Bestimmung Unsicherheiten bzw. zu grossen Auslegungsspielraum. So stellt sich bspw. die Frage, wie ein Unternehmen erkennen kann, ob eine andere, ihm / ihr nicht im Detail bekannte kritische Infrastruktur derart von der Funktionsfähigkeit des Unternehmens abhängig ist, dass die kritische Infrastruktur bei einer Beeinträchtigung der Funktionsfähigkeit des Unternehmens gefährdet ist. Swissgrid beantragt weitere Präzisierungen bzgl. wann eine Meldepflicht einsetzt. In diesem Zusammenhang geben wir zu bedenken, dass detaillierte Konkretisierungen mit Blick auf die Vielfalt an kritischen Infrastrukturen subsidiär zu regeln sind. Swissgrid teilt diesbezüglich die Meinung in den Erläuterungen auf S. 26, dass sich der Bundesrat bei der Festlegung von Vorgaben an einschlägigen Fachnormen orientieren und diese auch für verbindlich erklären können soll.

Die in Bst. b. vorgesehene Einschätzung bzw. die Zuordnung eines Angriffs zu einem Staat durch den Betroffenen dürfte nur schwer bis gar nicht durchführbar sein. Dies vor allem nicht, wenn eine Meldung möglichst rasch erfolgen soll und damit zu einem Zeitpunkt, wo erst unvollständige Informationen zum Cyberangriff vorliegen. Weiter ist davon auszugehen, dass der Betroffene nicht in der Lage ist zu erkennen bzw. zu unterscheiden, ob ein Angriff staatlich geduldet, gefördert oder effektiv staatlich durchgeführt wurde und oder von der Täterschaft falsche Spuren gelegt wurden.

Aus Sicht Swissgrid ist die in Bst. c enthaltene Schwelle eher niedrig angesetzt und könnte damit bei fast jedem Cyberangriff erfüllt sein. Mit Blick auf das Stromnetz, sind aus Sicht von Swissgrid Cyberangriffe zu melden, wenn u.a. folgende Informationen oder Systeme betroffen bzw. beeinträchtigt sind:

- Besonders schützenswerte Personendaten;
- Informationen zu den kritischen Infrastrukturen und Systemen (inkl. Schnittstellen und Zugangsmöglichkeiten) der kritischen Infrastruktur Betreiberin;
- Daten des Stromnetzbetriebs; oder
- Infrastrukturen und Systeme, welche für die Erfüllung des Kernauftrags der kritischen Infrastruktur Betreiberin kritisch sind.

Art. 74e *Inhalt der Meldung*

> [1] *Die Meldung muss Informationen zur kritischen Infrastruktur, zur Art und Ausführung des Cyberangriffs, zu seinen Auswirkungen und zum geplanten weiteren Vorgehen der Betreiberin der kritischen Infrastruktur enthalten.*

Zum Vergleich, Art. 24 revDSG

> [2] *In der Meldung nennt er mindestens die Art der Verletzung der Datensicherheit, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen.*

Art. 74e Abs. 1 ISG enthält, anders als Art. 24 Abs. 2 revDSG, keine Pflicht, bereits ergriffene Massnahmen zu melden. Wurde darauf bewusst verzichtet?

Art. 74f *Übermittlung der Meldung*

> [2] *Das System muss der Betreiberin einer kritischen Infrastruktur ermöglichen, die Meldung des Cyberangriffs oder seiner Auswirkungen gesamthaft oder in Teilen an weitere Stellen und Behörden zu übermitteln.*

Aus Sicht Swissgrid, hat das System insb. die Übermittlung der Meldung an den EDÖB zu ermöglichen. Zudem wäre es wünschenswert, wenn über das System auch die Informationen, welche dem EDÖB gemäss revDSG ergänzend zu liefern sind, übermittelt werden könnten.

Art. 74i *Widerhandlungen gegen Verfügungen des NCSC*

> [1] *Mit Busse bis zu 100 000 Franken wird bestraft, wer einer vom NCSC unter Hinweis auf die Strafdrohung dieses Artikels erlassenen rechtskräftigen Verfügung oder dem Entscheid einer Rechtsmittelinstanz vorsätzlich nicht Folge leistet.*

> [3] *Fällt eine Busse von höchstens 20 000 Franken in Betracht und würde die Ermittlung der nach Artikel 6 VStrR strafbaren Personen Untersuchungsmassnahmen bedingen, die im Hinblick auf die verwirkte Strafe unverhältnismässig wären, so kann die Behörde von einer Verfolgung dieser Personen absehen und an ihrer Stelle den Geschäftsbetrieb zur Bezahlung der Busse verurteilen.*

Bei Art. 74i Abs. 1 ISG ist für Swissgrid unklar, ob unter «vorsätzlich» auch der Eventualvorsatz erfasst ist. Weiter stellt sich die Frage, wer die relevanten Personen sind, welche sanktioniert werden und ob diesbezüglich bewusst von den Verantwortlichkeiten im revDSG (Art. 63) abgewichen wird. Folgt man dem erläuternden Bericht des ISG, würde dies zudem bedeuten, dass unter Umständen eine andere Person (Person «in der Linie») für die Meldung verantwortlich wäre, aber eine Führungsperson («Leitungsebene von Unternehmen», Erläuterungen S. 22) zur Rechenschaft gezogen werden könnte. Soll eine Führungsperson sanktioniert werden, könnte diese Person durch Herausverlangen des Organigramms einfach bestimmt werden. Somit würde sich aber Art. 74i Abs. 3 erübrigen, da keine «unverhältnismässigen Ermittlungen» erforderlich wären. Wir beantragen eine Prüfung und ggf. Überarbeitung dieser Bestimmung bzw. der Erläuterungen.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse
Swissgrid AG

Konrad Zöschg
Head of Technology

Michael Schmid
Head of Legal, Regulatory & Compliance

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

Herr Bundesrat Ueli Maurer
Eidgenössisches Finanzdepartement EFD
Geschäftsstelle Nationales Zentrum für Cybersicherheit NCSC

ausschliesslich per E-Mail:
ncsc@gs-efd.admin.ch

Zürich, 7. April 2022

Stellungnahme zum Entwurf des Bundesgesetzes über die Informationssicherheit beim Bund (ISG): Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrter Herr Bundesrat Maurer
Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit zu oben genanntem Geschäft Stellung zu beziehen und nehmen diese hiermit gerne fristgerecht wahr.

SWITCH wurde 1987 von der Schweizerischen Eidgenossenschaft gemeinsam mit den damals acht Universitätskantonen als privatrechtliche Stiftung errichtet. Entsprechend dem Stiftungszweck erbringt SWITCH im Wesentlichen Informatikdienstleistungen gegenüber kantonalen Universitäten, Eidgenössischen Technischen Hochschulen, Fachhochschulen und pädagogischen Hochschulen sowie anderen Organisationen der öffentlichen Hand und kritischen Infrastrukturen in der Schweiz.

SWITCH selbst betreibt drei kritische Infrastrukturen für die Schweiz: das Domain Name System (DNS) für die ccTLD .ch, das Nationale Netzwerk für Forschung und Lehre (NREN) der Schweiz und das Multisektor-CERT SWITCH-CERT, neben dem GovCERT im NCSC das zweite nationale CERT für die Schweiz. Dieses erbringt in enger Zusammenarbeit mit dem GovCERT operative Sicherheits-Dienstleistungen für sämtliche oben erwähnte Hochschulen (entspricht allen Organisationen des Teilsektors gemäss Art. 74b lit. a E-ISG) sowie relevante Unternehmen der KI-Sektoren Banken, Energie sowie Industrie und Logistik.

Begrüssung einer Meldepflicht

SWITCH beschäftigt sich als Betreiberin von kritischen Infrastrukturen täglich mit der Cybersicherheit ihres eigenen Unternehmens und leistet als Multisektor-CERT einen relevanten Beitrag an die Cybersicherheit kritischer Infrastrukturen, insbesondere aufgrund der Bedrohungslage des wichtiger werdenden Bereichs der Vorfallbewältigung sowie durch die Erarbeitung national relevanter Threat Intelligence auch präventiv.

Die Anzahl von Cyberangriffen nimmt rasant zu. Dies gilt insbesondere für Betreiberinnen von kritischen Infrastrukturen, die eine wichtige Funktion für Wirtschaft und Gesellschaft übernehmen und diese auch im Falle eines Cybervorfalls oder -angriffs gewährleisten müssen. Der gegenseitige Informationsaustausch ist ein sehr wichtiges Mittel zum Schutz vor Cyberrisiken.

Deswegen begrüsst SWITCH die Meldepflicht für Betreiberinnen von kritischen Infrastrukturen und erachtet eine solche auch als zweckmässig, um die Qualität des spezifischen Lagebildes und darauf basierend die Resilienz der kritischen Infrastrukturen in der Schweiz zu erhöhen.

Zu den einzelnen Bestimmungen

Begriffe (Art. 5 E-ISG)

Die in Art. 5 E-ISG vorgenommene Differenzierung zwischen Cybervorfall (lit. d) und Cyberangriff (lit. e) ist sinnvoll, da somit gewährleistet ist, dass nicht jede Schwachstelle gemeldet werden muss, sondern nur der Cyberangriff auf kritische Infrastrukturen meldepflichtig ist, während eine freiwillige Meldung von Cybervorfällen möglich bleibt. Allerdings wird dieser Zweck nicht durchwegs erreicht, weil mit der aktuell vorgeschlagenen Definition in lit. d auch die blosse Möglichkeit der Beeinträchtigung der Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder der Nachvollziehbarkeit ihrer Bearbeitung die Meldepflicht auslöst. Wir würden es begrüssen, wenn die Meldepflicht nur auf effektive Beeinträchtigungen Anwendung findet und Art. 5 lit. d und lit. e E-ISG dahingehend angepasst würden. Damit wird einerseits der Aufwand auf Seiten der Betreiberinnen kritischer Infrastrukturen reduziert und andererseits das Meldevolumen beim NCSC auf für das Lagebild relevante Vorfälle limitiert.

Meldepflicht (Art. 74a E-ISG)

Dieser Artikel statuiert die Meldepflicht, deren Zweck und Frist. Es wird festgehalten, dass Betreiberinnen kritischer Infrastrukturen im Falle von Cyberangriffen der Meldepflicht unterstellt sind und dass sie Cyberangriffe nach deren Entdeckung dem NCSC «so rasch als möglich» melden müssen. Die Bestimmung ermöglicht, insbesondere auch im Zusammenspiel mit Art. 74e Abs. 2 E-ISG, eine den Umständen angemessene Beurteilung eines Cyberangriffs, ohne diesen wesentlichen Prozess in das Korsett eines festen Zeitrahmens zu zwängen. Gleichzeitig sorgt die Unbestimmtheit des zeitlichen Rahmens, innert dessen die Meldung zu erfolgen hat, für Rechtsunsicherheit bei den Adressaten der Bestimmung. Eine Meldung sollte unter diesen Umständen nur als verspätet betrachtet werden, wenn der meldepflichtige Betreiber eine mögliche Meldung unbegründet und ungerechtfertigt verzögert hat.

Sodann ist insbesondere bei Betreiberinnen von kritischen Infrastrukturen, die anderen Betreiberinnen von kritischen Infrastrukturen gegenüber Leistungen erbringen, nicht klar abgrenzbar, wen in einem solchen Szenario die Meldepflicht trifft. Die Meldepflicht sollte nur bestehen, wenn ein Cyberangriff auf die eigene Infrastruktur erfolgt. Wir empfehlen, Art. 74a E-ISG mit Blick auf die vorgenannte zeitliche Komponente sowie mit Blick auf die Verantwortlichkeit betreffend Meldepflicht entsprechend anzupassen respektive zu konkretisieren.

Bereiche (Art. 74b E-ISG)

Im Erläuterungsbericht wird korrekterweise die Notwendigkeit festgestellt, die Definition für kritische Infrastrukturen gemäss Art. 5 ISG zu präzisieren. Insbesondere soll konkretisiert werden, wann eine Organisation als kritische Infrastruktur gilt und wann nicht. Art. 74b E-ISG grenzt die Unternehmen und Organisationen, die als kritische Infrastruktur gelten, nach Bereichen ein. Dabei orientiert sich die

Vernehmlassungsvorlage vernünftigerweise an den in der Strategie zum Schutz kritischer Infrastrukturen (SKI) aufgelisteten Sektoren und Teilsektoren.[1]

Bei denjenigen Bereichen, bezüglich derer sich das E-ISG nicht auf bestehende Definitionen stützen kann, ist jedoch mit Unsicherheiten und Diskussionspotenzial zu rechnen. Dies betrifft die Anbieter von digitalen Diensten (lit. f), Unternehmen, die die Bevölkerung mit Gütern des täglichen Bedarfs versorgen (lit. r) und die Hersteller von Hard- und Software (lit. s). Insbesondere die Unterstellung der Hersteller von Hard- und Software weitet den Kreis der Meldepflichtigen potenziell auf zahlreiche in- und ausländische Unternehmen in der Lieferkette von kritischen Infrastrukturen aus. Es ist fraglich, ob die Meldepflicht für diese Hersteller von Hard- und Software erkennbar ist.

Die Schweizerische Eidgenossenschaft hat SWITCH kraft Delegationsvertrag mit der Verwaltung der .ch-Domain-Namen beauftragt. Wir sind davon ausgegangen, dass die Verwaltung der .ch-Domain-Namen unter die Meldepflicht fallen würde, weil das DNS für .ch schon lange als kritische Infrastruktur erfasst ist und SWITCH entsprechend auch in die Stabsorganisation des Bundesamtes für wirtschaftliche Landesversorgung (BWL) im Sektor IKT, Abteilung FDA, eingebunden ist. Allerdings lässt sich die Verwaltung der .ch-Domain-Namen, unter keinen Buchstaben von Art. 74b subsumieren. Unter lit. f sind nur die Registrare erwähnt, nicht aber die Domain Registry.

Ausnahmen von der Meldepflicht (Art. 74c E-ISG)

Während Art. 74b E-ISG die meldepflichtigen Bereiche grosszügig umreisst, gibt Art. 74c E-ISG dem Bundesrat die Aufgabe, Einrichtungen, die in einem kritischen Sektor oder Teilsektor tätig sind, nach Massgabe der gesetzlich verankerten Kriterien auszunehmen. Der Bundesrat kann auf Verordnungsebene gemäss Wortlaut von Art. 74c E-ISG aber nur bestimmte Kategorien von Betreiberinnen kritischer Infrastrukturen von der Meldepflicht ausnehmen. Dabei ist zu beachten, dass die gemäss Art. 74b meldepflichtige Einrichtungen sowohl kritische als auch nicht kritische Dienste erbringen können. Eine Differenzierung nach Tätigkeitsfeld scheint jedoch nach der vorliegenden Bestimmung nicht beabsichtigt und möglich zu sein. Dies wäre jedoch wünschenswert, um auch den Grundsatz der Verhältnismässigkeit zu wahren. Insbesondere bei kleineren Hochschulen scheint es uns wichtig, die Meldepflicht mit Augenmass anzuwenden und die (vielen) kleinen Organisationen von einer Meldepflicht auszunehmen. Dazu wird es auf Verordnungsebene klare Kriterien brauchen.

Zu meldende Cyberangriffe (Art. 74d E-ISG)

Diese Bestimmung zählt alternative Kriterien auf, unter denen ein Cyberangriff meldepflichtig ist. Abgesehen von Art. 74d Abs. 1 lit. a E-ISG, berücksichtigt die Bestimmung das Schadensausmass oder Schadenspotenzial eines Cyberangriffs nicht. Es ist zudem sehr unklar, wann aus Sicht des Bundes eine kritische Infrastruktur als «gefährdet» gelten soll. Sofern keine entsprechenden Präzisierungen auf Gesetzesebene erfolgen, ist es notwendig, dies zumindest auf Verordnungsebene zu präzisieren.

In Anbetracht der Komplexität der Attribution von Angriffen ist lit. b zwar wünschenswert, aber aus unserer Sicht höchstens in Ausnahmefällen relevant. Heute finden sich in den meisten Fällen, wenn überhaupt, nur Hinweise auf die Urheber von Angriffen und nur in Ausnahmenfällen harte Beweise. Gerade State Actors arbeiten zudem oft mit Verschleierungsmethoden, welche zu Falschattributionen führen. Wir schlagen daher vor, lit. b ersatzlos zu streichen. Wenn lit. b so erhalten bleiben sollte,

[1] https://www.babs.admin.ch/de/aufgabenbabs/ski/nationalestrategie.html

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

braucht es dazu zwingend auf Verordnungsebene klare Kriterien und Vorgaben, um eine sinnvolle Anwendung sicherzustellen.

Übermittlung der Meldung (Art. 74f E-ISG)

Die Meldepflicht für Cyberangriffe soll die bestehenden Meldepflichten nicht ersetzen, sondern nur ergänzen. Dabei erscheint es uns wichtig, dass eine Koordination der verschiedenen Meldepflichten angestrebt wird, so dass der administrative Aufwand für die Meldepflichtigen möglichst geringgehalten wird. Eine zentrale Meldeplattform, welche den Meldepflichtigen gleichzeitig die Erfüllung verschiedener Meldepflichten erlaubt, wäre daher unbedingt erstrebenswert. Eine solche Koordination kann nur auf Bundesebene erfolgen und muss in der Verantwortung des NCSC liegen.

Auf Gesetzesebene ist aktuell nur die direkte Meldung von betroffenen Organisationen explizit vorgesehen. Als Multisektor-CERT erwarten wir, dass Meldungen z.B. auch über ein gemeinsames Sektor-CERT erfolgen können. Da dies auf Gesetzesebene nicht explizit ausgeschlossen wird, gehen wir davon aus, dass betroffene Organisationen die Freiheit haben, sich entsprechend zu organisieren. Wir denken dabei primär an die Hochschulen gemäss Art. 74b lit. a E-ISG, welche alle bei SWITCH-CERT organisiert sind und in einem durch SWITCH-CERT kanalisierten Meldewesen Optimierungspotential sehen können. Das gilt ebenso für die weiteren Sektor-CERT, insbesondere SWITCH-CERT für Banken und SWITCH-CERT für Energie.

Widerhandlungen gegen Verfügungen des NCSC (Art. 74i E-ISG)

Wie im Erläuterungsbericht statuiert wird, ist der Informationsaustausch zwischen kritischen Infrastrukturen und dem Bund in der Schweiz gut etabliert. Diese kooperative Basis soll weiter ausgebaut werden. Der negative Anreiz in Form einer Busse steht diesem Ansatz entgegen. Zudem erachten wir eine persönliche Strafbarkeit von natürlichen Personen als kontraproduktiv, da es Personen abschreckt, im Bereich der Cyber-Sicherheit Verantwortung zu übernehmen. Aus den genannten Gründen regen wir daher an, Art. 74i E-ISG ersatzlos zu streichen. Alternativ wird angeregt, eine strafrechtliche Sanktionierung der Betriebe anstelle der natürlichen Personen vorzusehen, zumal meist ein Organisationsversagen und kein Versagen von einzelnen Personen vorliegen wird.

Wir bedanken uns für die Möglichkeit einer Stellungnahme und hoffen, dass unsere Anliegen soweit als möglich berücksichtigt werden können.

Wir würden es sodann begrüssen, wenn auch zur Verordnung eine Vernehmlassung eröffnet würde.

Bei Fragen stehen wir Ihnen jederzeit gerne zur Verfügung.

Freundliche Grüsse

Martin Leuthold
Head of Data, Security & Network

Angelo Marchetta
Legal Counsel

Par mail uniquement à ncsc@gs-efd.admin.ch
DFF
Département fédéral des finances
Case postale
3003 Berne

Systèmes d'information et télécommunications
Guillaume Meyer
Directeur

T. +41 22 308 33 75
F. +41 22 308 35 45
Meyer.G@tpg.ch

Grand-Lancy, le 13 avril 2022

Notre référence : GM/Dch/#693'164

Prise de position concernant la consultation relative à l'introduction d'une obligation de signaler les cyberattaques et à la modification de la LSI

Madame, Monsieur

Avant toutes choses, nous vous remercions vivement de nous avoir offert la possibilité, dans le cadre de la présente consultation de l'avant-projet mis en ligne, de nous exprimer et de vous communiquer notre point de vue.

Les Transports publics genevois (ci-après les tpg) saluent l'idée du Conseil fédéral de permettre aux cantons et aux communes de combler une lacune dans le dispositif de la cybersécurité et de permettre une détection précoce des attaques contre les entreprises et autorités suisses. Dans ce sens, les tpg saisissent parfaitement le besoin de cette loi permettant au Centre national pour la cybersécurité (NSCS) d'avoir une vue d'ensemble sur les cyberattaques en Suisse.

Nous vous prions de bien vouloir trouver ci-dessous, nos commentaires sur certains articles du projet :

1. Définitions (art. 5, let.d)

Nous sommes d'avis qu'il faudrait modifier dans les définitions, la lettre d de l'article 5 dans sa formulation : « et pouvant avoir pour » par « et ayant pour ». La différence est mineure dans la forme mais majeure sur le fond. La définition proposée (inspirée du NIST US) inclut les événements ayant des conséquences avérées ou potentielles. Cette définition inclut donc l'ensemble des tentatives d'exploitation de vulnérabilités observées tous les jours sur les services informatiques exposés sur Internet, dès lors qu'elles comportent une charge utile pertinente et potentiellement impactante pour la cible. Cette définition est certes pertinente pour des entités informatiques chargées de leur traitement technique (auquel s'adresse le NIST US), car permettant de prévenir les risques de

potentiels incidents, mais toutefois dangereuse au sens juridique, car sans autre ajustement cette définition pourrait aboutir à une obligation de signalement sur des événements si fréquents qu'elle aboutirait à un bruit extrêmement contre-productif pour le NCSC d'une part, et d'un coût disproportionné pour les organisations dans le périmètre d'application de la loi.

Si la volonté est de ne pas modifier la définition du mot « cyberincident », alors il faudrait soit revoir le principe de l'obligation de signalement pour permettre l'omission de ce type d'événement trop fréquent (mais pas dans le sens de l'objectif recherché par ce projet de modification LSI) ; soit ajouter à l'art. 74c une exception relative à la singularité de l'événement à signaler, afin d'exclure de l'obligation de signalement l'ensemble des événements de sécurité observés fréquemment dans le « bruit de fond » des observations habituelles.

Observons sur ce sujet que les pays européens ont très bien compris le problème, puisqu'ils définissent le cyberincident dans la directive 2016/1148 instaurant l'obligation de signalement pour les opérateurs d'infrastructures critiques ainsi (art. 4 al. 7) : « tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information », éliminant ainsi automatiquement tous les événements de sécurité observés tous les jours en « bruits de fond » ayant un potentiel de dommage mais neutralisés par les mesures de sécurité en place.

2. Domaines : Fabricants de matériel et de logiciels informatiques (art. 74b, let.s)

Nous sommes favorables au remplacement de la formule « cryptage » par « chiffrement » car l'anglicisme « cryptage », malheureusement souvent employé de manière erronée (y compris chez les informaticiens), correspond en français à une opération de cryptographie absurde consistant à chiffrer sans avoir connaissance de la clef de chiffrement – se référer aux références de cryptographie et mathématiques pour plus de détails.

Nous restons bien évidemment à disposition pour des renseignements et échanges complémentaires. Vous pouvez sans autre contacter M. Denis Chiaradonna, juriste tpg, chiaradonna.d@tpg.ch

Nous vous réitérons nos remerciements pour cette consultation et restons à votre disposition pour tout complément d'information.

Veuillez agréer, Madame, Monsieur, nos salutations distinguées.

Denis Berdoz
Directeur général

Guillaume Meyer
Directeur SIT

Trust Valley
EPFL Innovation Park, Bâtiment C
CH-1015 Lausanne

Département fédéral des finances DFF
Conseiller fédéral Ueli Maurer
Bundesgasse 3, 3003 Berne

Envoi par courriel à : ncsc@gs-efd.admin.ch

Lausanne, 14 Avril 2022

Objet: Obligation pour les exploitants d'infrastructures critiques de signaler les cyberattaques. Prise de position sur la loi fédérale sur la sécurité de l'information au niveau fédéral

Monsieur le Conseiller Fédéral, Mesdames et Messieurs,

Nous vous remercions de nous donner l'occasion de nous prononcer sur les modifications de la loi fédérale sur la sécurité de l'information au sein de la Confédération. La Trust Valley saisit cette opportunité dans le cadre de la procédure de consultation sur l'avant-projet de modification de la loi sur la sécurité de l'information relatif à l'introduction d'une obligation de signaler les cyberattaques graves contre les infrastructures critiques.

Présentation de la Trust Valley
La Trust Valley est un pôle d'excellence lémanique dans la confiance numérique et la cybersécurité pour fédérer un écosystème unique dont un des objectifs est de mettre en place des alliances stratégiques pour des actions concrètes. C'est une alliance pour l'excellence, portée par de multiples acteurs publics, privés et académiques et plus de cinquante partenaires.

Un soutien de principe à l'obligation de signalement des cyberattaques sur les infrastructures critiques
Cet avant-projet crée les bases légales nécessaires à l'introduction de l'obligation de signalement et définit les tâches du Centre National pour la Cybersécurité (NCSC), qu'il institue comme centrale de signalement des cyberattaques.

En effet, cette obligation d'annonce va concerner et va impacter l'ensemble des acteurs de la Trust Valley, à savoir :

- Les cantons de Vaud et Genève, leurs communes et institutions publiques : police, sauvetage, hôpitaux, … (une réponse séparée des Cantons a été produite)
- Les hautes écoles (une réponse séparée de l'EPFL a été produite)
- Les industriels actifs dans les secteurs de fabrication de matériel et de logiciel informatiques dont les produits sont utilisés par des infrastructures critiques.

Ainsi, la Trust Valley apporte un soutien de principe à l'obligation de signalement des cyberattaques sur les infrastructures critiques.

Précisions sur les entités soumises à l'obligation de déclarer
La Trust Valley a noté l'ambition d'inclure dans ce devoir d'annonce les services postaux, les agences de presse, les sociétés de radiodiffusion et télévision, les transports, banques, assurances et sociétés d'approvisionnement en biens d'usage quotidien indispensable. Selon le type de déclaration, cela va occasionner une charge de travail non négligeable à prendre

en compte. La Trust Valley, avec son modèle public-privé-académique (PPP) pourrait avoir un rôle dans cette approche commune vis-à-vis du NCSC pour adresser la mise en application d'une telle évolution de la loi sur la sécurité de l'information. Toutefois la Trust Valley estime que le projet de loi a besoin de précisions pour que la réglementation soit supportable par les hautes écoles et les entreprises notamment en référence à l'extension aux entreprises de la chaîne d'approvisionnement qui selon notre compréhension indique justement que l'économie est largement concernée et ce pour leur permettre d'atteindre les objectifs attendus. En effet, le projet de loi mentionne à l'art. 74b P-LIS une multitude de branches concernées. L'art. 74b, let. s, P-LISG, en particulier, cite les exploitants de matériels et de logiciels dont les produits sont utilisés par des infrastructures critiques. Le champ d'application de l'obligation de notification est ainsi étendu ce qui laisse supposer que les personnes concernées sont encore plus nombreuses que ne le montre l'énumération 74b P-LIS. Dans le cas actuel, la liste précise sur les entités soumises à l'obligation de déclarer convient d'être éclairci ainsi que l'objet de cette déclaration et les phases qui seront mises en place selon les entités concernées.

Une étroite collaboration

La Trust Valley salue l'effort de la Confédération de vouloir formaliser les devoirs vis-à-vis de ces infrastructures critiques, la volonté de fourniture de solutions techniques et d'accompagnement dans la gestion des cyberincidents. La Trust Valley est convaincue que les cybermenaces ne peuvent être endiguées efficacement que dans le cadre d'un partenariat entre l'Etat, l'économie et les académiques. Les dispositions pénales qui peuvent conduire à la responsabilité pénale personnelle des responsables doivent être totalement rejetées. De plus, les membres de la Trust Valley savent par expérience que la restauration et l'assainissement des infrastructures peuvent prendre plusieurs semaines en cas de cyberincident majeur. C'est pourquoi la Trust Valley préconise une étroite collaboration entre le NCSC et les fournisseurs du secteur privé pour soutenir l'exploitant en cas de cyberincident. Cela garantit la capacité supplémentaire nécessaire en cas de crise. Afin de garantir la confidentialité et la rapidité d'action, un certain nombre d'acteurs du domaine pourrait être partie prenante en tant que fournisseurs du secteur privé. Les fournisseurs du secteur privé pourraient remplir certains critères et se soumettre à une certification afin de pouvoir être sollicités par le NCSC. Le NCSC pourrait ainsi faire appel rapidement et efficacement à un nombre prédéfini de fournisseurs de cybersécurité et la confidentialité des données sensibles serait garantie.

Nous vous remercions de l'attention que vous portez à nos préoccupations et restons à votre disposition pour toute information complémentaire.

Meilleures Salutations,

Lennig Pedron
Directrice de la Trust Valley

UNIVERSITÄT
BERN

Verwaltungsdirektion
Abteilung Informatikdienste

Bern, 08. März 2022

Vernehmlassung zur Einführung einer Meldepflicht für Cyberangriffe – Stellungnahme der Universität Bern

Management Summary

Der Bund plant, im Rahmen einer Revision des Informationssicherheitsgesetzes (ISG) eine Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen einzuführen.

- Die Informatikdienste der Universität Bern begrüssen die geplante Meldepflicht
- Das geplante System für die elektronische Meldung von Cyberangriffen sollte einfach ausgestaltet, gleichzeitig aber gegen Missbrauch gesichert sein
- Die inhaltlichen und zeitlichen Erwartungen bzgl. der Pflicht zu ergänzenden Auskünften sollten präzisiert werden
- Das NCSC sollte Betreiberinnen kritischer Infrastrukturen über gemeldete Cyberangriffe informieren (mindestens Betreiberinnen innerhalb desselben Tätigkeitsbereichs, aus welchem der Cyberangriff gemeldet wurde).

Ausgangslage

Der Bund plant, im Rahmen einer Revision des Informationssicherheitsgesetzes (ISG) eine Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen einzuführen. Am 12. Januar 2022 hat der Bundesrat dazu die Vernehmlassung eröffnet, welche bis zum 14. April 2022 dauert.

Die Vorlage sieht insbesondere vor, dass Betreiberinnen von kritischen Infrastrukturen dem NCSC (Nationales Zentrum für Cybersicherheit) Cyberangriffe nach deren Entdeckung so rasch als möglich melden müssen, damit das NCSC Angriffsmuster frühzeitig erkennen, mögliche Betroffene warnen und ihnen geeignete Präventions- und Abwehrmassnahmen empfehlen kann. Die Meldung soll u.a. elektronisch möglich sein und muss Informationen zur betroffenen kritischen Infrastruktur, zur Art und Ausführung des Cyberangriffs, zu seinen Auswirkungen und zum geplanten weiteren Vorgehen der Betreiberin der kritischen Infrastruktur enthalten. Bei Verletzung der Melde- und Auskunftspflicht sieht die Vorlage einen mehrstufigen Eskalationsprozess (Information, Bussandrohung, Busse) vor.

swissuniversities ist zwar nicht offiziell zur Teilnahme an der Vernehmlassung eingeladen worden, möchte aber dennoch Stellung nehmen, da gemäss der Vorlage auch die Hochschulen zu den kritischen Infrastrukturen gehören. Die IT-Leitenden der Schweizer Universitäten haben sich dahingehend untereinander abgestimmt, dass jede/r für sich eine eigenständige Einschätzung der Vorlage zu Handen der jeweiligen Hochschulleitung abgibt.

Einschätzung

Die Informatikdienste der Universität Bern begrüssen die geplante Meldepflicht, da sie zur Transparenz bzgl. der Cyber-Bedrohungslage in der Schweiz beiträgt.

Dr. Cord-Ulrich Fündeling
Leiter Informatikdienste
Hochschulstrasse 6
3012 Bern
Schweiz

Telefon +41 31 684 38 00
cord.fuendeling@unibe.ch
www.id.unibe.ch

Was die konkrete Umsetzung angeht, gilt es, die Meldung eines Cyberangriffs so einfach wie möglich und den Aufwand dafür gering zu halten. In diesem Sinne ist die gem. Art. 74f geplante Bereitstellung eines sicheren Systems für die elektronische Meldung von Cyberangriffen zu begrüssen. Zu klären ist, wie dabei das Erfordernis der Einfachheit des Meldesystems mit dem Risiko von dessen Missbrauch durch Unbefugte in Einklang gebracht werden wird.

Hinsichtlich der geplanten Auskunftspflicht gem. Art. 74g ist unklar, welche inhaltlichen und zeitlichen Erwartungen mit dieser Pflicht verbunden sind, und welcher Aufwand dadurch entsprechend für die Betreiberinnen kritischer Infrastrukturen generiert werden wird. In den die Vorlage ergänzenden Erläuterungen wird präzisiert, dass die Auskunftspflicht auf Informationen beschränkt ist, die benötigt werden, um das Angriffsmuster und die Angriffsmethode eines gemeldeten Cyberangriffs identifizieren (Frühwarnung) und damit Auswirkungen des Cyberangriffs auf andere kritische Infrastrukturen verhindern zu können. Die Vorlage sollte in diesem Sinne präzisiert werden. Gerade in der Situation der Abwehr eines Cyberangriffs dürfen die Ressourcen der Betreiberinnen kritischer Infrastrukturen nicht über Gebühr durch Auskunftsbegehren beansprucht werden.

Bezüglich der Aufgaben des NCSC gem. Art. 74 wäre es im Sinne einer partnerschaftlichen Zusammenarbeit wünschenswert, wenn das NCSC die Betreiberinnen kritischer Infrastrukturen über gemeldete Cyberangriffe auf andere Betreiberinnen kritischer Infrastrukturen informieren würde (bzw. mindestens Betreiberinnen aus dem jeweils gleichen Tätigkeitsbereich gem. Art. 74b).

UNIVERSITÉ DE GENÈVE
FACULTÉ DE DROIT
Centre de droit du numérique

Digital Law Center
www.digitallawcenter.ch

Département fédéral des finances DFF
Monsieur Ueli Maurer
Conseiller fédéral
Bundesgasse 3
3003 Berne

ncsc@gs-efd.admin.ch

Genève, le 14 avril 2022

Procédure de consultation relative à l'obligation de signaler les cyberattaques pour les infrastructures critiques – prise de position

Monsieur le Conseiller fédéral, Mesdames, Messieurs,

Nous avons pris connaissance du projet cité en titre, qui a retenu toute notre attention et vous adressons, par la présente, notre position quant à celui-ci.

Nous approuvons de manière générale le projet qui nous semble être un moyen approprié afin d'atteindre le but visé, dans la mesure où les cyberattaques sont devenues l'une des principales menaces pour la sécurité et l'économie suisse. Leur signalement permettrait une meilleure vue d'ensemble de la situation en Suisse, d'aider les victimes à gérer les cyberattaques et d'avertir à temps les autres exploitants d'infrastructures critiques. Nous nous permettons les 4 commentaires suivants :

1. Délai

Nous estimons qu'il serait **utile de préciser le délai de signalement** prévu pour l'instant de façon indéterminée (*cf.* art. 74a al. 1 P-LSI « *le plus rapidement possible après leur découverte* »), sans remettre en cause la possibilité d'un signalement en deux temps (*cf.* art. 74e al. 2 P-LSI).

Nous comprenons que les entreprises ignorent souvent à quel point l'attaque est grave et ce qui s'est passé précisément (AP-LSI, p. 21), ce qui pourrait expliquer pourquoi ne pas préciser de délai. Or, la précision d'un délai renforcerait la sécurité juridique, d'autant que la possibilité d'un signalement en deux temps permet précisément de tenir compte du fait que les entreprises ignorent souvent l'étendue de l'attaque. A titre de comparaison, les obligations FINMA sont plus précises, puisqu'il est prévu aussi un signalement en deux temps mais de façon précise, soit une obligation de signalement dans les 24h après une première évaluation de la gravité de la cyberattaque critique et, dans les 72 heures, via la plate-forme de saisie (Communication FINMA sur la surveillance 05/2020, p. 4). Les réglementations étrangères sont souvent aussi plus précises. Par exemple, en Europe il est prévu un délai de 24h à 72h suivant l'impact/la gravité de l'incident et un délai de 1 mois pour soumettre le rapport final (art. 20 directive SRI). Aux Etats-Unis, il est prévu un délai de 72h et, exceptionnellement, 24h en cas de paiement d'une rançon (CISA sec. 2242(a)(1)(A).

2. Définition de cyberattaques et cyberincidents

Nous estimons qu'il serait **utile de préciser la définition de cyberattaques et cyberincidents** (*cf.* art. 5 let. d et e), soit que ces événements peuvent aussi survenir et être qualifiés comme tels **même en l'absence de toute violation de la sécurité des données** ou d'autres dispositions légales ou réglementaires.

Cette précision renforcerait selon nous la sécurité juridique. A titre de comparaison, la LPD du 25 septembre 2020 (nLPD) (et le RGPD) prévoit une obligation d'annonce en cas de "*violation de la sécurité des données entraînant vraisemblablement un risque élevé*" (art. 24 nLPD ; art. 33 RGPD), ce qui rend incertain d'annoncer en cas de cyberincident malgré le respect de toutes les mesures de sécurité des données.

3. Liste des secteurs

Nous saluons le fait que la liste des secteurs critiques est large et inclut des secteurs, tels que les hautes écoles, contrairement à d'autres législations, notamment européennes. Nous partageons votre avis selon lequel les **hautes écoles sont d'une grande importance** pour la formation et l'économie en Suisse, leurs activités de recherche en particulier, constituant un moteur de l'innovation, ce qui fait ainsi d'elles une cible privilégiée pour les cyberattaques, comme nous le montre encore l'actualité récente.

Nous considérons en revanche important **d'assouplir la possibilité de mettre à jour et de préciser** les secteurs critiques, par exemple à travers une autorité délégatrice et/ou un mécanisme souple d'adaptation. A titre de comparaison, aux Etats-Unis, les 16 secteurs d'infrastructures identifiés comme critiques peuvent être définis plus clairement par la Cybersecurity and Infrastructure Security Agency (CISA sec. 2242(b)(1)). En Chine, les entités concernées sont aussi identifiées et précisées par les régulateurs sectoriels (Règlement sur la protection de la sécurité des infrastructures d'information critiques, art. 8 ss).

4. Mesures complémentaires

Nous tenons finalement à souligner le fait que l'objet de cette consultation, notamment l'introduction de l'obligation de **signalement des cyberattaques, ne représente qu'un pan de la lutte** contre la cybercriminalité. Il est également important que tout un travail en amont soit fait, par des mesures de sensibilisation, de prévention et de formation des acteurs des milieux concernés ainsi que de la population de manière générale, au niveau fédéral et cantonal.

A la lumière de ce qui précède, nous réitérons notre soutien au projet.

Nous vous remercions de l'attention que pour porterez à la présente et vous prions de croire, Monsieur le Conseiller fédéral, à l'expression de notre haute considération.

* * *

Prof. Yaniv Benhamou
Prof. Jacques de Werra
Mme Louise Wang

Pour le Digital Law Center