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
Bundesamt für Kommunikation
Zukunftstrasse 44
Postfach 256
2501 Biel

16. März 2022

Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten); Vernehmlassung

Sehr geehrte Damen und Herren

Die Kantonsregierungen wurden mit Schreiben vom 3. Dezember 2021 über die Änderung der Verordnung über Fernmeldedienste (FDV) (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten) zur Vernehmlassung eingeladen. Der Regierungsrat des Kantons Aargau bedankt sich für die Möglichkeit einer Stellungnahme und hat folgende Bemerkungen:

1. Heute werden über 70 % aller Notrufe über Mobiltelefone abgewickelt. Betriebsunterbrüche in den Mobilnetzen sind dadurch sensitiv. Sie haben direkte Auswirkungen auf das Notrufwesen und die Ereignisbewältigung durch die Blaulichtorganisationen, ebenso auf die Betreiber kritischer Infrastrukturen (KI), die auf einen zuverlässigen und sicheren Betrieb der neuen Generation von Mobilfunknetzen angewiesen sind. Aus diesen Gründen sollte dargelegt werden, wie die Blaulichtorganisationen und die KI in die Alarmierungs- und Meldeprozesse einbezogen werden.

2. Cyberangriffe haben nicht nur hohe wirtschaftliche Auswirkungen, sondern gefährden auch die Sicherheit des Landes, da sie zu Ausfällen oder fehlerhaftem Funktionieren von KI führen können. Aus diesem Grund haben Anbieter von Internetzugängen diese und Adressierungselemente zu blockieren, von denen eine Gefährdung für KI ausgehen. Nur so kann die Sicherheit der angebotenen Dienstleistungen gewährleistet werden. Der Regierungsrat regt daher an, die Einführung einer Pflicht zur selektiven Blockierung von Internetzugängen oder Adressierungselementen, von denen eine Gefährdung im Zusammenhang mit KI ausgeht, zu prüfen.

3. Um die Bearbeitung und Verteilung der eingegangenen Störungsmeldungen zu verbessern, sieht die revidierte Verordnung vor, die Rolle der Nationalen Alarmzentrale (NAZ) zu stärken, da sie gemäss erläuterndem Bericht eine sichere Informatikinfrastruktur und einen 24-Stunden-Betrieb unterhält (Art. 96 FDV). Cyberangriffe dagegen sind einer zu schaffenden Meldestelle gemäss Art. 96b FDV zu melden. Darüber hinaus bestehen jedoch weitere Organisationen, die sich um Cyberangriffe kümmern. Daher sollen beispielsweise auch das National Cyber Security Center (NCSC), die Melde- und Analysestelle Informationssicherung (MELANI) sowie die kantonalen Notrufzentralen eingebunden werden. In diesem Zusammenhang ist von Bedeutung, dass nicht ausschliesslich das Bundesamt für Kommunikation (BAKOM) von der NAZ über die gemeldeten Störungen informiert wird.

Das BAKOM wird gebeten, die Rollen sämtlicher Stellen im Gesamtprozess von Meldung und Alarmierung im Cyber-Bereich im erläuternden Bericht detailliert aufzuführen. Dabei ist die Schaffung eines Single Point of Contact grundsätzlich anzustreben, damit die Krisenbewältigung erleichtert wird.

4. Im bisherigen Art. 96 FDV müssen Anbieterinnen von Fernmeldediensten Störungen im Betrieb ihrer Fernmeldeanlagen und Fernmeldedienste dem BAKOM unverzüglich melden, wenn eine relevante Anzahl Kundinnen und Kunden betroffen ist. Aktuell gehen die Notruforganisationen davon aus, dass Störungen relevant sind, welche voraussichtlich mehr als 15 Minuten dauern und wovon mindestens 1'000 Kundinnen und Kunden betroffen sind. Neu sollen nur noch Störungen gemeldet werden, die potenziell mindestens 30'000 Kundinnen und Kunden betreffen. Die Zahl von 30'000 potenziell betroffenen Kundinnen und Kunden entspricht dem Äquivalent einer Schweizer Stadt mittlerer Grösse. Eine Störung, die den gesamten Kanton Appenzell Innerhoden mit seinen 16'300 Einwohnerinnen und Einwohnern betreffen würde, würde gemäss vorliegendem Entwurf somit nicht gemeldet. Zudem ist es wichtig, dass die Dauer von Störungen abgeschätzt werden kann. Aus diesen Gründen ist der Regierungsrat der Meinung, dass die bisherige Regelung beibehalten werden sollte. Dies bedeutet, dass weiterhin Störungen gemeldet werden, die mehr als 15 Minuten dauern und mindestens 1'000 Kundinnen und Kunden betreffen.
5. Bereits heute setzen einige Staaten ihre Cybermittel regelmässig im Sinne eines "Kalten-Cyber-Kriegs" ein. Der Krieg in der Ukraine belegt eindrücklich, dass Panzerangriffen und Luftschlägen der massive Einsatz von Cybermitteln vorausgeht sowie Cyberattacken die klassischen militärischen Operationen begleiten. Davon dürften auch Staaten, die an den eigentlichen Kampfhandlungen nicht beteiligt sind, betroffen sein. Die Armee hat in den vergangenen Jahren Schritte unternommen, um sich auf ein solches Szenario vorzubereiten. So ist die Führungsunterstützungsbasis (FUB) im Bereich Verteidigung für Aktionsplanung, Lageverfolgung, Ereignisbewältigung und Ausbildung der Mitarbeiterinnen und Mitarbeiter und Angehörigen der Armee (AdA) im Cyber-Raum verantwortlich. Mit der Weiterentwicklung der Armee wurde zur Unterstützung der Berufsorganisation der FUB eine Cyber-Kompanie gebildet. Ab 2022 werden sämtliche Cyber-Formationen der Schweizer Armee in das neu gegründete Cyber-Bataillon 42 integriert. Die Rolle der Armee im Zusammenhang mit der Bedrohung KI durch Cyber-Angriffe von staatlicher Seite und deren Abwehr ist daher in der revidierten Verordnung über Fernmeldedienste zu berücksichtigen und ihre Verwendung zu beschreiben.

Wir danken Ihnen für die Berücksichtigung unserer Vernehmlassung.

Freundliche Grüsse

Im Namen des Regierungsrats

Alex Hürzeler
Landammann

Joana Filippi
Staatsschreiberin

Kopie
- tp-secretariat@bakom.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
tp-secretariat@bakom.admin.ch

Appenzell, 3. März 2022

Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten)
Stellungnahme Kanton Appenzell I.Rh.

Sehr geehrte Damen und Herren

Mit Schreiben vom 3. Dezember 2021 haben Sie uns die Vernehmlassungsunterlagen zur Änderung der Verordnung über Fernmeldedienste hinsichtlich der Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten zukommen lassen.

Die Standeskommission hat die Unterlagen geprüft. Sie unterstützt die Vorlage im Grundsatz. Die volkswirtschaftlichen Kosten von Cyberangriffen sind hoch und stiegen in den letzten Jahren stark an. Es erscheint daher richtig, wirksame Massnahmen zur Verhinderung von Cyberangriffen und zur Sicherheit von 5G-Netzen umzusetzen. Der Einbezug der diversen Schweizer Internet Access Provider (IAP) ist dabei zentral, damit die Anzahl von Cyberangriffen markant gesenkt werden kann.

Wir stellen folgende **Anträge**:

1. Es sei darzulegen, wie die Blaulichtorganisationen und die kritischen Infrastrukturen (KI) in die Alarmierungs- und Meldeprozesse einbezogen werden.

   Heute werden über 70% aller Notrufe über Mobiltelefone abgewickelt. Betriebsunterbrüche in den Mobilnetzen sind deshalb sensitiv. Sie haben direkte Auswirkungen auf das Notrufwesen und die Ereignisbewältigung durch die Blaulichtorganisationen, ebenso wie auf die Betreiberinnen und Betreiber von kritischen Infrastrukturen, die auf einen zuverlässigen und sicheren Betrieb der neuen Generation von Mobilfunknetzen angewiesen sind.

2. Es sei eine Pflicht zur selektiven Blockierung von Internetzugängen oder Adressierungselementen einzuführen, von denen eine Gefährdung im Zusammenhang mit kritischen Infrastrukturen ausgeht.

   Cyberangriffe haben nicht nur hohe wirtschaftliche Auswirkungen, sondern sie gefährden auch die Sicherheit des Landes, da sie zu Ausfällen oder fehlerhaftem Funktionieren von kritischen Infrastrukturen führen können. Aus diesem Grund haben Anbieterinnen und Anbieter von Internetzugängen diese und Adressierungselemente zu blockieren, von denen eine Gefährdung für kritische Infrastrukturen ausgeht. Nur so kann die Sicherheit der ange-

botenen Dienstleistungen gewährleistet werden. Die Anbieterinnen und Anbieter sollen indessen nicht nur berechtigt sein, Internetzugänge oder Adressierungselemente zu blockieren, sie sollen im Falle von kritischen Infrastrukturen dazu verpflichtet sein.

3. Die Rollen der einzelnen Akteurinnen und Akteure sowie Stellen seien detailliert zu beschreiben.

   Um die Bearbeitung und Verteilung der eingegangenen Störungsmeldungen zu verbessern, sieht die revidierte Verordnung vor, die Rolle der Nationalen Alarmzentrale (NAZ) zu stärken, da sie eine sichere Informatikinfrastruktur und einen 24-Stunden-Betrieb unterhält (Art. 96 n FDV). Cyberangriffe dagegen sind einer zu schaffenden Meldestelle gemäss Art. 96b zu melden. Darüber hinaus bestehen weitere Organisationen, die sich um Cyberangriffe kümmern. So sind beispielsweise auch das National Cyber Security Center (NCSC), die Melde- und Analysestelle Informationssicherung (MELANI) sowie die kantonalen Notrufzentralen einzubinden. In diesem Zusammenhang kann es nicht sein, dass ausschliesslich das Bundesamt für Kommunikation von der Nationalen Alarmzentrale über die gemeldeten Störungen informiert wird. Die Rollen sämtlicher Stellen im Gesamtprozess von Meldung und Alarmierung im Cyber-Bereich sind im erläuternden Bericht detailliert aufzuführen. Dabei ist die Schaffung eines Single Point of Contact (SPOC) grundsätzlich anzustreben, weil damit die Krisenbewältigung erleichtert wird.

4. Die Anbieterinnen und Anbieter seien zu verpflichten, unverzüglich Störungen im Betrieb ihrer Fernmeldeanlagen und Fernmeldedienste zu melden, wenn 1’000 Kundinnen und Kunden potentiell von einem Ausfall betroffen sind, der länger als 15 Minuten dauert.

   Die Zahl von 30'000 potenziell betroffenen Kundinnen und Kunden entspricht dem Äquivalent einer Schweizer Stadt mittlerer Grösse. Eine Störung, die den gesamten Kanton Appenzell I.Rh. mit seinen 16'300 Einwohnerinnen und Einwohnern betreffen würde, würde gemäss vorliegendem Entwurf somit nicht gemeldet. Zudem ist es wichtig, dass die Dauer von Störungen abgeschätzt werden kann. Aktuell gehen die Notruforganisationen davon aus, dass Störungen relevant sind, welche voraussichtlich mehr als 15 Minuten dauern und mindestens 1’000 Kundinnen und Kunden davon betroffen sind.

   Die Schwelle von 30'000 potenziell betroffenen Kundinnen und Kunden stammt aus den technischen und administrativen Vorschriften betreffend die Meldung von Netzstörungen des Bundesamts für Kommunikation vom 31. Januar 2014 i.V.m. Anhang 1 Ziff. 8 der Verordnung über Fernmeldedienste und Adressierungselemente (SR 784.101.113). Der Schwellenwert hat damit bisher keine demokratisch legitimierte Grundlage und ist im Zuge der Aufnahme in die Verordnung über Fernmeldedienste zu senken.

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

Im Auftrage von Landammann und Standeskommission
Der Ratschreiber-Stv.:

Michael Bührer

Zur Kenntnis an:
- Volkswirtschaftsdepartement Appenzell I.Rh., Marktgasse 2, 9050 Appenzell
- Justiz-, Polizei- und Militärdepartement Appenzell I.Rh., Marktgasse 10d, 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

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

Eidg. Departement für Umwelt, Verkehr,
Energie und Kommunikation

per E-Mail an:
tp-secretariat@bakom.admin.ch

(PDF- und Wordversion)

Herisau, 4. März 2022

Eidg. Vernehmlassung; Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und Fernmeldeinfrastrukturen und –diensten); Stellungnahme des Regierungsrates von Appenzell Ausserrhoden

Sehr geehrte Damen und Herren

Mit Schreiben vom 3. Dezember 2021 unterbreitet das Eidg. Departement für Umwelt, Verkehr, Energie und Kommunikation einen Änderungsentwurf der Verordnung über Fernmeldedienste (FDV) bis zum 18. März 2022 zur Vernehmlassung.

Der Regierungsrat von Appenzell Ausserrhoden nimmt dazu wie folgt Stellung:

Er begrüsst den vorliegenden Entwurf im Grundsatz. Begrüsst wird insbesondere, dass mit der Vorlage die unbefugte Manipulation von Fernmeldeanlagen durch fernmeldetechnische Übertragungen bekämpft wird. Insbesondere Massnahmen zur Schaffung eines Mindestniveaus an 5G-Netzwerksicherheit in der Schweiz erachtet der Regierungsrat als dringend erforderlich. Ein hohes Sicherheitsniveau beim Betrieb von Mobilfunknetzen der neusten Generation ist ebenso sicherzustellen.

Der Regierungsrat beantragt folgende Ergänzungen:

- Es ist darzulegen, wie die Blaulichtorganisationen und die kritischen Infrastrukturen (KI) in die Alarmierungs- und Meldeprozesse einbezogen werden. Da heute über 70 % aller Notrufe über Mobiltelefone abgewickelt werden, sind Betriebsunterbrüche in den Mobilnetzen aus diesen Gründen sensitiv. Sie haben direkte Auswirkungen auf das Notrufwesen und die Ereignisbewältigung durch die Blaulichtorganisationen, ebenso wie auf die Betreiber von KI, die auf einen zuverlässigen und sicheren Betrieb der neuen Generation von Mobilfunknetzen angewiesen sind.
- Einführung einer Pflicht zur selektiven Blockierung von Internetzugängen oder Adressierungselementen, von denen eine Gefährdung im Zusammenhang mit KI ausgeht. Cyberangriffe haben nicht nur hohe wirtschaftliche Auswirkungen, sondern sie gefährden auch die Sicherheit des Landes, da sie zu Ausfällen oder fehlerhaftem Funktionieren von KI führen können. Aus diesem Grund haben Anbieter von Internetzugängen diese und Adressierungselemente zu blockieren, von denen eine Gefährdung für KI ausgeht. Nur so kann die Sicherheit der angebotenen Dienstleistungen gewährleistet werden.

- Die Rollen der einzelnen Akteure und Stellen sind detailliert zu beschreiben. Um die Bearbeitung und Verteilung der eingegangenen Störungsmeldungen zu verbessern, sieht die revidierte Verordnung vor, die Rolle der Nationalen Alarmzentrale (NAZ) zu stärken, da sie eine sichere Informatikinfrastruktur und einen 24-Stunden-Betrieb unterhält (Art. 96). Cyberangriffe dagegen sind einer zu schaffenden Meldestelle gemäss Art. 96b zu melden. Darüber hinaus bestehen weitere Organisationen, die sich um Cyberangriffe kümmern. So sind beispielsweise auch das National Cyber Security Center (NCSC), die Melde- und Analysestelle Informationssicherung (MELANI) sowie die kantonalen Notrufzentralen einzubinden. In diesem Zusammenhang kann es nicht sein, dass ausschliesslich das BAKOM von der NAZ über die gemeldeten Störungen informiert wird. Die Rollen sämtlicher Stellen im Gesamtprozess von Meldung und Alarmierung im Bereich Cyber sind im Erläuternden Bericht detailliert aufzuführen. Dabei ist die Schaffung eines Single Point of Contact (SPOC) grundsätzlich anzustreben, weil damit die Krisenbewältigung erleichtert wird.
- Die Anbieter werden verpflichtet, unverzüglich Störungen im Betrieb ihrer Fernmeldeanlagen und Fernmeldedienste zu melden, wenn 1000 Kunden, die potentiell von einem Ausfall betroffen sind, der länger als 15 Minuten dauert. Die Zahl von 30'000 potenziell betroffenen Kunden entspricht dem Äquivalent einer Schweizer Stadt mittlerer Grösse. Eine Störung, die z. B. den gesamten Kanton Appenzell Innerhoden mit seinen 16'300 Einwohnern betreffen würde, würde gemäss vorliegendem Entwurf somit nicht gemeldet. Zudem ist es wichtig, dass die Dauer von Störungen abgeschätzt werden kann. Aktuell gehen die Notruforganisationen davon aus, dass Störungen relevant sind, welche voraussichtlich mehr als 15 Minuten dauern und mindestens 1000 Kundinnen und Kunden davon betroffen sind.
- Im Zusammenhang mit der Bedrohung kritischer Infrastrukturen durch Cyber-Angriffe von staatlicher Seite und deren Abwehr sind die Aufgaben der Armee aufzuzeigen und in die FDV zu integrieren. Die klassische Machtpolitik erlebt seit einigen Jahren eine Renaissance. Bereits heute setzen einige Staaten ihre Cybermittel regelmässig im Sinne eines "Kalten" Cyber-Krieges ein. Im Falle eines bewaffneten Konflikts in Europa ist mit einer breiten Verwendung dieser Mittel zu rechnen. Davon dürften auch Staaten, die an den eigentlichen Kampfhandlungen nicht beteiligt sind, betroffen sein. Die Armee hat in den vergangenen Jahren Schritte unternommen, sich auf ein solches Szenario vorzubereiten. So ist die Führungsunterstützungsbasis (FUB) im Bereich Verteidigung für Aktionsplanung, Lageverfolgung, Ereignisbewältigung und Ausbildung der Mitarbeitenden und Angehörigen der Armee im Cyber-Raum verantwortlich. Mit der Weiterentwicklung der Armee (WEA) wurde zur Unterstützung der Berufsorganisation der FUB eine Cyber-Kompanie gebildet. Ab 2022 werden sämtliche Cyber Formationen der Schweizer Armee in das neu gegründete Cyber Bataillon 42 integriert. Die Rolle der Armee ist in der revidierten FDV zu berücksichtigen und ihre Verwendung zu beschreiben.

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

Frau Bundesrätin
Simonetta Sommaruga
Eidgenössisches Departement
für Umwelt, Verkehr, Energie und Kommunikation UVEK
Bundeshaus Nord
3003 Bern

RRB Nr.:	242/2022	9. März 2022
Direktion:	Wirtschafts-, Energie- und Umweltdirektion	
Klassifizierung:	Nicht klassifiziert	

Änderung der Verordnung über Fernmeldedienst (FDV): Vernehmlassung
Stellungnahme des Kantons Bern

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Der Regierungsrat dankt Ihnen für die Möglichkeit zur Stellungnahme. Er unterstützt grundsätzlich die Änderung der Verordnung über Fernmeldedienste (FDV).

Mit dem gewählten zweistufigen Vorgehen wird einerseits die unbefugte Manipulation von 5G-Fernmeldeanlagen bekämpft und es wird ein definiertes Sicherheitsniveau eingeführt. Andererseits wird in einer zweiten Etappe ein weiteres Massnahmenpaket erarbeitet, bei welchem die Härtung im Sinne der Stromversorgungssicherheit im Fokus stehen wird. Beide Vorhaben sind aus unserer Sicht wichtig und geeignet, um die Verfügbarkeit der immer wichtiger werdenden Mobilkommunikation der 5G Technologie sicherzustellen.

Wir weisen an dieser Stelle ausdrücklich darauf hin, dass sich die mobile Kommunikation der Blaulicht-und Sicherheitsorganisationen, mangels Vorhandenseins eines Systems für die mobile breitbandige Sicherheitskommunikation (MSK), in wesentlichen Aspekten auf die Mobilfunksysteme der heutigen Anbieter stützen. Aktuell werden über 70% aller Notrufe über Mobiltelefone abgewickelt. Betriebsunterbrüche in den Mobilnetzen sind dadurch sensitiv und haben direkte Auswirkungen auf das Notrufwesen und der Ereignisbewältigung der Blaulichtorganisationen.

Eine weitere Anspruchsgruppe sind die Betreiber von kritischen Infrastrukturen, welche aufgrund ihrer Kritikalität auf einen zuverlässigen und sicheren Betrieb der neuen Generation von Mobilfunknetzen angewiesen sind.

Wir regen an, dass die Alarmierungs- und Meldeprozesse detailliert zu beschreiben sind. Um die Bearbeitung und Verteilung der eingegangenen Störungsmeldungen zu verbessern, sieht die revidierte Verordnung vor, die Rolle der Nationalen Alarmzentrale (NAZ) zu stärken. Der Empfang von Meldungen über Cyberangriffe soll zu einer Kernaufgabe der NAZ werden, da sie eine sichere Informatikinfrastruktur betreibt und einen 24-Stunden-Betrieb sicherstellt. Die

Schaffung eines Single Point of Contact (SPOC) ist zielführend, weil damit die Krisenbewältigung erleichtert wird. Trotzdem befassen sich national noch weitere Organisationen mit der Abwehr von Cyberangriffen. Es ist aus unserer Sicht nicht sinnvoll, dass ausschliesslich das BAKOM von der NAZ über die gemeldeten Störungen informiert wird. So sind beispielsweise auch das National Cyber Security Center (NCSC), die Melde- und Analysestelle Informationssicherung (MELANI) sowie die kantonalen Notrufzentralen von Polizei, Feuerwehr und Sanität einzubinden. Deren Rolle im Gesamtprozess von Meldung- und Alarmierung im Bereich Cyber sind im Erläuternden Bericht aufzuführen.

Im Zusammenhang mit der Bedrohung kritischer Infrastrukturen durch Cyber-Angriffe von staatlicher Seite und deren Abwehr sind die Aufgaben der Armee aufzuzeigen und in die FDV zu integrieren. Die klassische Machtpolitik erlebt seit einigen Jahren eine Renaissance. Bereits heute setzen einige Staaten ihre Cybermittel regelmässig im Sinne eines "Kalten" Cyber-Krieges ein. Im Falle eines bewaffneten Konflikts in Europa ist mit einer breiten Verwendung dieser Mittel zu rechnen. Davon dürften auch Staaten, die an den eigentlichen Kampfhandlungen nicht beteiligt sind, betroffen sein. Die Armee hat in den vergangenen Jahren Schritte unternommen, sich auf ein solches Szenario vorzubereiten. So ist die Führungsunterstützungsbasis (FUB) im Bereich Verteidigung für Aktionsplanung, Lageverfolgung, Ereignisbewältigung und Ausbildung der Mitarbeitenden und AdA im Cyber-Raum verantwortlich. Mit der Weiterentwicklung der Armee (WEA) wurde zur Unterstützung der Berufsorganisation der FUB eine Cyber-Kompanie gebildet. Ab 2022 werden sämtliche Cyber Formationen der Schweizer Armee in das neu gegründete Cyber Bataillon 42 integriert. Die Rolle der Armee ist in der revidierten FDV zu berücksichtigen und ihre Verwendung zu beschreiben.

Der sofortigen Information an die kantonalen Notrufzentralen von Polizei, Feuerwehr und Sanität ist ein hohes Gewicht beizumessen. Nur sie können die Risiken von Beeinträchtigungen abschätzen und Sofortmassnahmen anordnen (bspw. die Umsetzung von Notfalltreffpunkten o.ä.). Entsprechend sind die Informationsprozesse in der FDV zu verankern.

Ergänzungs- und Anpassungsanträge

Wir beantragen die folgenden Anpassungen oder Anträge zum vorliegenden Entwurf der FDV:

Art. 96

Störungen im Mobilfunkbereich haben direkte Auswirkungen. So sind unter Umständen Notrufnummern nicht mehr erreichbar, oder die Einsatzkräfte von Polizei, Rettungsdienst und Feuerwehr sind aufgrund der nicht mehr vorhandenen Datenübertragungsmöglichkeiten in ihrem Handeln beeinträchtigt. In vielen Kantonen wurden inzwischen Notfalltreffpunkte installiert, welche bei Störungen im Kommunikationsbereich besetzt werden können. Dies setzt jedoch voraus, dass die kantonalen Notrufzentralen sofort und unverzüglich über Ausfälle, bereits im niederschwelligen Bereich, informiert werden. Die im Art. 96 formulierte Grösse von 30'000 Kundinnen und Kunden, welche von einem Ausfall betroffen sind, ist deutlich zu hoch gewählt. Zudem ist es wichtig, dass die Dauer von Störungen abgeschätzt werden kann. Aktuell gehen die Notruforganisationen davon aus, dass Störungen relevant sind, welche voraussichtlich mehr als 15 Minuten dauern und mindestens 1'000 Kundinnen und Kunden davon betroffen sind.

Eine Information an die NAZ, NCSC, MELANI, sowie nachgelagert an das BAKOM sind für die Nachbereitung der Störung wichtig. Die erwähnten Organe haben jedoch nur einen sekundären Einfluss auf die Behebung einer Störung oder der Bewältigung einer entsprechenden Lage.

Dies obliegt primär den kantonalen Behörden, welche entsprechende Massnahmen sofort umsetzen können. Es ist unklar, warum die Anzahl der betroffenen Kundinnen und Kunden nun auf Stufe FDV und nicht mehr in der TAV geregelt werden soll.

Antrag 1:

a) Die von einer potentiellen Störung betroffene Anzahl von Kundinnen und Kunden ist von 30'000 auf 1'000 Kundinnen oder Kunden zu senken, welche potentiell von einem Ausfall grösser als 15 Minuten betroffen sind.
b) In jedem Fall haben die Anbieterinnen von Fernmeldediensten ab einer Störungsgrösse von 1'000 Kundinnen und Kunden (+15 Minuten) die zuständigen kantonalen Notrufzentralen von Polizei, Sanität und Feuerwehr (112, 117, 118, 144) zu informieren, bevor die Meldungen an die NAZ (i.S. eines SPOC) oder weitere Organe abgesetzt werden.
c) Die Anzahl der betroffenen Kundinnen und Kunden soll weiterhin in der TAV geregelt werden und nicht auf Stufe FDV.

Art. 96a

Im Abs. 1 wird spezifisch und abschliessend von DDoS-Angriffen gesprochen. Aufgrund des technologischen schnellen Wandels ist es möglich, dass es zukünftig andere Arten von Angriffen geben kann, welche es zu berücksichtigen gilt.

Im Abs. 3 werden die Anbieterinnen von Internetzugängen berechtigt, Internetzugänge und Adressierungselemente, welche die Systeme beeinträchtigen, zu sperren oder einzuschränken. Sie dürfen die Massnahmen aufrechterhalten, solange die Bedrohung anhält. Diese kann zu Unterbrüchen im Bereich der Notrufe führen und damit zu potentiellen Risiken für hilfsbedürftige Personen.

Antrag 2:

a) Abs. 1: Es soll im erwähnten Absatz nicht abschliessend von DDoS-Angriffen gesprochen werden, sondern die DDoS-Angriffe sind als Beispiel o.ä. aufzuführen.
b) Abs. 1: Die Details von potentiellen Angriffsmechanismen sollen nicht abschliessend in der FDV geregelt werden, sondern in den technisch- administrativen Vorschriften (TAV). Dies ermöglicht ein adäquates Handeln und ein relativ niederschwelliges Anpassen der zu berücksichtigenden Regelungen.
c) Abs. 3: Die Einschränkungen im Bedrohungsfall sollen sehr selektiv erfolgen und nur im Ausnahmefall dazu führen, dass keine Notrufnummern mehr über die betroffenen Anschlüsse gewählt werden können.
d) Abs. 3: Sind durch die Einschränkungen potenziell mehr als 1'000 Kundinnen und Kunden über die prognostizierte Dauer von mehr als 15 Minuten betroffen, sind die betroffenen kantonalen Notrufzentralen über die Einschränkungen zu informieren.

Art. 96f

Es wird im Abs. 2 definiert, dass der Betrieb der Netzwerkbetriebszentren und deren Sicherheitsbetriebszentren nebst der Schweiz im Europäischen Wirtschaftsraum und im Vereinigten Königreich stattfinden kann. Ist eine Betreiberin primär ausserhalb der Schweiz tätig, ist der operative und der juristische Durchgriff im Ereignisfall schwierig bis unmöglich. Nebst der schwierigen Erreichbarkeit im Ausland, ist auch die Priorisierung von Massnahmen und Ressourcen deutlich erschwert. Es wird angeregt, dass eine ständige Vertretung in der Schweiz gefordert wird.

Antrag 3:

a) Ein ständiger Firmensitz oder ein ständiger Ableger in der Schweiz ist unumgänglich und soll entsprechend in der FDV verankert werden.
b) Insbesondere beim Betrieb von sicherheitskritischen Fernmeldeanlagen ist dem ständigen Firmensitz oder einer ständigen Vertretung in der Schweiz ein hohes Gewicht beizumessen.

Ergänzende Rückmeldungen

In der vorliegenden Revision der FDV soll auch die Problematik des kostenpflichtigen Zuganges zur SOS-DB (NotDB) und der Nutzung von DLWL für die Notrufzentralen (PSAP) abschliessend geregelt werden. Dieses Bedürfnis wurde schon lange von Seiten der Notrufzentralen kommuniziert und soll nun einfliessen.

Antrag 4:

1) Kostenlose Nutzung des DLWL für alle Notrufzentralen.
2) Kostenlose Nutzung der SOS-DB für alle Notrufzentralen.

Die Vorlage sollte innerhalb des Bundes mit den anderen Vorlagen zum Thema Cybersicherheit abgestimmt werden. So hat der Bund vor kurzem die Vernehmlassung zur Vorlage «Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe» eröffnet. Es wird aus der aktuellen Vorlage jedoch nicht ersichtlich, wie die beiden Vorlagen hinsichtlich des Themas «Cyber-kriminalität» zusammenhängen und aufeinander abgestimmt wurden.

Antrag 5:
Die aktuelle Vorlage ist mit anderen Vorlagen zum Thema Cybersicherheit abzustimmen und soll entsprechend in der Vorlage erwähnt werden.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen.

Freundliche Grüsse

Im Namen des Regierungsrates

Beatrice Simon
Regierungspräsidentin

Christoph Auer
Staatsschreiber

Verteiler
– Wirtschafts- Energie- und Umweltdirektion
– Bau- und Verkehrsdirektion
– Sicherheitsdirektion

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

BASEL LANDSCHAFT
REGIERUNGSRAT

Regierungsrat, Rathausstrasse 2, 4410 Liestal

Per E-Mail an:
tp-secretariat@bakom.admin.ch

Liestal, 15. Februar 2022

Stellungnahme zur Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit Schreiben vom 3. Dezember 2021 haben Sie den Regierungsrat des Kantons Basel-Landschaft eingeladen, im Rahmen der Vernehmlassung zur Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten) Stellung zu nehmen. Gerne lassen wir Ihnen diese Stellungnahme hiermit zukommen.

Der Regierungsrat begrüsst grundsätzlich den vorliegenden Entwurf der Verordnung über Fernmeldedienste (FDV). Mit dem vorliegenden Entwurf wird die unbefugte Manipulation von Fernmeldeanlagen durch fernmeldetechnische Übertragungen bekämpft. Insbesondere Massnahmen zur Schaffung eines Mindestniveaus an 5G-Netzwerksicherheit in der Schweiz erachtet der Regierungsrat als dringend erforderlich. Ein hohes Sicherheitsniveau beim Betrieb von Mobilfunknetzen der neusten Generation ist ebenso sicherzustellen.

Der Regierungsrat beantragt ausserdem folgende Ergänzungen:

1. Es ist darzulegen, wie die Blaulichtorganisationen und die Kritischen Infrastrukturen (KI) in die Alarmierungs- und Meldeprozesse einbezogen werden.

Begründung: Heute werden über 70 Prozent aller Notrufe über Mobiltelefone abgewickelt. Betriebsunterbrüche in den Mobilnetzen sind dadurch sensitiv. Sie haben direkte Auswirkungen auf das Notrufwesen und die Ereignisbewältigung durch die Blaulichtorganisationen, ebenso wie auf die Betreiber von KI, die auf einen zuverlässigen und sicheren Betrieb der neuen Generation von Mobilfunknetzen angewiesen sind.

2. Einführung einer Pflicht zur selektiven Blockierung von Internetzugängen oder Adressierungselementen, von denen eine Gefährdung im Zusammenhang mit KI ausgeht.

Begründung: Cyberangriffe haben nicht nur hohe wirtschaftliche Auswirkungen, sondern sie gefährden auch die Sicherheit des Landes, da sie zu Ausfällen oder fehlerhaftem Funktionieren von

KI führen können. Aus diesem Grund haben Anbieterinnen von Internetzugängen diese und Adressierungselemente zu blockieren, von denen eine Gefährdung für KI ausgeht. Nur so kann die Sicherheit der angebotenen Dienstleistungen gewährleistet werden.

3. Die Rollen der einzelnen Akteure und Stellen sind detailliert zu beschreiben.

Begründung: Um die Bearbeitung und Verteilung der eingegangenen Störungsmeldungen zu verbessern, sieht die revidierte Verordnung vor, die Rolle der Nationalen Alarmzentrale (NAZ) zu stärken, da sie eine sichere Informatikinfrastruktur und einen 24-Stunden-Betrieb unterhält (Art. 96). Cyberangriffe dagegen sind einer zu schaffenden Meldestelle gemäss Art. 96 b zu melden. Darüber hinaus bestehen weitere Organisationen, die sich um Cyberangriffe kümmern. So sind beispielsweise auch das National Cyber Security Center (NCSC), die Melde- und Analysestelle Informationssicherung (MELANI) sowie die kantonalen Notrufzentralen einzubinden. In diesem Zusammenhang kann es nicht sein, dass ausschliesslich das BAKOM von der NAZ über die gemeldeten Störungen informiert wird. Die Rollen sämtlicher Stellen im Gesamtprozess von Meldung und Alarmierung im Bereich Cyber sind im Erläuternden Bericht detailliert aufzuführen. Dabei ist die Schaffung eines Single Point of Contact (SPOC) grundsätzlich anzustreben, weil damit die Krisenbewältigung erleichtert wird.

4. Die Anbieterinnen sind zu verpflichten, Störungen im Betrieb ihrer Fernmeldeanlagen und Fernmeldedienste unverzüglich zu melden, wenn diese länger als 15 Minuten dauern und mindestens 1000 Kunden betreffen.

Begründung: Die in Art. 96 vorgesehene Zahl von 30'000 potenziell betroffenen Kunden entspricht dem Äquivalent einer Schweizer Stadt mittlerer Grösse. Eine Störung, die den gesamten Kanton Appenzell Innerhoden mit seinen 16'300 Einwohnern betreffen würde, würde gemäss vorliegendem Entwurf somit nicht gemeldet. Zudem ist es wichtig, dass die Dauer von Störungen abgeschätzt werden kann. Aktuell gehen die Notruforganisationen davon aus, dass Störungen relevant sind, welche voraussichtlich mehr als 15 Minuten dauern und mindestens 1000 Kundinnen und Kunden betreffen.

5. Im Zusammenhang mit der Bedrohung kritischer Infrastrukturen durch Cyber-Angriffe von staatlicher Seite und deren Abwehr sind die Aufgaben der Armee aufzuzeigen und in die FDV zu integrieren.

Begründung: Die klassische Machtpolitik erlebt seit einigen Jahren eine Renaissance. Bereits heute setzen einige Staaten ihre Cybermittel regelmässig im Sinne eines "Kalten" Cyber-Krieges ein. Im Falle eines bewaffneten Konflikts in Europa ist mit einer breiten Verwendung dieser Mittel zu rechnen. Davon dürften auch Staaten, die an den eigentlichen Kampfhandlungen nicht beteiligt sind, betroffen sein. Die Armee hat in den vergangenen Jahren Schritte unternommen, sich auf ein solches Szenario vorzubereiten. So ist die Führungsunterstützungsbasis (FUB) im Bereich Verteidigung für Aktionsplanung, Lageverfolgung, Ereignisbewältigung und Ausbildung der Mitarbeitenden und AdA im Cyber-Raum verantwortlich. Mit der Weiterentwicklung der Armee (WEA) wurde zur Unterstützung der Berufsorganisation der FUB eine Cyber-Kompanie gebildet. Ab 2022 werden sämtliche Cyber Formationen der Schweizer Armee in das neu gegründete Cyber Bataillon 42 integriert. Die Rolle der Armee ist in der revidierten FDV zu berücksichtigen und ihre Verwendung zu beschreiben.

6. Die Anbieterinnen sind zu verpflichten, den Kundinnen und Kunden bei der Behebung des kompromittierenden Systems Hilfe zur Selbsthilfe zu leisten bzw. diese zu instruieren.

Begründung: Gemäss Art. 96a Abs. 3 des Vorentwurfs (VE FDV) sind Internet Access Provider (IAP) berechtigt, Internetzugänge oder Adressierungselemente, die das ordnungsgemässe Funktionieren von Fernmeldeanlagen zu beeinträchtigen drohen, zu sperren oder deren Nutzung einzuschränken. Darüber hinaus haben sie ihre Kundinnen und Kunden, die Opfer unbefugter Manipulationen geworden sind oder werden könnten, unverzüglich über solche Sperrungen oder Einschränkungen zu informieren. Sie dürfen diese Massnahmen aufrechterhalten, solange die Bedrohung anhält. Diese Massnahme erscheint auf den ersten Blick effizient, da sie die Störung umgehend beseitigt. Im Endeffekt verlagert Art. 96 Abs. 3 VE FDV aber das Problem – und damit die Aufgabe – der Störungsbeseitigung auf den Endnutzer der kompromittierten Geräte und damit die Kunden der IAP. Diese werden mangels fachlichem Know-how in den wenigsten Fällen in der Lage sein, selbst die erforderlichen Massnahmen ergreifen zu können und ein System (meist ohne Back-ups) neu aufzusetzen. Zudem wird der Endbenutzer ohne Hilfe und Angaben zur zu beseitigenden Malware und zum infizierten System (mehrere Geräte sind im Internet der Dinge über einen WLAN-Router indirekt am Netz des IAP, z. B. Waschmaschine, Kühlschrank, Drucker, Staubsaugerroboter etc.) in den wenigsten Fällen zum Deblockieren des Anschlusses führen, da Massnahmen aufrechterhalten werden, solange die Bedrohung anhält.

7. Im Rahmen eines Sicherungselements sollten die Anbieterinnen verpflichtet werden, den Kundinnen und Kunden so rasch als möglich den Internetzugriff mittels Unterstützung wieder zu gewährleisten.

Begründung: Im Rahmen des im Entwurfes der Stellungnahme des Regierungsrates genannten Aufflammens der Machtpolitik ist zusätzlich zu beachten, dass sich das System des Art. 96 Abs. 3 VE FDV nicht gegen sich selbst richtet. Staatliche Akteure könnten durch eine gezielte Operation eine Vielzahl von Computersystemen in der Schweiz infizieren, deren Zugriff gestützt auf Art. 96 Abs. 3 FE FDV in der Folge blockiert würde. Als Konsequenz wäre die Kommunikation des Staates mit seinen Bürgern oder die Wirtschaft gezielt unterbunden bzw. destabilisiert.

Der Regierungsrat dankt Ihnen für die Gelegenheit zur Stellungnahme und für die Berücksichtigung unserer Anliegen.

Hochachtungsvoll

Thomas Weber
Regierungspräsident

Elisabeth Heer Dietrich
Landschreiberin

Regierungsrat des Kantons Basel-Stadt

Rathaus, Marktplatz 9
CH-4001 Basel

Tel: +41 61 267 80 54
Fax: +41 61 267 85 72
E-Mail: staatskanzlei@bs.ch
www.regierungsrat.bs.ch

Per E-Mail an:
tp-secretariat@bakom.admin.ch.

Basel, 22. Februar 2022

Regierungsratsbeschluss vom 22. Februar 2022

Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten)
Stellungnahme des Kantons Basel-Stadt

Sehr geehrte Frau Bundesrätin Sommaruga
Sehr geehrte Damen und Herren

Mit Schreiben vom 3. Dezember 2021 haben Sie uns eingeladen, zur Änderung der Verordnung über Fernmeldedienste Stellung zu nehmen. Wir danken für diese Gelegenheit und lassen Ihnen nachstehend unsere Bemerkungen zukommen.

Der Regierungsrat des Kantons Basel-Stadt begrüsst die mit der Änderung der Verordnung über Fernmeldedienste (FDV) vorgeschlagenen Massnahmen zur Erhöhung der Sicherheit der Fernmeldedienste. Die zunehmende Bedeutung des Internets und die Abhängigkeit der privaten Haushalte und Unternehmen von Fernmeldediensten erhöht die Bedeutung der Risikoprävention. Die neuen Regelungen tragen dazu bei, einen Mindeststandard an Sicherheitsvoraussetzungen zu etablieren und stärken damit das Vertrauen der Nutzerinnen und Nutzer in digitale Technologien.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen.

Freundliche Grüsse
Im Namen des Regierungsrates des Kantons Basel-Stadt

Beat Jans
Regierungspräsident

Barbara Schüpbach-Guggenbühl
Staatsschreiberin

ETAT DE FRIBOURG
STAAT FREIBURG

Conseil d'Etat 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 de l'environnement, des transports,
de l'énergie et de la communication DETEC
Madame la Conseillère fédérale
Simonetta Sommaruga
Palais fédéral Nord
3003 Berne

Courriel : tp-secretariat@bakom.admin.ch

Fribourg, le 8 mars 2022

2022-200
Modification de l'ordonnance sur les services de télécommunication (OST)

Madame la Conseillère fédérale,

Nous vous remercions de nous avoir associés à la consultation sur la modification de l'ordonnance sur les services de télécommunication (OST). Le projet précité a retenu toute notre attention.

Le Conseil d'Etat salue la présente modification de l'OST qui vise à donner au Conseil fédéral des compétences accrues dans le domaine de la sécurité de l'information et des infrastructures et services de télécommunications. Les objectifs définis, à savoir lutter de manière plus efficace contre la manipulation non autorisée d'installations de télécommunication et garantir un haut niveau de sécurité dans l'exploitation de la dernière génération de réseaux de télécommunication (5G), revêtent une importance essentielle dans un contexte où la cybercriminalité devient un phénomène de plus en plus récurrent. Du point de vue sécuritaire, il est important de noter que les infrastructures de télécommunication font partie des infrastructures stratégiques critiques dont la protection demande la plus grande attention. Une importance particulière doit être accordée à la sécurisation des réseaux de télécommunication de dernière génération car les nouvelles applications concerneront probablement aussi des domaines sensibles tels que la finance, l'énergie ou encore la santé.

Enfin, les enjeux évoqués dans le rapport explicatif sont importants du point de vue économique. Les entreprises et notamment les PME font de plus de plus l'objet de cyberattaques qui occasionnent souvent des dégâts importants, tant sur le plan financier que réputationnel. L'identification des scénarios de risque et l'adoption de mesures de sécurité appropriées sont donc fondamentales pour éviter des dommages économiques considérables à l'avenir.

Partant de ce constat, le Conseil d'Etat soutient les mesures proposées car elles améliorent globalement la sécurité des informations et des infrastructures en matière de télécommunication. Il estime en outre que l'orientation du projet de modifications vers les standards internationaux en la matière est pertinente. Néanmoins, le Conseil d'Etat souhaite apporter les commentaires généraux suivants concernant le projet de modification de l'OST :

> *Approche transversale* : La lutte contre la cybercriminalité et la gestion des risques en la matière requièrent une approche globale et transversale qui tient notamment compte des questions de sensibilisation et de formation. On constate en effet qu'une partie relativement importante des PME n'est pas consciente des risques élevés en matière de cybercriminalité. De ce point de vue, il aurait été souhaitable que le Conseil fédéral soumette une stratégie globale en matière de cybersécurité et que les modifications légales proposées s'y réfèrent chaque fois, dans une perspective transversale. Or le rapport explicatif concernant la révision de l'OTS ne mentionne pas la manière dont la proposition s'inscrit dans une telle stratégie, et quelles autres mesures sont prévues afin de gérer les risques importants de manière globale.

> *Approche subsidiaire* : Le Conseil d'Etat constate que les mesures proposées reposent exclusivement sur l'action privée et en partie volontaire des prestataires en matière de services de télécommunication. Si cette approche se justifie dans l'optique de la subsidiarité, elle ne tient pas entièrement compte de l'importance stratégique du secteur et de l'évolution rapide des menaces en matière de cybercriminalité. Pour cette raison, le Conseil d'Etat est de l'avis qu'une action étatique plus décidée doit être possible si les analyses de risques révèlent une telle nécessité. Dans cette perspective, les mesures introduites dans le cadre de la présente révision doivent faire l'objet d'une évaluation régulière et, le cas échéant, être complétées par des obligations plus formelles.

> *Positionnement de la place économique suisse* : Le Conseil d'Etat saisit l'occasion pour souligner que la cybersécurité constitue de plus en plus un facteur de compétitivité et d'attractivité économique. La Suisse dispose d'avantages concurrentiels importants en la matière en raison de sa stabilité et de son excellente réputation sur le plan international quant à la qualité de ses services et infrastructures. Il est donc important d'exploiter davantage ce potentiel économique et de renforcer le positionnement de la Suisse. A cet égard, l'élaboration d'une stratégie transversale qui prend également en compte les aspects de promotion économique aurait été souhaitable, comme indiqué plus haut.

En outre, nous appuyons les modifications particulières suivantes.

> *L'intégration des organismes feux bleus et des infrastructures critiques dans les processus d'alarme et d'annonce doit être précisée* : Aujourd'hui en effet, plus de 70% des appels d'urgence sont passés au moyen d'appareils téléphoniques cellulaires. Il s'ensuit que les coupures des réseaux de téléphonie mobile ont des conséquences importantes. Elles ont des implications directes pour les appels d'urgence et pour la maîtrise des événements par les organismes feux bleus, de même que pour les exploitants d'infrastructures critiques, qui doivent pouvoir compter sur des réseaux de téléphonie mobile de la dernière génération qui soient fiables et sûrs.

> *Les rôles des différents acteurs et organes doivent être décrits dans le détail* : Pour améliorer le traitement et la diffusion des signalements de perturbations reçus, l'ordonnance révisée prévoit de renforcer le rôle de la Centrale nationale d'alarme (CENAL), attendu qu'elle exploite une infrastructure informatique sûre, 24 heures sur 24 (art. 96). Par contre, les cyberattaques doivent être annoncées à un service de signalement (art. 96b) devant encore être créé. Il existe en outre d'autres organisations qui s'occupent des cyber-attaques. Ainsi, le « National Cyber Security Center (NCSC) », la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) et les centrales d'alarme cantonales, par exemple, doivent être intégrés dans les activités. Pour cette raison, il n'est pas possible que seul l'OFCOM soit informé par la CENAL sur les signalements de perturbations reçus. Les rôles de tous les services au sein du processus global d'annonce et d'alarme dans le domaine cybernétique doivent être présentés dans le détail dans le rapport explicatif. La création d'un point de contact unique (SPOC) doit fondamentalement être visée pour simplifier la gestion des crises.

> *Les fournisseurs sont tenus d'annoncer sans délai les perturbations de l'exploitation de leurs installations et services de télécommunication si 30'000 clients sont potentiellement concernés par une panne qui durera plus de 15 minutes* : Le nombre de 30'000 clients potentiellement touchés correspond à une ville suisse de taille moyenne. Par conséquent, selon le projet soumis, une perturbation touchant l'ensemble du canton d'Appenzell Rhodes-Intérieures, qui compte 16'300 habitants, ne serait pas annoncée. Il est par ailleurs important que la durée de la perturbation soit évaluée. Actuellement, les organisations d'appels d'urgence considèrent comme étant problématiques les perturbations dont on peut s'attendre à ce qu'elles toucheront pendant plus de 15 minutes au moins 1'000 clientes et clients.

> *Les tâches de l'armée en relation avec les menaces contre les infrastructures critiques par des cyberattaques provenant d'Etats, et concernant la défense contre ces attaques, doivent être présentées et intégrées dans l'OST* : Depuis quelques années, on assiste à une renaissance de la politique de puissance classique. Aujourd'hui déjà, certains Etats utilisent régulièrement leurs moyens cybernétiques dans le sens d'une « guerre froide cybernétique ». En cas de conflit armé en Europe, il faut s'attendre à une utilisation à grande échelle de ces moyens, et des Etats qui ne seraient pas directement concernés par le conflit seraient vraisemblablement aussi touchés. Ces dernières années, l'armée a pris des mesures pour se préparer à un tel scénario. Ainsi, dans le domaine Défense, la Base d'aide au commandement (BAC) est responsable de la planification des actions, du suivi de la situation, de la maîtrise des événements et de la formation du personnel ainsi que des militaires dans l'espace cybernétique. Avec la poursuite du développement de l'armée (DEVA), une cybercompagnie a été constituée pour appuyer l'organisation professionnelle de la BAC. A partir de 2022, toutes les cyberformations de l'armée suisse seront intégrées dans le nouveau cyberbataillon 42. L'OST révisée doit tenir compte du rôle de l'armée et décrire les tâches de cette dernière.

En vous remerciant de nous avoir consultés, nous vous prions d'agréer, Madame la Conseillère fédérale, l'expression de nos respectueuses salutations.

Au nom du Conseil d'Etat :

Olivier Curty, Président

Danielle Gagnaux-Morel, Chancelière d'Etat

Copie

—

à la Direction de l'économie, de l'emploi et de la formation professionnelle ;
à la Direction de la sécurité, de la justice et du sport ;
à la Chancellerie d'Etat.

Département fédéral de l'environnement,
des transports, de l'énergie et de la
communication (DETEC)
Madame Simonetta Sommaruga
Conseillère fédérale
Bundesplatz 3
3003 Berne

Concerne : révision de l'ordonnance sur les services de télécommunications - consultation fédérale

Madame la Conseillère fédérale,

Votre courrier du 3 décembre 2021 relatif à l'objet cité en titre nous est bien parvenu et a retenu toute notre attention.

Notre Conseil vous remercie de lui avoir soumis le projet de révision de l'ordonnance sur les services de télécommunications pour examen. Le sujet est particulièrement important pour les services de secours et de sécurité à la population du Canton, qui dépendent fortement de la disponibilité des infrastructures de téléphonie mobile pour exercer leur mission puisqu'une majorité des citoyens les contactent par ce biais.

Nous suggérons que les processus d'alarme et d'annonce soient décrits en détail. Afin d'améliorer le traitement et la répartition des annonces de perturbations reçues, l'ordonnance révisée prévoit de renforcer le rôle de la Centrale nationale d'alarme (CENAL). La réception des messages concernant les cyberattaques doit devenir une tâche essentielle de la CENAL, étant donné qu'elle entretient une infrastructure informatique sécurisée et qu'elle est opérationnelle 24 heures sur 24. La création d'un Single Point of Contact (SPOC) va dans le bon sens, car elle facilite la gestion des crises.

Toutefois, il existe d'autres organisations qui s'occupent des cyber-attaques. Il n'est pas acceptable que seul l'OFCOM soit informé par la CENAL des perturbations signalées. Il convient par exemple d'impliquer également les centrales d'appels d'urgence cantonales de la police, des pompiers et des services sanitaires. Leur rôle dans le processus global d'annonce et d'alarme dans le domaine cybernétique doit être mentionné dans le rapport explicatif.

Il convient d'accorder une grande importance à l'information immédiate aux centrales d'appels d'urgence cantonales de la police, des pompiers et des services sanitaires. Elles seules peuvent évaluer les risques d'atteinte et ordonner des mesures immédiates (p. ex. la mise en œuvre de points de rencontre d'urgence ou autres). En conséquence, les processus d'information doivent être ancrés dans l'OST.

Nous vous proposons les modifications suivantes :

Section 3, article 96 : remplacer 30'000 par 1'000 clients touchés au moins.

En effet, la population contacte les services d'urgence principalement par le réseau mobile et il est primordial que les centrales d'appels d'urgence du Canton soient averties rapidement des perturbations même partielles affectant celui-ci.

Section 4, article 96a : généraliser les mesures de sécurité techniques à mettre en place.

La mesure de contrôle anti-spoofing proposée ne permet pas d'éviter entièrement les attaques en déni de service distribué (DDOS), ces dernières n'étant qu'un exemple parmi d'autres de compromission possible des infrastructures de communication. De plus, les technologies et les failles de sécurité évoluent rapidement, et les menaces proviennent aussi des réseaux externes. Il faudrait donc plutôt demander aux opérateurs de mettre en place tous les moyens techniques raisonnables pour configurer leur réseau en respectant les bonnes pratiques de sécurité, notamment le contrôle des ressources d'adressage falsifiées (alinéa 1).

A l'article 96a alinéa 3 de l'Ordonnance révisée, les fournisseurs d'accès à Internet sont autorisés à bloquer ou à limiter les accès à Internet et les ressources d'adressage qui portent atteinte aux systèmes. Ils peuvent maintenir ces mesures tant que la menace persiste. Cela peut entraîner des interruptions dans le domaine des appels d'urgence et donc des risques potentiels pour les personnes ayant besoin d'aide. Les restrictions en cas de menace doivent être très sélectives et ne doivent conduire qu'exceptionnellement à ce qu'aucun numéro d'urgence ne puisse plus être composé via les raccordements concernés.

Section 5, article 96d : Appliquer l'ordonnance à toutes les actuelles et futures générations de téléphonie mobile.

Les cycles de vie techniques sont bien plus rapides que ceux des ordonnances fédérales. La cinquième génération mentionnée va être utilisée pour une durée de temps limitée et ne devrait pas être évoquée.

Par ailleurs, le processus de communication découlant des modifications proposées doit être optimisé pour faire en sorte que les organisations locales soient averties au plus tôt des dérangements. Les mesures de blocage liées à la sécurité ne doivent si possible pas empêcher les appels vers les numéros d'urgence à trois chiffres.

Article 96f de l'Ordonnance révisée
Il est défini à l'alinéa 2 que les concessionnaires de radiocommunication mobile peuvent exploiter leurs centres d'opération de réseau et leurs centres de gestion de la sécurité en Suisse, dans l'Espace économique européen et au Royaume-Uni. Si un exploitant opère principalement en dehors de la Suisse, le recours opérationnel et juridique en cas d'événement est difficile, voire impossible. Outre la difficulté d'accès à l'étranger, la priorisation des mesures et des ressources est également nettement plus difficile. Il est suggéré d'exiger une représentation permanente en Suisse.

Proposition :
a) Un siège permanent de l'entreprise ou une antenne permanente en Suisse est indispensable et doit être ancré en conséquence dans l'OST.
b) Il convient d'accorder une grande importance au siège permanent de l'entreprise ou à une représentation permanente en Suisse, en particulier lors de l'exploitation d'installations de télécommunication critiques pour la sécurité.

La présente révision de l'OST doit également régler définitivement la problématique de l'accès payant à la base de données d'urgence (SOS-DB / NotDB) et de l'utilisation de

l'acheminement dynamique des appels d'urgence (DLWL) pour les centrales d'appels d'urgence (PSAP). Ce besoin a été communiqué depuis longtemps par les centrales d'appels d'urgence et il est également mentionné dans notre courrier du 9 mars dernier relatif aux adaptations des dispositions du service universel et doit maintenant être pris en compte.

Nous vous prions de croire, Madame la Conseillère fédérale, à l'assurance de notre haute considération.

AU NOM DU CONSEIL D'ÉTAT

La chancelière : Le président :

Michèle Righetti Serge Dal Busco

Copie à (Word et PDF) : tp-secretariat@bakom.admin.ch

kanton glarus

Telefon 055 646 68 00
E-Mail: sicherheitjustiz@gl.ch
www.gl.ch

Sicherheit und Justiz
Postgasse 29
8750 Glarus

Eidgenössisches Departement für
Umwelt, Verkehr, Energie und Kommunikation UVEK
3003 Bern

Glarus, 18. März 2022
Unsere Ref: 2021-275

Vernehmlassung i. S. Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten)

Hochgeachtete Frau Bundesrätin
Sehr geehrte Damen und Herren

Das Eidgenössische Departement für Umwelt, Verkehr, Energie und Kommunikation gab uns in eingangs genannter Angelegenheit die Möglichkeit zur Stellungnahme. Dafür danken wir und lassen uns gerne wie folgt vernehmen:

Mit dem vorliegenden Entwurf der revidierten Verordnung über Fernmeldedienste (FDV) wird die unbefugte Manipulation von Fernmeldeanlagen durch fernmeldetechnische Übertragungen bekämpft. Insbesondere Massnahmen zur Schaffung eines Mindestniveaus an 5G-Netzwerksicherheit in der Schweiz erachten wir als dringend erforderlich.

In der Vorlage ist noch darzulegen, wie die Blaulichtorganisationen und die Kritischen Infrastrukturen (KI) in die Alarmierungs- und Meldeprozesse einbezogen werden. Heute werden über 70% aller Notrufe über Mobiltelefone abgewickelt. Betriebsunterbrüche in den Mobilnetzen sind dadurch sensitiv. Sie haben direkte Auswirkungen auf das Notrufwesen und die Ereignisbewältigung durch die Blaulichtorganisationen, ebenso wie auf die Betreiber von KI, die auf einen zuverlässigen und sicheren Betrieb der neuen Generation von Mobilfunknetzen angewiesen sind.

Eingeführt werden soll auch eine Pflicht zur selektiven Blockierung von Internetzugängen oder Adressierungselementen, von denen eine Gefährdung im Zusammenhang mit KI ausgeht. Cyberangriffe haben nicht nur hohe wirtschaftliche Auswirkungen, sondern sie gefährden auch die Sicherheit des Landes, da sie zu Ausfällen oder fehlerhaftem Funktionieren von KI führen können. Aus diesem Grund haben Anbieter von Internetzugängen diese und Adressierungselemente zu blockieren, von denen eine Gefährdung für KI ausgeht. Nur so kann die Sicherheit der angebotenen Dienstleistungen gewährleistet werden.

Die Rollen der einzelnen Akteure und Stellen sind zudem detailliert zu beschreiben. Um die Bearbeitung und Verteilung der eingegangenen Störungsmeldungen zu verbessern, sieht die revidierte Verordnung vor, die Rolle der Nationalen Alarmzentrale (NAZ) zu stärken, da sie eine sichere Informatikinfrastruktur und einen 24-Stunden-Betrieb unterhält (Art. 96). Cyberangriffe dagegen sind einer zu schaffenden Meldestelle gemäss Art. 96 b zu melden. Darüber hinaus bestehen weitere Organisationen, die sich um Cyberangriffe kümmern. So sind beispielsweise

auch das National Cyber Security Center (NCSC), die Melde- und Analysestelle Informationssicherung (MELANI) sowie die kantonalen Notrufzentralen einzubinden. In diesem Zusammenhang kann es nicht sein, dass ausschliesslich das BAKOM von der NAZ über die gemeldeten Störungen informiert wird. Die Rollen sämtlicher Stellen im Gesamtprozess von Meldung und Alarmierung im Bereich Cyber sind im Erläuternden Bericht detailliert aufzuführen.

Die Anbieter sollen des Weiteren unbedingt verpflichtet werden, unverzüglich Störungen im Betrieb ihrer Fernmeldeanlagen und Fernmeldedienste zu melden, wenn 1000 Kunden, die potentiell von einem Ausfall betroffen sind, der länger als 15 Minuten dauert. Im Zusammenhang mit der Bedrohung kritischer Infrastrukturen durch Cyber-Angriffe von staatlicher Seite und deren Abwehr sind die Aufgaben der Armee sodann aufzuzeigen und in die FDV zu integrieren.

Gemäss Art. 96f Abs. 2 kann der Betrieb der Netzwerkbetriebszentren und deren Sicherheitsbetriebszentren nebst der Schweiz im Europäischen Wirtschaftsraum und im Vereinigten Königreich stattfinden. Ist eine Betreiberin primär ausserhalb der Schweiz tätig, ist der operative und der juristische Durchgriff im Ereignisfall schwierig bis unmöglich. Nebst der schwierigen Erreichbarkeit im Ausland ist auch die Priorisierung von Massnahmen und Ressourcen deutlich erschwert. Ein ständiger Firmensitz oder ein ständiger Ableger in der Schweiz ist unumgänglich und soll entsprechend in der FDV verankert werden.

Bei dieser Gelegenheit soll schliesslich mit der vorliegenden Revision der FDV auch die schon länger pendente Forderung umgesetzt werden, den Zugang zur SOS-DB (NotDB), zukünftig LIS-Proxy, und die Nutzung der Dynamischen Leitweglenkung (DLWL) für die Notrufzentralen von der Kostenpflicht zu befreien.

Genehmigen Sie, hochgeachtete Frau Bundesrätin, sehr geehrte Damen und Herren, den Ausdruck unserer vorzüglichen Hochachtung.

Freundliche Grüsse

Dr. Andrea Bettiga
Regierungsrat

E-Mail an (PDF- und Word-Version):
- tp-secretariat@bakom.admin.ch

Die Regierung
des Kantons Graubünden

La Regenza
dal chantun Grischun

Il Governo
del Cantone dei Grigioni

Sitzung vom	Mitgeteilt den	Protokoll Nr.
15. März 2022	16. März 2022	245/2022

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
UVEK

Per E-Mail an: tp-secretariat@bakom.admin.ch (PDF- und Word-Version)

Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten)

Vernehmlassung

Sehr geehrte Frau Bundesrätin Sommaruga
Sehr geehrte Damen und Herren

Für die uns eingeräumte Möglichkeit zur Vernehmlassung in vorbezeichneter Angelegenheit danken wir Ihnen bestens.

1. Allgemeine Bemerkungen

Die vorgeschlagenen Änderungen der Verordnung über Fernmeldedienste (FDV) werden von der Regierung des Kantons Graubünden grundsätzlich begrüsst. Mit der revidierten FDV wird die unbefugte Manipulation von Fernmeldeanlagen durch fernmeldetechnische Übertragungen wirksam bekämpft und ein hohes Sicherheitsniveau beim Betrieb von Mobilfunknetzen der neuesten Generation (5G-Netze) geschaffen.

2. Bemerkungen zu Art. 96 Abs. 1

Gemäss Art. 96 Abs. 1 des Verordnungsentwurfs müssen die Anbieterinnen von Fernmeldediensten Störungen im Betrieb ihrer Fernmeldeanlagen und -dienste, welche potenziell mindestens 30 000 Kundinnen und Kunden betreffen, unverzüglich der nationalen Alarmzentrale melden.

Die Zahl von 30 000 potenziell betroffenen Kundinnen und Kunden entspricht dem Äquivalent einer Schweizer Stadt mittlerer Grösse. Eine Pflicht zur Störungsmeldung im Sinne der erwähnten Bestimmung bestünde beispielsweise für den Kanton Appenzell Innerhoden mit seinen 16 300 Einwohnern somit nicht. Aktuell gehen die Notruforganisationen davon aus, dass Störungen relevant sind, welche voraussichtlich mehr als 15 Minuten dauern und von welchen mindestens 1000 Kundinnen und Kunden oder eine Gemeinde bzw. Fraktionen betroffen sind.

Im Kanton Graubünden haben wir aktuell 48 Gemeinden, welche weniger als 1000 Einwohnerinnen und Einwohner haben und teilweise in sehr abgelegenen Tälern liegen. Ein Unterbruch bzw. eine Störung der Fernmeldeanlagen und -dienste kann, wenn ein Notruf (Notfallnummern 117/118/144) abgesetzt werden muss und dies nicht möglich ist, fatale Folgen haben. Ebenfalls wird der vom Amt für Militär und Zivilschutz Graubünden den Gemeinden angebotene SMS-Dienst immer mehr genutzt. Wenn z. B. in der Gemeinde Albula/Alvra mit dem Brienzer Rutsch auf dem Gebiet der Fraktion Brienz/Brinzauls (100 Einwohnerinnen und Einwohner) eine Störung im Betrieb der Fernmeldeanlagen und -dienste eintritt, können bei einem Ereignis keine Informationen mehr an die Bevölkerung abgegeben werden, was zu vermeiden ist.

Vor diesem Hintergrund beantragen wir die Statuierung einer Pflicht zur Meldung einer Störung, wenn mindestens 1000 Kundinnen und Kunden oder eine Gemeinde bzw. Fraktionen potenziell betroffen sind und die Störung länger als 15 Minuten dauert.

Für die Berücksichtigung unserer Anliegen danken wir Ihnen bestens.

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

Département fédéral de l'environnement,
des transports, de l'énergie et de la communication DETEC
Madame la Conseillère fédérale
Simonetta Sommaruga
Palais fédéral Nord
3003 Berne

Par email : tp-secretariat@bakom.admin.ch

Delémont, le 18 janvier 2022

Modification de l'ordonnance sur les services de télécommunication (sécurité des informations et des infrastructures et services de télécommunication) - ouverture de la procédure de consultation

Madame la Conseillère fédérale,

Le Gouvernement de la République et Canton du Jura accuse réception de votre courrier relatif à la procédure de consultation susmentionnée et il vous remercie de l'avoir consulté.

S'il peut être en accord sur le projet de manière générale, il formule toutefois le souhait que, lors de perturbations de l'exploitation de leurs installations et services de télécommunication, les fournisseurs soient tenus de les annoncer si 1'000 clients (et non 30'000 comme proposé) sont impactés par une panne d'une durée de plus de 10 minutes.

Il vous informe également que Monsieur Damien Rérat (032.420.67.23, damien.rerat@jura.ch), Commandant de la Police cantonale, est la personne de contact en cas d'éventuelles questions.

Tout en vous remerciant de prendre note de ce qui précède, le Gouvernement de la République et Canton du Jura vous présente, Madame la Conseillère fédérale, ses salutations les plus respectueuses.

AU NOM DU GOUVERNEMENT DE LA
RÉPUBLIQUE ET CANTON DU JURA

David Eray
Président

Jean-Baptiste Maître
Chancelier d'État

KANTON
LUZERN

Bau-, Umwelt- und Wirtschaftsdepartement
Bahnhofstrasse 15
Postfach 3768
6002 Luzern
Telefon 041 228 51 55
buwd@lu.ch
www.lu.ch

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK

per Email an
tp-secretariat@bakom.admin.ch
(Word und PDF)

Luzern, 8. März 2022

Protokoll-Nr.: 275

Änderung der Verordnung über Fernmeldedienste, Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten); Vernehmlassung

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit Schreiben vom 3. Dezember 2021 haben Sie die Kantone eingeladen, zur erwähnten Änderung der Verordnung über Fernmeldedienste Stellung zu nehmen.

Im Namen und Auftrag des Regierungsrats teile ich Ihnen mit, dass wir der beabsichtigten Änderung der Verordnung über Fernmeldedienste (FDV) im Grundsatz zustimmen. In Anlehnung an die Musterstellungnahme der Regierungskonferenz Militär, Zivilschutz und Feuerwehr (RK MZF) vom 13. Januar 2022 beantragen wir Ihnen allerdings die folgenden Ergänzungen:

- 70% der Notrufe erfolgen über Mobiltelefone, weshalb dargelegt werden muss, wie die Blaulichtorganisationen und die kritischen Infrastrukturen in die Alarmierungs- und Meldeprozesse einbezogen werden.
- Es ist eine Pflicht zur selektiven Blockierung von Internetzugängen oder Adressierungselementen vorzusehen, von denen eine Gefährdung im Zusammenhang mit kritischen Infrastrukturen ausgeht, zumal Cyberangriffe nebst wirtschaftlichen Auswirkungen auch die Sicherheit des Landes gefährden können.
- Die Rollen der einzelnen Akteure und Stellen sind detailliert zu beschreiben. Eine Information der Nationalen Alarmzentrale (NAZ) über gemeldete Störungen (ausschliesslich) an das BAKOM erscheint zu eng gefasst.
- Die Anbieter sind bereits dann zu verpflichten, Störungen im Betrieb ihrer Fernmeldeanlagen und Fernmeldedienste unverzüglich zu melden, wenn 1'000 Kunden potentiell von einem Ausfall betroffen sind, der länger als 15 Minuten dauert. Die in der Änderung der FDV vorgesehene Zahl von 30'000 potentiell betroffenen Kunden ist zu hoch angesetzt.
- Im Zusammenhang mit der Bedrohung kritischer Infrastrukturen durch Cyber-Angriffe von staatlicher Seite und deren Abwehr sind die Aufgaben der Armee aufzuzeigen und in die FDV zu integrieren.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme und Berücksichtigung unserer Anträge und Bemerkungen.

Freundliche Grüsse

Fabian Peter
Regierungsrat

mailto:tp-secretariat@bakom.admin.ch

Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC
Palais fédéral
3003 Berne

Révision de l’ordonnance sur les services de télécommunication (consultations des 3 et 10 décembre 2021 concernant la sécurité informatique et le service universel)

Madame la conseillère fédérale,

Le Conseil d'État de la République et Canton de Neuchâtel a pris connaissance des projets d’adaptation de l’ordonnance sur les services de télécommunication et vous remercie de l'avoir associé à la procédure de consultation.

Nous profitons ici de souligner l'importance d'un service de qualité permettant de garantir un accès stable aux technologies de communication, ceci aussi bien pour les citoyennes et les citoyens que pour les sociétés du tissu économique. La situation en marge de la pandémie nous a montré l’importance de ces services dans le cadre des mesures de télétravail qui vont très certainement être partiellement maintenues par les entreprises.

Nous soutenons la modification de l’ordonnance, tout en soulignant les 3 points qui suivent. Le premier concerne les aspects liés à la sécurité informatique et la consultation du 3 décembre 2021, alors que les deux autres concernent le service universel mis en consultation le 10 décembre 2021 :

1) En marge des modifications liées à la sécurité des informations et des infrastructures et services de télécommunication, les mesures visant à coordonner les efforts et obliger les opérateurs télécoms à mettre en œuvre des systèmes permettant de détecter, bloquer et communiquer les incidents liés à des adressages dangereux ou frauduleux paraît opportun.

2) L’adaptation des bandes passantes du service universel par la création d’une catégorie (80/8 Mbit/s) adaptée à une utilisation en télétravail et à l’accès aux moyens télévisuels usuels paraît pertinente. Ceci est important pour quelques régions à faible densité qui ne

bénéficient pas encore de réseaux câblés efficients. Nous avons néanmoins une remarque en marge de la tarification : nous trouverions pertinent que le tarif de l'offre publique soit un tarif maximal et que la société mandatée doive régulièrement réévaluer le prix de la prestation. Un tarif unique pour tous est aussi important dans un esprit de solidarité entre les villes et les régions dites périphériques.

3) Dans les régions à très faible densité, il existe des réticences à accepter l'installation d'antennes « 5g » qui permettent de délivrer les deux options de service universel. Des défraiements corrects des propriétaires qui jouent le jeu pourraient être envisagés. Contrairement aux systèmes satellitaires qui ont des limites en termes de volume de données, ces technologies terrestres sont économiquement viables et permettent une couverture de ces régions où le coût du câblage par la fibre optique est prohibitif.

En vous réitérant nos remerciements de nous avoir consultés sur ces dossiers et de la qualité de la documentation fournie, nous vous prions de croire, Madame la conseillère fédérale, à l'expression de notre haute considération.

Neuchâtel, le 23 mars 2022

Au nom du Conseil d'État :

Le président, L. FAVRE

La chancelière, S. DESPLAND

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
Eidg. Departement für Umwelt, Verkehr,
Energie und Kommunikation UVEK
Frau Bundesrätin Simonetta Sommaruga
Bundeshaus Nord
3003 Bern

Telefon 041 618 79 02
staatskanzlei@nw.ch
Stans, 8. März 2022

Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen). Stellungnahme

Sehr geehrte Frau Bundesrätin

Mit Schreiben vom 3. Dezember 2021 hat das Eidgenössische Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK die Kantone eingeladen, sich zur Änderung der Verordnung über Fernmeldedienste (FDV) im Hinblick auf die Umsetzung von Art. 48a FMG vernehmen zu lassen. Wir bedanken uns für diese Möglichkeit und lassen uns wie folgt vernehmen.

1 Im Allgemeinen

Mit dem vorliegenden Entwurf der revidierten FDV wird die unbefugte Manipulation von Fernmeldeanlagen durch fernmeldetechnische Übertragungen bekämpft. Insbesondere Massnahmen zur Schaffung eines Mindestniveaus an 5G-Netzwerksicherheit in der Schweiz wird als erforderlich erachtet. Ein hohes Sicherheitsniveau beim Betrieb von Mobilfunknetzen der neusten Generation ist ebenso sicherzustellen.

Der Kanton Nidwalden begrüsst deshalb den Entwurf der Verordnung über Fernmeldedienste.

2 Zur Vorlage

2.1

Heute werden über 70% aller Notrufe über Mobiltelefone abgewickelt. Betriebsunterbrüche in den Mobilnetzen sind dadurch sensitiv. Sie haben direkte Auswirkungen auf das Notrufwesen und die Ereignisbewältigung durch die Blaulichtorganisationen, ebenso wie auf die Betreiber von kritischen Infrastrukturen, die auf einen zuverlässigen und sicheren Betrieb der neuen Generation von Mobilfunknetzen angewiesen sind.

Antrag: Es ist darzulegen, wie die Blaulichtorganisationen und die kritischen Infrastrukturen in die Alarmierungs- und Meldeprozesse einbezogen werden.

2.2

Cyberangriffe haben nicht nur hohe wirtschaftliche Auswirkungen, sondern sie gefährden auch die Sicherheit des Landes, da sie zu Ausfällen oder fehlerhaftem Funktionieren von kritischen Infrastrukturen führen können. Aus diesem Grund haben Anbieter von Internetzugängen diese und Adressierungselemente zu blockieren, von denen eine Gefährdung für kritischen Infrastrukturen ausgeht. Nur so kann die Sicherheit der angebotenen Dienstleistungen gewährleistet werden.

Antrag: Einführung einer Pflicht zur selektiven Blockierung von Internetzugängen oder Adressierungselementen von denen eine Gefährdung im Zusammenhang mit kritischen Infrastrukturen ausgeht.

2.3

Um die Bearbeitung und Verteilung der eingegangenen Störungsmeldungen zu verbessern, sieht die revidierte Verordnung vor, die Rolle der Nationalen Alarmzentrale (NAZ) zu stärken, da sie eine sichere Informatikinfrastruktur und einen 24-Stunden-Betrieb unterhält (Art. 96). Der Kanton Nidwalden begrüsst, dass bei Störungsmeldung die Fernmeldedienstanbieter verpflichtet werden, mit der Nationalen Alarmzentrale zusammenzuarbeiten. Bis dato wurde die Störungsmeldungen lediglich zu Bürozeiten durch das BAKOM bearbeitet. Mit der Anpassung der Verordnung wird sichergestellt, dass Störungsmeldungen in Echtzeit bearbeitet und verteilt werden können. Diese Änderung ist für die Blaulichtorganisation von zentraler Bedeutung.

Cyberangriffe dagegen sind einer zu schaffenden Meldestelle gemäss Art. 96b zu melden. Darüber hinaus bestehen weitere Organisationen, die sich um Cyberangriffe kümmern. So sind beispielsweise auch das National Cyber Security Center (NCSC), die Melde- und Analysestelle Informationssicherung (MELANI) sowie die kantonalen Notrufzentralen einzubinden. In diesem Zusammenhang ist es unglücklich, dass ausschliesslich das BAKOM von der NAZ über die gemeldeten Störungen informiert wird. Die Rollen sämtlicher Stellen im Gesamtprozess von Meldung und Alarmierung im Bereich Cyber sind im erläuternden Bericht detailliert aufzuführen. Dabei ist die Schaffung eines Single Point of Contact (SPOC) grundsätzlich anzustreben, weil damit die Krisenbewältigung erleichtert wird.

Antrag: Die Rollen der einzelnen Akteure und Stellen sind detailliert zu beschreiben.

2.4

Die Zahl von 30'000 potenziell betroffenen Kundinnen und Kunden entspricht dem Äquivalent einer Schweizer Stadt mittlerer Grösse. Eine Störung, die z.B. den gesamten Kanton Appenzell Innerhoden mit seinen 16'300 Einwohnerinnen und Einwohnern betreffen würde, würde gemäss vorliegendem Entwurf somit nicht gemeldet. Zudem ist es wichtig, dass die Dauer von Störungen abgeschätzt werden kann. Aktuell gehen die Notruforganisationen davon aus, dass Störungen relevant sind, welche voraussichtlich mehr als 15 Minuten dauern und mindestens 1'000 Kundinnen und Kunden davon betroffen sind.

Antrag: Die Anbietenden werden verpflichtet, unverzüglich Störungen im Betrieb ihrer Fernmeldeanlagen und Fernmeldedienste zu melden, wenn 1'000 Kundinnen und Kunden, die potentiell von einem Ausfall betroffen sind, der länger als 15 Minuten dauert.

2.5

Die klassische Machtpolitik erlebt seit einigen Jahren eine Renaissance. Bereits heute setzen einige Staaten ihre Cybermittel regelmässig im Sinne eines "Kalten" Cyber-Krieges ein. Im Falle eines bewaffneten Konflikts in Europa ist mit einer breiten Verwendung dieser Mittel zu rechnen. Davon dürften auch Staaten, die an den eigentlichen Kampfhandlungen nicht beteiligt sind, betroffen sein. Die Armee hat in den vergangenen Jahren Schritte unternommen, sich

auf ein solches Szenario vorzubereiten. So ist die Führungsunterstützungsbasis (FUB) im Bereich Verteidigung für Aktionsplanung, Lageverfolgung, Ereignisbewältigung und Ausbildung der Mitarbeitenden und Angehörige der Armee (AdA) im Cyber-Raum verantwortlich. Mit der Weiterentwicklung der Armee (WEA) wurde zur Unterstützung der Berufsorganisation der FUB eine Cyber-Kompanie gebildet. Ab 2022 werden sämtliche Cyber-Formationen der Schweizer Armee in das neu gegründete Cyber-Bataillon 42 integriert. Die Rolle der Armee ist in der revidierten FDV zu berücksichtigen und ihre Verwendung zu beschreiben.

Antrag: Im Zusammenhang mit der Bedrohung kritischer Infrastrukturen durch Cyber-Angriffe von staatlicher Seite und deren Abwehr sind die Aufgaben der Armee aufzuzeigen und in die FDV zu integrieren.

Wir bedanken uns für Ihre Kenntnisnahme und die Berücksichtigung unserer Anträge

Freundliche Grüsse
NAMENS DES REGIERUNGSRATES

Karin Kayser-Frutschi
Landammann

lic. iur. Armin Eberli
Landschreiber

Geht an:
- tp-secretariat@bakom.admin.ch

Kanton
Obwalden

Der Vorsteher des Volkswirtschaftsdepartements VD

CH-6060 Sarnen, St. Antonistrasse 4, VD

A-Post
Eidgenössisches Departement für
Umwelt, Verkehr, Energie und
Kommunikation UVEK
Frau Bundesrätin
Simonetta Sommaruga
Bundeshaus Nord
3003 Bern

Vorab per E-Mail an:
tp-secretariat@bakom.admin.ch
mailto:ehra@bj.admin.ch
mailto:recht@bwo.admin.ch

Sarnen, 16. März 2022/wi/OWSTK.4232

Vernehmlassung zur Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit Schreiben vom 3. Dezember 2021 haben Sie die Kantone zur Vernehmlassung betreffend Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten) eingeladen. Die Vernehmlassungsfrist dauert bis zum 18. März 2022. Wir danken Ihnen für die Möglichkeit zur Stellungnahme und äussern uns gerne wie folgt:

1. Übersicht über die Vorlage

Gemäss erläuterndem Bericht ist die Änderung von Artikel 48*a* FMG am 1. Januar 2021 in Kraft getreten. Sie räumt dem Bundesrat erweiterte Kompetenzen im Bereich der Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten ein. Bis anhin regelte der Bundesrat gestützt auf die vorherige Fassung von Artikel 48*a* FMG einzig die Meldung von Störungen im Betrieb von Fernmeldenetzen und -diensten (vgl. Art. 96 Abs. 1 FDV). Der vorliegende Entwurf zur Änderung der FDV will diese Bestimmung durch eine erste Reihe von Massnahmen ergänzen, mit denen die unbefugte Manipulation von Fernmeldeanlagen durch fernmeldetechnische Übertragungen bekämpft und ein hohes Sicherheitsniveau beim Betrieb von Mobilfunknetzen der neusten Generation (5G-Netze) sichergestellt werden soll. Sie werden in einer zweiten Etappe durch ein weiteres Massnahmenpaket

St. Antonistrasse 4, 6060 Sarnen
Tel. 041 666 63 30
volkswirtschaftsdepartement@ow.ch
www.ow.ch

vervollständigt, dessen Umfang noch zu prüfen ist, und bei dem insbesondere die Gewährleistung der Stromversorgung der Mobilfunknetze im Fokus stehen wird.

2. Stellungnahme des Kantons Obwalden

Der Kanton Obwalden begrüsst grundsätzlich den vorliegenden Entwurf zur Verordnung über Fernmeldedienste (FDV). Mit dem gewählten zweistufigen Vorgehen wird einerseits die unbefugte Manipulation von 5G-Fernmeldeanlagen bekämpft und es wird ein definiertes Sicherheitsniveau eingeführt. Andererseits wird in einer zweiten Etappe ein weiteres Massnahmenpaket erarbeitet, bei welchem die Härtung im Sinne der Stromversorgungssicherheit im Fokus stehen wird. Beide Vorhaben sind aus unserer Sicht wichtig und geeignet, um die Verfügbarkeit der immer wichtiger werdenden Mobilkommunikation der 5G Technologie sicherzustellen.

Wir weisen an dieser Stelle ausdrücklich darauf hin, dass sich die mobile Kommunikation der Blaulicht- und Sicherheitsorganisationen, mangels Vorhandenseins eines Systems für die mobile breitbandige Sicherheitskommunikation (MSK[1]), in wesentlichen Aspekten auf die Mobilfunksysteme der heutigen Anbieter stützen. Aktuell werden deutlich über 70% aller Notrufe über Mobiltelefone abgewickelt. Nebst den Notrufen sind die Ereignisorganisationen auf eine funktionierende Alarmierung über die Mobilnetze angewiesen. Vor allem die Milizfeuerwehren stützen sich – mangels Alternativen – auf die Alarmierung über die bestehenden Mobilfunknetze. Dementsprechend sind Betriebsunterbrüche in den Mobilnetzen möglichst zu vermeiden, da sie direkte Auswirkungen auf die Ereignisbewältigung der Blaulichtorganisationen haben.

Eine weitere Anspruchsgruppe sind die Betreiber von kritischen Infrastrukturen, welche aufgrund ihrer Kritikalität auf einen zuverlässigen und sicheren Betrieb der neuen Generation von Mobilfunknetzen angewiesen sind.

Wir regen an, dass die Alarmierungs- und Meldeprozesse detailliert zu beschreiben sind. Um die Bearbeitung und Verteilung der eingegangenen Störungsmeldungen zu verbessern, sieht die revidierte Verordnung vor, die Rolle der Nationalen Alarmzentrale (NAZ) zu stärken. Der Empfang von Meldungen über Cyberangriffe soll zu einer Kernaufgabe der NAZ werden, da sie eine sichere Informatikinfrastruktur und einen 24-Stunden-Betrieb unterhält. Die Schaffung eines Single Point of Contact (SPOC) ist zielführend, weil damit die Krisenbewältigung erleichtert wird.

Doch bestehen weitere Organisationen, die sich um Cyberangriffe kümmern. Es kann nicht sein, dass ausschliesslich das BAKOM von der NAZ über die gemeldeten Störungen informiert wird. So sind beispielsweise auch das National Cyber Security Center (NCSC), die Melde- und Analysestelle Informationssicherung (MELANI) sowie die kantonalen Notrufzentralen von Polizei, Feuerwehr und Sanität einzubinden. Deren Rolle im Gesamtprozess von Meldung- und Alarmierung im Bereich Cyber sind im Erläuternden Bericht aufzuführen.

Im Zusammenhang mit der Bedrohung kritischer Infrastrukturen durch Cyber-Angriffe von staatlicher Seite und deren Abwehr sind die Aufgaben der Armee aufzuzeigen und in die FDV zu integrieren. Die klassische Machtpolitik erlebt seit einigen Jahren eine Renaissance. Bereits heute setzen einige Staaten ihre Cybermittel regelmässig im Sinne eines "kalten" Cyber-Kriegs ein. Im Falle eines bewaffneten Konflikts in Europa ist mit einer breiten Verwendung dieser Mittel zu rechnen. Davon dürften auch Staaten, die an den eigentlichen Kampfhandlungen nicht beteiligt sind, betroffen sein. Die Armee hat in den vergangenen Jahren Schritte unternommen, sich auf ein solches Szenario vorzubereiten. So ist die Führungsunterstützungsbasis (FUB) im Bereich Verteidigung für Aktionsplanung, Lage-

[1] Vgl. Bundesgesetzüber den Bevölkerungsschutz und den Zivilschutz, Art. 20 «Mobiles breitbandiges Sicherheitskommunikationssystem» (Link).

verfolgung, Ereignisbewältigung und Ausbildung der Mitarbeitenden und AdA im Cyber-Raum verantwortlich. Mit der Weiterentwicklung der Armee (WEA) wurde zur Unterstützung der Berufsorganisation der FUB eine Cyber-Kompanie gebildet. Ab 2022 werden sämtliche Cyber Formationen der Schweizer Armee in das neu gegründete Cyber Bataillon 42 integriert. Die Rolle der Armee ist in der revidierten FDV zu berücksichtigen und ihre Verwendung zu beschreiben.

Die sofortige Information an die kantonalen Notrufzentralen von Polizei, Feuerwehr und Sanität ist absolut notwendig. Nur sie können die Risiken von Beeinträchtigungen abschätzen und Sofortmassnahmen anordnen (bspw. die Umsetzung von Notfalltreffpunkten o.ä.). Entsprechend sind die Informationsprozesse in der FDV zu verankern.

Ergänzungen und Anpassungen
Wir beantragen die folgenden Anpassungen oder zum vorliegenden Entwurf der FDV:

Art. 96
Störungen im Mobilfunkbereich haben direkte Auswirkungen. So sind unter Umständen Notrufnummern nicht mehr erreichbar, oder die Einsatzkräfte von Polizei, Rettungsdienst und Feuerwehr sind aufgrund der nicht mehr vorhandenen Datenübertragungsmöglichkeiten in ihrem Handeln beeinträchtigt. In vielen Kantonen wurden inzwischen Notfalltreffpunkte installiert, welche bei Störungen im Kommunikationsbereich besetzt werden können. Dies setzt jedoch voraus, dass die kantonalen Notrufzentralen sofort und unverzüglich über Ausfälle, bereits im niederschwelligen Bereich, informiert werden. Die im Art. 96 formulierte Grösse von 30'000 Kundinnen und Kunden, welche von einem Ausfall betroffen sind, ist deutlich zu hoch gewählt. Zudem ist es wichtig, dass die Dauer von Störungen abgeschätzt werden kann. Aktuell gehen die Notruforganisationen davon aus, dass Störungen relevant sind, welche voraussichtlich mehr als 15 Minuten dauern und mindestens 1'000 Kundinnen und Kunden davon betroffen sind.

Eine Information an die NAZ, NCSC, MELANI, sowie nachgelagert an das BAKOM sind für die Nachbereitung der Störung wichtig. Die erwähnten Organe haben jedoch nur einen sekundären Einfluss auf die Behebung einer Störung oder der Bewältigung einer entsprechenden Lage. Dies obliegt primär den kantonalen Behörden, welche entsprechende Massnahmen sofort umsetzen können.

Es ist unklar, warum die Anzahl der betroffenen Kundinnen und Kunden nun auf Stufe FDV und nicht mehr in der TAV geregelt werden soll.

Anträge:

1. Die von einer potentiellen Störung betroffene Anzahl von Kundinnen und Kunden ist von 30'000 auf 1'000 Kundinnen oder Kunden zu senken, welche potentiell von einem Ausfall grösser als 15 Minuten betroffen sind.
2. In jedem Fall haben die Anbieterinnen von Fernmeldediensten ab einer Störungsgrösse von 1'000 Kundinnen und Kunden (+15 Minuten) die zuständigen kantonalen Notrufzentralen von Polizei, Sanität und Feuerwehr (112, 117, 118, 144) zu informieren, bevor die Meldungen an die NAZ (i.S. eines SPOC) oder weitere Organe abgesetzt werden.
3. Die Anzahl der betroffenen Kundinnen und Kunden soll weiterhin in der TAV geregelt werden und nicht auf Stufe FDV.

Art. 96a
Im Abs. 1 wird spezifisch und abschliessend von DDoS-Angriffen gesprochen. Aufgrund des technologischen schnellen Wandels ist es möglich, dass es zukünftig andere Arten von Angriffen geben kann, welche es zu berücksichtigen gilt.

Im Abs. 3 werden die Anbieterinnen von Internetzugängen berechtigt, Internetzugänge und Adressierungselemente, welche die Systeme beeinträchtigen, zu sperren oder einzuschränken. Sie dürfen die Massnahmen aufrechterhalten, solange die Bedrohung anhält. Die kann zu Unterbrüchen im Bereich der Notrufe führen und damit zu potentiellen Risiken für hilfsbedürftige Personen.

Anträge:

1. Abs. 1: Es soll im erwähnten Absatz nicht abschliessend von DDoS-Angriffen gesprochen werden, sondern die DDoS-Angriffe sind als Beispiel o.ä. aufzuführen.
2. Abs. 1: Die Details von potentiellen Angriffsmechanismen sollen nicht abschliessend in der FDV geregelt werden, sondern in den technisch- administrativen Vorschriften (TAV). Dies ermöglicht ein adäquates Handeln und ein relativ niederschwelliges Anpassen der zu berücksichtigenden Regelungen.
3. Abs. 3: Die Einschränkungen im Bedrohungsfall sollen sehr selektiv erfolgen und nur im Ausnahmefall dazu führen, dass keine Notrufnummern mehr über die betroffenen Anschlüsse gewählt werden können.
4. Abs. 3: Sind durch die Einschränkungen potentiell mehr als 1'000 Kundinnen und Kunden über die prognostizierte Dauer von mehr als 15 Minuten betroffen, sind die betroffenen kantonalen Notrufzentralen über die Einschränkungen zu informieren.

Art. 96f

Es wird im Abs. 2 definiert, dass der Betrieb der Netzwerkbetriebszentren und deren Sicherheitsbetriebszentren nebst der Schweiz im Europäischen Wirtschaftsraum und im Vereinigten Königreich stattfinden kann. Ist eine Betreiberin primär ausserhalb der Schweiz tätig, ist der operative und der juristische Durchgriff im Ereignisfall schwierig bis unmöglich. Nebst der schwierigen Erreichbarkeit im Ausland, ist auch die Priorisierung von Massnahmen und Ressourcen deutlich erschwert. Es wird angeregt, dass eine ständige Vertretung in der Schweiz gefordert wird.

Anträge:

1. Ein ständiger Firmensitz oder ein ständiger Ableger in der Schweiz ist unumgänglich und soll entsprechend in der FDV verankert werden.
2. Insbesondere beim Betrieb von sicherheitskritischen Fernmeldeanlagen ist dem ständigen Firmensitz oder einer ständigen Vertretung in der Schweiz ein hohes Gewicht beizumessen.

Ergänzende Rückmeldung

Wir erlauben uns an dieser Stelle noch auf eine weitere Pendenz hinzuweisen, welche in die vorliegende Revision der Verordnung einfliessen sollte. In der vorliegenden Revision der FDV soll auch die Problematik des kostenpflichtigen Zugangs zur SOS-DB (NotDB), zukünftig LIS-Proxy, und der Nutzung der Dynamischen Leitweglenkung (DLWL) für die Notrufzentralen geregelt werden. Dieses Bedürfnis wurde schon lange von Seiten der Notrufzentralen kommuniziert und soll nun einfliessen. Aus diesem Grunde stellen wir die folgenden zusätzlichen Anträge, welche in die Revision einfliessen sollen oder zumindest für eine weitere Revision vorbereitet werden sollen:

1. Kostenlose Nutzung der DLWL für alle Notrufzentralen, inkl. der entsprechenden Verpflichtung der zuständigen Provider.
2. Kostenlose Nutzung der SOS-DB (zukünftig LIS-Proxy) für alle Notrufzentralen.

Wir danken Ihnen, sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren, für die Kenntnisnahme unserer Stellungnahme.

Freundliche Grüsse
Volkswirtschaftsdepartement

Daniel Wyler
Landammann

Kopie an:
– Kantonale Mitglieder der Bundesversammlung
– Regierungsrat (Zirkulationsmappe)
– Sicherheits- und Justizdepartement
– Kantonspolizei
– Volkswirtschaftsdepartement
– Volkswirtschaftsamt
– Staatskanzlei mit den Akten (OWSTK.4232)

Regierung des Kantons St.Gallen, Regierungsgebäude, 9001 St.Gallen

Eidgenössisches Departement für Umwelt,
Verkehr, Energie und Kommunikation
Bundeshaus Nord
3003 Bern

Regierung des Kantons St.Gallen
Regierungsgebäude
9001 St.Gallen
T +41 58 229 74 44
info.sk@sg.ch

St.Gallen, 7. März 2022

Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten); Vernehmlassungsantwort

Sehr geehrte Frau Bundesrätin

Mit Schreiben vom 3. Dezember 2021 laden Sie uns ein, zur Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten) Stellung zu nehmen. Wir danken für diese Gelegenheit und nehmen gern wie folgt Stellung:

Wir begrüssen im Grundsatz die vorgelegte Revision der Verordnung über Fernmeldedienste (SR 784.101.1; abgekürzt FDV). Sie trägt dazu bei, die Sicherheit von Fernmeldenetzen zu erhöhen, indem der Schutz von Fernmeldeanlagen vor unbefugten Manipulationen verbessert und die Sicherheit der 5G-Netze erhöht wird. Im vorgelegten Entwurf wird jedoch der Unsicherheitsfaktor Mensch nicht hinreichend berücksichtigt − dies beispielsweise bei der Gewährleistung des Daten- und Persönlichkeitsschutzes. Die Darstellung einer solchen Gesamtsicht und den entsprechenden konkreten Beitrag der neuen Massnahmen wird im vorliegenden technischen Entwurf vermisst.

Wir stellen folgende Anträge:

– Über 70 Prozent aller Notrufe werden über Mobiltelefone abgewickelt. Betriebsunterbrüche in den Mobilnetzen sind dadurch sensitiv und haben direkte Auswirkungen auf das Notrufwesen und die Ereignisbewältigung der Blaulichtorganisationen. Aus diesem Grund wurden in vielen Kantonen Notfalltreffpunkte installiert, die bei Störungen im Kommunikationsbereich besetzt werden können. Dies setzt jedoch voraus, dass die kantonalen Notrufzentralen bereits über Ausfälle im niederschwelligen Bereich informiert werden. Die von einer potenziellen Störung betroffene Anzahl von Kundinnen und Kunden ist somit deutlich herabzusetzen. Zusätzlich ist eine nachgelagerte Kommunikation an die weiteren Organisationen, die im Rahmen von Cyberangriffen tätig sind, vorzunehmen. Namentlich sind dies die Nationale Alarmzentrale (NAZ), das National Cyber Security Center (NCSC), die Melde- und Analysestelle Informationssicherung (MELANI) sowie die kantonalen Notrufzentralen.

– Im Fall eines bewaffneten Konflikts in Europa ist die Möglichkeit von Cyberangriffen nicht auszuschliessen. Davon dürften auch Staaten, die nicht in den eigentlichen Konflikt involviert sind, betroffen sein. Die Armee hat in den vergangenen Jahren Schritte unternommen, um sich auf solche Szenarien vorzubereiten und hat eine Cyberkompanie gebildet. Die Rolle der Armee ist in der revidierten FDV entsprechend zu berücksichtigen und ihre Verwendung zu beschreiben.

– Im Zusammenhang mit unbefugten Manipulationen von Fernmeldeanlagen wird spezifisch und abschliessend von einer Angriffsart, namentlich von DDoS-Angriffen, gesprochen. Aufgrund des technologischen schnellen Wandels ist es aber jederzeit möglich, dass es zukünftig auch andere Arten von Angriffen geben kann, die es zu berücksichtigen gilt. Daher soll der besagte Absatz offener formuliert werden, indem nicht lediglich die DDoS-Angriffe erwähnt, sondern auch weitere Angriffsmöglichkeiten aufgenommen werden.

– Im Bereich der Sicherheitsmassnahmen sind konkrete Schritte gegen infizierte oder verwundbare Fernmeldeanlagen vorgesehen. Darin werden die Anbieter von Internetzugängen berechtigt, Internetzugänge und Adressierungselemente, welche die Systeme beeinträchtigen, zu sperren oder einzuschränken. Sie dürfen die Massnahmen aufrechterhalten, solange die Bedrohung anhält. Dies kann zu Unterbrüchen im Bereich der Notrufe und damit zu potenziellen Risiken für hilfsbedürftige Personen führen. Die Einschränkungen im Bedrohungsfall sollen daher selektiv erfolgen und nur im Ausnahmefall dazu führen, dass keine Notrufnummern mehr über die betroffenen Anschlüsse gewählt werden können.

– Im Bereich «Betrieb sicherheitskritischer Fernmeldeanlagen» wird definiert, dass die Netzwerkbetriebszentren und deren Sicherheitsbetriebszentren nebst der Schweiz im Europäischen Wirtschaftsraum und im Vereinigten Königreich betrieben werden können. Im Ereignisfall ist es jedoch schwierig bis unmöglich, operativ und juristisch einzugreifen, wenn Betreiber primär ausserhalb der Schweiz tätig sind. Ein ständiger Firmensitz oder ein ständiger Ableger in der Schweiz ist somit unumgänglich und soll entsprechend in der FDV verankert werden. Insbesondere beim Betrieb von sicherheitskritischen Fernmeldeanlagen ist dem ständigen Firmensitz oder einer ständigen Vertretung in der Schweiz ein hohes Gewicht beizumessen.

– Im Rahmen der vorliegenden Revision soll auch die Problematik im Zusammenhang mit dem kostenpflichtigen Zugang zur SOS-Notrufdatenbank (SOSDB) und der Nutzung der Digitalen Leitweglenkung (DLWL) bearbeitet werden. Die vonseiten der Notrufzentralen bereits seit längerer Zeit gehegten Forderungen, dass diese beiden Zugänge für alle Notrufzentralen kostenlos werden sollen, sind jetzt anzugehen.

Unsere weiteren Anliegen zu den einzelnen Artikeln sind der Beilage zu entnehmen. Wir danken Ihnen für die Berücksichtigung unserer Anliegen.

Im Namen der Regierung

Marc Mächler
Präsident

Dr. Benedikt van Spyk
Staatssekretär

Beilage:
Anhang

Zustellung auch per E-Mail (pdf- und Word-Version) an:
tp-secretariat@bakom.admin.ch

Kanton Schaffhausen
Volkswirtschaftsdepartement
Mühlentalstrasse 105
CH-8200 Schaffhausen
www.sh.ch

Telefon 052 632 73 80
dino.tamagni@sh.ch

Volkswirtschaftsdepartement

Eidgenössisches Departement
für Umwelt, Verkehr, Energie
und Kommunikation

per E-Mail an:
tp-secretariat@bakom.admin.ch

Schaffhausen, 1. Februar 2022

Vernehmlassung zur Änderung der Verordnung über Fernmeldedienste FDV (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten); Stellungnahme

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit Schreiben vom 3. Dezember 2021 haben Sie uns den Entwurf in obgenannter Angelegenheit zur Vernehmlassung unterbreitet. Wir bedanken uns für diese Möglichkeit und teilen Ihnen mit, dass wir die geplanten Änderungen der FDV mit dem Ziel, die Cybersicherheit zu verbessern, vollumfänglich begrüssen. Wir erachten die formulierten Pflichten an die Anbieterinnen von Internetzugängen als massvoll und vertretbar.

Freundliche Grüsse

Volkswirtschaftsdepartement
Der Vorsteher:

Dino Tamagni
Regierungsrat

KANTON solothurn

Finanzdepartement

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

Peter Hodel
Regierungsrat

Eidgenössisches Departement
für Umwelt, Energie und
Kommunikation
Bundesrätin Simonetta Sommaruga
Bundeshaus Nord
3003 Bern

7. März 2022

Vernehmlassung zur Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und – diensten)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit Schreiben vom 3. Dezember 2021 haben Sie uns die Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und – diensten) zur Vernehmlassung unterbreitet. Wir danken Ihnen für die Gelegenheit zur Stellungnahme und nehmen diese gerne wahr.

Gerne nehmen wir diese Gelegenheit wahr und können Ihnen mitteilen, dass wir grundsätzlich mit den Änderungen der Verordnung über Fernmeldedienste (FDV) einverstanden sind. An dieser Stelle verweisen wir zudem auf die Stellungnahme der Feuerwehr Koordination Schweiz (FKS) vom 18. Februar 2022. Die Solothurnische Gebäudeversicherung schliesst sich dieser explizit an.

Freundliche Grüsse

sig.
Peter Hodel
Regierungsrat

Der Regierungsrat des Kantons Thurgau

Thurgau

Staatskanzlei, Regierungsgebäude, 8510 Frauenfeld

Eidgenössisches
Departement für Umwelt, Verkehr, Energie
und Kommunikation (UVEK)
Frau Simonetta Sommaruga
Bundesrätin
Bundeshaus Nord
3003 Bern

Frauenfeld, 1. März 2022
138

Änderung der Verordnung über Fernmeldedienste: Sicherheit von Informationen und Fernmeldeinfrastrukturen und -diensten

Vernehmlassung

Sehr geehrte Frau Bundesrätin

Wir danken Ihnen für die Möglichkeit zur Stellungnahme zum Entwurf für eine Änderung der Verordnung über Fernmeldedienste (FDV; SR 784.101.1) und teilen Ihnen mit, dass wir den vorliegenden Entwurf grundsätzlich unterstützen. Für einzelne Bemerkungen gestatten wir uns, auf die Stellungnahme der Regierungskonferenz Militär, Zivilschutz und Feuerwehr (RK MZF) hinzuweisen, der wir uns vollumfänglich anschliessen.

Mit freundlichen Grüssen

Die Präsidentin des Regierungsrates

Der Staatsschreiber

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

Numero			Bellinzona
1084	cl	0	9 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

Dipartimento federale dell'ambiente, dei trasporti e delle comunicazioni DATEC
Palazzo federale
3003 Berna

tp-secretariat@bakom.admin.ch

Procedura di consultazione - Modifica dell'ordinanza sui servizi di telecomunicazione (sicurezza delle informazioni, delle infrastrutture e dei servizi di telecomunicazione)

Gentili signore, egregi signori,

la ringraziamo per averci consultato in merito alla modifica dell'ordinanza in oggetto, sulla quale esprimiamo volentieri le seguenti osservazioni.

Lo scrivente Consiglio sostiene il progetto di modifica dell'ordinanza sui servizi di telecomunicazione (OST) presentato; esso mira a combattere la manipolazione non autorizzata delle apparecchiature di telecomunicazione ed è in linea con quanto discusso negli ultimi anni a livello di sicurezza e di "Enterprise Incident Response", dove il peso è passato dal credere di poter proteggere perfettamente un'infrastruttura al gestire eventuali attacchi e conseguenze in aggiunta ad una protezione standardizzata. Oggi la protezione delle infrastrutture informatiche fa parte del "business model" di ogni azienda e i metodi di protezione sono standardizzati e basati su linee guida internazionali. Tipicamente la protezione è assicurata al 90-95% (a dipendenza del budget) lasciando un 5-10% di probabilità d'avere degli attacchi chiamati "zero day", ovvero sconosciuti fino al momento dell'utilizzo.
In particolare, riteniamo che sia urgente e necessario attuare ed estendere le misure per raggiungere un livello minimo di sicurezza anche per la rete 5G (e successive) in Svizzera.
A tal proposito segnaliamo alcuni ambiti, legati prevalentemente alle attività della difesa, della sicurezza, degli interventi di soccorso e della protezione di infrastrutture strategiche, nei quali i principi contenuti nella modifica in oggetto andrebbero estesi.

Oggi, più del 70% delle chiamate d'emergenza sono effettuate tramite telefoni cellulari; di conseguenza, le interruzioni della rete di telefonia mobile hanno conseguenze significative. Hanno implicazioni dirette per le chiamate di emergenza e per il controllo degli eventi da parte delle organizzazioni a tutela della sicurezza e di soccorso, così come per gli operatori di infrastrutture critiche, che devono poter contare su reti di telefonia mobile affidabili e sicure allo stato dell'arte.

Le organizzazioni legate alla sicurezza ed al soccorso e le infrastrutture critiche vanno di conseguenza integrate maggiormente nei processi di allarme e notifica.

Gli attacchi informatici non solo hanno un forte impatto economico, ma mettono anche in pericolo la sicurezza del paese, in quanto possono portare a guasti o malfunzionamenti delle infrastrutture critiche e/o sensibili. Per questo motivo, i fornitori di servizi Internet devono poter bloccare queste e altre risorse di indirizzamento che rappresentano una minaccia per le infrastrutture di cui sopra. Questo aspetto è regolato dall'art. 96 cpv. 3 ma va maggiormente sviluppato in funzione della criticità e della sensibilità dell'obbiettivo colpito. L'introduzione di un obbligo di bloccare selettivamente l'accesso a Internet e alle risorse di indirizzamento che rappresentano una minaccia per le infrastrutture critiche/strategiche è auspicato.
A complemento di quanto sopra si impone però una riflessione affinché le misure citate non collidano con le prescrizioni inerenti alla sfera privata degli utenti "comuni". Se per un'azienda è plausibile il controllo delle transazioni da e per la rete interna questo è meno praticabile su vasta scala e in relazione a piccole realtà domestiche dove una certa privacy e libertà sono auspicabili (es: sfera sessuale, medica, libertà di espressione o religiosa).
Una selezione si impone in funzione della criticità della minaccia e dell'obbiettivo colpito:

1) Per esempio si potrebbero esplicitamente quantificare il minimo di banda da cui iniziare questi "blocchi". Questo eviterebbe che un privato che si trova vittima di un malware e che genera traffico malevolo ma di entità limitata dal proprio abbonamento di casa, si trovi il proprio traffico analizzato in qualche ufficio del fornitore di servizi in modo mirato.

2) Alternativamente si potrebbe anche specificare che i blocchi dovrebbero esser frutto di analisi aggregate e anonimizzate (con prova del rispetto della privacy), dove la decisione sia basata su un tipico grafico gravità/estensione e quindi ponderato secondo il reale rischio che un attacco porta, salvaguardando comunque la possibilità di intervenire in modo più deciso ed incisivo qualora si verifichino attacchi miranti a colpire obbiettivi critici ed a valenza strategica.

Per migliorare il trattamento e la diffusione delle segnalazioni di perturbazioni che si ricevono, la revisione dell'ordinanza in consultazione prevede un ruolo rafforzato della Centrale nazionale d'allarme (CE-NAL), che gestisce 24 ore su 24 un'infrastruttura informatica sicura (art. 96). D'altra parte, gli attacchi informatici devono essere segnalati a un servizio di segnalazione (art. 96b) che deve ancora essere istituito. Inoltre, ci sono altre organizzazioni che si occupano di attacchi informatici. Per esempio, la Centrale nazionale di sicurezza informatica (CNSC), la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) e le centrali d'allarme cantonali devono essere incluse nelle attività. Per questo motivo, non è possibile che l'UFCOM sia il solo ad essere informato dalla CENAL sulle segnalazioni di interferenze ricevute. I ruoli di tutti i servizi all'interno del processo globale di segnalazione e di allarme nel dominio cibernetico devono essere presentati in dettaglio nel rapporto esplicativo. La creazione di un unico punto di contatto (SPOC) dovrebbe essere un obiettivo chiave per semplificare la gestione delle crisi.

In merito all'art. 96 e all'obbligo di segnalazione di interferenze il numero di 30.000 clienti potenzialmente interessati proposti corrisponde a una città svizzera di medie dimensioni. Perciò, secondo il progetto presentato, una perturbazione che riguarda tutto il cantone di Appenzello Interno, che ha 16.300 abitanti, non sarebbe annunciata. È anche importante valutare la durata della perturbazione. Attualmente, le organizzazioni per le chiamate di emergenza considerano problematiche le interruzioni che possono interessare almeno 1.000 clienti per più di 15 minuti per cui riteniamo che questo valore sia più consono e cautelativo rispetto a quello proposto.

Si osserva inoltre che i compiti dell'Esercito svizzero in relazione alle minacce contro le infrastrutture critiche da parte di attacchi informatici di Stati terzi e alla difesa contro questi attacchi devono essere presentati e integrati nell'OST.
Già oggi, alcuni stati impiegano regolarmente i loro mezzi informatici nell'ottica di una "guerra fredda cibernetica". Nel caso di un conflitto armato in Europa (come peraltro dimostrato dal recente conflitto in Ucraina), occorre considerare che questi mezzi possono essere utilizzati su larga scala e che anche gli Stati non direttamente coinvolti nel conflitto possono potenzialmente esserne colpiti. Negli ultimi anni, l'esercito ha preso provvedimenti per prepararsi a un tale scenario. Per esempio, la Base d'aiuto alla condotta (BAC) nel settore della difesa è responsabile della pianificazione delle azioni, del monitoraggio della situazione, della gestione degli eventi così come della formazione del personale e dei militari in difesa da attacchi provenienti dal cyberspazio, dalla guerra elettronica e dalla crittologia. Con l'ulteriore sviluppo dell'Esercito (DEVA), è stata formata una compagnia informatica per sostenere l'organizzazione professionale della BAC. A partire dal 2022, tutta la formazione cyber dell'Esercito svizzero sarà integrata nel nuovo battaglione cyber 42. La revisione dell'OST deve dunque tenere conto del ruolo delle forze armate integrandone i compiti.

Le chiediamo, signora consigliera federale, di prendere in considerazione le nostre raccomandazioni.

Vogliate gradire, gentili signore ed egregi signori, i sensi della nostra massima stima.

PER IL CONSIGLIO DI STATO

Il Presidente	Il Cancelliere
Manuele Bertoli	Arnoldo Coduri

Copia a:
- Dipartimento delle istituzioni (di-dir@ti.ch)
- Dipartimento delle finanze e dell'economia (dfe-dir@ti.ch)
- Dipartimento del territorio (dt-dir@ti.ch)
- Divisione dell'ambiente (dt-da@ti.ch)
- Deputazione ticinese alle Camere federali (can-relazioniesterne@ti.ch)
- Pubblicazione in Internet

Eidgenössisches Departement
für Umwelt, Verkehr, Energie
und Kommunikation (UVEK)
Bundeshaus Nord
3003 Bern

Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten); Vernehmlassung

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit Schreiben vom 3. Dezember 2021 haben Sie den Regierungsrat des Kantons Uri eingeladen, zur obigen Vorlage Stellung zu nehmen. Wir danken Ihnen für diese Möglichkeit.

Der Regierungsrat begrüsst die vorgeschlagenen Änderungen, die in einer ersten Reihe von Massnahmen die unbefugte Manipulation von Fernmeldeanlagen durch fernmeldetechnische Übertragung bekämpfen und ein hohes Sicherheitsniveau beim Betrieb von Mobilfunknetzen der neusten Generation (5G-Netze) zum Ziel haben. Er erachtet es ebenso wichtig, dass in einer zweiten Etappe durch geeignete Massnahmen ein weiteres Massnahmenpaket definiert wird, bei dem insbesondere die Gewährleistung der Stromversorgung der Mobilfunknetze im Fokus stehen muss.

Der Regierungsrat verzichtet auf eine detaillierte Stellungnahme.

Wir bedanken uns für die Gelegenheit zur Stellungnahme und grüssen Sie freundlich.

Altdorf, 15. März 2022

Im Namen des Regierungsrats

Der Landammann Der Kanzleidirektor

Urban Camenzind Roman Balli

canton de vaud
LIBERTÉ ET PATRIE

CONSEIL D'ETAT

Château cantonal
1014 Lausanne

Madame la Conseillère fédérale
Simonetta Sommaruga
Cheffe du DETEC
Palais fédéral Nord
3003 Berne

Envoi par courriel :
Tp-secrétariat@bakom.admin.ch

Réf. : ID/DES/Polcant

Lausanne, le 17 mars 2022

Modification de l'Ordonnance sur les services de télécommunication (OST) - Ouverture de la procédure de consultation

Madame la Conseillère fédérale,

Par courrier du 3 décembre 2021, vous nous avez invités à prendre position sur le projet mentionné sous rubrique. Le Canton de Vaud vous remercie de la possibilité ainsi offerte. Vous trouverez ci-après notre prise de position.

GENERALITES

Nous souscrivons fondamentalement au projet soumis d'Ordonnance sur les services de télécommunication (OST).

Du point de vue des services « feux bleus », il est important de tenir compte de la manipulation illicite possible du réseau 5G et d'adopter des mesures supplémentaires permettant de garantir la protection du réseau. Nous rendons également attentif à la nécessité de mettre en place un système de communication à large bande (Projet MSK) afin d'éviter à l'avenir des pannes sur les réseaux existants. Pour rappel, 70% des appels reçus par les centrales d'urgence sont faites par les appareils mobiles.

Nous suggérons que les processus d'alerte et de notification soient décrits en détail. Afin d'améliorer le traitement et la distribution des messages d'incident reçus, le règlement révisé prévoit de renforcer le rôle de la centrale nationale d'alarme d'alerte (CENAL). La réception des messages de cyber-attaques doit devenir une tâche essentielle de la CENAL, car elle dispose d'une infrastructure informatique sécurisée et d'une exploitation 24 heures sur 24. La création d'un Single Point of Contact (SPOC) est un objectif, car elle facilite la gestion des crises.

Il y a d'autres organisations qui s'occupent de cyber-attaques. Il n'est pas possible que seul l'OFCOM soit informé par la CENAL des perturbations signalées. Par exemple, le National Cyber Security Center (NCSC), l'unité de signalement et d'analyse de l'AI (MELANI) ainsi que les centres cantonaux d'appel d'urgence de la police, des pompiers et des services sanitaires doivent être inclus. Leur rôle dans l'ensemble du processus de notification et d'alerte dans le domaine de la cyber doit être indiqué dans le rapport explicatif. Les processus d'information doivent donc être ancrés dans l'ordonnance (OST).

COMPLEMENTS ET MODIFICATIONS

Nous demandons les modifications suivantes au projet de l'OST :

Art. 96

Les interférences dans le secteur de la téléphonie mobile ont des effets immédiats. Par exemple, les numéros d'urgence peuvent ne plus être disponibles ou les forces de police, de secours et de lutte contre les incendies peuvent être entravées par le manque de moyens de transmission de données. Dans de nombreux cantons, des points de rencontre d'urgence ont été installés et peuvent être occupés en cas de panne dans la zone de communication. Cela suppose toutefois que les centres cantonaux d'urgence soient immédiatement et immédiatement informés des pannes, déjà dans le secteur à bas niveau. La taille de 30 000 clientes et clients concernés par une défaillance, telle que formulée à l'article 96, est nettement trop élevée. De plus une jauge fixe ne nous paraît pas idéale. Un seuil d'alerte paramétrable selon la région, le site, l'émetteur, la population, la topographie, la présence d'infrastructures critique ou autres nous paraîtraient plus appropriés (sous réserve de faisabilité technique).

Demande :
Lors d'une défaillance du système de plus de 15 minutes concernant des clients et clientes (pas de jauge fixe, mais un seuil paramétrable), les prestataires de services de télécommunications doivent informer en priorité les centres d'appel d'urgence cantonaux de la police, des services sanitaires et des pompiers (112, 117, 118, 144). On doit diminuer au maximum les intermédiaires.

Art. 96a

Au paragraphe 1, il est question spécifiquement et en dernier lieu d'attaques de la DDoS. En raison de l'évolution rapide de la technologie, il est possible que d'autres types d'attaques puissent être envisagées dans le futur.

Au paragraphe 3, on autorise les fournisseurs d'accès à Internet à bloquer ou à restreindre les accès à Internet et les éléments d'adressage qui affectent les systèmes. Ils peuvent maintenir les mesures tant que la menace persiste. Cela peut entraîner des interruptions dans le domaine des appels d'urgence et donc des risques pour les personnes nécessitant une assistance.

Demandes :

a) *Par. 1 : Dans le paragraphe susmentionné, il ne s'agit pas de parler d'attaques DDoS, mais de mentionner les attaques DDoS comme exemples.*

b) *Par. 1 : Les détails des mécanismes d'attaque potentiels ne doivent pas être réglés de manière exhaustive dans l'OST, mais dans les règles technico-administratives (LTC). Cela permet d'agir de manière adéquate et d'adapter les règles à prendre en considération de manière relativement peu contraignante.*

c) *Par. 3 : Les restrictions en cas de menace doivent être très sélectives et ne conduire qu'à titre exceptionnel à l'impossibilité de composer des numéros d'urgence sur les lignes concernées.*

Art 96f

Au paragraphe 2, il est précisé que des centres d'exploitation du réseau et de leurs centres d'exploitation de la sécurité peuvent se trouver hors de la Suisse dans l'Espace économique européen et au Royaume-Uni. Lorsqu'un exploitant opère principalement en dehors de la Suisse, il est difficile, voire impossible, de parvenir à un accord opérationnel et juridique en cas d'événement ou de disfonctionnement. Outre les difficultés d'accès à l'étranger, la priorisation des mesures et des ressources est également nettement plus difficile. Il est suggéré d'exiger une représentation permanente en Suisse.

Demande :

En ce qui concerne notamment l'exploitation d'installations de télécommunications critiques pour la sécurité, il convient d'accorder une grande importance au siège ou à une représentation permanente en Suisse. Ceci doit être ancré dans l'OST.

CE QUI MANQUE

Deux sujets qui ont été remontés à plusieurs reprises par le Comité de pilotage intercantonal des centrales d'urgence (Steuerungsausschuss Notrufe) n'ont pas été pris en compte dans le cadre de l'ordonnance. Il s'agit de la gratuité d'utilisation pour les services d'urgence à la SOS-DB (base de données d'urgence) et à l'application de transfert dynamique des appels (DLWL). Ceci ne doit pas être un enjeu commercial.

Demande :

Intégrer dans l'OST la notion de gratuité d'accès pour toutes les centrales d'urgence à la SOS-DB et à l'application DLWL.

Nous vous prions de croire, Madame la Conseillère fédérale, à l'assurance de nos sentiments les meilleurs.

AU NOM DU CONSEIL D'ETAT

LA PRESIDENTE	LE CHANCELIER
Nuria Gorrite	Aurélien Buffat

Copies
- OAE
- Polcant

Conseil d'Etat
Staatsrat

CP 478, 1951 Sion

CANTON DU VALAIS
KANTON WALLIS

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

Département fédéral de l'environnement,
des transports, de l'énergie et de la
communication
Madame Simonetta Sommaruga
Conseillère fédérale
Palais fédéral Nord
3003 Berne

Date 16 mars 2022

Modification de l'ordonnance sur les services de télécommunication (sécurité des informations et des infrastructures et services de télécommunication) – Prise de position cantonale

Madame la Conseillère fédérale,

Le Conseil d'Etat du canton du Valais vous remercie de lui avoir soumis la consultation sur les modifications apportées à l'Ordonnance des Services de Télécommunications (OST) en lien avec la sécurité de l'information, des infrastructures et des services de télécommunications.

Le Gouvernement valaisan salue les modifications proposées qui permettront d'améliorer le niveau de sécurité des fournisseurs d'accès Internet (FAI) et des opérateurs de télécommunications mobiles.

Les accès Internet, tout comme les communications mobiles, dont fait partie la 5G, sont nécessaires au bon fonctionnement de l'économie du pays et de la société en général et doivent de fait être protégés adéquatement.

Nous avons pris bonne note des éléments suivants en lien avec les fournisseurs d'accès à Internet qui :

- pourront bloquer les adresses IP falsifiées en provenance de leurs usagers;
- auront l'obligation de tenir à jour les appareils fournis à leurs usagers, notamment les routeurs d'accès à Internet;
- pourront bloquer les accès Internet menaçant leurs services ou leurs usagers et devront en informer les usagers potentiellement concernés;
- auront l'obligation de proposer un service de signalement des manipulations et incidents.

Ces mesures renforceront la sécurité globale de leurs infrastructures, mais aussi celles de leurs usagers privés ou entreprises.

Nous saluons également le fait que les opérateurs 5G devront mettre en œuvre un Système de gestion de la sécurité de l'information (SGSI) conforme aux normes internationales telle l'ISO 27001 afin d'assurer une gestion de la sécurité complète et conforme aux standards. Nous notons avec satisfaction qu'ils devront implémenter un plan de gestion de la continuité et un plan de gestion des incidents. Ces mesures serviront assurément à élever leur niveau de maturité face aux risques cyber et diminuer la fréquence des pannes de leurs services.

L'obligation de conserver en Suisse, dans l'UE ou en Grande-Bretagne, l'exploitation des NOC (Network Operation Center) et SOC (Security Operation Center) garantira au mieux que ces centres névralgiques restent en main de tiers de confiance.

En conclusion, le Canton du Valais est favorable aux modifications de l'OST proposées par la consultation du Conseil Fédéral du 3 décembre 2021 en relevant que ces modifications amélioreront sensiblement la sécurité des services de télécommunications.

Nous vous remercions de nous avoir consultés et vous prions d'agréer, Madame la Conseillère fédérale, l'expression de notre considération distinguée.

Au nom du Conseil d'Etat

Le président	Le chancelier
Frédéric Favre	**Philipp Spörri**

Copie à tp-secretariat@bakom.admin.ch

Baudirektion, Postfach, 6301 Zug

Per E-Mail

tp-secretariat@bakom.admin.ch

T direkt +41 41 728 53 11
roman.wuelser@zg.ch
Zug, 10. März 2022 RW/las
Laufnummer: 54307

Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten)
Stellungnahme des Kantons Zug

Sehr geehrte Damen und Herren

Mit Schreiben vom 3. Dezember 2021 hat das Eidgenössische Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK die Kantonsregierungen eingeladen, im Rahmen der Vernehmlassung zu den Änderungen der Verordnung über Fernmeldedienste Stellung zu nehmen. Der Regierungsrat des Kantons Zug hat das Geschäft der Baudirektion zur direkten Erledigung weitergeleitet.

Am 1. Januar 2021 ist die Änderung des Art. 48c des Fernmeldegesetzes (FMG; SR 784.10) in Kraft getreten. Der Bund regelte darin die Meldung von Störungen im Betrieb von Fernmeldenetzen und -diensten. Die nun vorgeschlagenen Änderungen in der Verordnung (FDV; SR 784.101.1) sollen den Schutz von Fernmeldeanlagen vor unbefugten Manipulationen verbessern und die Sicherheit der 5G-Netze erhöhen.

Folgende Massnahmen sind in der Vorlage enthalten:
- Pflicht der Anbieterinnen zur Filterung von IP-Paketen mit gefälschter Quell-IP-Adresse (Spoofing);
- Pflicht der Anbieterinnen, die Sicherheit der von ihnen den Kunden zur Verfügung gestellten Geräte gemäss dem aktuellen Stand der Technik zu gewährleisten;
- Recht, Internetzugänge oder Adressierungselemente, von denen eine Gefährdung von Fernmeldeanlagen ausgeht, zu sperren oder deren Nutzung einzuschränken sowie Pflicht zur Information der Kunden;
- Pflicht der Anbieterinnen, eine Meldestelle für die Meldung von Manipulationen zu führen und auf Meldungen innerhalb einer angemessenen Frist mit geeigneten Abwehrmassnahmen zu reagieren.

Aufgrund der von Jahr zu Jahr steigenden Cyberangriffen besteht ein Handlungsbedarf an Schutzmassnahmen zur Sicherstellung der fernmeldetechnischen Übertragung. Hohe wirtschaftliche Auswirkungen und Ausfälle oder fehlerhaftes Funktionieren kritischer Infrastrukturen sind zu umgehen. Daher stimmen wir den Massnahmen grundsätzlich zu. Es ist zu prüfen, ob die Massnahmen auf alle Mobilfunkdienste und nicht nur auf die fünfte Generation auszuweiten sind.

Durch die vorliegende Verordnung wird die heutige Lebensdauer von Fernmeldeanlagen (Smartphones, IOT) weiter verkürzt, da deren Sicherheit oft durch die Versorgung von Sicherheitsupdates der Hersteller limitiert wird. Mit der Verordnung wird zwar durch Internetsperrung bei Endkunden bei infizierten Fernmeldeanlagen ein Risikobewusstsein geschaffen, aber zur Vermeidung von zusätzlichem Elektroschrott sind auch Regelungen beim Verkauf und den Herstellern der Fernmeldeanlagen zu prüfen (Mindestversorgung mit Updates, Updatefähigkeit, o. ä.)

Im Weiteren schliessen wir uns der Stellungnahme der Regierungskonferenz Militär, Zivilschutz und Feuerwehr (RK MZF) an. Einzig den Punkt 4 würden wir dahingehend relativieren, dass nicht auch Alltagsstörungen im Betrieb mit 1000 potenziell betroffenen Kundinnen und Kunden gemeint sein sollten, sondern nur effektiv relevante Störungen, welche nicht durch andere Systemanbieter kompensiert werden können.

Wir danken für die Möglichkeit zur Stellungnahme.

Freundliche Grüsse
Baudirektion

Florian Weber
Regierungsrat

Kopie an:
- Sicherheitsdirektion, info.sd@zg.ch
- Amt für Umwelt, info.afu@zg.ch
- Amt für Raum und Verkehr, info.arv@zg.ch

Kanton Zürich
Regierungsrat

Eidgenössisches Departement für Umwelt,
Verkehr, Energie und Kommunikation
3003 Bern

9. März 2022 (RRB Nr. 389/2022)
Änderung der Verordnung über Fernmeldedienste(Vernehmlassung)

Sehr geehrte Frau Bundesrätin

Mit Schreiben vom 3. Dezember 2021 haben Sie uns den Entwurf der Änderung der Verordnung vom 9. März 2007 über Fernmeldedienste (FDV, SR 784.101.1) zur Vernehmlassung unterbreitet. Wir danken für die Gelegenheit zur Stellungnahme und äussern uns wie folgt:

Grundsätzlich begrüssen wir die vorgeschlagenen Änderungen der FDV. Wir erachten eine Beschränkung des Geltungsbereichs der Art. 96e–96g auf die fünfte Mobilfunkgeneration (vgl. Art. 96d E-FDV) allerdings als nicht sachgerecht. Aufgrund der Tatsache, dass die dritte und vierte Mobilfunkgeneration sowie WiFi Hotspots von den Mobilfunkbetreibern neben 5G für die nächsten Jahre weiterhin betrieben werden, sollten die genannten Artikel technologieneutral Anwendung finden.
Soweit der zentralen Rolle der Sicherheit von Netzen und Diensten in der Verordnung damit Rechnung getragen wird, dass Mobilfunkkonzessionäre ihre Netzwerkbetriebszentren (Network Operations Centres) und ihre Sicherheitsbetriebszentren (Security Operations Centres) in der Schweiz, im Europäischen Wirtschaftsraum oder im Vereinigten Königreich betreiben müssen, erscheint uns dies unter sicherheitspolitischen Überlegungen verständlich.

Gemäss Art. 96b E-FDV betreiben schliesslich Anbieterinnen von Internetzugängen eine spezialisierte Stelle, die Meldungen über unbefugte Manipulationen von Fernmeldeanlagen durch fernmeldetechnische Übertragungen entgegennimmt. Sie leiten innert angemessener Frist geeignete Abwehrmassnahmen ein. Um dieser Regelung Nachachtung zu verschaffen, erachten wir eine genauere Bestimmung der Frist als wünschenswert.

Genehmigen Sie, sehr geehrte Frau Bundesrätin,
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 / Secrétariat général
Postfach, CH-3001 Bern
Tel. +41(0)31 300 58 58, gs@svp.ch
www.svp.ch, PC-Kto: 30-8828-5

Elektronisch an:
tp-secretariat@bakom.admin.ch

Bern, 7. März 2022

Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten)

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 Schweiz begrüsst zwar die Etablierung von Mindestanforderungen im Bereich der Sicherheit der Fernmeldeinfrastrukturen, kann dem vorliegenden Verordnungsentwurf in dieser Form jedoch nicht zustimmen.

Durch die Änderung von Art. 48a FMG, welche per 1. Januar 2021 in Kraft getreten ist, hat der Bundesrat mehr Befugnisse erhalten, um im Bereich der Sicherheit von Informationen und Fernmeldeinfrastrukturen weitergehende Vorschriften zu erlassen. Grundsätzlich unterstützt die SVP die Etablierung von Mindestanforderungen im Bereich der Sicherheit der Fernmeldeinfrastruktur, allerdings bedarf der vorliegende Verordnungsentwurf diverser Anpassungen. Darüber hinaus setzt die SVP voraus, dass die Ausgestaltung der untergeordneten technischen und administrativen Vorschriften (TAV) durch das BAKOM in enger Zusammenarbeit mit der Branche erfolgt. Generell ist es der SVP ein Anliegen, dass die Regulierung mit Augenmass erfolgt, um sowohl unnötig hohe Aufwände seitens der Betreiberinnen als auch eine Bevormundung der Endbenutzerinnen und Endbenutzer zu vermeiden und dennoch ein effizientes Mass an Sicherheit zu gewährleisten.

Aus Sicht der SVP stellt sich die Frage, weshalb Kriterien und Schwellenwerte neu auf Verordnungsstufe gehoben (z. B. in Art. 96 Abs. 1 E-FDV) und diese nicht auch weiterhin in der TAV festgehalten werden. Hierdurch könnten diese - unter vorgängiger Konsultation der Branchenvertreter - flexibler den aktuellen Gegebenheiten angepasst werden. Die genaue Festlegung der Schwellenwerte du Kriterien hat dabei durch das BAKOM in enger Zusammenarbeit mit der Branche zu erfolgen.

In Art. 96a und im Besonderen in Abs. 2 E-FDV sollen die Anbieter dazu verpflichtet werden, die ihren Kundinnen und Kunden zur Verfügung gestellten Fernmeldeanlagen unverzüglich zu aktualisieren, sofern sie weiterhin die Kontrolle über diese Anlagen ausüben. Aus Sicht der SVP bedarf es hier genauerer Formulierungen oder entsprechende Ausführungsbestimmungen in den TAV. Sollte es sich bei den genannten «Fernmeldeanlagen» um Router und dergleichen handeln, so ist eine zeitnahe Aktualisierung durch die Anbieter, sofern dies technisch möglich ist, durchaus sinnvoll. Allerdings darf die Bestimmung nicht dazu führen, dass Anbieter generell dazu verpflichtet werden, ihre Kundinnen und Kunden zu bevormunden und deren

Endgeräte (z. B. Mobiltelefone) automatisch zu aktualisieren. Ganz abgesehen davon, dass dies technisch wohl kaum umsetzbar wäre. Das regelmässige Durchführen von Updates auf dem Smartphone obliegt den Endbenutzern, insofern muss die Wahlfreiheit auch in Zukunft gewährleistet bleiben. Eine generelle Pflicht zur erzwungenen Aktualisierung von Endgeräten lehnt die SVP ab. Entsprechend bedarf die Formulierung von Art. 96a Abs. 2 E-FDV einer Überarbeitung.

Des Weiteren sieht Art. 96g Abs. 2 E-FDV vor, dass das BAKOM bei einem Verdacht auf Verletzung der Vorgaben ein externes Audit zu Lasten des Mobilfunkkonzessionärs verlangen kann. Da solche Audits kostspielig und durchaus auch grössere Kostenfolgen nach sich ziehen können, ist es aus Sicht der SVP angezeigt, die Formulierung dahingehend zu ändern, als dass das BAKOM bei einem «begründeten Verdacht», also bei einem qualifizierten Verdacht und nicht nur bei einem schlichten Verdachtsmoment, eine entsprechende Überprüfung verlangen kann. So orientieren sich Regulierungsansätze in anderen Bereichen ebenfalls am Grundsatz des qualifizierten Verdachtes (z. B. Art. 9 Abs. 1 Geldwäschereigesetz, Art. 5 VSoTr etc.).

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

SCHWEIZERISCHE VOLKSPARTEI

Der Parteipräsident	Der Generalsekretär
Marco Chiesa Ständerat	Peter Keller Nationalrat

Sozialdemokratische Partei der Schweiz / Parti Socialiste Suisse
Zentralsekretariat / Secrétariat central
Theaterplatz 4, 3011 Bern
Postfach / Case postale, 3001 Bern
Tel. 031 329 69 69 / info@spschweiz.ch / www.spschweiz.ch / www.pssuisse.ch

Per Mail an: tp-secretariat@bakom.admin.ch

Bern, 18. März 2022

Änderung der Verordnung über Fernmeldedienste (FDV): Stellungnahme SP Schweiz

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

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

Die Änderung von Artikel 48a FMG (SR 784.10) ist am 1.1.2021 in Kraft getreten. Sie räumt dem BR erweiterte Kompetenzen im Bereich der Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten ein. Bis anhin regelte der BR gestützt auf die vorherige Fassung von Artikel 48a FMG einzig die Meldung von Störungen im Betrieb von Fernmeldenetzen und -diensten (vgl. Art. 96 Abs. 1 FDV; SR 784.101.1). ***Der vorliegende Entwurf zur Änderung der FDV will diese Bestimmung durch eine erste Reihe von Massnahmen ergänzen, mit denen die unbefugte Manipulation von Fernmeldeanlagen durch fernmeldetechnische Übertragungen bekämpft und ein hohes Sicherheitsniveau beim Betrieb von Mobilfunknetzen der neusten Generation (5G-Netze) sichergestellt werden soll****. Sie werden in einer zweiten Etappe durch ein weiteres Massnahmenpaket vervollständigt, dessen Umfang noch zu prüfen ist, und bei dem insbesondere die Gewährleistung der Stromversorgung der Mobilfunknetze im Fokus stehen wird.*

⇒ **Die SP Schweiz begrüsst die vorgesehenen Änderungen der Verordnung über Fernmeldedienste (FDV). Wir verzichten allerdings auf eine detaillierte Stellungnahme dazu.**

Wir danken für die Berücksichtigung unserer Anliegen.

Mit freundlichen Grüssen

SP Schweiz

Mattea Meyer
Co-Präsidentin

Cédric Wermuth
Co-Präsident

Claudia Alpiger
Politische Fachsekretärin

Schweizer Bauernverband
Union Suisse des Paysans
Unione Svizzera dei Contadini
sbv | usp | usc

125 jahre | ans | anni

Eidgenössisches Departement für Umwelt,
Verkehr, Energie und Kommunikation UVEK
Frau Bundesrätin Sommaruga
Bundeshaus Nord

3003 Bern

tp-secretariat@bakom.admin.ch

Brugg, 7. März 2022

Zuständig: Martin Brugger
Sekretariat: Ursula Boschung
Dokument: Schweizerischer Bauernverband SBV

Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten) Vernehmlassungsverfahren 2021/101

Sehr geehrte Frau Bundesrätin Sommaruga
Sehr geehrte Damen und Herren

Mit Ihrem Schreiben vom 3.12.2021 laden Sie uns ein, zur oben genannten Vorlage Stellung zu nehmen. Für die uns gegebene Möglichkeit danken wir Ihnen bestens und sind gerne bereit, uns in dieser Angelegenheit vernehmen zu lassen.

Grundsätzliche Erwägungen

Der Schweizer Bauernverband vertritt die Interessen des Landwirtschaftssektors und der rund fünfzigtausend landwirtschaftlichen Betriebe und Bauernfamilien in der Schweiz. Der Bauernverband strich im Zusammenhang mit dem digitalen Wandel in der Landwirtschaft in den letzten Jahren wiederholt die Wichtigkeit von Sicherheitsaspekten bei der Digitalisierung hervor: Sicherheit im digitalen Raum ist eine unabdingbare Voraussetzung für eine förderliche Entwicklung und für die breite Akzeptanz des digitalen Wandels.

In der Vorlage werden aus Sicht der Landwirtschaft zielführende Ergänzungen in der Verordnung über Fernmeldedienste vorgeschlagen. Die Anpassungen setzen eine ganze Reihe von Massnahmen um, mit denen die unbefugte Manipulation von Fernmeldeanlagen durch fernmeldetechnische Übertragungen bekämpft und ein hohes Sicherheitsniveau beim Betrieb von Mobilfunknetzen der neusten Generation (5G) sichergestellt werden soll.

Das Internet und der Mobilfunk haben eine stetig zunehmende Bedeutung für private Haushalte und Unternehmen. Mit wachsender Komplexität und Abhängigkeit kommt der Risikoprävention eine immer grössere Bedeutung zu. Risikoprävention sowie eine verlässliche Sicherheit im digitalen Raum sind auch für die Landwirtschaft wichtig. Wie die übrigen Branchen und Bevölkerungsgruppen sind auch die Landwirtschaftsbetriebe und die in ihnen tätigen Menschen zunehmend auf eine sichere digitale Kommunikation und die Sicherheit digitaler Tools angewiesen.

Schlussbemerkungen

Aus Sicht des Schweizer Bauernverbandes tragen die neuen Regelungen in der FDV dazu bei, die digitale Entwicklung zu unterstützen, indem sie minimale Sicherheitsstandards und -Massnahmen verpflichtend etablieren und dadurch das Vertrauen der User und der Unternehmen in die Digitalisierung und die damit verbundenen Anwendungen fördern.

Laurstrasse 10 | 5201 Brugg | Telefon +41 (0)56 462 51 11
info@sbv-usp.ch | www.sbv-usp.ch

Schweizer Bauernverband
Union Suisse des Paysans
Unione Svizzera dei Contadini
sbv | usp | usc

125 jahre | ans | anni

Wir hoffen, dass Sie unsere Anliegen berücksichtigen werden und danken Ihnen nochmals für die Möglichkeit zur Stellungnahme.

Freundliche Grüsse

Schweizer Bauernverband

Markus Ritter
Präsident

Martin Rufer
Direktor

Laurstrasse 10 | 5201 Brugg | Telefon +41 (0)56 462 51 11
info@sbv-usp.ch | www.sbv-usp.ch

economiesuisse

Eidg. Departement für Umwelt, Verkehr,
Energie und Kommunikation UVEK
Bundeshaus Nord
CH-3003 Bern

Per E-Mail an:
tp-secretariat@bakom.admin.ch

29. März 2022

[Betreff]: Stellungnahme economiesuisse

Sehr geehrte Frau Bundesrätin Sommaruga
Sehr geehrte Damen und Herren

Mit Schreiben vom 3. Dezember 2020 haben Sie uns eingeladen, zu einer Revision der Fernmeldeverordnung (FDV) im Bereich der Cyber-Sicherheit 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 unsere Mitglieder sind an einem effizienten Schutz vor Cyber-Risiken interessiert. Für die Schweizer Fernmeldedienstanbieterinnen und Internet Access Provider stellt dieser gar ein ureigenes unternehmerisches Interesse dar, da sie nur mit sicheren Netzen und Dienstleistungen am Markt bestehen können. Der Wettbewerb bietet in dieser Hinsicht die grundlegend richtigen Anreize und belohnt einen verantwortungsvollen Umgang mit dem Thema Cyber-Sicherheit: Wer sich nicht seriös um dieses Thema kümmert, wird am Markt keine Chance haben.

Dennoch braucht es auch passende Rahmenbedingungen, welche die vorhandenen Anreize zusätzlich stärken und die Marktakteure in ihren Bemühungen unterstützen. In diesem Sinne begrüssen wir die Vernehmlassungsvorlage grundsätzlich. Sie setzt auf eine prinzipienbasierte Regulierung, auf Management-Systeme für Cyber-Risiken und auf internationale Standards. Sie schreibt insgesamt ein erwünschtes Sicherheitsniveau (Zielbild) vor, anstatt die Prozesse und Organisation zur Erreichung dieses Sicherheitsniveaus im Detail zu regulieren. Damit bietet sie genügend Spielraum für eine effiziente Umsetzung durch die Schweizer Fernmelde- und Internetanbieterinnen. Ebenso bleibt sie im Umfang verhältnismässig und bietet in Bezug auf Art. 48a FMG die nötige Rechtssicherheit. Die Wirtschaft erwartet, dass diese Vorzüge auch bei sämtlichen weiteren Umsetzungsschritten von Art. 48a FMG zum Tragen kommen, insbesondere bei der «Härtung» der Mobilfunknetze punkto Stromversorgung in Mangellagen.

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

Trotz dem grundsätzlich positiven Gesamtbild möchten wir nach Rücksprache mit unseren betroffenen Mitgliedern auf Verbesserungspotentiale hinweisen:

- In gewissen Bereichen könnte der Detaillierungsgrad des Entwurfs noch reduziert werden, damit in der Praxis mehr Flexibilität besteht. So wären gewisse Schwellenwerte und Kriterien (bspw. Art. 96 E-FDV Abs. 1) in den technischen und administrativen Vorschriften (TAV) des BAKOM besser aufgehoben. Dadurch könnten die betroffenen Unternehmen im Dialog mit der Verwaltung und unter Berücksichtigung der aktuellen technologischen Entwicklung die effektivste Umsetzung suchen.
- Zudem braucht es genügend lange Umsetzungsfristen und Vorlaufzeiten (bspw. mind. 6 Monate bei Art. 96a E-FDV). Auch hier wäre eine Definition der genauen Fristen in den TAV zu bevorzugen, da so besser auf die Situation der einzelnen Firmen eingegangen werden kann.
- Die Verantwortung der Unternehmen ist klar von jener ihrer Kundinnen und Kunden abzugrenzen. Dinge wie die Aktualisierung von Smartphone-Software müssen in der Verantwortung der Nutzenden bleiben und können nicht den anbietenden Unternehmen übertragen werden. «Customer Premise Equipment» soll im Sinne eines Basis-Sicherheitsstandards reguliert werden.
- Die Anforderungen der Regulierung sollen punktuell stärker an die technische Machbarkeit geknüpft werden (bspw. Art. 96a E-FDV Abs. 2).
- Die in Art. 96e verlangten Management-Systeme sollen gem. gängigen Standards und Zertifizierungen akzeptiert werden. Der Markt hat hier bereits ausreichende Grundlagen geschaffen, so dass ein Swiss finish mit einem allfälligen eigenen Anforderungsprofil nicht zielführend ist.
- Eine Auditierung gem. Art. 96g soll nur bei begründeten Verdachtsmomenten greifen, da sonst die Risiken und Unsicherheiten für die betroffenen Unternehmen sehr gross sind. Die Beweislast würde mit der vorgeschlagenen Formulierung einseitig bei ihnen liegen.
- Die vorgesehene Verpflichtung zum Betrieb einer Meldestelle für unbefugte Manipulationen an Fernmeldeanlagen (Art.96b E-FDV) beurteilen wir kritisch. Diese Bestimmung weicht insofern von den sonstigen Anpassungen ab, als dass sie konkrete organisatorische Vorschriften macht, anstatt sich auf Handlungsgrundsätze zu beschränken. Angesichts des vorhandenen Fachwissens und der unterschiedlichen kommerziellen Voraussetzungen der Schweizer Internetanbieterinnen erscheint uns diese Regelung unpassend. Die betroffenen Unternehmen sollten selbst entscheiden können, auf welche Weise sie Meldungen zu allfälligen Manipulationen verarbeiten, solange sie die Sicherheit gewährleisten können.
- Gegen die Meldepflicht von Störungen an den Bund gem. Art. 96 E-FDV ist a priori nichts einzuwenden. Wichtig ist jedoch, dass solche Meldepflichten nicht unübersichtlich werden und zu Doppelspurigkeiten führen. Entsprechend regen wir an, dass sämtliche Meldungen an einen «one stop shop» vorgenommen werden können und vorliegend darauf verzichtet wird, die Nationale Alarmzentrale (NAZ) als Meldestelle zu bezeichnen. Stattdessen könnte analog zur Vorlage über die Revision des Informationsgesetzes das NCSC designiert werden.

Herzlichen Dank für die Berücksichtigung unserer Argumente. Ergänzend unterstützen wir integral die Stellungnahmen unserer betroffenen Mitglieder, insb. asut, SUISSEDIGITAL und Swisscom.

Freundliche Grüsse
economiesuisse

Beat Ruff
Stv. Leiter Infrastruktur, Energie und Umwelt

Lukas Federer
Projektleiter Infrastrukturen

Eidgenössisches Departement für Umwelt,
Verkehr, Energie und Kommunikation
Bundesamt für Kommunikation

Per E-Mail an: tp-secretariat@bakom.admin.ch

Bern, 17. März 2022

Stellungnahme zur Änderung der Verordnung über Fernmeldedienste (FDV): Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten

Sehr geehrte Frau Bundesrätin,
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 der Verordnung über Fernmeldedienste ist für die Mitglieder von asut von hoher Relevanz.

asut begrüsst die vorgeschlagene Revision der FDV. Die Revision hat das Potential, das Vertrauen von Wirtschaft und Gesellschaft in die Sicherheit von Fernmeldenetzen als kritische Infrastruktur weiter zu stärken. Störungsmeldungen sollten jedoch statt an die NAZ künftig an das NCSC erfolgen. asut erachtet es als sinnvoll, dass die geplanten Vorgaben auf internationalen Standards basieren. Die Hoheit über die Netze muss aber zwingend bei den Netzbetreiberinnnnen bleiben. Dieser Grundsatz muss unbedingt auch auf der Stufe der technischen und administrativen Vorschriften gelten.

asut begrüsst die vorgeschlagene Revision der FDV im Grundsatz, weil es Neutralität zeigt und messbare technische Kriterien beinhaltet, schlägt jedoch folgende Anpassungen vor:

Definition eines minimale Sicherheitsniveau kann Vertrauen stärken

Grundsätzlich sind alle Anbieterinnen von Telekommunikationsnetzwerken oder Komponenten bestrebt, die Sicherheit ihrer Telekommunikationsnetze und -infrastrukturen hoch zu halten und laufend zu verbessern. Sie kommen damit einem klaren und immer wichtigeren Bedürfnis ihrer Kundinnen und Kunden nach, insbesondere im B2B-Bereich. Marktbedürfnissen und Wettbewerb führen daher zu einer laufenden Steigerung des Sicherheitsniveaus. Aus diesem Grund wäre eigentlich eine Anpassung der rechtlichen Grundlagen nicht zwingend nötig. Doch schafft die Definition eines Mindestniveaus einen Orientierungsrahmen und kann dazu beitragen, das Vertrauen von Wirtschaft und Gesellschaft in die Sicherheit von Fernmeldenetzen insgesamt weiter zu erhöhen. Insofern wird die Revision von asut begrüsst.

asut
Schweizerischer Verband der Telekommunikation
Hirschengraben 8
3011 Bern

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

@asut_ch

Das Schadenspotential von Cyberangriffen ist gross und grundsätzlich kann jedes IT-Gerät davon betroffen sein. Die Anbieterinnen von Fernmeldediensten (FDA) können ihre Verantwortungen jedoch nur für ihre eigenen Systeme wahrnehmen und in einem begrenzten Ausmass auch für ihre Kunden (z.B. Phishing-Filter). Obwohl Cyberangriffe häufig über das Internet initiiert oder ausgeführt werden, können die FDA keine umfassenden Schutz davor bieten. Und in vielen Fällen dürfen sie es auch gar nicht, da der Fernmeldeverkehr geschützt ist und es in der Verantwortung der Anwenderinnen und Anwender liegt, welches Email sie öffnen oder welchen Link sie anklicken. Cybersicherheit ist daher eine Aufgabe, die von allen Akteuren in ihrem Bereich selbst gelöst werden muss und diese Aufgabe kann nicht an die FDA delegiert werden..

Meldestelle für Störungen (Art. 96 FDV)

Neu sollen Störungen im Betrieb von Fernmeldeanlagen und -diensten, sofern mindestens 30'000 Kundinnen und Kunden betroffen sind, nicht wie bisher dem Bundesamt für Kommunikation (BAKOM), sondern der Nationalen Alarmzentrale (NAZ) gemeldet werden. Gegen die Änderung der zuständigen Stelle, der Störungen zu melden sind, ist grundsätzlich nichts einzuwenden.

Wichtig ist jedoch, dass die Zuständigkeiten der verschiedenen Amtsstellen, denen die FDA Vorfälle zu melden haben, zweifelsfrei definiert sind und ihre Anzahl so gering wie möglich gehalten wird. So können sowohl auf der Seite der Bundesverwaltung wie auch der Betreiberinnen von 5G-Netzen und der Internet Access Provider (IAP) Doppelspurigkeiten reduziert, Missverständnisse vermieden, Antwortzeiten kurzgehalten und das Risiko falscher Reaktionen minimiert werden. Darum ist es richtig, keine zusätzliche Meldestelle zu schaffen. Idealerweise nimmt künftig sogar nur eine einzige Bundesstelle sämtliche Störungsmeldungen entgegen und leitet diese bei Bedarf an die andere Bundesstellen weiter.

Im Rahmen des neuen Informationssicherheitsgesetzes (ISG) will das Eidgenössische Finanzdepartement, das NCSC als zentrale Meldestelle für Cybervorfälle definieren. asut schlägt darum vor, in Art. 96 FDV das NCSC statt die NAZ als entsprechende Meldestelle festzulegen. Der Bund hat dafür die gesetzlichen Grundlagen zu schaffen, die Prozesse entsprechend zu planen und beim NCSC die nötigen Infrastrukturen und Kompetenzen bereitzustellen. asut erachtet es als wichtig, dass die Revision der FDV und die Anpassung der ISG koordiniert erfolgen.

Vorgaben zur Sicherheit von CPE klar formulieren

Im erläuternden Bericht zur Änderung der Verordnung über Fernmeldedienste (FDV) führt das BAKOM aus, welche Massnahmen für die Geräte vorgesehen sind, welche die IAP ihren Kundinnen und Kunden zur Verfügung stellen (sogenanntes «Customer Premises Equipment», CPE). Diese Massnahmen sollen in den technischen und administrativen Vorschriften (TAV) zur FDV festgehalten werden.

asut befürwortet die Definition eines Basis-Sicherheitsstandards für CPE. Die Formulierungen im erläuternden Bericht können jedoch zu Missverständnissen führen und erfordern deshalb folgende Anpassungen und Präzisierungen (Änderungen sind jeweils <u>unterstrichen</u>):

Wortlaut im Erläuternden Bericht	**Kommentar von asut**
Nicht benötigte Dienste auf dem CPE müssen deaktiviert sein.	Auf den CPE (z.B. TV Boxen und Router) stehen unzählige Funktionen zur Verfügung. Einige Kundinnen und Kunden nutzen viele davon, andere nur die wenigsten. Für die IAP ist es unmöglich, die Funktionen entsprechend den individuellen Bedürfnissen zu aktivieren oder zu deaktivieren. Grundsätzlich liegt es nicht im Interesse der IAP, auf ihren CPE nicht gewünschte oder sogar unsichere Dienste anzubieten. <u>asut schlägt vor, diesen Punkt ersatzlos zu streichen.</u>

Wortlaut im Erläuternden Bericht	Kommentar von asut
CPE müssen zeitnah mit vom Hersteller als kritisch eingestuften Sicherheitsupdates versorgt werden. Werden die CPE vom Hersteller als «End of Life» klassifiziert, müssen sie ausgetauscht werden.	Der Begriff «End of Life» wird nicht einheitlich verwendet. So ist denkbar, dass ein Hersteller ein Gerät als «End of Life» deklariert, aber weiterhin Sicherheitsupdates vom Hersteller selbst oder vom FDA zur Verfügung gestellt werden. asut schlägt vor, diesem Aspekt folgendermassen Rechnung zu tragen: «CPE müssen zeitnah mit vom Hersteller oder den FDA als kritisch eingestuften Sicherheitsupdates versorgt werden. Werden die CPE nicht mehr vom Hersteller oder den FDA mit kritisch eingestuften Sicherheitsupdates versorgt, müssen sie ausgetauscht werden.»

Massnahmen basieren auf internationalen Standards

Die Vorlage orientiert sich im Wesentlichen an Massnahmen, welche auch in anderen Ländern, insbesondere der EU, implementiert werden und basieren auf international anerkannten Sicherheitsnormen und -initiativen (z.B. ENISA, NESAS, GSMA knowledge base, SCAS, 3GGP, ISO). Indem auf eine nationale Sonderlösungen weitgehend verzichtet wird, können die Massnahmen effizient umgesetzt und die Sicherheitsstandards laufend den technischen Entwicklungen angepasst werden. Zudem orientieren sich auch die international tätigen Technologiefirmen sowie zunehmend auch die Schweizer Geschäftskunden an diesen Standards (z.B. Finanzbranche). Letzteres führt branchenübergreifend zu einer Erhöhung der Netzwerksicherheit und zeigt zudem, dass Markt und Wettbewerb automatisch zu einer Steigerung des Sicherheitsniveaus führen. asut erachtet darum dieses Vorgehen als richtig.

asut befürwortet die Schaffung von Rechten für die Fernmeldedienstanbieterinnen anstelle von Pflichten; es ist richtig und wichtig, dass die Entscheidungskompetenz betreffend Massnahmen für eben ihre Netze in den Händen der Netzbetreiberinnen bleibt. Für kleinere Anbieterinnen ist eine vorgegebene Zertifizierung mit grossem Aufwand und Kosten verbunden, sowohl einmalig als auch wiederkehrend. Eine konkrete Bestimmung käme hier einem schwerwiegenden Eingriff in die Wirtschaftsfreiheit gleich. Es sollte deshalb unbedingt den Netzbetreiberinnen überlassen werden, wie sie das Sicherheitsmanagement umsetzen; auf die Vorgabe von konkreten Standards soll verzichtet werden (sowohl in der Verordnung als auch in einer TAV). Das BAKOM sollte erst bei Vorfällen aktiv werden und dann den Sachverhalt untersuchen gemäss Vorgabe in Art. 96g Abs. 2 E-FDV.

Es ist zentral, dass sich die schweizerische Gesetzgebung in einem international anerkannten und von den internationalen Zulieferern bekannten Rahmen bewegt. Spezielle Regelungen für die Schweiz (sogenannter Swiss finish), sind zu vermeiden. Sie bremsen den technologischen Fortschritt und die Innovationskraft der Schweiz. Zurzeit gehören die Schweizer Fernmeldenetze zu den besten der Welt und bilden damit eine wichtige Grundlage für die Wettbewerbsfähigkeit der Schweiz.

Diesem Grundsatz muss der Bund unbedingt auch bei den noch folgenden technischen Präzisierungen auf Stufe technischer und administrativer Vorschriften (TAV) treu bleiben (Art. 96e Abs. 3 und 96g Abs. 1 E-FDV).

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

Freundliche Grüsse

Peter Grütter
Präsident

Centre Patronal

Madame la Conseillère fédérale
Simonetta Sommaruga
DETEC
3003 Berne

Par courrier électronique :
tp-secretariat@bakom.admin.ch

Paudex, le 16 mars 2022
PGB

Procédures de consultation relatives à la révision de l'ordonnance sur les services de télécommunication (OST) :

1. **adaptation des dispositions du service universel**
2. **sécurité des infrastructures et services de télécommunication**

Madame la Conseillère fédérale,

Nous avons pris connaissance des deux procédures de consultation mentionnées en titre, qui concernent toutes deux l'ordonnance fédérale sur les services de télécommunication (OST) et que nous avons donc examinées ensemble. Par la présente, nous prenons la liberté de vous faire connaître notre position sur ces deux dossiers.

1. Adaptation des dispositions du service universel

Le service universel vise à garantir à toute la population les services de télécommunication considérés comme essentiels, à des prix abordables et dans toutes les régions du pays ; il est conçu comme un mécanisme de sécurité pour les situations où la concurrence ne fonctionne pas de manière satisfaisante.

L'actuelle concession de service universel a été octroyée à Swisscom pour les années 2018 à 2022. Il est prévu qu'elle soit prolongée jusqu'à fin 2023 et qu'une nouvelle concession soit octroyée dès le 1er janvier 2024. Le contenu de cette nouvelle concession doit être adapté en tenant compte des évolutions constatées sur les plans social, économique et technique.

La principale adaptation proposée dans la prochaine concession de service universel consiste à y inclure une offre supplémentaire d'accès internet à très haut débit (80 Mbit/s en téléchargement et 8 Mbit/s en téléversement) en plus de l'offre de base (10 Mbit/s en téléchargement et 1 Mbit/s en téléversement).

Appréciation :

Concernant la volonté d'inclure dans le service universel une possibilité d'accès internet à très haut débit, nous y sommes favorables pour autant que ce soit techniquement et économiquement réalisable – ce qui semble a priori être le cas.

Concernant l'article 14b OST, nous nous étonnons de sa nouvelle teneur, qui – selon ce que nous comprenons – interdit au détenteur de la concession de service universel de conclure des contrats de service universel là où existe une offre commerciale au moins équivalente, tout en lui permettant de fournir ces mêmes prestations dans le cadre d'une relation commerciale normale faisant abstraction du service universel. Une telle interdiction peut-elle être valablement contrôlée ? Va-t-on obliger les clients du service universel à changer de

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

contrat lorsqu'ils déménagent ? Nous nous demandons s'il ne s'agit pas là d'un perfectionnisme excessif. Le rapport explicatif ne fournit par ailleurs aucune justification à l'appui d'une telle adaptation.

2. Sécurité des infrastructures et services de télécommunication

Les adaptations proposées visent, d'une part, à impliquer activement les fournisseurs d'accès à Internet (FAI) dans la lutte contre les cyberattaques et, d'autre part, à impliquer activement les fournisseurs de services de télécommunication (FST) dans la sécurité des nouveaux réseaux mobiles 5G.

Concrètement, les FAI auront l'obligation de filtrer les paquets IP dont l'IP source est falsifiée (utilisés dans les attaques contre la disponibilité des services web, ou attaques DDoS). Ils auront aussi la responsabilité de s'assurer de la sécurité des appareils qu'ils mettent à la disposition de leurs clients (par exemple niveau de sécurité des routeurs wifi). Les FAI auront en outre la possibilité de bloquer ou de restreindre les accès internet si cela est nécessaire pour protéger certaines installations. Il leur incombera enfin de mettre sur pied un service de signalement des manipulations non autorisées.

Concernant les FST impliqués dans des réseaux 5G, seront tenus de signaler immédiatement toute perturbation touchant au moins 30'000 clients. Ils devront exploiter des installations et des systèmes de sécurité conformes aux normes reconnues. Leurs centres opérationnels et de gestion de la sécurité devront se trouver en Suisse, dans l'Espace économique européen ou au Royaume-Uni.

Appréciation :

La cybersécurité est aujourd'hui une préoccupation majeure. Il nous paraît donc justifié, voire indispensable, que les fournisseurs d'accès internet et les gestionnaires de réseaux mobiles soient impliqués et prennent des responsabilités dans ce domaine. En ce sens, nous approuvons les adaptations proposées – en laissant toutefois aux fournisseurs de services concernés le soin de se prononcer sur le caractère praticable ou suffisant des efforts demandés.

En vous remerciant de l'attention que vous porterez à ce qui précède, nous vous prions d'agréer, Madame la Conseillère fédérale, l'expression de notre haute considération.

Centre Patronal

Pierre-Gabriel Bieri

Eidgenössischen Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK
Bundesrätin Simonetta Sommaruga
Bundeshaus Nord, 3003 Bern

Einreichung per Mail an: tp-secretariat@bakom.admin.ch

Bern, 18. März 2022

Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten)

Stellungnahme von digitalswitzerland

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, uns zur «Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten)» äussern zu können. Diese Gelegenheit nimmt der Verein digitalswitzerland gerne wahr.

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 Ansprechpartnerin in allen Digitalisierungsfragen und engagiert sich für die Lösung vielfältiger Herausforderungen.

Cybersecurity ist das Gebot der Stunde

Mit der Anfang 2021 in Kraft getretenen Änderung von Artikel 48a des Fernmeldegesetzes (FMG) erhielt der Bundesrat mehr Kompetenzen im Bereich der Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten. Nun soll mit der Anpassung der Verordnung über Fernmeldedienste (FDV) eine Reihe von ergänzenden Massnahmen erfolgen, mit denen die unbefugte Manipulation von Fernmeldeanlagen bekämpft und die Netzwerksicherheit von 5G-Mobilfunknetzen sichergestellt werden soll.

digitalswitzerland begrüsst die vorgeschlagene Revision der FDV. Es ist wichtig, dass die Sicherheit der Fernmeldenetze als kritische Infrastruktur von allen Seiten gestärkt wird. Weiter kann die Definition eines Mindestniveaus dazu beitragen, das Vertrauen der Bevölkerung und der Wirtschaft in die Fernmeldenetze weiter zu festigen.

Aus Sicht von digitalswitzerland sind die Prozesse im Interesse der Sicherheit möglichst klar und effizient zu gestalten. Es gilt Doppelspurigkeit zu vermeiden und Vorgaben auf internationale Standards abzustimmen. Deshalb schlägt digitalswitzerland punktuelle Anpassungen der Vorlage vor.

Doppelspurigkeit vermeiden, Klarheit schaffen, Standards berücksichtigen

digitalswitzerland begrüsst die vorgeschlagene Revision der FDV grundsätzlich, schlägt jedoch folgende Anpassungen vor:

Meldestelle für Störungen (Art. 96 FDV)

Aus Sicht von digitalswitzerland sollten Störungsmeldungen, welche potenziell mindestens 30'000 Kundinnen und Kunden betreffen, künftig an das Nationale Zentrum für Cybersicherheit (NCSC) erfolgen.[1] Denn im Rahmen des neuen Informationssicherheitsgesetzes (ISG), welches sich bis zum 25. März 2022 ebenfalls in Vernehmlassung befindet, wird das NCSC als zentrale Meldestelle für Cybervorfälle bei kritischen Infrastrukturen definiert.

Es ist wichtig, dass die Zuständigkeiten der verschiedenen Meldestellen zweifelsfrei definiert sind und ihre Anzahl so gering wie möglich gehalten wird. So können sowohl auf der Seite der Bundesverwaltung wie auch der Netzbetreiberinnen und der Internet Access Provider (IAP) Doppelspurigkeiten reduziert, Missverständnisse vermieden, Antwortzeiten kurzgehalten und das Risiko falscher Reaktionen minimiert werden. Darum ist es richtig, keine zusätzliche Meldestelle zu schaffen. Idealerweise nimmt künftig sogar nur eine einzige Bundesstelle sämtliche Störungsmeldungen entgegen und leitet diese bei Bedarf an die andere Bundesstellen weiter.

Klare Formulierung der Vorgaben zur Sicherheit von CPE

Im erläuternden Bericht zur Revision wird festgehalten, welche Massnahmen für die Geräte (sogenanntes «Customer Premises Equipment», CPE) vorgesehen sind, welche die Anbieterinnen von Internetzugängen (sogenannte «Internet Access Provider», IAP) ihren Kundinnen und Kunden zur Verfügung stellen. Diese Massnahmen sollen in den technischen und administrativen Vorschriften (TAV) zur FDV festgehalten werden.

digitalswitzerland befürwortet die Definition eines Basis-Sicherheitsstandards für CPE. Es ist ein wichtiger Schritt zur Erhöhung der Cyber-Resilienz. Einzelne Formulierungen im erläuternden Bericht können jedoch zu Missverständnissen führen und erfordern deshalb folgende Präzisierungen.

Wortlaut erläuternder Bericht	Vorschläge und Kommentar
CPE müssen zeitnah mit vom Hersteller als kritisch eingestuften Sicherheitsupdates versorgt werden. Werden die CPE vom Hersteller als «End of Life» klassifiziert, müssen sie ausgetauscht werden.	Der Begriff «End of Life» wird nicht einheitlich verwendet. So ist denkbar, dass ein Hersteller ein Gerät als «End of Life» deklariert, aber weiterhin Sicherheitsupdates vom Hersteller selbst oder vom FDA zur Verfügung gestellt werden. Diesem Aspekt ist folgendermassen Rechnung zu tragen (Änderungen kursiv markiert): «CPE müssen zeitnah mit vom Hersteller *oder den FDA* als kritisch eingestuften Sicherheitsupdates versorgt werden. *Werden die CPE nicht mehr vom Hersteller oder den FDA mit kritisch eingestuften Sicherheitsupdates versorgt*, müssen sie ausgetauscht werden.»

[1] Im aktuellen Entwurf ist die Meldung an die Nationale Alarmzentrale (NAZ) vorgesehen.

Internationale Standards konsequent berücksichtigen

Die Vorlage orientiert sich im Wesentlichen an Massnahmen, welche auch in anderen Ländern, insbesondere der EU, implementiert werden und basieren auf international anerkannten Sicherheitsnormen und -initiativen (z.B. ENISA, NESAS, 3GGP, EU 5G Toolbox, ISO). Indem auf eine nationale Sonderlösungen weitgehend verzichtet wird, können die Massnahmen effizient umgesetzt und die Sicherheitsstandards laufend den technischen Entwicklungen angepasst werden.

digitalswitzerland begrüsst dieses Vorgehen. Nun ist es wichtig, dass der Bund diesen Grundsatz auch bei den noch folgenden technischen Präzisierungen auf Stufe der technischen und administrativen Vorschriften (TAV) treu bleibt.

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
Deputy Managing Director digitalswitzerland

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

Fédération des Entreprises Romandes
FER Genève - FPE Bulle - UPCF Fribourg
FER Arcju - FER Neuchâtel - FER Valais

tp-secretariat@bakom.admin.ch

Département fédéral de
l'environnement, des transports, de
l'énergie et de la communication
(DETEC)
Palais fédéral Nord
3003 Berne

Madame Simonetta Sommaruga
Conseillère fédérale

Genève, le 18 mars 2022
DZ/3489 – FER No 07-2022

Modification de l'ordonnance sur les services de télécommunication (sécurité des informations et des infrastructures et services de télécommunication)

Madame la Conseillère fédérale,

Notre fédération vous remercie de l'avoir consultée dans le cadre de la modification citée en titre, dont elle a pris connaissance avec intérêt. Elle vous livre ci-après sa prise de position.

La FER salue l'approche et le travail effectué. Le contenu de cette procédure de consultation correspond à ce que l'on peut attendre du travail législatif, tant du point de vue de la gouvernance que des actions prévues, qui sont en adéquation avec la gestion du risque international dans son état actuel.

Notre fédération est alignée sur les actions techniques et organisationnelles proposées, telle la mise en place obligatoire des procédures de filtrage d'adresses IP pour les opérateurs, l'obligation de déclarer la mise en place d'un SGSI se basant sur les normes ISO, l'obligation de développer et maintenir une gestion des risques, la mise en place d'une gestion des incidents et de traçabilité des preuves, la garantie de la communication aussi bien aux instances de régulation (OFCOM, NCSC) qu'aux tiers impactés (clients) et la possibilité de déclencher des audits.

Tout cela correspond au niveau de maturité internationale, et n'attire pas de remarques détaillées de notre part. Cependant, il est nécessaire de relever l'apparition dans le texte d'approches que l'on peut considérer comme parallèles :

1) La cybermenace

Est-ce que la cybermenace est une affaire d'État ? Si tel est le cas, nous pourrions parler de la protection des technologies de l'information comme faisant partie de la souveraineté, car nécessaire à la vie des entreprises et considéré dès lors comme une richesse essentielle.

Selon notre lecture, les cybermenaces doivent être placées à la croisée de la population et du territoire et par ailleurs, attendre des fournisseurs d'accès internet (FAI) qu'ils couvrent le risque «d'une manière adéquate», ne sera pas suffisant. Par exemple, les cybermenaces dont sont victimes les PME, pourraient être mieux couvertes si l'on applique aux opérateurs de VPN certaines règles appliquées aux FAI.

Le mode de fonctionnement basé sur des VPN chiffrés dont les adresses IP sources changent régulièrement amène à ce que les mécanismes prévus par les FAI ne voient pas la menace ou la détecte une fois qu'elle est dans l'espace de communication interne à la Confédération. Les solutions point à point sans traçage des sources sont un avantage pour la cybercriminalité qu'il ne faudrait pas négliger.

La FER Genève en particulier apporte depuis des décennies son accompagnement et ses compétences au sein des PME, et le fait aussi désormais au travers d'un accompagnement de maturité Cyber qu'elle met en place actuellement.

Mais au regard des 500'000 entreprises existantes au sein de la Confédération et le temps nécessaire pour les sensibiliser aux cybermenaces, il faudrait un siècle pour augmenter leur maturité, alors qu'humainement parlant, nous ne l'avons pas.

2) Les cyberrisques ont plusieurs facettes

Le rapport explicatif montre clairement le niveau de maturité atteint et attendu, les prescriptions techniques et administratives en sont la preuve. Mais les infections subies par des environnements techniques de type CPE ne peut être effectuées que par des États ou des groupes criminels organisés et sont loin des menaces qui ciblent le tissu économique des entreprises. Outre la mise en évidence de la différence, c'est la prise en charge de toutes les facettes des cyberrisques qui permettra la résilience numérique.

3) La protection de la 5G

Les FAI étant déjà considérés comme des infrastructures critiques, la protection de la 5G et des objets connectés est un vaste chantier qui reste encore à baliser et nécessitera de l'omniprésence du législateur dans la durée, les objets connectés ne font que timidement leur apparition pour le moment.

Il faut retenir que la 5G n'est que le vecteur de propagation : elle permettrait l'augmentation du vol de données et le chantage uniquement si les objets connectés sont faillibles, mal configurés, ont des failles de sécurité potentielles ou leur système de sécurité est immature au regard du risque connu.

Tout cela rend l'exercice difficile et force le législateur à communiquer sur les méthodes de communication, le type de chiffrement, la protection adéquate et le niveau de sécurité attendu.

Vaste chantier qui dépasse clairement les limites fédérales, celle des fournisseurs d'accès et d'autres intermédiaires de communication et dont le débat se déplace au niveau des fournisseurs d'objets

connectés et de leur obligation, sans doute à travers des organes supra, tels l'IETF et leurs Best Current Practice, les accords de l'Organisation mondiale du commerce et de l'ENISA.

Cela étant dit, toutes considérations faites, l'adaptation de la loi notamment à travers l'article 96 semble à propos et bienvenue.

En conclusion, notre fédération soutient cette modification d'ordonnance sur les services de télécommunication.

En vous remerciant de l'attention que vous porterez à la présente, nous vous prions de croire, Madame la Conseillère fédérale, à l'expression de notre haute considération.

Blaise Matthey
Secrétaire général

Raoul Diez
Directeur Contrôle et Sécurité
FER Genève

FKS CSSP CSP

Frau Bundesrätin
Simonetta Sommaruga
Vorsteherin des Eidgenössischen Departements für Umwelt, Verkehr, Energie und Kommunikation UVEK
Bundeshaus Nord
3003 Bern

Zustellung per E-Mail an:
tp-secretariat@bakom.admin.ch

Bern, 30. September 20202 / PRP

Änderung der Verordnung über Fernmeldedienste (FDV)
Eröffnung des Vernehmlassungsverfahrens

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit Schreiben vom 3. Dezember 2021 haben Sie die Feuerwehr Koordination Schweiz (FKS) zur Stellungahme in titelerwähnter Sache eingeladen. Wir bedanken uns dafür und nehmen wie folgt Stellung.

Einleitung
Die Feuerwehr Koordination Schweiz begrüsst grundsätzlich den vorliegenden Entwurf zur Verordnung über Fernmeldedienste (FDV). Mit dem gewählten zweistufigen Vorgehen wird einerseits die unbefugte Manipulation von 5G-Fernmeldeanlagen bekämpft und es wird ein definiertes Sicherheitsniveau eingeführt. Andererseits wird in einer zweiten Etappe ein weiteres Massnahmenpaket erarbeitet, bei welchem die Härtung im Sinne der Stromversorgungssicherheit im Fokus stehen wird. Beide Vorhaben sind aus unserer Sicht wichtig und geeignet, um die Verfügbarkeit der immer wichtiger werdenden Mobilkommunikation der 5G Technologie sicherzustellen.

Wir weisen an dieser Stelle ausdrücklich darauf hin, dass sich die mobile Kommunikation der Blaulicht- und Sicherheitsorganisationen, mangels Vorhandenseins eines Systems für die mobile breitbandige Sicherheitskommunikation (MSK[1]), in wesentlichen Aspekten auf die Mobilfunksysteme der heutigen Anbieter stützen. Aktuell werden deutlich über 70% aller Notrufe über Mobiltelefone abgewickelt. Nebst den Notrufen sind die Ereignisorganisationen auf eine funktionierende Alarmierung über die Mobilnetze angewiesen. Vor allem die Milizfeuerwehren stützen sich - mangels Alternativen - auf die Alarmierung über die bestehenden Mobilfunknetze. Dementsprechend sind Betriebsunterbrüche in den Mobilnetzen möglichst zu vermeiden, da sie direkte Auswirkungen auf die Ereignisbewältigung der Blaulichtorganisationen haben.

[1] Vgl. Bundesgesetzüber den Bevölkerungsschutz und den Zivilschutz, Art. 20 «Mobiles breitbandiges Sicherheitskommunikationssystem» (Link)

Eine weitere Anspruchsgruppe sind die Betreiber von kritischen Infrastrukturen, welche aufgrund ihrer Kritikalität auf einen zuverlässigen und sicheren Betrieb der neuen Generation von Mobilfunknetzen angewiesen sind.
Wir regen an, dass die Alarmierungs- und Meldeprozesse detailliert zu beschreiben sind. Um die Bearbeitung und Verteilung der eingegangenen Störungsmeldungen zu verbessern, sieht die revidierte Verordnung vor, die Rolle der Nationalen Alarmzentrale (NAZ) zu stärken. Der Empfang von Meldungen über Cyberangriffe soll zu einer Kernaufgabe der NAZ werden, da sie eine sichere Informatikinfrastruktur und einen 24-Stunden-Betrieb unterhält. Die Schaffung eines Single Point of Contact (SPOC) ist zielführend, weil damit die Krisenbewältigung erleichtert wird.

Doch bestehen weitere Organisationen, die sich um Cyberangriffe kümmern. Es kann nicht sein, dass ausschliesslich das BAKOM von der NAZ über die gemeldeten Störungen informiert wird. So sind beispielsweise auch das National Cyber Security Center (NCSC), die Melde- und Analysestelle Informationssicherung (MELANI) sowie die kantonalen Notrufzentralen von Polizei, Feuerwehr und Sanität einzubinden. Deren Rolle im Gesamtprozess von Meldung- und Alarmierung im Bereich Cyber sind im Erläuternden Bericht aufzuführen.

Im Zusammenhang mit der Bedrohung kritischer Infrastrukturen durch Cyber-Angriffe von staatlicher Seite und deren Abwehr sind die Aufgaben der Armee aufzuzeigen und in die FDV zu integrieren. Die klassische Machtpolitik erlebt seit einigen Jahren eine Renaissance. Bereits heute setzen einige Staaten ihre Cybermittel regelmässig im Sinne eines "Kalten" Cyber-Krieges ein. Im Falle eines bewaffneten Konflikts in Europa ist mit einer breiten Verwendung dieser Mittel zu rechnen. Davon dürften auch Staaten, die an den eigentlichen Kampfhandlungen nicht beteiligt sind, betroffen sein. Die Armee hat in den vergangenen Jahren Schritte unternommen, sich auf ein solches Szenario vorzubereiten. So ist die Führungsunterstützungsbasis (FUB) im Bereich Verteidigung für Aktionsplanung, Lageverfolgung, Ereignisbewältigung und Ausbildung der Mitarbeitenden und AdA im Cyber-Raum verantwortlich. Mit der Weiterentwicklung der Armee (WEA) wurde zur Unterstützung der Berufsorganisation der FUB eine Cyber-Kompanie gebildet. Ab 2022 werden sämtliche Cyber Formationen der Schweizer Armee in das neu gegründete Cyber Bataillon 42 integriert. Die Rolle der Armee ist in der revidierten FDV zu berücksichtigen und ihre Verwendung zu beschreiben.

Der sofortigen Information an die kantonalen Notrufzentralen von Polizei, Feuerwehr und Sanität ist absolut notwendig. Nur sie können die Risiken von Beeinträchtigungen abschätzen und Sofortmassnahmen anordnen (bspw. die Umsetzung von Notfalltreffpunkten o.ä.). Entsprechend sind die Informationsprozesse in der FDV zu verankern.

Ergänzungen und Anpassungen
Wir beantragen die folgenden Anpassungen oder zum vorliegenden Entwurf der FDV:

Art. 96
Störungen im Mobilfunkbereich haben direkte Auswirkungen. So sind unter Umständen Notrufnummern nicht mehr erreichbar, oder die Einsatzkräfte von Polizei, Rettungsdienst und Feuerwehr sind aufgrund der nicht mehr vorhandenen Datenübertragungsmöglichkeiten in ihrem Handeln beeinträchtigt. In vielen Kantonen wurden inzwischen Notfalltreffpunkte installiert, welche bei Störungen im Kommunikationsbereich besetzt werden können. Dies setzt jedoch voraus, dass die kantonalen Notrufzentralen sofort und unverzüglich über Ausfälle, bereits im niederschwelligen Bereich, informiert werden. Die im Art. 96 formulierte Grösse von 30'000 Kundinnen und Kunden, welche von einem Ausfall betroffen sind, ist deutlich zu hoch gewählt. Zudem ist es wichtig, dass die Dauer von Störungen abgeschätzt werden kann. Aktuell gehen die Notruforganisationen davon aus, dass Störungen relevant sind, welche voraussichtlich mehr als 15 Minuten dauern und mindestens 1'000 Kundinnen und Kunden davon betroffen sind.

Eine Information an die NAZ, NCSC, MELANI, sowie nachgelagert an das BAKOM sind für die Nachbereitung der Störung wichtig. Die erwähnten Organe haben jedoch nur einen sekundären Einfluss auf die Behebung einer Störung oder der Bewältigung einer entsprechenden Lage. Dies obliegt primär den kantonalen Behörden, welche entsprechende Massnahmen sofort umsetzen können.

Es ist unklar, warum die Anzahl der betroffenen Kundinnen und Kunden nun auf Stufe FDV und nicht mehr in der TAV geregelt werden soll.

Antrag:

a) Die von einer potentiellen Störung betroffene Anzahl von Kundinnen und Kunden ist von 30'000 auf 1'000 Kundinnen oder Kunden zu senken, welche potentiell von einem Ausfall grösser als 15 Minuten betroffen sind.
b) In jedem Fall haben die Anbieterinnen von Fernmeldediensten ab einer Störungsgrösse von 1'000 Kundinnen und Kunden (+15 Minuten) die zuständigen kantonalen Notrufzentralen von Polizei, Sanität und Feuerwehr (112, 117, 118, 144) zu informieren, bevor die Meldungen an die NAZ (i.S. eines SPOC) oder weitere Organe abgesetzt werden.
c) Die Anzahl der betroffenen Kundinnen und Kunden soll weiterhin in der TAV geregelt werden und nicht auf Stufe FDV.

Art. 96a

Im Abs. 1 wird spezifisch und abschliessend von DDoS-Angriffen gesprochen. Aufgrund des technologischen schnellen Wandels ist es möglich, dass es zukünftig andere Arten von Angriffen geben kann, welche es zu berücksichtigen gilt.

Im Abs. 3 werden die Anbieterinnen von Internetzugängen berechtigt, Internetzugänge und Adressierungselemente, welche die Systeme beeinträchtigen, zu sperren oder einzuschränken. Sie dürfen die Massnahmen aufrechterhalten, solange die Bedrohung anhält. Die kann zu Unterbrüchen im Bereich der Notrufe führen und damit zu potentiellen Risiken für hilfsbedürftige Personen.

Antrag:

a) Abs. 1: Es soll im erwähnten Absatz nicht abschliessend von DDoS-Angriffen gesprochen werden, sondern die DDoS-Angriffe sind als Beispiel o.ä. aufzuführen.
b) Abs. 1: Die Details von potentiellen Angriffsmechanismen sollen nicht abschliessend in der FDV geregelt werden, sondern in den technisch- administrativen Vorschriften (TAV). Dies ermöglicht ein adäquates Handeln und ein relativ niederschwelliges Anpassen der zu berücksichtigenden Regelungen.
c) Abs. 3: Die Einschränkungen im Bedrohungsfall sollen sehr selektiv erfolgen und nur im Ausnahmefall dazu führen, dass keine Notrufnummern mehr über die betroffenen Anschlüsse gewählt werden können.
d) Abs. 3: Sind durch die Einschränkungen potentiell mehr als 1'000 Kundinnen und Kunden über die prognostizierte Dauer von mehr als 15 Minuten betroffen, sind die betroffenen kantonalen Notrufzentralen über die Einschränkungen zu informieren.

Art. 96f

Es wird im Abs. 2 definiert, dass der Betrieb der Netzwerkbetriebszentren und deren Sicherheitsbetriebszentren nebst der Schweiz im Europäischen Wirtschaftsraum und im Vereinigten Königreich stattfinden kann. Ist eine Betreiberin primär ausserhalb der Schweiz tätig, ist der operative und der juristische Durchgriff im Ereignisfall schwierig bis unmöglich. Nebst der schwierigen Erreichbarkeit im Ausland, ist auch die Priorisierung von Massnahmen und Ressourcen deutlich erschwert. Es wird angeregt, dass eine ständige Vertretung in der Schweiz gefordert wird.

Antrag:

a) Ein ständiger Firmensitz oder ein ständiger Ableger in der Schweiz ist unumgänglich und soll entsprechend in der FDV verankert werden.
b) Insbesondere beim Betrieb von sicherheitskritischen Fernmeldeanlagen ist dem ständigen Firmensitz oder einer ständigen Vertretung in der Schweiz ein hohes Gewicht beizumessen.

Ergänzende Rückmeldung
Wir erlauben uns an dieser Stelle noch auf eine weitere Pendenz hinzuweisen, welche in die vorliegende Revision der Verordnung einfliessen sollte.

In der vorliegenden Revision der FDV soll auch die Problematik des kostenpflichtigen Zuganges zur SOS-DB (NotDB), zukünftig LIS-Proxy, und der Nutzung der Dynamischen Leitweglenkung (DLWL) für die Notrufzentralen geregelt werden.

Dieses Bedürfnis wurde schon lange von Seiten der Notrufzentralen kommuniziert und soll nun einfliessen.

Aus diesem Grunde stellen wir die folgenden zusätzlichen Anträge, welche in die Revision einfliessen sollen oder zumindest für eine weitere Revision vorbereitet werden sollen:

1) Kostenlose Nutzung der DLWL für alle Notrufzentralen, inkl. der entsprechenden Verpflichtung der zuständigen Provider.
2) Kostenlose Nutzung der SOS-DB (zukünftig LIS-Proxy) für alle Notrufzentralen.

Wir danken nochmals für die Gelegenheit zur Stellungnahme, bitten um Berücksichtigung unserer Anliegen und stehen für weitere Auskünfte gerne zur Verfügung.

Freundliche Grüsse
Feuerwehr Koordination Schweiz FKS

MLaw Petra Prévôt
Generalsekretärin

GEBÄUDE
VERSICHERUNG ZUG

Gebäudeversicherung Zug, Grafenaustrasse 1, 6300 Zug

Per E-Mail tp-secretariat@bakom.admin.ch

Eidg. Departement für Umwelt,
Verkehr, Energie und
Kommunikation UVEK
Bundeshaus Nord
3003 Bern

T direkt +41 41 726 90 71
roland.faessler@zg.ch
Zug, 11. März 2022 FARL

Änderung der Verordnung über Fernmeldedienste (FDV)
Eröffnung des Vernehmlassungsverfahrens

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit Schreiben vom 10. November 2021 haben Sie die Feuerwehr Koordination Schweiz (FKS) zur Stellungahme in titelerwähnter Sache eingeladen. Als Mitglied der FKS nehmen wir betreffend die Änderung der Verordnung über Fernmeldedienste (FDV) wie folgt Stellung.

Einleitung
Die Gebäudeversicherung Zug begrüsst grundsätzlich den vorliegenden Entwurf zur Verordnung über Fernmeldedienste (FDV). Mit dem gewählten zweistufigen Vorgehen wird einerseits die unbefugte Manipulation von 5G-Fernmeldeanlagen bekämpft und es wird ein definiertes Sicherheitsniveau eingeführt. Andererseits wird in einer zweiten Etappe ein weiteres Massnahmenpaket erarbeitet, bei welchem die Härtung im Sinne der Stromversorgungssicherheit im Fokus stehen wird. Beide Vorhaben sind aus unserer Sicht wichtig und geeignet, um die Verfügbarkeit der immer wichtiger werdenden Mobilkommunikation der 5G Technologie sicherzustellen.

Wir weisen an dieser Stelle ausdrücklich darauf hin, dass sich die mobile Kommunikation der Blaulicht- und Sicherheitsorganisationen, mangels Vorhandenseins eines Systems für die mobile breitbandige Sicherheitskommunikation (MSK[1]), in wesentlichen Aspekten auf die Mobilfunksysteme der heutigen Anbieter stützen. Aktuell werden deutlich über 70% aller Notrufe über Mobiltelefone abgewickelt. Nebst den Notrufen sind die Ereignisorganisationen auf eine funktionierende Alarmierung über die Mobilnetze angewiesen. Vor allem die Milizfeuerwehren stützen sich - mangels Alternativen - auf die Alarmierung über die bestehenden Mobilfunk-

[1] Vgl. Bundesgesetzüber den Bevölkerungsschutz und den Zivilschutz, Art. 20 «Mobiles breitbandiges Sicherheitskommunikationssystem» (Link)

netze. Dementsprechend sind Betriebsunterbrüche in den Mobilnetzen möglichst zu vermeiden, da sie direkte Auswirkungen auf die Ereignisbewältigung der Blaulichtorganisationen haben.

Eine weitere Anspruchsgruppe sind die Betreiber von kritischen Infrastrukturen, welche aufgrund ihrer Kritikalität auf einen zuverlässigen und sicheren Betrieb der neuen Generation von Mobilfunknetzen angewiesen sind.
Wir regen an, dass die Alarmierungs- und Meldeprozesse detailliert zu beschreiben sind. Um die Bearbeitung und Verteilung der eingegangenen Störungsmeldungen zu verbessern, sieht die revidierte Verordnung vor, die Rolle der Nationalen Alarmzentrale (NAZ) zu stärken. Der Empfang von Meldungen über Cyberangriffe soll zu einer Kernaufgabe der NAZ werden, da sie eine sichere Informatikinfrastruktur und einen 24-Stunden-Betrieb unterhält. Die Schaffung eines Single Point of Contact (SPOC) ist zielführend, weil damit die Krisenbewältigung erleichtert wird.

Zusätzlich kümmern sich weitere Organisationen um Cyberangriffe. Dabei soll jedoch nicht ausschliesslich das BAKOM von der NAZ über die gemeldeten Störungen informiert werden, sondern beispielsweise auch das National Cyber Security Center (NCSC), die Melde- und Analysestelle Informationssicherung (MELANI) sowie die kantonalen Notrufzentralen von Polizei, Feuerwehr und Sanität eingebunden werden. Deren Rolle im Gesamtprozess von Meldung- und Alarmierung im Bereich Cyber sind im Erläuternden Bericht aufzuführen.

Im Zusammenhang mit der Bedrohung kritischer Infrastrukturen durch Cyber-Angriffe von staatlicher Seite und deren Abwehr sind die Aufgaben der Armee aufzuzeigen und in die FDV zu integrieren. Die klassische Machtpolitik erlebt seit einigen Jahren eine Renaissance. Bereits heute setzen einige Staaten ihre Cybermittel regelmässig im Sinne eines "Kalten" Cyber-Krieges ein. Im Falle eines bewaffneten Konflikts in Europa ist mit einer breiten Verwendung dieser Mittel zu rechnen. Davon dürften auch Staaten, die an den eigentlichen Kampfhandlungen nicht beteiligt sind, betroffen sein. Die Armee hat in den vergangenen Jahren Schritte unternommen, sich auf ein solches Szenario vorzubereiten. So ist die Führungsunterstützungsbasis (FUB) im Bereich Verteidigung für Aktionsplanung, Lageverfolgung, Ereignisbewältigung und Ausbildung der Mitarbeitenden und AdA im Cyber-Raum verantwortlich. Mit der Weiterentwicklung der Armee (WEA) wurde zur Unterstützung der Berufsorganisation der FUB eine Cyber-Kompanie gebildet. Ab 2022 werden sämtliche Cyber Formationen der Schweizer Armee in das neu gegründete Cyber Bataillon 42 integriert. Die Rolle der Armee ist in der revidierten FDV zu berücksichtigen und ihre Verwendung zu beschreiben.

Der sofortigen Information an die kantonalen Notrufzentralen von Polizei, Feuerwehr und Sanität ist absolut notwendig. Nur sie können die Risiken von Beeinträchtigungen abschätzen und Sofortmassnahmen anordnen (bspw. die Umsetzung von Notfalltreffpunkten o.ä.). Entsprechend sind die Informationsprozesse in der FDV zu verankern.

Ergänzungen und Anpassungen
Wir beantragen die folgenden Anpassungen oder zum vorliegenden Entwurf der FDV:

Art. 96
Störungen im Mobilfunkbereich haben direkte Auswirkungen. So sind unter Umständen Notrufnummern nicht mehr erreichbar, oder die Einsatzkräfte von Polizei, Rettungsdienst und Feuerwehr sind aufgrund der nicht mehr vorhandenen Datenübertragungsmöglichkeiten in ihrem Handeln beeinträchtigt. In vielen Kantonen wurden inzwischen Notfalltreffpunkte installiert, welche bei Störungen im Kommunikationsbereich besetzt werden können. Dies setzt jedoch voraus, dass die kantonalen Notrufzentralen sofort und unverzüglich über Ausfälle, bereits im niederschwelligen Bereich, informiert werden. Die im Art. 96 formulierte Grösse von 30'000 Kundinnen und Kunden, welche von einem Ausfall betroffen sind, ist deutlich zu hoch gewählt. Zudem ist es wichtig, dass die Dauer von Störungen abgeschätzt werden kann. Aktuell gehen die Notruforganisationen davon aus, dass Störungen relevant sind, welche voraussichtlich mehr als 15 Minuten dauern und mindestens 1'000 Kundinnen und Kunden davon betroffen sind.

Eine Information an die NAZ, NCSC, MELANI, sowie nachgelagert an das BAKOM sind für die Nachbereitung der Störung wichtig. Die erwähnten Organe haben jedoch nur einen sekundären Einfluss auf die Behebung einer Störung oder der Bewältigung einer entsprechen-den Lage. Dies obliegt primär den kantonalen Behörden, welche entsprechende Massnahmen sofort umsetzen können.

Es ist unklar, warum die Anzahl der betroffenen Kundinnen und Kunden nun auf Stufe FDV und nicht mehr in der TAV geregelt werden soll.

Antrag:

a) Die von einer potentiellen Störung betroffene Anzahl von Kundinnen und Kunden ist von 30'000 auf 1'000 Kundinnen oder Kunden zu senken, welche potentiell von einem Ausfall grösser als 15 Minuten betroffen sind.
b) In jedem Fall haben die Anbieterinnen von Fernmeldediensten ab einer Störungsgrösse von 1'000 Kundinnen und Kunden (>15 Minuten) die zuständigen kantonalen Notrufzentralen von Polizei, Sanität und Feuerwehr (112, 117, 118, 144) zu informieren, bevor die Meldungen an die NAZ (i.S. eines SPOC) oder weitere Organe abgesetzt werden.
c) Die Anzahl der betroffenen Kundinnen und Kunden soll weiterhin in der TAV geregelt werden und nicht auf Stufe FDV.

Art. 96a
Im Abs. 1 wird spezifisch und abschliessend von DDoS-Angriffen gesprochen. Aufgrund des technologischen schnellen Wandels ist es möglich, dass es zukünftig andere Arten von Angriffen geben kann, welche es zu berücksichtigen gilt.

Im Abs. 3 werden die Anbieterinnen von Internetzugängen berechtigt, Internetzugänge und Adressierungselemente, welche die Systeme beeinträchtigen, zu sperren oder einzuschränken. Sie dürfen die Massnahmen aufrechterhalten, solange die Bedrohung anhält. Die kann zu Unterbrüchen im Bereich der Notrufe führen und damit zu potentiellen Risiken für hilfsbedürftige Personen.

Antrag:
a) Abs. 1: Es soll im erwähnten Absatz nicht abschliessend von DDoS-Angriffen gesprochen werden, sondern die DDoS-Angriffe sind als Beispiel o.ä. aufzuführen.
b) Abs. 1: Die Details von potentiellen Angriffsmechanismen sollen nicht abschliessend in der FDV geregelt werden, sondern in den technisch- administrativen Vorschriften (TAV). Dies ermöglicht ein adäquates Handeln und ein relativ niederschwelliges Anpassen der zu berücksichtigenden Regelungen.
c) Abs. 3: Die Einschränkungen im Bedrohungsfall sollen sehr selektiv erfolgen und nur im Ausnahmefall dazu führen, dass keine Notrufnummern mehr über die betroffenen Anschlüsse gewählt werden können.
d) Abs. 3: Sind durch die Einschränkungen potentiell mehr als 1'000 Kundinnen und Kunden über die prognostizierte Dauer von mehr als 15 Minuten betroffen, sind die betroffenen kantonalen Notrufzentralen über die Einschränkungen zu informieren.

Art. 96f
Es wird im Abs. 2 definiert, dass der Betrieb der Netzwerkbetriebszentren und deren Sicherheitsbetriebszentren nebst der Schweiz im Europäischen Wirtschaftsraum und im Vereinigten Königreich stattfinden kann. Ist eine Betreiberin primär ausserhalb der Schweiz tätig, ist der operative und der juristische Durchgriff im Ereignisfall schwierig bis unmöglich. Nebst der schwierigen Erreichbarkeit im Ausland, ist auch die Priorisierung von Massnahmen und Ressourcen deutlich erschwert. Es wird angeregt, dass eine ständige Vertretung in der Schweiz gefordert wird.

Antrag:
a) Ein ständiger Firmensitz oder ein ständiger Ableger in der Schweiz ist unumgänglich und soll entsprechend in der FDV verankert werden.
b) Insbesondere beim Betrieb von sicherheitskritischen Fernmeldeanlagen ist dem ständigen Firmensitz oder einer ständigen Vertretung in der Schweiz ein hohes Gewicht beizumessen.

Ergänzende Rückmeldung
Wir erlauben uns an dieser Stelle noch auf eine weitere Pendenz hinzuweisen, welche in die vorliegende Revision der Verordnung einfliessen sollte.

In der vorliegenden Revision der FDV soll auch die Problematik des kostenpflichtigen Zuganges zur SOS-DB (NotDB), zukünftig LIS-Proxy, und der Nutzung der Dynamischen Leitweglenkung (DLWL) für die Notrufzentralen geregelt werden.

Dieses Bedürfnis wurde schon lange von Seiten der Notrufzentralen kommuniziert und soll nun einfliessen.

Aus diesem Grunde stellen wir die folgenden zusätzlichen Anträge, welche in die Revision einfliessen sollen oder zumindest für eine weitere Revision vorbereitet werden sollen:

1) Kostenlose Nutzung der DLWL für alle Notrufzentralen, inkl. der entsprechenden Verpflichtung der zuständigen Provider.
2) Kostenlose Nutzung der SOS-DB (zukünftig LIS-Proxy) für alle Notrufzentralen.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme, bitten um Berücksichtigung unserer Anliegen und stehen für weitere Auskünfte gerne zur Verfügung.

Freundliche Grüsse
Gebäudeversicherung Zug

Richard Schärer
Direktor GVZG

Roland Fässler
Leiter Abteilung Feuerwehr / Feuerwehrinspektor

Bahnhofstrasse 55
5000 Aarau
Telefon 031 320 11 44
www.144.ch

interverband für rettungswesen
interassociation de sauvetage
interassociazione di salvataggio

Frau Bundesrätin
Simonetta Sommaruga
Vorsteherin des Eidgenössischen Departements für Umwelt, Verkehr, Energie und Kommunikation (UVEK)
Bundeshaus Nord
3003 Bern

Zustellung per Mail an:
Bundesamt für Kommunikation (BAKOM)
Zukunftsstrasse 44
2501 Biel
Per E-Mail: tp-secretariat@bakom.admin.ch

Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten)
Eröffnung des Vernehmlassungsverfahrens

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit Schreiben vom 3. Dezember 2021 haben Sie den Interverband für Rettungswesen – IVR eingeladen, zum titelerwähnten Verordnungsentwurf Stellung zu nehmen. Wir bedanken uns für diese Möglichkeit und erlauben uns, folgend Bemerkungen anzufügen und Anträge zu formulieren.

Einleitung
Der Interverband für Rettungswesen begrüsst grundsätzlich den vorliegenden Entwurf zur Verordnung über Fernmeldedienste (FDV). Mit dem gewählten zweistufigen Vorgehen wird einerseits die unbefugte Manipulation von 5G-Fernmeldeanlagen bekämpft und es wird ein definiertes Sicherheitsniveau eingeführt. Andererseits wird in einer zweiten Etappe ein weiteres Massnahmenpaket erarbeitet, bei welchem die Härtung im Sinne der Stromversorgungssicherheit im Fokus stehen wird. Beide Vorhaben sind aus unserer Sicht wichtig und geeignet, um die Verfügbarkeit der immer wichtiger werdenden Mobilkommunikation der 5G Technologie sicherzustellen.

Wir weisen an dieser Stelle ausdrücklich darauf hin, dass sich die mobile Kommunikation der Blaulicht- und Sicherheitsorganisationen, mangels Vorhandenseins eines Systems für die mobile breitbandige Sicherheitskommunikation (MSK[1]), in wesentlichen Aspekten auf die Mobilfunksysteme der heutigen Anbieter stützen. Aktuell werden deutlich über 70% aller Notrufe über Mobiltelefone abgewickelt. Nebst den Notrufen sind die Ereignisorganisationen auf eine funktionierende Alarmierung über die Mobilnetze angewiesen. Vor allem die Milizfeuerwehren stützen sich - mangels Alternativen - auf die Alarmierung über die bestehenden Mobilfunknetze. Dementsprechend sind Betriebsunterbrüche in den

[1] Vgl. Bundesgesetzüber den Bevölkerungsschutz und den Zivilschutz, Art. 20 «Mobiles breitbandiges Sicherheitskommunikationssystem» (Link)

Bahnhofstrasse 55
5000 Aarau
Telefon 031 320 11 44
www.144.ch

Mobilnetzen möglichst zu vermeiden, da sie direkte Auswirkungen auf die Ereignisbewältigung der Blaulichtorganisationen haben.

Eine weitere Anspruchsgruppe sind die Betreiber von kritischen Infrastrukturen, welche aufgrund ihrer Kritikalität auf einen zuverlässigen und sicheren Betrieb der neuen Generation von Mobilfunknetzen angewiesen sind.

Wir regen an, dass die Alarmierungs- und Meldeprozesse detailliert zu beschreiben sind. Um die Bearbeitung und Verteilung der eingegangenen Störungsmeldungen zu verbessern, sieht die revidierte Verordnung vor, die Rolle der Nationalen Alarmzentrale (NAZ) zu stärken. Der Empfang von Meldungen über Cyberangriffe soll zu einer Kernaufgabe der NAZ werden, da sie eine sichere Informatikinfrastruktur und einen 24-Stunden-Betrieb unterhält. Die Schaffung eines Single Point of Contact (SPOC) ist zielführend, weil damit die Krisenbewältigung erleichtert wird.

Doch bestehen weitere Organisationen, die sich um Cyberangriffe kümmern. Es kann nicht sein, dass ausschliesslich das BAKOM von der NAZ über die gemeldeten Störungen informiert wird. So sind beispielsweise auch das National Cyber Security Center (NCSC), die Melde- und Analysestelle Informationssicherung (MELANI) sowie die kantonalen Notrufzentralen von Polizei, Feuerwehr und Sanität einzubinden. Deren Rolle im Gesamtprozess von Meldung- und Alarmierung im Bereich Cyber sind im Erläuternden Bericht aufzuführen.

Im Zusammenhang mit der Bedrohung kritischer Infrastrukturen durch Cyber-Angriffe von staatlicher Seite und deren Abwehr sind die Aufgaben der Armee aufzuzeigen und in die FDV zu integrieren. Die klassische Machtpolitik erlebt seit einigen Jahren eine Renaissance. Bereits heute setzen einige Staaten ihre Cybermittel regelmässig im Sinne eines "Kalten" Cyber-Krieges ein. Im Falle eines bewaffneten Konflikts in Europa ist mit einer breiten Verwendung dieser Mittel zu rechnen. Davon dürften auch Staaten, die an den eigentlichen Kampfhandlungen nicht beteiligt sind, betroffen sein. Die Armee hat in den vergangenen Jahren Schritte unternommen, sich auf ein solches Szenario vorzubereiten. So ist die Führungsunterstützungsbasis (FUB) im Bereich Verteidigung für Aktionsplanung, Lageverfolgung, Ereignisbewältigung und Ausbildung der Mitarbeitenden und AdA im Cyber-Raum verantwortlich. Mit der Weiterentwicklung der Armee (WEA) wurde zur Unterstützung der Berufsorganisation der FUB eine Cyber-Kompanie gebildet. Ab 2022 werden sämtliche Cyber Formationen der Schweizer Armee in das neu gegründete Cyber Bataillon 42 integriert. Die Rolle der Armee ist in der revidierten FDV zu berücksichtigen und ihre Verwendung zu beschreiben.

Der sofortigen Information an die kantonalen Notrufzentralen von Polizei, Feuerwehr und Sanität ist ein hohes Gewicht beizumessen. Nur sie können die Risiken von Beeinträchtigungen abschätzen und Sofortmassnahmen anordnen (bspw. die Umsetzung von Notfalltreffpunkten o.ä.). Entsprechend sind die Informationsprozesse in der FDV zu verankern.

Ergänzungen und Anpassungen
Wir beantragen die folgenden Anpassungen oder zum vorliegenden Entwurf der FDV:

Art. 96
Störungen im Mobilfunkbereich haben direkte Auswirkungen. So sind unter Umständen Notrufnummern nicht mehr erreichbar, oder die Einsatzkräfte von Polizei, Rettungsdienst und Feuerwehr sind aufgrund der nicht mehr vorhandenen Datenübertragungsmöglichkeiten in ihrem Handeln beeinträchtigt. In vielen Kantonen wurden inzwischen Notfalltreffpunkte

Bahnhofstrasse 55
5000 Aarau
Telefon 031 320 11 44
www.144.ch

installiert, welche bei Störungen im Kommunikationsbereich besetzt werden können. Dies setzt jedoch voraus, dass die kantonalen Notrufzentralen sofort und unverzüglich über Ausfälle, bereits im niederschwelligen Bereich, informiert werden. Die im Art. 96 formulierte Grösse von 30'000 Kundinnen und Kunden, welche von einem Ausfall betroffen sind, ist deutlich zu hoch gewählt. Zudem ist es wichtig, dass die Dauer von Störungen abgeschätzt werden kann. Aktuell gehen die Notruforganisationen davon aus, dass Störungen relevant sind, welche voraussichtlich mehr als 15 Minuten dauern und mindestens 1'000 Kundinnen und Kunden davon betroffen sind.

Eine Information an die NAZ, NCSC, MELANI, sowie nachgelagert an das BAKOM sind für die Nachbereitung der Störung wichtig. Die erwähnten Organe haben jedoch nur einen sekundären Einfluss auf die Behebung einer Störung oder der Bewältigung einer entsprechenden Lage. Dies obliegt primär den kantonalen Behörden, welche entsprechende Massnahmen sofort umsetzen können.

Es ist unklar, warum die Anzahl der betroffenen Kundinnen und Kunden nun auf Stufe FDV und nicht mehr in der TAV geregelt werden soll.

Antrag:

a) Die von einer potentiellen Störung betroffene Anzahl von Kundinnen und Kunden ist von 30'000 auf 1'000 Kundinnen oder Kunden zu senken, welche potentiell von einem Ausfall grösser als 15 Minuten betroffen sind.
b) In jedem Fall haben die Anbieterinnen von Fernmeldediensten ab einer Störungsgrösse von 1'000 Kundinnen und Kunden (+15 Minuten) die zuständigen kantonalen Notrufzentralen von Polizei, Sanität und Feuerwehr (112, 117, 118, 144) zu informieren, bevor die Meldungen an die NAZ (i.S. eines SPOC) oder weitere Organe abgesetzt werden.
c) Die Anzahl der betroffenen Kundinnen und Kunden soll weiterhin in der TAV geregelt werden und nicht auf Stufe FDV.

Art. 96a

Im Abs. 1 wird spezifisch und abschliessend von DDoS-Angriffen gesprochen. Aufgrund des technologischen schnellen Wandels ist es möglich, dass es zukünftig andere Arten von Angriffen geben kann, welche es zu berücksichtigen gilt.

Im Abs. 3 werden die Anbieterinnen von Internetzugängen berechtigt, Internetzugänge und Adressierungselemente, welche die Systeme beeinträchtigen, zu sperren oder einzuschränken. Sie dürfen die Massnahmen aufrechterhalten, solange die Bedrohung anhält. Die kann zu Unterbrüchen im Bereich der Notrufe führen und damit zu potentiellen Risiken für hilfsbedürftige Personen.

Antrag:

a) Abs. 1: Es soll im erwähnten Absatz nicht abschliessend von DDoS-Angriffen gesprochen werden, sondern die DDoS-Angriffe sind als Beispiel o.ä. aufzuführen.
b) Abs. 1: Die Details von potentiellen Angriffsmechanismen sollen nicht abschliessend in der FDV geregelt werden, sondern in den technisch- administrativen Vorschriften (TAV). Dies ermöglicht ein adäquates Handeln und ein relativ niederschwelliges Anpassen der zu berücksichtigenden Regelungen.
c) Abs. 3: Die Einschränkungen im Bedrohungsfall sollen sehr selektiv erfolgen und nur im Ausnahmefall dazu führen, dass keine Notrufnummern mehr über die betroffenen Anschlüsse gewählt werden können.
d) Abs. 3: Sind durch die Einschränkungen potentiell mehr als 1'000 Kundinnen und Kunden über die prognostizierte Dauer von mehr als 15 Minuten betroffen, sind die betroffenen kantonalen Notrufzentralen über die Einschränkungen zu informieren.

Bahnhofstrasse 55
5000 Aarau

Telefon 031 320 11 44
www.144.ch

interverband für rettungswesen
interassociation de sauvetage
interassociazione di salvataggio

Art. 96f
Es wird im Abs. 2 definiert, dass der Betrieb der Netzwerkbetriebszentren und deren Sicherheitsbetriebszentren nebst der Schweiz im Europäischen Wirtschaftsraum und im Vereinigten Königreich stattfinden kann. Ist eine Betreiberin primär ausserhalb der Schweiz tätig, ist der operative und der juristische Durchgriff im Ereignisfall schwierig bis unmöglich. Nebst der schwierigen Erreichbarkeit im Ausland, ist auch die Priorisierung von Massnahmen und Ressourcen deutlich erschwert. Es wird angeregt, dass eine ständige Vertretung in der Schweiz gefordert wird.

Antrag:

a) Ein ständiger Firmensitz oder ein ständiger Ableger in der Schweiz ist unumgänglich und soll entsprechend in der FDV verankert werden.
b) Insbesondere beim Betrieb von sicherheitskritischen Fernmeldeanlagen ist dem ständigen Firmensitz oder einer ständigen Vertretung in der Schweiz ein hohes Gewicht beizumessen.

Ergänzende Rückmeldung
Wir erlauben uns an dieser Stelle noch auf eine weitere Pendenz hinzuweisen, welche in die vorliegende Revision der Verordnung einfliessen sollte.

In der vorliegenden Revision der FDV soll auch die Problematik des kostenpflichtigen Zuganges zur SOS-DB (NotDB), zukünftig LIS-Proxy, und der Nutzung der Dynamischen Leitweglenkung (DLWL) für die Notrufzentralen geregelt werden.

Dieses Bedürfnis wurde schon lange von Seiten der Notrufzentralen kommuniziert und soll nun einfliessen.

Aus diesem Grunde stellen wir die folgenden zusätzlichen Anträge, welche in die Revision einfliessen sollen oder zumindest für eine weitere Revision vorbereitet werden sollen:

1) Kostenlose Nutzung der DLWL für alle Notrufzentralen, inkl. der entsprechenden Verpflichtung der zuständigen Provider.
2) Kostenlose Nutzung der SOS-DB (zukünftig LIS-Proxy) für alle Notrufzentralen.

Wir bedanken uns für die Prüfung unserer Anliegen. Gerne stehen wir oder das Gremium Notrufe für weitere Auskünfte zur Verfügung.

Freundliche Grüsse

Roman Wüst

Präsident Interverband für Rettungswesen

Justiz-, Polizei- und Militärdepartement

KANTON
APPENZELL INNERRHODEN

Kantonspolizei
Unteres Ziel 20
9050 Appenzell
Telefon +41 71 788 94 62
roman.brunner@kapo.ai.ch
https://www.ai.ch

Frau Bundesrätin
Simonetta Sommaruga
Vorsteherin des Eidgenössischen Departements für Umwelt, Verkehr, Energie und Kommunikation (UVEK)
Bundeshaus Nord
3003 Bern

Zustellung per Mail an:
Bundesamt für Kommunikation (BAKOM)
Zukunftsstrasse 44
2501 Biel
Per E-Mail: tp-secretariat@bakom.admin.ch

Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten)
Eröffnung des Vernehmlassungsverfahrens

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit Schreiben vom 3. Dezember 2021 haben Sie die Kantonspolizei Appenzell Innerrhoden eingeladen, zum titelerwähnten Verordnungsentwurf Stellung zu nehmen. Wir bedanken uns für diese Möglichkeit und erlauben uns, folgend Bemerkungen anzufügen und Anträge zu formulieren.

Einleitung
Die Kantonspolizei Appenzell Innerrhoden begrüsst grundsätzlich den vorliegenden Entwurf zur Verordnung über Fernmeldedienste (FDV). Mit dem gewählten zweistufigen Vorgehen wird einerseits die unbefugte Manipulation von 5G-Fernmeldeanlagen bekämpft und es wird ein definiertes Sicherheitsniveau eingeführt. Andererseits wird in einer zweiten Etappe ein weiteres Massnahmenpaket erarbeitet, bei welchem die Härtung im Sinne der Stromversorgungssicherheit im Fokus stehen wird. Beide Vorhaben sind aus unserer Sicht wichtig und geeignet, um die Verfügbarkeit der immer wichtiger werdenden Mobilkommunikation der 5G Technologie sicherzustellen.

Wir weisen an dieser Stelle ausdrücklich darauf hin, dass sich die mobile Kommunikation der Blaulicht- und Sicherheitsorganisationen, mangels Vorhandenseins eines Systems für die mobile breitbandige Sicherheitskommunikation (MSK[1]), in wesentlichen Aspekten auf die

[1] Vgl. Bundesgesetzüber den Bevölkerungsschutz und den Zivilschutz, Art. 20 «Mobiles breitbandiges Sicherheitskommunikationssystem» (Link)

Mobilfunksysteme der heutigen Anbieter stützen. Aktuell werden deutlich über 70% aller Notrufe über Mobiltelefone abgewickelt. Nebst den Notrufen sind die Ereignisorganisationen auf eine funktionierende Alarmierung über die Mobilnetze angewiesen. Vor allem die Milizfeuerwehren stützen sich - mangels Alternativen - auf die Alarmierung über die bestehenden Mobilfunknetze. Dementsprechend sind Betriebsunterbrüche in den Mobilnetzen möglichst zu vermeiden, da sie direkte Auswirkungen auf die Ereignisbewältigung der Blaulichtorganisationen haben.

Eine weitere Anspruchsgruppe sind die Betreiber von kritischen Infrastrukturen, welche aufgrund ihrer Kritikalität auf einen zuverlässigen und sicheren Betrieb der neuen Generation von Mobilfunknetzen angewiesen sind.

Wir regen an, dass die Alarmierungs- und Meldeprozesse detailliert zu beschreiben sind. Um die Bearbeitung und Verteilung der eingegangenen Störungsmeldungen zu verbessern, sieht die revidierte Verordnung vor, die Rolle der Nationalen Alarmzentrale (NAZ) zu stärken. Der Empfang von Meldungen über Cyberangriffe soll zu einer Kernaufgabe der NAZ werden, da sie eine sichere Informatikinfrastruktur und einen 24-Stunden-Betrieb unterhält. Die Schaffung eines Single Point of Contact (SPOC) ist zielführend, weil damit die Krisenbewältigung erleichtert wird.

Doch bestehen weitere Organisationen, die sich um Cyberangriffe kümmern. Es kann nicht sein, dass ausschliesslich das BAKOM von der NAZ über die gemeldeten Störungen informiert wird. So sind beispielsweise auch das National Cyber Security Center (NCSC), die Melde- und Analysestelle Informationssicherung (MELANI) sowie die kantonalen Notrufzentralen von Polizei, Feuerwehr und Sanität einzubinden. Deren Rolle im Gesamtprozess von Meldung- und Alarmierung im Bereich Cyber sind im Erläuternden Bericht aufzuführen.

Im Zusammenhang mit der Bedrohung kritischer Infrastrukturen durch Cyber-Angriffe von staatlicher Seite und deren Abwehr sind die Aufgaben der Armee aufzuzeigen und in die FDV zu integrieren. Die klassische Machtpolitik erlebt seit einigen Jahren eine Renaissance. Bereits heute setzen einige Staaten ihre Cybermittel regelmässig im Sinne eines "Kalten" Cyber-Krieges ein. Im Falle eines bewaffneten Konflikts in Europa ist mit einer breiten Verwendung dieser Mittel zu rechnen. Davon dürften auch Staaten, die an den eigentlichen Kampfhandlungen nicht beteiligt sind, betroffen sein. Die Armee hat in den vergangenen Jahren Schritte unternommen, sich auf ein solches Szenario vorzubereiten. So ist die Führungsunterstützungsbasis (FUB) im Bereich Verteidigung für Aktionsplanung, Lageverfolgung, Ereignisbewältigung und Ausbildung der Mitarbeitenden und AdA im Cyber-Raum verantwortlich. Mit der Weiterentwicklung der Armee (WEA) wurde zur Unterstützung der Berufsorganisation der FUB eine Cyber-Kompanie gebildet. Ab 2022 werden sämtliche Cyber Formationen der Schweizer Armee in das neu gegründete Cyber Bataillon 42 integriert. Die Rolle der Armee ist in der revidierten FDV zu berücksichtigen und ihre Verwendung zu beschreiben.

Der sofortigen Information an die kantonalen Notrufzentralen von Polizei, Feuerwehr und Sanität ist absolut notwendig. Nur sie können die Risiken von Beeinträchtigungen abschätzen und Sofortmassnahmen anordnen (bspw. die Umsetzung von Notfalltreffpunkten o.ä.). Entsprechend sind die Informationsprozesse in der FDV zu verankern.

Ergänzungen und Anpassungen
Wir beantragen die folgenden Anpassungen oder zum vorliegenden Entwurf der FDV:

Art. 96
Störungen im Mobilfunkbereich haben direkte Auswirkungen. So sind unter Umständen Notrufnummern nicht mehr erreichbar, oder die Einsatzkräfte von Polizei, Rettungsdienst und Feuerwehr sind aufgrund der nicht mehr vorhandenen Datenübertragungsmöglichkeiten in ihrem Handeln beeinträchtigt. In vielen Kantonen wurden inzwischen Notfalltreffpunkte installiert, welche bei Störungen im Kommunikationsbereich besetzt werden können.

Dies setzt jedoch voraus, dass die kantonalen Notrufzentralen sofort und unverzüglich über Ausfälle, bereits im niederschwelligen Bereich, informiert werden. Die im Art. 96 formulierte Grösse von 30'000 Kundinnen und Kunden, welche von einem Ausfall betroffen sind, ist deutlich zu hoch gewählt. Zudem ist es wichtig, dass die Dauer von Störungen abgeschätzt werden kann. Aktuell gehen die Notruforganisationen davon aus, dass Störungen relevant sind, welche voraussichtlich mehr als 15 Minuten dauern und mindestens 1'000 Kundinnen und Kunden davon betroffen sind.

Eine Information an die NAZ, NCSC, MELANI, sowie nachgelagert an das BAKOM sind für die Nachbereitung der Störung wichtig. Die erwähnten Organe haben jedoch nur einen sekundären Einfluss auf die Behebung einer Störung oder der Bewältigung einer entsprechenden Lage. Dies obliegt primär den kantonalen Behörden, welche entsprechende Massnahmen sofort umsetzen können.

Es ist unklar, warum die Anzahl der betroffenen Kundinnen und Kunden nun auf Stufe FDV und nicht mehr in der TAV geregelt werden soll.

Antrag:

a) Die von einer potentiellen Störung betroffene Anzahl von Kundinnen und Kunden ist von 30'000 auf 1'000 Kundinnen oder Kunden zu senken, welche potentiell von einem Ausfall grösser als 15 Minuten betroffen sind.
b) In jedem Fall haben die Anbieterinnen von Fernmeldediensten ab einer Störungsgrösse von 1'000 Kundinnen und Kunden (+15 Minuten) die zuständigen kantonalen Notrufzentralen von Polizei, Sanität und Feuerwehr (112, 117, 118, 144) zu informieren, bevor die Meldungen an die NAZ (i.S. eines SPOC) oder weitere Organe abgesetzt werden.
c) Die Anzahl der betroffenen Kundinnen und Kunden soll weiterhin in der TAV geregelt werden und nicht auf Stufe FDV.

Art. 96a

Im Abs. 1 wird spezifisch und abschliessend von DDoS-Angriffen gesprochen. Aufgrund des technologischen schnellen Wandels ist es möglich, dass es zukünftig andere Arten von Angriffen geben kann, welche es zu berücksichtigen gilt.

Im Abs. 3 werden die Anbieterinnen von Internetzugängen berechtigt, Internetzugänge und Adressierungselemente, welche die Systeme beeinträchtigen, zu sperren oder einzuschränken. Sie dürfen die Massnahmen aufrechterhalten, solange die Bedrohung anhält. Die kann zu Unterbrüchen im Bereich der Notrufe führen und damit zu potentiellen Risiken für hilfsbedürftige Personen.

Antrag:

a) Abs. 1: Es soll im erwähnten Absatz nicht abschliessend von DDoS-Angriffen gesprochen werden, sondern die DDoS-Angriffe sind als Beispiel o.ä. aufzuführen.
b) Abs. 1: Die Details von potentiellen Angriffsmechanismen sollen nicht abschliessend in der FDV geregelt werden, sondern in den technisch- administrativen Vorschriften (TAV). Dies ermöglicht ein adäquates Handeln und ein relativ niederschwelliges Anpassen der zu berücksichtigenden Regelungen.
c) Abs. 3: Die Einschränkungen im Bedrohungsfall sollen sehr selektiv erfolgen und nur im Ausnahmefall dazu führen, dass keine Notrufnummern mehr über die betroffenen Anschlüsse gewählt werden können.
d) Abs. 3: Sind durch die Einschränkungen potentiell mehr als 1'000 Kundinnen und Kunden über die prognostizierte Dauer von mehr als 15 Minuten betroffen, sind die betroffenen kantonalen Notrufzentralen über die Einschränkungen zu informieren.

Art. 96f
Es wird im Abs. 2 definiert, dass der Betrieb der Netzwerkbetriebszentren und deren Sicherheitsbetriebszentren nebst der Schweiz im Europäischen Wirtschaftsraum und im Vereinigten Königreich stattfinden kann. Ist eine Betreiberin primär ausserhalb der Schweiz tätig, ist der operative und der juristische Durchgriff im Ereignisfall schwierig bis unmöglich. Nebst der schwierigen Erreichbarkeit im Ausland, ist auch die Priorisierung von Massnahmen und Ressourcen deutlich erschwert. Es wird angeregt, dass eine ständige Vertretung in der Schweiz gefordert wird.

Antrag:

a) Ein ständiger Firmensitz oder ein ständiger Ableger in der Schweiz ist unumgänglich und soll entsprechend in der FDV verankert werden.
b) Insbesondere beim Betrieb von sicherheitskritischen Fernmeldeanlagen ist dem ständigen Firmensitz oder einer ständigen Vertretung in der Schweiz ein hohes Gewicht beizumessen.

Ergänzende Rückmeldung
Wir erlauben uns an dieser Stelle noch auf eine weitere Pendenz hinzuweisen, welche in die vorliegende Revision der Verordnung einfliessen sollte.

In der vorliegenden Revision der FDV soll auch die Problematik des kostenpflichtigen Zuganges zur SOS-DB (NotDB), zukünftig LIS-Proxy, und der Nutzung der Dynamischen Leitweglenkung (DLWL) für die Notrufzentralen geregelt werden.

Dieses Bedürfnis wurde schon lange von Seiten der Notrufzentralen kommuniziert und soll nun einfliessen.

Aus diesem Grunde stellen wir die folgenden zusätzlichen Anträge, welche in die Revision einfliessen sollen oder zumindest für eine weitere Revision vorbereitet werden sollen:

1) Kostenlose Nutzung der DLWL für alle Notrufzentralen, inkl. der entsprechenden Verpflichtung der zuständigen Provider.
2) Kostenlose Nutzung der SOS-DB (zukünftig LIS-Proxy) für alle Notrufzentralen.

Wir bedanken uns für die Prüfung unserer Anliegen. Gerne stehen wir oder das Gremium Notrufe für weitere Auskünfte zur Verfügung.

Freundliche Grüsse

Justiz-, Polizei- und Militärdepartement
Kantonspolizei

Christian Schmid, Kommandant

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

tp-secretariat@bakom.admin.ch

Bern, 17. März 2022

09.02.01cst

Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten)

Sehr geehrte Damen und Herren

Der Vorstand der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) hat sich an seiner Sitzung vom 7. März 2022 mit der Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten) befasst. Er unterstützt die beabsichtigten Änderungen grundsätzlich und schliesst sich im Übrigen der Haltung der Konferenz der Kantonalen Polizeikommandanten der Schweiz (KKPKS) an. Wir bitten Sie, deren Anliegen zu berücksichtigen und danken Ihnen für die gute Zusammenarbeit.

Mit freundlichen Grüssen

Sig. F. Düblin

Florian Düblin
Generalsekretär

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

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

Der Präsident

Eidgenössisches Departement für Umwelt,
Verkehr, Energie und Kommunikation
UVEK

Per E-Mail:
tp-secretariat@bakom.admin.ch

Bern, 3. März 2022

Vernehmlassungsantwort der KKPKS zur Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und –diensten)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Die Konferenz der Kantonalen Polizeikommandanten der Schweiz (KKPKS) bedankt sich für die Einladung, zur oben erwähnten Vernehmlassung Stellung zu nehmen.

Die KKPKS begrüsst grundsätzlich den vorliegenden Entwurf zur Verordnung über Fernmeldedienste (FDV). Mit dem gewählten zweistufigen Vorgehen wird einerseits die unbefugte Manipulation von 5G-Fernmeldeanlagen bekämpft und es wird ein definiertes Sicherheitsniveau eingeführt. Andererseits wird in einer zweiten Etappe ein weiteres Massnahmenpaket erarbeitet, bei welchem die Härtung im Sinne der Stromversorgungssicherheit im Fokus stehen wird. Beide Vorhaben sind aus unserer Sicht wichtig und geeignet, um die Verfügbarkeit der immer wichtiger werdenden Mobilkommunikation der 5G Technologie sicherzustellen.

Wir weisen an dieser Stelle ausdrücklich darauf hin, dass sich die mobile Kommunikation der Blaulicht- und Sicherheitsorganisationen, mangels Vorhandenseins eines Systems für die mobile breitbandige Sicherheitskommunikation (MSK[1]), in wesentlichen Aspekten auf die Mobilfunksysteme der heutigen Anbieter stützen. Aktuell werden deutlich über 70% aller Notrufe über Mobiltelefone abgewickelt. Nebst den Notrufen sind die Ereignisorganisationen auf eine funktionierende Alarmierung über die Mobilnetze angewiesen. Vor allem die Milizfeuerwehren stützen sich - mangels Alternativen - auf die Alarmierung über die bestehenden Mobilfunknetze. Dementsprechend sind Betriebsunterbrüche in den Mobilnetzen möglichst zu vermeiden, da sie direkte Auswirkungen auf die Ereignisbewältigung der Blaulichtorganisationen haben.

[1] Vgl. Bundesgesetzüber den Bevölkerungsschutz und den Zivilschutz, Art. 20 «Mobiles breitbandiges Sicherheitskommunikationssystem»

Der Präsident

Eine weitere Anspruchsgruppe sind die Betreiber von kritischen Infrastrukturen, welche aufgrund ihrer Kritikalität auf einen zuverlässigen und sicheren Betrieb der neuen Generation von Mobilfunknetzen angewiesen sind.

Wir regen an, dass die Alarmierungs- und Meldeprozesse detailliert zu beschreiben sind. Um die Bearbeitung und Verteilung der eingegangenen Störungsmeldungen zu verbessern, sieht die revidierte Verordnung vor, die Rolle der Nationalen Alarmzentrale (NAZ) zu stärken. Der Empfang von Meldungen über Cyberangriffe soll zu einer Kernaufgabe der NAZ werden, da sie eine sichere Informatikinfrastruktur und einen 24-Stunden-Betrieb unterhält. Die Schaffung eines Single Point of Contact (SPOC) ist zielführend, weil damit die Krisenbewältigung erleichtert wird.

Doch bestehen weitere Organisationen, die sich um Cyberangriffe kümmern. Es kann nicht sein, dass ausschliesslich das BAKOM von der NAZ über die gemeldeten Störungen informiert wird. So sind beispielsweise auch das National Cyber Security Center (NCSC), die Melde- und Analysestelle Informationssicherung (MELANI) sowie die kantonalen Notrufzentralen von Polizei, Feuerwehr und Sanität einzubinden. Deren Rolle im Gesamtprozess von Meldung- und Alarmierung im Bereich Cyber sind im Erläuternden Bericht aufzuführen.

Im Zusammenhang mit der Bedrohung kritischer Infrastrukturen durch Cyber-Angriffe von staatlicher Seite und deren Abwehr sind die Aufgaben der Armee aufzuzeigen und in die FDV zu integrieren. Die klassische Machtpolitik erlebt seit einigen Jahren eine Renaissance. Bereits heute setzen einige Staaten ihre Cybermittel regelmässig im Sinne eines "Kalten" Cyber-Krieges ein. Im Falle eines bewaffneten Konflikts in Europa ist mit einer breiten Verwendung dieser Mittel zu rechnen. Davon dürften auch Staaten, die an den eigentlichen Kampfhandlungen nicht beteiligt sind, betroffen sein. Die Armee hat in den vergangenen Jahren Schritte unternommen, sich auf ein solches Szenario vorzubereiten. So ist die Führungsunterstützungsbasis (FUB) im Bereich Verteidigung für Aktionsplanung, Lageverfolgung, Ereignisbewältigung und Ausbildung der Mitarbeitenden und AdA im Cyber-Raum verantwortlich. Mit der Weiterentwicklung der Armee (WEA) wurde zur Unterstützung der Berufsorganisation der FUB eine Cyber-Kompanie gebildet. Ab 2022 werden sämtliche Cyber Formationen der Schweizer Armee in das neu gegründete Cyber Bataillon 42 integriert. Die Rolle der Armee ist in der revidierten FDV zu berücksichtigen und ihre Verwendung zu beschreiben.

Der sofortigen Information an die kantonalen Notrufzentralen von Polizei, Feuerwehr und Sanität ist absolut notwendig. Nur sie können die Risiken von Beeinträchtigungen abschätzen und Sofortmassnahmen anordnen (bspw. die Umsetzung von Notfalltreffpunkten o.ä.). Entsprechend sind die Informationsprozesse in der FDV zu verankern.

Ergänzungen und Anpassungen
Wir beantragen die folgenden Anpassungen zum vorliegenden Entwurf der FDV:

Art. 96
Störungen im Mobilfunkbereich haben direkte Auswirkungen. So sind unter Umständen Notrufnummern nicht mehr erreichbar, oder die Einsatzkräfte von Polizei, Rettungsdienst und Feuerwehr sind aufgrund der nicht mehr vorhandenen Datenübertragungsmöglichkeiten in ihrem Handeln be-

Der Präsident

einträchtigt. In vielen Kantonen wurden inzwischen Notfalltreffpunkte installiert, welche bei Störungen im Kommunikationsbereich besetzt werden können. Dies setzt jedoch voraus, dass die kantonalen Notrufzentralen sofort und unverzüglich über Ausfälle, bereits im niederschwelligen Bereich, informiert werden. Die im Art. 96 formulierte Grösse von 30'000 Kundinnen und Kunden, welche von einem Ausfall betroffen sind, ist deutlich zu hoch gewählt. Zudem ist es wichtig, dass die Dauer von Störungen abgeschätzt werden kann. Aktuell gehen die Notruforganisationen davon aus, dass Störungen relevant sind, welche voraussichtlich mehr als 15 Minuten dauern und mindestens 1'000 Kundinnen und Kunden davon betroffen sind.

Eine Information an die NAZ, NCSC, MELANI, sowie nachgelagert an das BAKOM sind für die Nachbereitung der Störung wichtig. Die erwähnten Organe haben jedoch nur einen sekundären Einfluss auf die Behebung einer Störung oder der Bewältigung einer entsprechenden Lage. Dies obliegt primär den kantonalen Behörden, welche entsprechende Massnahmen sofort umsetzen können.

Es ist unklar, warum die Anzahl der betroffenen Kundinnen und Kunden nun auf Stufe FDV und nicht mehr in der TAV geregelt werden soll.

Antrag:
a) Die von einer potentiellen Störung betroffene Anzahl von Kundinnen und Kunden ist von 30'000 auf 1'000 Kundinnen oder Kunden zu senken, welche potentiell von einem Ausfall grösser als 15 Minuten betroffen sind.
b) In jedem Fall haben die Anbieterinnen von Fernmeldediensten ab einer Störungsgrösse von 1'000 Kundinnen und Kunden (+15 Minuten) die zuständigen kantonalen Notrufzentralen von Polizei, Sanität und Feuerwehr (112, 117, 118, 144) zu informieren, bevor die Meldungen an die NAZ (i.S. eines SPOC) oder weitere Organe abgesetzt werden.
c) Die Anzahl der betroffenen Kundinnen und Kunden soll weiterhin in der TAV geregelt werden und nicht auf Stufe FDV.

Art. 96a
Im Abs. 1 wird spezifisch und abschliessend von DDoS-Angriffen gesprochen. Aufgrund des technologischen schnellen Wandels ist es möglich, dass es zukünftig andere Arten von Angriffen geben kann, welche es zu berücksichtigen gilt.

Im Abs. 3 werden die Anbieterinnen von Internetzugängen berechtigt, Internetzugänge und Adressierungselemente, welche die Systeme beeinträchtigen, zu sperren oder einzuschränken. Sie dürfen die Massnahmen aufrechterhalten, solange die Bedrohung anhält. Die kann zu Unterbrüchen im Bereich der Notrufe führen und damit zu potentiellen Risiken für hilfsbedürftige Personen.

Antrag:
a) Abs. 1: Es soll im erwähnten Absatz nicht abschliessend von DDoS-Angriffen gesprochen werden, sondern die DDoS-Angriffe sind als Beispiel o.ä. aufzuführen.
b) Abs. 1: Die Details von potentiellen Angriffsmechanismen sollen nicht abschliessend in der FDV geregelt werden, sondern in den technisch- administrativen Vorschriften (TAV). Dies ermöglicht ein adäquates Handeln und ein relativ niederschwelliges Anpassen der zu berücksichtigenden Regelungen.

Der Präsident

c) Abs. 3: Die Einschränkungen im Bedrohungsfall sollen sehr selektiv erfolgen und nur im Ausnahmefall dazu führen, dass keine Notrufnummern mehr über die betroffenen Anschlüsse gewählt werden können.
d) Abs. 3: Sind durch die Einschränkungen potentiell mehr als 1'000 Kundinnen und Kunden über die prognostizierte Dauer von mehr als 15 Minuten betroffen, sind die betroffenen kantonalen Notrufzentralen über die Einschränkungen zu informieren.

Art. 96f
Es wird im Abs. 2 definiert, dass der Betrieb der Netzwerkbetriebszentren und deren Sicherheitsbetriebszentren nebst der Schweiz im Europäischen Wirtschaftsraum und im Vereinigten Königreich stattfinden kann. Ist eine Betreiberin primär ausserhalb der Schweiz tätig, ist der operative und der juristische Durchgriff im Ereignisfall schwierig bis unmöglich. Nebst der schwierigen Erreichbarkeit im Ausland, ist auch die Priorisierung von Massnahmen und Ressourcen deutlich erschwert. Es wird angeregt, dass eine ständige Vertretung in der Schweiz gefordert wird.

Antrag:
a) Ein ständiger Firmensitz oder ein ständiger Ableger in der Schweiz ist unumgänglich und soll entsprechend in der FDV verankert werden.
b) Insbesondere beim Betrieb von sicherheitskritischen Fernmeldeanlagen ist dem ständigen Firmensitz oder einer ständigen Vertretung in der Schweiz ein hohes Gewicht beizumessen.

Ergänzende Rückmeldung
Wir erlauben uns an dieser Stelle noch auf eine weitere Pendenz hinzuweisen, welche in die vorliegende Revision der Verordnung einfliessen sollte.

In der vorliegenden Revision der FDV soll auch die Problematik des kostenpflichtigen Zuganges zur SOS-DB (NotDB), zukünftig LIS-Proxy, und der Nutzung der Dynamischen Leitweglenkung (DLWL) für die Notrufzentralen geregelt werden.

Dieses Bedürfnis wurde schon lange von Seiten der Notrufzentralen kommuniziert und soll nun einfliessen.

Aus diesem Grunde stellen wir die folgenden zusätzlichen Anträge, welche in die Revision einfliessen sollen oder zumindest für eine weitere Revision vorbereitet werden sollen:
1) Kostenlose Nutzung der DLWL für alle Notrufzentralen, inkl. der entsprechenden Verpflichtung der zuständigen Provider.
2) Kostenlose Nutzung der SOS-DB (zukünftig LIS-Proxy) für alle Notrufzentralen.

Wir bedanken uns für die Prüfung unserer Anliegen. Gerne stehen wir oder das Gremium Notrufe für weitere Auskünfte zur Verfügung.

Besten Dank für Ihre Kenntnisnahme.

Der Präsident

Freundliche Grüsse

Der Präsident

_____

Mark Burkhard, Kdt Polizei Basel-Landschaft

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

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

Frau Bundesrätin
Simonetta Sommaruga, Vorsteherin UVEK
Bundeshaus Nord, 3003 Bern
tp-secretariat@bakom.admin.ch

17. Januar 2022

Änderung der Verordnung über Fernmeldedienste (FDV)
Eröffnung des Vernehmlassungsverfahrens

Sehr geehrte Frau Bundesrätin

Mit Schreiben vom 3. Dezember 2021 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 den vorliegenden Entwurf der Verordnung über Fernmeldedienste (FDV) grundsätzlich.

Begründung: Mit dem vorliegenden Entwurf der revidierten FDV wird die unbefugte Manipulation von Fernmeldeanlagen durch fernmeldetechnische Übertragungen bekämpft. Insbesondere Massnahmen zur Schaffung eines Mindestniveaus an 5G-Netzwerksicherheit in der Schweiz erachten wir als dringend erforderlich. Ein hohes Sicherheitsniveau beim Betrieb von Mobilfunknetzen der neusten Generation ist ebenso sicherzustellen.

Der Vorstand der RK MZF beantragt folgende Ergänzungen:

1. Es ist darzulegen, wie die Blaulichtorganisationen und die Kritischen Infrastrukturen (KI) in die Alarmierungs- und Meldeprozesse einbezogen werden.

Heute werden über 70% aller Notrufe über Mobiltelefone abgewickelt. Betriebsunterbrüche in den Mobilnetzen sind dadurch sensitiv. Sie haben direkte Auswirkungen auf das Notrufwesen und die Ereignisbewältigung durch die Blaulichtorganisationen, ebenso wie auf die Betreiber von KI, die auf einen zuverlässigen und sicheren Betrieb der neuen Generation von Mobilfunknetzen angewiesen sind.

2. Einführung einer Pflicht zur selektiven Blockierung von Internetzugängen oder Adressierungselementen von denen eine Gefährdung im Zusammenhang mit KI ausgeht.

Begründung: Cyberangriffe haben nicht nur hohe wirtschaftliche Auswirkungen, sondern sie gefährden auch die Sicherheit des Landes, da sie zu Ausfällen oder fehlerhaftem Funktionieren von KI führen können. Aus diesem Grund haben Anbieter von Internetzugängen diese und Adressierungselemente zu blockieren, von denen eine Gefährdung für KI ausgeht. Nur so kann die Sicherheit der angebotenen Dienstleistungen gewährleistet werden.

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

3. Die Rollen der einzelnen Akteure und Stellen sind detailliert zu beschreiben.

Begründung: Um die Bearbeitung und Verteilung der eingegangenen Störungsmeldungen zu verbessern, sieht die revidierte Verordnung vor, die Rolle der Nationalen Alarmzentrale (NAZ) zu stärken, da sie eine sichere Informatikinfrastruktur und einen 24-Stunden-Betrieb unterhält (Art. 96). Cyberangriffe dagegen sind einer zu schaffenden Meldestelle gemäss Art. 96 b zu melden. Darüber hinaus bestehen weitere Organisationen, die sich um Cyberangriffe kümmern. So sind beispielsweise auch das National Cyber Security Center (NCSC), die Melde- und Analysestelle Informationssicherung (MELANI) sowie die kantonalen Notrufzentralen einzubinden. In diesem Zusammenhang kann es nicht sein, dass ausschliesslich das BAKOM von der NAZ über die gemeldeten Störungen informiert wird. Die Rollen sämtlicher Stellen im Gesamtprozess von Meldung und Alarmierung im Bereich Cyber sind im Erläuternden Bericht detailliert aufzuführen. Dabei ist die Schaffung eines Single Point of Contact (SPOC) grundsätzlich anzustreben, weil damit die Krisenbewältigung erleichtert wird.

4. Die Anbieter werden verpflichtet, unverzüglich Störungen im Betrieb ihrer Fernmeldeanlagen und Fernmeldedienste zu melden, wenn 1000 Kunden, die potentiell von einem Ausfall betroffen sind, der länger als 15 Minuten dauert.

Begründung: Die Zahl von 30'000 potenziell betroffenen Kunden entspricht dem Äquivalent einer Schweizer Stadt mittlerer Grösse. Eine Störung, die den gesamten Kanton Appenzell Innerhoden mit seinen 16'300 Einwohnern betreffen würde, würde gemäss vorliegendem Entwurf somit nicht gemeldet. Zudem ist es wichtig, dass die Dauer von Störungen abgeschätzt werden kann. Aktuell gehen die Notruforganisationen davon aus, dass Störungen relevant sind, welche voraussichtlich mehr als 15 Minuten dauern und mindestens 1000 Kundinnen und Kunden davon betroffen sind.

5. Im Zusammenhang mit der Bedrohung kritischer Infrastrukturen durch Cyber-Angriffe von staatlicher Seite und deren Abwehr sind die Aufgaben der Armee aufzuzeigen und in die FDV zu integrieren.

Die klassische Machtpolitik erlebt seit einigen Jahren eine Renaissance. Bereits heute setzen einige Staaten ihre Cybermittel regelmässig im Sinne eines "Kalten" Cyber-Krieges ein. Im Falle eines bewaffneten Konflikts in Europa ist mit einer breiten Verwendung dieser Mittel zu rechnen. Davon dürften auch Staaten, die an den eigentlichen Kampfhandlungen nicht beteiligt sind, betroffen sein. Die Armee hat in den vergangenen Jahren Schritte unternommen, sich auf ein solches Szenario vorzubereiten. So ist die Führungsunterstützungsbasis (FUB) im Bereich Verteidigung für Aktionsplanung, Lageverfolgung, Ereignisbewältigung und Ausbildung der Mitarbeitenden und AdA im Cyber-Raum verantwortlich. Mit der Weiterentwicklung der Armee (WEA) wurde zur Unterstützung der Berufsorganisation der FUB eine Cyber-Kompanie gebildet. Ab 2022 werden sämtliche Cyber Formationen der Schweizer Armee in das neu gegründete Cyber Bataillon 42 integriert. Die Rolle der Armee ist in der revidierten FDV zu berücksichtigen und ihre Verwendung zu beschreiben.

Wir ersuchen Sie, sehr geehrte Frau Bundesrätin, die Empfehlungen des Vorstandes der RK MZF zu berücksichtigen.

Mit freundlichen Grüssen

Regierungskonferenz
Militär, Zivilschutz und Feuerwehr

elo. sig.
Regierungsrat Paul Winiker
Präsident RK MZF

elo. sig.
PD Dr. phil. Alexander Krethlow
Generalsekretär RK MZF

Kopie an:

- Generalsekretariat EnDK
- Generalsekretariat KKJPD

Salt.

Salt Mobile SA
Rue du Caudray 4
CH-1020 Renens 1

Bundesamt für Kommunikation BAKOM
Abteilung Telekomdienste
Zukunftstrasse 44
Postfach
CH-2501 Biel

Eingereicht als pdf und word per email an: *tp-secretariat@bakom.admin.ch*

Renens, 17. März 2022

Änderung der Verordnung über Fernmeldedienste (FDV) betreffend Art. 48a FMG - Sicherheit

Sehr geehrte Frau Bundesrätin, sehr geehrter Herr Direktor, sehr geehrte Damen und Herren

Wir möchten uns für die Möglichkeit zur Anhörung betreffend die Revision der Verordnung über Fernmeldedienste (FDV) bedanken und nehmen dazu gerne fristgerecht Stellung wie folgt.

Grundlage der aktuellen Revision der FDV ist die bereits vom Parlament verabschiedete Revision des Fernmeldegesetzes mit dem Artikel 48a betreffend Sicherheit.

Allgemeine Vorbemerkungen

Wir begrüssen grundsätzlich die Bestrebungen des Bundesrates, mit Massnahmen die Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten zu verbessern. Es gibt jedoch nur ein Internet, Cyberangriffe sind grundsätzlich von allen Fernmeldenetzen aus möglich und beschränken sich nicht auf die Mobilnetze. Wenn auch ein Grossteil der Bevölkerung mobile Dienste nutzt, so wird der mit Abstand grösste Teil der Daten immer noch via Festnetz übertragen. Somit müssten die Sicherheitsauflagen zwingend auf die Festnetze ausgedehnt werden, um die gewünschte Wirkung erzielen zu können.

Schwerwiegende und nicht verhältnismässige Eingriffe in die Wirtschafts- und Eigentumsfreiheit der Fernmeldedienstanbieterinnen sollen dabei vermieden werden. Gewisse Aspekte werden bereits heute in der Branche auf freiwilliger Basis umgesetzt. Salt ist der Meinung, dass nur dort reguliert werden soll, wo zwingend notwendig. Wir erachten den Ansatz als sinnvoll, wo möglich eine Zuteilung von Kompetenzen anstelle von einer Auferlegung von Pflichten für die Internetdienstanbieterinnen vorzusehen.

Die an einigen Stellen vorgesehen Delegationsnormen and das BAKOM verunmöglichen es uns zum jetzigen Zeitpunkt konkret Stellung zu nehmen. Von solchen Kompetenzdelegationen soll abgesehen werden. Wir ersuchen das BAKOM, diese Bestimmungen unbedingt mit Bedacht auszuformulieren.

Verordnungsentwurf über Fernmeldedienste (Art. 96ff E-FDV)

Konkrete Änderungsvorschläge in den entsprechenden Artikeln sind in Rot ausformuliert.

3. Abschnitt: Störungsmeldung

Kein Titel (Art. 96 E-FDV)

Aus unserer Sicht macht es Sinn, die Störungsmeldungen direkt und zentral an die nationale Alarmzentrale zu schicken. Die Auflage mit potentiell mindestens 30'000 betroffenen Kundinnen und Kunden ist bereits schwierig zu beurteilen und zudem nicht abschliessend definiert. In der aktuellen Regelung in den entsprechenden technischen und administrativen Vorschriften (TAV) ist z.B. eine gewisse Anzahl an betroffenen Mobilfunkstandorten pro Technologie (2G-5G) definiert. Hier ist nun nicht klar, was unter Fernmeldediensten zu verstehen ist. Sind es die Grunddienste wie Daten, Sprache, TV oder gar wiederum auch pro Technologie? Dies müsste entsprechend präzisiert werden.

Weiter müsste vorgesehen werden, dass diese Daten nicht veröffentlicht werden dürfen. Wir bereits mit der aktuellen Regelung erfahren, können diese Informationen zu Falschdarstellungen in den Medien führen. So steht eine Anbieterin, welche keine oder weniger Störungen meldet viel besser da als jene, die mehr Störungen meldet. Es handelt sich jedoch dabei um Selbsteinschätzungen der Anbieterinnen, und nicht um eine von den Behörden überprüfte Zahl.

Art. 96 E-FDV

1 Die Anbieterinnen von Fernmeldediensten müssen Störungen im Betrieb ihrer Fernmeldeanlagen und -dienste, welche potenziell mindestens 30'000 Kundinnen und Kunden für einen Fernmeldedienst oder eine Technologie betreffen, unverzüglich der Nationalen Alarmzentrale melden.

2 Die Nationale Alarmzentrale informiert das BAKOM über die gemeldeten Störungen.

3 Die gemeldeten Störungen dürfen nur in aggregierter Form veröffentlicht werden.

4. Abschnitt: Unbefugte Manipulation von Fernmeldeanlagen

Sicherheitsmassnahmen (Art. 96a E-FDV)

Bereits heute werden sogenannte DDoS-Attacken auf unseren Netzen bekämpft. Mit dieser neuen Regelung in Absatz 1 werden klare gesetzliche Grundlagen geschaffen.

Die Anwendung von allgemein gültigen Sicherheitsstandards auf die Endgeräte bei unseren Kunden (CPE) gemäss Absatz 2 stellt einen zentralen Baustein in der Kette der Abwehr von Attacken dar. Hier ist eine Anlehnung an internationale Normen sinnvoll. Wir fragen uns, wie das Wort *unverzüglich* in diesem Zusammenhang zu verstehen ist und schlagen vor es mit *regelmässig* zu ersetzen. Wir führen bereits heute Sicherheitstest mit all den unseren Kunden zur Verfügung gestellten Endgeräten durch.

Wir befürworten die Regelung unter Absatz 3 mit einer Schaffung von Rechten für die Fernmeldedienstanbieterinnen anstelle von Pflichten. Es ist richtig und wichtig, dass die Entscheidungskompetenz betreffend Massnahmen für eben ihre Netze in den Händen der Netzbetreiberinnen bleibt.

Art. 96a Sicherheitsmassnahmen E-FDV

1 Die Anbieterinnen von Internetzugängen bekämpfen Angriffe auf die Verfügbarkeit von Diensten, die durch eine Vielzahl von gezielten Anfragen durch eine grosse Zahl von Quellen verursacht werden (Distributed-Denial-of-Service attack; DDoS-Angriff), indem sie mit vertretbaren technischen Möglichkeiten verhindern, dass ausgehende Verbindungen mit gefälschten Adressierungselementen möglich sind.

2 Sie konfigurieren die Sicherheitseigenschaften aller Fernmeldeanlagen, die sie ihren Kundinnen und Kunden zur Verfügung stellen, gemäss den anerkannten Regeln der Technik und aktualisieren sie ~~unverzüglich~~ regelmässig, sofern sie weiterhin die Kontrolle über diese Anlagen ausüben.

3 Sie sind berechtigt, Internetzugänge oder Adressierungselemente, die das ordnungsgemässe Funktionieren von Fernmeldeanlagen zu beeinträchtigen drohen, zu sperren oder deren Nutzung einzuschränken. Sie informieren ihre Kundinnen und Kunden, die Opfer unbefugter Manipulationen geworden sind oder werden könnten, unverzüglich über solche Sperrungen oder Einschränkungen. Sie dürfen diese Massnahmen aufrechterhalten, solange die Bedrohung anhält.

Meldestelle (Art. 96b E-FDV)

Die Organisation dieser Meldestelle soll in der Hand jeder einzelnen Anbieterin von Internetzugängen bleiben. So haben wir bereits heute Verpflichtungen aus dem kürzlich revidierten FMG für solche Meldestellen wie z.B. betreffend unerwünschte Werbeanrufe resp. deren Sperrung. Dies ist auch wichtig, da die Anbieterin selbst dann die geeigneten Abwehrmassnahmen einleiten soll.

Art. 96b Meldestelle E-FDV

Die Anbieterinnen von Internetzugängen betreiben eine spezialisierte Stelle, die Meldungen über unbefugte Manipulationen von Fernmeldeanlagen durch fernmeldetechnische Übertragungen entgegennimmt. Sie leiten innert angemessener Frist geeignete Abwehrmassnahmen ein.

Vollzug (Art. 96c E-FDV)

Dazu steht im erläuternden Bericht folgendes: *Das BAKOM vollzieht die vorliegende Bestimmung und erlässt die entsprechenden technischen und administrativen Vorschriften. Dabei wird es vom NCSC mit der notwendigen fachlichen Expertise unterstützt.* Wir fragen uns, warum dies hier zwingend definiert werden muss. Wer sonst würde das denn vollziehen und worauf bezieht sich die vorliegende Bestimmung? Der Schreibfehler sollte noch korrigiert werden.

Art. 96c Vollzug E-FDV
Das BAKOM vollzieht diesen Abschnitt~~s~~ in Zusammenarbeit mit dem NCSC.

5. Abschnitt: Sicherheit von Netzen und Diensten, die von Mobilfunkkonzessionärinnen betrieben werden

Geltung (Art. 96d E-FDV)

Der Geltungsbereich wurde wohl in Anlehnung an die 5G-Toolbox in der EU übernommen, welche dann aber in der Schweiz nur teilweise zum Einsatz kommen soll. 5G ist die aktuell neuste eingesetzte Technologie auf Mobilnetzen – es handelt sich also um eine Momentaufnahme; die Vorgängerinnen sind aber immer noch im Einsatz und es wird auch Nachfolgetechnologien geben. Es ist somit fraglich, warum die betroffenen Artikel nicht grundsätzlich für die Mobilnetze und somit alle Generationen gelten sollen.

Art. 96d Geltung E-FDV
Die Artikel 96e–96g gelten für Mobilfunknetze der fünften Generation, die den international festgelegten technischen Spezifikationen entsprechen.

Sicherheitsmanagement (Art. 96e E-FDV)

Salt betreibt bereits heute ein Risikomanagement. Auch aus dem erläuternden Bericht lässt sich nicht ableiten, in welchem Umfang ein solches «System» gemäss Absatz 1 aufgebaut werden soll. Bereits der Begriff des «Systems» ist interpretierbar. Ist in Absatz wirklich gemeint, dass dieses «System» kontinuierlich überprüft werden soll, oder allenfalls eher die Sicherheitsziele?

Gemäss dem erläuternden Bericht soll das BAKOM in den TAV auf die Norm ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements verweisen, was wir mittragen können.

Pläne für das betriebliche Kontinuitätsmanagement und Pläne für das Management von Sicherheitsvorfällen sind zwingend nötig und bestehen bereits bei Salt.

Aktuell sieht das BAKOM davon ab, konkrete Zertifizierungen gemäss Absatz 3 zu verlangen. Dies sollte auf jeden Fall auch so bleiben.

Für kleinere Anbieterinnen wie Salt ist eine vorgegebene Zertifizierung mit grossem Aufwand und Kosten verbunden, sowohl einmalig als auch wiederkehrend. Eine konkrete Bestimmung käme hier einem schwerwiegenden Eingriff in den Wettbewerb gleich. Es sollte deshalb unbedingt den Netzbetreiberinnen

überlassen werden, wie sie das Sicherheitsmanagement konkret umsetzen. Das BAKOM sollte erst bei Vorfällen aktiv werden und dann den Sachverhalt untersuchen gemäss Vorgabe in Art. 96g Abs. 2.

Art. 96e Sicherheitsmanagement E-FDV

1 Die Mobilfunkkonzessionärinnen müssen ein Managementsystem für die Informationssicherheit auf der Grundlage einer Risikoanalyse und der sich daraus ergebenden Sicherheitsziele entwickeln, umsetzen und kontinuierlich überprüfen.

2 Im Rahmen dieses Sicherheitsmanagementsystems setzen sie einen Plan für das betriebliche Kontinuitätsmanagement und einen Plan für das Management von Sicherheitsvorfällen um.

3 Sie stellen sicher, dass ihr Sicherheitsmanagementsystem, ihr Plan für das Kontinuitätsmanagement und ihr Plan für das Management von Sicherheitsvorfällen den anerkannten Sicherheitsnormen entsprechen.

Betrieb sicherheitskritischer Fernmeldeanlagen (Art. 96f E-FDV)

Wir begrüssen, dass eine Zertifizierung nach anerkannte Sicherheitsnormen verlangt wird. Es gilt zu verhindern, dass die Schweiz hier schweiz-spezifische Normen anwenden würde. Die Schweizer Mobilnetze wurden vom Bundesamt für wirtschaftliche Landesversorgung (BWL) als systemrelevant und als kritische Infrastruktur eingestuft. Alle zum Mobilnetz gehörenden Fernmeldeanlagen sind u.E. somit sicherheitskritisch. Wir verstehen darum nicht, was das BAKOM hier genau definieren soll.

Die Vorgabe, die Netzwerkbetriebszentren und Sicherheitsbetriebszentren nur in der Schweiz, der EWR oder UK zu betreiben ist eine Einschränkung für international organisierte Unternehmen. Hier müssten noch weitere Länder einbezogen werden können, z.B. wo gemäss Staatenliste des EDÖB ein angemessener Schutz für Personendaten vorliegt.

Art. 96f Betrieb sicherheitskritischer Fernmeldeanlagen E-FDV

1 Die Mobilfunkkonzessionärinnen stellen sicher, dass die von ihnen betriebenen sicherheitskritischen Fernmeldeanlagen nach anerkannten Sicherheitsnormen zertifiziert sind. Das BAKOM definiert die betroffenen Anlagen.

2 Die Mobilfunkkonzessionärinnen betreiben ihre Netzwerkbetriebszentren (Network Operations Centres) und ihre Sicherheitsbetriebszentren (Security Operations Centres) in der Schweiz, im Europäischen Wirtschaftsraum oder im Vereinigten Königreich, sowie Staaten, wo gemäss Liste des EDÖB ein angemessener Schutz für Personendaten vorliegt.

Anwendbare Vorschriften und Aufsicht (Art. 96g E-FDV)

Dieser Artikel räumt dem BAKOM in Absatz 1 grosses Ermessen zu. Je nach Auswahl der entsprechenden Normen kann dies zu grossem Aufwand und Kosten bei einer Mobilnetzbetreiberin führen. Wir bereits unter Art. 96e erwähnt kann die konkrete Forderung nach Zertifizierungen zu einem erheblichen Aufwand insb. bei kleineren Anbietern führen. Es ist deshalb davon abzusehen, solche potentiellen Vorgaben in einer TAV zu verankern. Die Wahl der Zertifizierungen soll den Anbieterinnen überlassen werden. Absatz 1 von Art. 96g sei somit zu streichen.

In Absatz 2 sollte definiert werden, auf was sich eine Rechtsverletzung beziehen kann. Der Umfang eines möglichen Audits sollte beschränkt werden.

Art. 96g Anwendbare Vorschriften und Aufsicht E-FDV

~~1 Das BAKOM erlässt die technischen und administrativen Vorschriften. Es erklärt anerkannte Normen im Bereich der Informationssicherheit sowie der Telekommunikationsinfrastrukturen und –dienste obligatorisch.~~

2 Besteht ein Verdacht auf Rechtsverletzung und erweist es sich zur Feststellung des Sachverhalts als notwendig, kann das BAKOM von den Mobilfunkkonzessionären verlangen, sich auf eigene Kosten und bei einer qualifizierten Stelle einem Audit zu unterziehen oder ihre davon betroffenen Fernmeldeanlagen prüfen zu lassen.

Schlussbemerkungen

Generell beantragt Salt, dass bei den Punkten mit schwerwiegenden Eingriffen in bestehende Prozesse oder Vorgaben für die technischen Ausrüstungen und Systemimplementierungen oder Zertifizierungspflichten eine Übergangsfrist von mindestens 12 Monaten nach Inkrafttreten der revidierten Verordnung oder einer entsprechenden TAV vorgesehen wird.

Salt ist als Mobilnetzbetreiberin und Festnetzanbieterin von gewissen der vorgesehenen Anpassungen unmittelbar und stark betroffen. Wir hoffen deshalb auf die nötige Gewichtung unserer Aussagen und auf wohlwollende Aufnahme unserer Positionen.

Freundliche Grüsse

Felix Weber, Regulatory Affairs Manager, Salt Mobile SA

PER E-MAIL
tp-secretariat@bakom.admin.ch

Frau Simonetta Sommaruga
Bundesrätin / UVEK

Herr Bernard Maissen
Direktor / BAKOM

Gilles Marchand
Generaldirektor SRG SSR
Giacomettistrasse 1
3000 Bern 31

Datum 18. März 2022

E-Mail
Direktwahl
Datum

Vernehmlassung Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten)

Sehr geehrte Frau Bundesrätin, geschätzte Frau Sommaruga
Sehr geehrter Herr Direktor, geschätzter Herr Maissen

Die Schweizerische Radio- und Fernsehgesellschaft («SRG») bezieht sich auf die Eröffnung des Vernehmlassungsverfahrens zur Verordnung über Fernmeldedienste am 3. Dezember 2021, die wir mit Interesse zur Kenntnis genommen haben.

Medien leisten einen wichtigen Beitrag im demokratischen Meinungs- und Willensbildungsprozess und bei der Verbreitung von behördlichen Warnungen und Verhaltensanweisungen im Falle von Katastrophen und Notlagen. Elektronische Medien (Fernsehen, Radio), Internetdienste und Mobile Apps werden als Bestandteil der kritischen Infrastrukturen betrachtet.

Stationäres und mobiles Internet spielen bei der Produktion, der Verbreitung und dem Empfang von Medienangeboten (IPTV, OTT, Mobile Apps und Webseiten) bereits heute eine grosse Rolle. Sie werden weiter an Bedeutung gewinnen – gerade auch mit den Möglichkeiten, die neue Technologien wie 5G bieten. Daher begrüssen wir die neuen Vorschriften zur Bekämpfung der unbefugten Manipulation von Fernmeldeanlagen durch fernmeldetechnische Übertragungen und zur Gewährleistung der Sicherheit von Mobilfunknetzen der fünften Generation. Wichtig ist aus unserer Sicht zudem der Erlass des zweiten Massnahmenpakets, der die Stromversorgung gewährleisten soll.

Gleichzeitig möchten wir darauf hinweisen, dass die SRG bei der Erfüllung ihres Leistungsauftrages immer stärker auf resiliente Fernmeldeinfrastrukturen und -dienste Dritter angewiesen ist. Wichtig erscheint uns in diesem Zusammenhang, dass die von den Medien benötigten Dienste und Infrastrukturen (inkl. Sendernetze und Stromversorgung) bestmöglich vor Ausfällen und Cyber-Angriffen geschützt sind.

Zwar ist die Resilienz der eigentlichen Sende- und Empfangsanlagen (z.B. Sender, Kabel, Antennen und spezifische Zuführungsnetze) mit Bezug auf Cyber-Angriffe gegeben. Deren Management und Steuerung beruht aber auf IT-Systemen, die wiederum Ziel von Cyber-Angriffen sein können.

Die zum Schutz der unbefugten Manipulation von Fernmeldeanlagen vorgeschlagenen Sicherheitsmassnahmen gehen aus Sicht der SRG zu wenig weit, weil sie auf Customer Premises Equipment (CPE) zugeschnitten sind und nur die Internet-Accessprovider in die Pflicht nehmen. Das generelle Ziel muss der Schutz aller exponierten Endgeräte sein. Zu prüfen ist daher der Erlass von zusätzlichen Vorschriften zum Schutz von Management- und Steuer-Systemen, die mit kritischen Systemen (z.B. Sendegeräten oder Stromversorgungsanlagen) verbunden sind.

Für Ihre Kenntnisnahme, sehr geehrte Frau Bundesrätin, sehr geehrter Herr Direktor, danken wir Ihnen.

Freundliche Grüsse

Gilles Marchand
Generaldirektor

SUISSEDIGITAL

per E-Mail an tp-secretariat@bakom.admin.ch

Bundesamt für Kommunikation BAKOM
Michel Donzé / Mark Fitzpatrick
Zukunftsstrasse 44
Postfach 252
CH-2501 Biel

Bern, 16. März 2022

Stellungnahme zur Änderung der FDV im Bereich Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -dienste

Sehr geehrte Frau Bundesrätin
Sehr geehrter Herr Direktor
Sehr geehrte Damen und Herren

Mit Schreiben vom 3. Dezember 2021 haben Sie interessierte Kreise eingeladen, bis zum 18. März 2022 zu den geplanten Änderungen der Fernmeldedienstverordnung (nachfolgend „E-FDV“) im Bereich der Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -dienste, Stellung zu nehmen. Wir danken Ihnen für diese Möglichkeit der Meinungsäusserung, die für uns und unsere Mitglieder sehr wichtig ist, weil die vorgeschlagenen Massnahmen beim Betrieb von Fernmeldeinfrastrukturen und -diensten zwangsläufig mit höheren Investitionen und Betriebskosten unserer Mitglieder verbunden sind, von welchen am Ende auch die Kundinnen und Kunden unserer Mitglieder betroffen sind. Die vorliegende Stellungnahme erfolgt innert Frist und äussert sich zu Themen, die unsere Mitglieder in ihrer Geschäftstätigkeit direkt betreffen.

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 prüfen u.a. auch selbstverpflichtende Branchenlösungen in diesem Bereich. Unsere Abklärungen bei den einzelnen Mitgliedern zeigen aber auch, dass sie diesem Thema bereits einen hohen Stellenwert zumessen. Da die Unternehmen in unserem Verband sehr unterschiedlich sind, stellen allgemeingültige Regeln eine Herausforderung dar. Es sollte daher bei der Implementierung und Umsetzung von Sicherheitsmassnahmen gemäss Verordnung unbedingt auf die Erfahrung und die Expertise der Fernmeldedienstanbieterinnen (FDA) abgestellt und auf die einzelnen Konstellationen ihrer Tätigkeiten Rücksicht genommen werden. Dieser generelle Hinweis bezieht sich vor allem auch auf die in Art. 96g Abs. 1 E-FDV enthaltene Delegation an das BAKOM, im Bereich von 5G-Infrastrukturen anerkannte industrielle Normen für verbindlich zu erklären, was wir im Grundsatz aber unterstützen, weil wir davon ausgehen, dass solche Regulierungen in engster Absprache und Zusammenarbeit mit den betroffenen Konzessionärinnen erfolgt.

2. Art. 96, 96a – g E-FDV

Grundsätzlich können wir den mit den vorgeschlagenen Änderungen vorgesehenen neuen **Massnahmen für Internetzugangsanbieterinnen** unter Beachtung der nachfolgenden Erwägungen zustimmen, das heisst

- der Pflicht zur Filterung gefälschter Adressierungselemente (Quell-IP-Adresse) bei ausgehenden Verbindungen;
- der Pflicht zur Konfiguration und Aktualisierung der Endkundengeräte (Customer Premises Equipment, CPE) hinsichtlich der Sicherheitseigenschaften nach anerkannten Regeln der Technik, wobei klarzustellen ist, dass dies einerseits ausschliesslich für die in der Rolle als Internetzugangsanbieterin abgegebenen Geräte gilt (d.h. für Geräte am Netzabschlusspunkt, insbesondere dem Modem, und nicht bspw. für verkaufte Geräte der Heimvernetzung) und dass andererseits die in der Verordnung erwähnten ankerkannten Regeln der Technik auf internationale Standards abstellen;
- der ausdrücklichen Berechtigung, gefährliche Internetzugänge und Adressierungselemente zu sperren sowie
- der Pflicht, eine Meldestelle einzurichten, die Gefahrenmeldungen entgegennimmt, und der Pflicht innert angemessener Frist geeignete Abwehrmassnahmen einzuleiten.

Wir sind weiter auch mit der Konkretisierung von **Art. 96 E-FDV** einverstanden, wonach eine Störung im Betrieb der Netze ab einer potenziellen Betroffenheit von 30'000 Kundinnen und Kunden durch die FDA der Nationalen Alarmzentrale zu melden sind. Mit Blick auf weitere legislatorische Projekte im Bereich Sicherheit, welche neue Meldepflichten und -stellen vorsehen, wird beansprucht, dass die Bestrebungen verwaltungsintern abgestimmt und harmonisiert werden, so dass den Unternehmen durch das Meldewesen ein möglichst kleiner administrativer Aufwand entsteht. Denn gerade in ausserordentlichen Situationen sind ihre Ressourcen durch die interne Problemlösung gebunden, entsprechend es kontraproduktiv wäre, gleichzeitig den administrativen Aufwand in solchen Fällen zu vergrössern. So sollten die Unternehmen bspw. bei einem Sicherheitsvorfall nicht mehrere Amtsstellen informieren müssen, vielmehr sollte eine zentrale Amtsstelle, je nach Bedarf, automatisch weitere Stellen informieren («one stop shop»).

Hinsichtlich der geplanten **Massnahmen spezifisch für 5G-Mobilfunknetzbetreiberinnen** verweisen wir auf die Stellungnahme unseres Mitglieds Sunrise UPC und unterstützen die dortigen Vorbringen integral.

3. Weiteres Massnahmepaket in der Pipeline

In Bezug auf das bereits angekündigte weitere Massnahmepaket zur Informationssicherheit, in welches Projekt wir aufgrund der laufenden Regulierungsfolgenabschätzung gewisse Einblicke erhielten, möchten wir hinsichtlich der gesetzlichen Grundlage folgendes festhalten: Der Gesetzgeber hat mit der FMG-Revision neu dem Bundesrat die Kompetenz erteilt, Ausführungsbestimmungen zu Art. 48a FMG zu erlassen, wobei erstens der Rahmen möglicher Anordnungen abschliessend abgesteckt ist und zweitens darauf abstützende Massnahmen immer verhältnismässig für die gesamte Branche sein müssen. Wenn in Art. 48a Abs. 2 lit. c FMG redundante Infrastrukturen erwähnt sind, dann kann dies nicht bedeuten und es kann nicht auf Verordnungsstufe vorgeschrieben werden, dass unbesehen der konkreten kritischen Exponierung, alle Netzinfrastrukturen in Zukunft grundsätzlich redundant aufgebaut sein müssen. Die Kosten hierfür wären für sehr viele unserer Mitglieder nicht tragbar. Wie eingangs erwähnt, steht das Thema Informationssicherheit im ureigenen Interesse unserer Mitglieder und des Verbandes. Wir werden Sie gerne zu gegebenem Zeitpunkt über unsere verbandsinternen Initiativen in diesem Bereich informieren.

***

Wir danken Ihnen im Voraus, dass Sie unsere Bemerkungen und Argumente in die weitere Ausarbeitung der E-FDV einbeziehen. 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

Sunrise UPC GmbH
Thurgauerstrasse 101B, 8152 Glattpark (Opfikon)

Mobile: +41 76 777 10 52
Matthias.Forster@sunrise.net

sunrise.ch
upc.ch

Eidgenössisches Departement für Umwelt,
Verkehr, Energie und Kommunikation
Bundesamt für Kommunikation

tp-secretariat@bakom.admin.ch

Opfikon, 17. März 2022

Stellungnahme zur Änderung der Verordnung über Fernmeldedienste (FDV): Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten

Sehr geehrte Frau Bundesrätin,
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 der Verordnung über Fernmeldedienste ist für Sunrise UPC von hoher Relevanz. Wir danken Ihnen deshalb für die Möglichkeit, zu geplanten Reform Stellungnehmen zu können.

Sunrise UPC begrüsst die vorgeschlagene Revision der FDV. Die Revision hat das Potential, das Vertrauen von Wirtschaft und Gesellschaft in die Sicherheit von Fernmeldenetzen als kritische Infrastruktur weiter zu stärken. Störungsmeldungen sollten jedoch statt an die NAZ künftig an das NCSC erfolgen. Sunrise UPC erachtet es als sinnvoll, dass die geplanten Vorgaben auf internationalen Standards basieren. Dieser Grundsatz muss unbedingt auch auf der Stufe technischen und administrativen Vorschriften gelten.

Ausgangslage

Aufgrund geopolitisch dominierter Machverschiebungen sind Hersteller von Netzelektronik für Fernmeldenetze in den Fokus geraten. Um die Sicherheit sowohl von Fernmeldenetzen an sich wie auch die von diesen übertragenen Daten zu gewährleisten, haben verschiedene Länder zusätzliche Sicherheitsmassnahmen angeordnet.

Mit der vorliegenden Revision will der Bundesrat in der Schweiz eine Rechtsgrundlage schaffen, um die Sicherheit schweizerischer Fernmeldenetze von Gesetzes wegen zu erhöhen. Verfolgt werden folgende Ziele:

- Ein *allgemeines Mindestniveau an 5G-Netzwerksicherheit* in der Schweiz, basierend insbesondere auf internationalen Standards, soll erreicht werden.
- Mit einheitlichen und klaren *Regeln für die Schweizer IAP* soll das allgemeine Schutzniveaus im Bereich der Cyber-Sicherheit erhöht werden.

Vorgeschlagen werden mehrere Massnahmen zwecks Erhöhung der Cybersicherheit mit speziellem Fokus auf die Sicherheit von Mobilfunknetzen:

- Verpflichtung zur Bekämpfung von DDos-Attacken und zur Filterung gefälschter Quell-IPs für IAP
- Verpflichtung für IAP, die Sicherheit von CPE zu gewährleisten
- Recht für IAP, Internetzugänge oder Adressierungselemente zu sperren
- Pflicht für IAP zum Betrieb einer Meldestelle für Manipulationen
- Allgemeinverbindlicherklärung von internationalen Sicherheitsstandards
- Pflicht für Mobilfunkkonzessionäre, ein Informationssicherheits- und Kontinuitäts-Management zu betreiben
- Pflicht Network Operation Centers (NOC) und Security Operation Centers (SOC) in der Schweiz, dem europäischen Wirtschaftsraum oder dem UK zu betreiben

Position von Sunrise UPC

Sunrise UPC – wie auch die anderen Anbieterinnen von Telekommunikationsnetzwerken oder Komponenten – ist fortlaufend bestrebt, die Sicherheit ihrer Telekommunikationsnetze und -infrastrukturen hoch zu halten und laufend zu verbessern. Sunrise UPC kommt damit einem klaren und immer wichtigeren Bedürfnis der Kundinnen und Kunden nach, insbesondere im B2B-Bereich. Marktbedürfnissen und Wettbewerb führen also zu einer laufenden Steigerung des Sicherheitsniveaus. *Aus diesem Grund wäre eigentlich eine Anpassung der rechtlichen Grundlagen nicht zwingend nötig.* Doch kann die Definition eines Mindestniveaus dazu beitragen, das Vertrauen von Wirtschaft und Gesellschaft in die Sicherheit von Fernmeldenetzen insgesamt weiter zu erhöhen. Insofern wird die Revision von Sunrise UPC begrüsst.

Definition eines minimale Sicherheitsniveau kann Vertrauen stärken

Das Schadenpotential von Cyberangriffen ist gross. Die Anbieterinnen für Fernmeldedienste (FDA) nehmen ihre Verantwortungen wahr, sie können aber selbsterklärend nicht allein für Cybersicherheit verantwortlich gemacht werden. Wichtig ist darum festzuhalten, dass Sicherheit die Aufgabe jedes Akteurs ist und bleibt.

Die Sicherheit der Netzwerke und speziell auch der Kundendaten geniesst bei Sunrise UPC seit jeher einen sehr hohen Stellenwert. *Mit verschiedenen etablierten Instrumenten sorgt Sunrise UPC bereits heute für höchste Sicherheitsstandards und setzt damit die meisten Massnahmen, die mit der Revision gefordert werden, bereits um.* Sunrise UPC betreibt ein Security Operations Center, ein Business Continuity Management System nach ISO 22301 und die gesamte Unternehmung wird von einem ISO 27001 zertifizierten Informationssicherheits-Management-System (ISMS) end to end abgedeckt. Zudem wird bei Sunrise UPC die Sicherheit laufend gemäss entsprechender internationaler Best practise weiterentwickelt.

Meldestelle für Störungen (Art. 96 FDV)

Neu sollen Störungen im Betrieb von Fernmeldeanlagen und -diensten, sofern mindestens 30'000 Kundinnen und Kunden betroffen sind, nicht wie bisher dem Bundesamt für Kommunikation (BAKOM), sondern der Nationalen Alarmzentrale (NAZ) gemeldet werden. *Gegen die Änderung der zuständigen Stelle, der Störungen zu melden sind, ist grundsätzlich nichts einzuwenden.*

Wichtig ist, dass die Zuständigkeiten der verschiedenen Amtsstellen, denen die FDA Vorfälle zu melden haben, zweifelsfrei definiert sind und ihre Anzahl so gering wie möglich gehalten wird.[1] So können sowohl auf der Seite der Bundesverwaltung wie auch der Betreiberinnen von 5G-Netzen und der Internet Access Provider (IAP) Doppelspurigkeiten reduziert, Missverständnisse vermieden, Antwortzeiten kurzgehalten und das Risiko falscher Reaktionen minimiert werden. Darum ist es richtig, keine zusätzliche Meldestelle zu schaffen. Idealerweise nimmt künftig sogar nur eine einzige Bundesstelle sämtliche Störungsmeldungen entgegen und leitet diese bei Bedarf an andere Bundesstellen weiter.

Im Rahmen des neuen Informationssicherheitsgesetzes (ISG) will das Eidgenössische Finanzdepartement, das NCSC als zentrale Meldestelle für Cybervorfälle definieren. *Sunrise UPC schlägt darum vor, in Art. 96 FDV das NCSC statt die NAZ als entsprechende Stelle festzulegen.* Der Bund hat dafür die gesetzlichen Grundlagen zu schaffen, die Prozesse entsprechend zu planen und beim NCSC die nötigen Infrastrukturen und Kompetenzen bereitzustellen. Sunrise UPC erachtet es als wichtig, dass die Revision der FDV und die Anpassung der SIG koordiniert erfolgen.

[1] Fernmeldedienstanbieterinnen müssen Störungen je nach ihrer Art bereits heute unterschiedlichen Stellen melden dem BAKOM, der Nationalen Alarmzentrale (NAZ) oder dem Nationalen Zentrum für Cybersicherheit (NCSC)

Vorgaben zur Sicherheit von CPE klar formulieren

Im erläuternden Bericht zur Änderung der Verordnung über Fernmeldedienste (FDV) führt das BAKOM aus, welche Massnahmen für die Geräte vorgesehen sind, welche die IAP ihren Kundinnen und Kunden zur Verfügung stellen (sogenanntes «Customer Premises Equipment», CPE).[2] Diese Massnahmen sollen in den technischen und administrativen Vorschriften (TAV) zur FDV festgehalten werden.

Sunrise UPC befürwortet die Definition eines Basis-Sicherheitsstandards für CPE. Bereits heute erfüllen ihre Endgeräte den Wortlaut der Verordnung. Die Formulierungen im erläuternden Bericht können jedoch zu Missverständnissen führen und erfordern deshalb folgende Anpassungen und Präzisierungen:

Wortlaut im erläuternden Bericht	**Kommentar von Sunrise UPC**
– *Nicht benötigte Dienste auf dem CPE müssen deaktiviert sein.*	Auf den CPE (z.B. TV Boxen und Router) stehen unzählige Funktionen zur Verfügung. Einige Kundinnen und Kunden nutzen viele davon, andere nur die wenigsten. Für die IAP ist es unmöglich, die Funktionen entsprechend den individuellen Bedürfnissen zu aktivieren oder zu deaktivieren. Grundsätzlich liegt es nicht im Interesse der IAP, auf ihren CPE nicht gewünschte oder sogar unsichere Dienste anzubieten. *Sunrise UPC schlägt vor, diesen Punkt ersatzlos zu streichen.*
– *CPE müssen zeitnah mit vom Hersteller als kritisch eingestuften Sicherheitsupdates versorgt werden. Werden die CPE vom Hersteller als «End of Life» klassifiziert, müssen sie ausgetauscht werden.*	Der Begriff «End of Life» wird nicht einheitlich verwendet. So ist denkbar, dass ein Hersteller ein Gerät als «End of Life» deklariert, weil er ein Nachfolgeprodukt verkaufen will, aber weiterhin Sicherheitsupdates vom Hersteller selbst oder vom FDA zur Verfügung gestellt werden. *Sunrise UPC schlägt vor, diesen Punkt folgendermassen zu formulieren (Ergänzung unterstrichen):* *– CPE müssen zeitnah mit vom Hersteller oder den FDA als kritisch eingestuften Sicherheitsupdates versorgt werden. Werden die CPE nicht mehr vom Hersteller oder den FDA mit kritisch eingestuften Sicherheitsupdates versorgt, müssen sie ausgetauscht werden.*

[2] Seiten 8 und 9, Ausführungen zu Art. 96a (Sicherheitsmassnahmen)

Massnahmen basieren auf internationalen Standards

Die Vorlage orientiert sich im Wesentlichen an Massnahmen, welche auch in anderen Ländern, insbesondere der EU, implementiert werden und basieren auf international anerkannten Sicherheitsnormen und -initiativen (z.B. ENISA, NESAS, GSMA knowledge base, SCAS, 3GGP, EU 5G Toolbox, ISO). Indem auf eine nationale Sonderlösungen weitgehend verzichtet wird, können die Massnahmen effizient umgesetzt und die Sicherheitsstandards laufend den technischen Entwicklungen angepasst werden. Zudem orientieren sich auch die international tätigen Technologiefirmen sowie zunehmend auch die Schweizer Geschäftskunden an diesen Standards (z.B. Finanzbranche). Letzteres führt branchenübergreifend zu einer Erhöhung der Netzwerksicherheit und zeigt zudem, dass Markt und Wettbewerb automatisch zu einer Steigerung des Sicherheitsniveaus führen.

Sunrise UPC erachtet darum dieses Vorgehen als richtig. Es ist zentral, dass sich die schweizerische Gesetzgebung in einem international anerkannten und von den internationalen Zulieferern bekannten Rahmen bewegt. Spezielle Regelungen für die Schweiz (sogenannter Swiss finish), sind zu vermeiden. Sie bremsen den technologischen Fortschritt und die Innovationskraft der Schweiz. Zurzeit gehören die Schweizer Fernmeldenetze zu den besten der Welt und bilden damit eine wichtige Grundlage für die Wettbewerbsfähigkeit der Schweiz.

Diesem Grundsatz muss der Bund unbedingt auch bei den noch folgenden technischen Präzisierungen auf Stufe technischer und administrativer Vorschriften (TAV) treu bleiben (vgl. Art. 96g FDV).

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

Swisscom (Schweiz) AG, Konzernrechtsdienst, 3050 Bern

Eidg. Departement für Umwelt, Verkehr,
Energie und Kommunikation UVEK
Bundeshaus Nord
3003 Bern

Per E-Mail an: tp-secretariat@bakom.admin.ch

Datum	18. März 2022	**Seite**
Ihr Kontakt	Martin Ghermi / Tel. +41 58 223 29 93 / E-Mail: martin.ghermi@swisscom.com	1 von 6
Thema	**Stellungnahme Swisscom zum Entwurf der revidierten FDV (Art. 96ff)**	

Sehr geehrte Frau Bundesrätin Sommaruga,
sehr geehrte Damen und Herren

Namens Swisscom (Schweiz) AG (nachfolgend "Swisscom") bedanken wir uns für die im Rahmen der aktuellen Vernehmlassung zum Entwurf der revidierten Verordnung über Fernmeldedienste (E-FDV) eingeräumte Möglichkeit, zu den vorgeschlagenen neuen Sicherheitsbestimmungen Stellung zu nehmen.

Einleitende Bemerkungen

Swisscom teilt die Einschätzung des Bundesrates, dass der Sicherheit von Fernmeldenetzen und -diensten besondere Beachtung geschenkt werden muss und entsprechende Vorkehrungen zu treffen sind. Bei neuen Regulierungsvorhaben soll ein risikobasierter Ansatz gewählt werden und die Umsetzung mit Augenmass erfolgen. Uns erscheint in diesem Zusammenhang wichtig, dass genügend lange Umsetzungsfristen vorgesehen werden. Nachfolgend werden einige Bemerkungen und Änderungsanträge von Swisscom mit Bezug auf die jeweilige Bestimmung im Entwurf der revidierten FDV (E-FDV) angebracht. In den Änderungsanträgen sind die konkreten Änderungen jeweils **fett** hervorgehoben.

Art. 96

Die aktuell geltende Regelung in den technischen und administrativen Vorschriften (TAV, SR 784.101.113/1.8) mit den darin enthaltenen Kriterien und Schwellenwerten für eine Meldepflicht hat sich nach der Wahrnehmung und den Erfahrungen der Fernmeldebranche in den vergangenen rund acht Jahren bewährt. Diese Tatsache wird dadurch belegt, dass in der Vergangenheit weder seitens der Behörden noch seitens der verpflichteten FDAs irgendwelche Änderungsmassnahmen beantragt wurden, weshalb an den aufgeführten und bewährten Kriterien und Schwellenwerten auf Stufe TAV festzuhalten ist.

Swisscom (Schweiz) AG
Konzernrechtsdienst
CH-3050 Bern

Telefon 058 223 29 93

Standortadresse
Alte Tiefenaustrasse 6
3048 Worblaufen

Heute sind in Ziffer 2 der TAV verschiedene Vorgaben enthalten, welche miteinander verknüpft und für die Meldung einer Störung massgebend sind. Im Entwurf wurde der Schwellenwert von 30'000 potenziell betroffenen Kunden auf Stufe Verordnung gehoben, indes ohne Begründung im Erläuterungsbericht. Swisscom regt an, sämtliche Kriterien und Schwellenwerte inklusive der massgebenden Dauer der zu meldenden Störungsausfälle wie bisher in den TAV zu belassen. Mit dem bewährten stufengerechten Regelungsansatz ist insbesondere sichergestellt, dass die entsprechenden Schwellenwerte bei Bedarf durch das BAKOM flexibel an geänderte Gegebenheiten angepasst werden können. Der Schwellenwert für die Dauer einer Störung sollte dabei weiterhin bei einer Stunde liegen. Sobald jedoch absehbar ist, dass eine Störung länger dauert, soll eine Meldung unverzüglich neu an die Nationale Alarmzentrale (NAZ) erfolgen.

Die Überschreitung tieferer Schwellenwerte wäre aufgrund des jeweils vorgängig zur erstellenden Störungsbildes sehr schwierig zu ermitteln und würden eher zu Verwirrungen und möglicherweise zu unnötigen bzw. falschen Meldungen führen. Vor diesem Hintergrund besteht insofern ein ausgewiesenes Interesse, dass an den bisher bewährten Kriterien und Schwellenwerten festgehalten wird.

Neben dem BAKOM kann die NAZ selbstverständlich auch weitere Behörden über solche Störungen informieren, z.B. kantonale Polizeibehörden.

Der Schwellenwert von 30'000 potenziell betroffenen Kunden im Festnetz resp. die entsprechende Anzahl Antennenstandorte in einem zusammenhängenden Gebiet im Mobilfunk (mindestens 25) sollen weiterhin in den TAV vorgeschrieben werden. Dies gilt auch für den Schwellenwert der Mindestdauer von einer Stunde für zu meldende Störungen bei Netzen oder Diensten. Aus diesen Überlegungen schlägt Swisscom vor, Art. 96 Absatz 1 E-FDV wie folgt zu ändern:

Äderungsantrag zu Art. 96 Absatz 1 E-FDV:
[1]Die Anbieterinnen von Fernmeldediensten müssen Störungen im Betrieb ihrer Fernmeldeanlagen und -dienste**, welche die Schwellenwerte in den technischen und administrativen Vorschriften des BAKOM überschreiten,** unverzüglich der Nationalen Alarmzentrale melden.

Art. 96a Sicherheitsmassnahmen

Swisscom stimmt den in diesem Artikel neu vorgeschlagenen Sicherheitsmassnahmen unter Berücksichtigung der folgenden Einschränkungen und Bemerkungen grundsätzlich zu.

Es ist richtig und auch konsequent, dass sich die Bestimmung in Absatz 1 auf die in der Botschaft zur Teilrevision des FMG skizzierte Absicht des Bundesrates beschränken muss, d.h. auf die Bekämpfung von DDoS Angriffen zum Schutz der Netze der FDAs. Wie korrekterweise im erläuternden Bericht aufgeführt, haben die Kunden selbst die Möglichkeit, ihre eigene Infrastruktur mit auf dem Markt erhältlichen Lösungen zu schützen.

Im Zusammenhang mit Absatz 2 müssen einerseits die detaillierten Vorgaben noch in den zu erstellenden TAV des BAKOM formuliert werden, welche den betroffenen FDAs vorzugsweise im Rahmen einer Konsultation zu unterbreiten wären, damit eine praxisnahe Umsetzung gewährleistet ist. Andererseits dürfen die Vorschriften nicht derart restriktiv sein, dass das Management der CPEs durch die FDAs unnötig erschwert oder gar verunmöglicht würde. Beispielsweise müssen gewisse Ports der CPEs im Auslieferungszustand offen sein, um das CPE via Fernwartungssystem der FDA konfigurieren zu können. Der Schutz der CPEs gegen Fremdeinwirkung ist in diesem Fall bereits via Access Control List (ACL) gewährleistet. Übrige für den Betrieb offene Ports müssen auch via ACL gesichert werden, sofern es die konkrete Anwendung zulässt. Dabei wird der Zugriff durch die FDAs mittels geeigneten Verschlüsselungsmassnahmen bewerkstelligt. Auch müssen gewisse Dienste, wie z.B. WLAN, standardmässig aktiviert sein, um die erwartete Kundenexperience zu erfüllen und unnötige Anrufe im Callcenter zu vermeiden.

Für einige vorzunehmende aufwändigere Umstellungen in den Prozessen und Systemen der FDAs müssen genügend lange Umsetzungsfristen resp. Vorlaufzeiten, d.h. mindestens 6 Monate, eingeräumt werden.

Die Sperrung von Anschlüssen basierend auf Absatz 3 des Art. 96a E-FDV soll, wie im erläuternden Bericht dargelegt, dann vorgenommen werden, wenn schädliche Aktivitäten von solchen Anschlüssen ausgehen. Solche schädlichen Aktivitäten können auch von überwachten Anschlüssen gemäss BÜPF/VÜPF ausgehen. Eine FDA sollte nach unserem Verständnis auch diese Anschlüsse zum Schutz der Netze und Dienste sperren, insbesondere dann, wenn eine beträchtliche Gefahr für Sicherheit und Stabilität der Kommunikationseinrichtungen besteht. Es ist aus unserer Sicht fraglich, ob die im erläuternden Bericht aufgeführten Bestimmungen (Art. 26 Abs. 2 Bst. a BÜPF sowie Art. 29 Abs. 2 und 3 VÜPF) genügen, um das darin enthaltene Vorgehen resp. die unterschiedliche Behandlung von überwachten und nicht überwachten Anschlüssen zu rechtfertigen. Eine solche Unterscheidung wäre im Übrigen in der Praxis auch nicht einfach zu bewerkstelligen und würde mitunter zur Folge haben, dass Überwachungsaufträge einem breiteren Kreis von Mitarbeitern zugänglich gemacht werden müssten.

Für die Implementation der Sicherheitsmassnahmen sowohl im Fest- als auch im Mobilfunknetz müssen sodann angemessene Umsetzungsfristen eingeräumt werden. Swisscom regt an, die betroffenen FDAs zu den zeitlichen Umsetzungsarbeiten eng einzubeziehen.

Die Beurteilung, ob Fernmeldeanlagen aktualisiert werden müssen, muss den FDAs überlassen werden, sofern sie diese den Kunden zur Verfügung stellen und sie weiterhin die Kontrolle über diese Anlagen haben. Für alle anderen Anlagen, die von den Kunden genutzt werden, sind diese selbst verantwortlich.

Für allenfalls aus Sicherheitsgründen notwendigen Änderungen bei zeitlich und inhaltlich beschränkten Router-Zugängen im Supportprozess wäre es zudem notwendig, vorgängig mit den Anbietern von Internetzugängen alternative Lösungsmöglichkeiten zu diskutieren. Die entsprechenden Ergebnisse wären im Nachgang dazu in einer nachgeordneten, noch zu erstellenden TAV des BAKOM abzubilden, wobei auch in diesem Kontext aufgrund der voraussichtlich grossen Anzahl betroffener Geräte genügend Zeit für die Umsetzung eingeräumt werden muss.

Fernmeldeanlagen können von den Anbietern von Internetzugängen aus verschiedenen Gründen und jeweils im konkreten Kundenkontakt ausgetauscht werden. Die Beurteilung, ob solche Anlagen aus sicherheitsrelevanten Gründen ausgetauscht werden müssen, darf nicht den Herstellern allein überlassen werden, sondern muss immer unter Einbezug der Beurteilung der verantwortlichen Anbieter von Internetzugängen erfolgen.

Bezüglich Kundenendgeräten im Mobilfunk (Smartphones) obliegt es heute bereits den Kunden, ihre Smartphones durch ein Update des Betriebssystems auf den neusten, auch sicherheitsrelevanten Stand zu bringen. In diesem Bereich werden die Anbieter von Internetzugängen die Entscheide der Kunden, ob und wann ein solches Update erfolgt, nicht übernehmen können, wenn man diesbezüglich die Kunden nicht bevormunden will. Ausserdem ist die technische Machbarkeit einer solchen erzwungenen Aktualisierung des Smartphone-Betriebssystems durch Anbieter von Internetzugängen völlig offen. Auch der Entscheid, ob ein Smartphone erneuert werden soll oder nicht, bleibt selbstverständlich immer dem Kunden überlassen. Dabei werden sich die Kunden, wie bereits heute, an den Informationen der Hersteller der Geräte resp. der Betriebssysteme (z.B. iOS oder Android) orientieren.

Die Sperrung von Zugängen erfolgt heute bereits aufgrund anderer gesetzlicher Vorgaben (UWG) bzw. entsprechender behördlicher Anordnungen und ist in den Prozessen für leitungsgebundene Internetzugänge etabliert. Anders präsentiert sich die Situation im Bereich der mobilen Internetzugänge. Hierfür müssten die technischen Möglichkeiten erst noch geschaffen werden, falls der Verordnungsgeber wirklich die Absicht hat, auch die Mobilfunkinternetzugänge in der gleichen Art zu regulieren.

Swisscom empfiehlt in diesem Zusammenhang ausdrücklich, dass eine abschliessende Beurteilung durch das BAKOM erst im Nachgang einer eingehenden technischen Analyse zusammen mit den Anbietern von mobilen Internetzugängen erfolgt. Swisscom stellt seine Expertise dem BAKOM für eine solche Analyse jedenfalls bei Bedarf gerne zur Verfügung. Dabei kommt den Betriebssystemen resp. den Herstellern von mobilen Endgeräten eine entscheidende Rolle zu (z.B. Apple mit iOS oder Google mit Android). Ohne deren Einbezug sind aus der Wahrnehmung von Swisscom keine sinnvollen resp. wirkungsvollen Lösungen

bei den mobilen Internetzugängen zu erreichen. Dies bedeutet, dass Absatz 2 von Art. 96a E-FDV wie folgt geändert werden muss.

Änderungsantrag zu Art. 96a Absatz 2 E-FDV: [2]Sie konfigurieren die Sicherheitseigenschaften aller Fernmeldeanlagen, die sie ihren Kundinnen und Kunden zur Verfügung stellen, gemäss den anerkannten Regeln der Technik und aktualisieren sie unverzüglich, sofern **dies technisch möglich ist** und sie weiterhin **allein** die Kontrolle über diese Anlagen ausüben.

Art. 96b Meldestelle

Aus Sicht Swisscom haben die meisten FDAs bereits eine solche Stelle, die derartige Meldungen entgegennimmt und Abwehrmassnahmen auslösen kann. Sollten allenfalls in den TAV weitere Anforderungen definiert werden, müssten diese zunächst geprüft werden, weshalb Swisscom eine Konsultation der betroffenen FDAs zu solchen Bestimmungen in den TAV als begrüssenswert erachtet.

Art. 96c Vollzug

Da der Vollzug des vierten Abschnitts der E-FDV durch das BAKOM in Zusammenarbeit mit dem NCSC erfolgen soll, müsste wohl aus naheliegenden Gründen die Meldestelle unter Art. 96b mit derjenigen Stelle, die im Rahmen der Revision des Informationssicherheitsgesetzes für kritische Infrastrukturen Meldungen an den NCSC sendet, zusammengelegt werden.

Art. 96d Geltung

Die Beschränkung des Geltungsbereichs auf 5G für die Art. 96e bis Art. 96g E-FDV ist aus unserer Sicht verhältnismässig und angemessen.

Art. 96e Sicherheitsmanagement

Hinsichtlich der Vorgaben gemäss Absatz 1 geht Swisscom davon aus, dass die beschriebenen Tätigkeiten basierend auf der Anwendung eines Information Security Management Systems (ISMS) beruhen, welche eine Zertifizierung nach ISO/IEC 27001 ermöglichen. Das ISMS enthält demgemäss die Bereiche gemäss dem erwähnten Standard und umfasst sämtliche Massnahmen zum Schutz von Informationen und informationsverarbeitenden Systemen. Es hat das Ziel, Informationen sowie informationsverarbeitende Systeme der FDA und ihren Kunden vor dem Verlust der Grundwerte zu schützen: Vertraulichkeit, Verfügbarkeit, Integrität und Sicherheit. Dabei ist das Security Management auf folgende Themenbereiche ausgerichtet:

- **Identify:** Sicherheitsrisiken von Assets identifizieren, behandeln und transparent machen;
- **Protect:** Massnahmen, um die Verfügbarkeit der identifizierten Assets zu gewährleisten;
- **Detect:** Überwachung von Assets, dass Sicherheitsereignisse festgestellt werden können;
- **Respond:** Massnahmen bei Sicherheitsereignissen auf Assets, um Schäden möglichst gering zu halten;
- **Recover:** Definition von Massnahmen, um Schäden zu minimieren und vereinbarte Verfügbarkeit der Assets wiederherzustellen.

Die Sicherheitsorganisation einer FDA sollte dabei ebenfalls einem Three Lines of Defense-Modell folgen. Die entsprechenden Stufen sind:

- **First Line of Defense:** sämtliche Mitarbeitende;
- **Second Line of Defense:** Die Security-Organisationseinheit und diverse Security-Funktionen;
- **Third Line of Defense:** Internal Audit.

Swisscom unterstützt die Vorgaben in den Absätzen 2 und 3 von Art. 96e E-FDV in dieser Form grundsätzlich. Ein Business Continuity Management System soll nach dessen Aufbau konsolidiert und möglichst weiter ausgebaut werden, mit dem Ziel einer allfälligen Zertifizierung, z.B. nach ISO 22301.

Art. 96f Betrieb sicherheitskritischer Fernmeldeanlagen

Was Absatz 1 betrifft, kann festgehalten werden, dass Swisscom die einschlägigen, international etablierten Sicherheitsnormen bereits anwendet.
Swisscom erfüllt sodann auch bereits die Vorgaben von Absatz 2 und betreibt sowohl das Network- als auch das Security Operation Center in der Schweiz. Länder der EU und des EWR erfüllen i.d.R. die gleichen Sicherheitsvoraussetzungen wie die Schweiz, weshalb wir der Bestimmung in dieser Form grundsätzlich zustimmen können.

Art. 96g Anwendbare Vorschriften und Aufsicht

Die Mobilfunkbetreiber wenden die einschlägigen, international etablierten Sicherheitsnormen bereits an. Spezielle, nur für die Schweiz anwendbare Vorschriften im Sinne eines "Swiss Finish" sind aus Sicht von Swisscom abzulehnen, da Sicherheitsnormen im international ausgerichteten Bereich der Informationssicherheit harmonisiert werden müssen.

Swisscom geht sodann davon aus, dass für sämtliche vom BAKOM zu erstellenden TAV im Rahmen der Bestimmungen von Art. 96d bis Art. 96g bei den betroffenen FDAs noch eine Konsultation durchgeführt wird und weitere Anwendungs- sowie Umsetzungsaspekte mit den betroffenen Adressaten eng abgesprochen werden.

Im Zusammenhang mit Art. 96g Abs. 2 E-FDV sollte nach Meinung von Swisscom sodann für die Pflicht zur Erstellung eines Audits auf Kosten der Mobilfunkkonzessionäre verlangt werden, dass für eine entsprechende Anordnung nicht nur (einfache) Verdachtsmomente, sondern ein qualifizierter Anlass bestehen muss. Mit anderen Worten müssen gute Gründe vorliegen, damit die Behörde die Mobilfunkkonzessionäre zu einem entsprechenden Audit, welches erfahrungsgemäss regelmässig mit nicht unwesentlichen Kostenfolgen verbunden sein dürfte, verpflichten könnte. Ein solch qualifizierter (begründeter) Verdacht besteht demnach nur, wenn ein allfälliger Anfangsverdacht oder gewisse Verdachtsmomente mindestens durch erste eigene Abklärungen der Behörde nicht ausgeräumt werden können. Bekanntlich orientieren sich auch Regulierungsansätze in anderen Rechtsbereichen an der Voraussetzung bzw. dem Aufgreifkriterium des "begründeten Verdachts" (siehe z.B. Art. 9 Abs. 1 des Geldwäschereigesetzes oder Art. 5 Verordnung über Sorgfaltspflichten und Transparenz bezüglich Mineralien und Metallen aus Konfliktgebieten und Kinderarbeit [VSoTr]). Swisscom schlägt vor, diesen sinnvollen konzeptionellen Ansatz analog auch in Art. 96g E-FDV wie folgt vorzusehen.

Äderungsantrag zu Art. 96g Absatz 2 E-FDV:

[2]Besteht ein **begründeter** Verdacht auf Rechtsverletzung und erweist es sich zur Feststellung des Sachverhalts als notwendig, kann das BAKOM von den Mobilfunkkonzessionären verlangen, sich auf eigene Kosten und bei einer qualifizierten Stelle einem Audit zu unterziehen oder ihre Fernmeldeanlagen prüfen zu lassen.

Für die Berücksichtigung unserer Bemerkungen und Anträge in der vorliegenden Stellungnahme bedanken wir uns bestens.

Freundliche Grüsse
Swisscom (Schweiz) AG

sign. Patrick Dehmer

Patrick Dehmer
General Counsel

sign. Martin Ghermi

Martin Ghermi
Senior Regulatory Manager

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Wettbewerbskommission WEKO
Commission de la concurrence COMCO
Commissione della concorrenza COMCO
Competition Commission COMCO

CH-3003 Bern, WEKO

Per E-Mail
Bundesamt für Kommunikation BAKOM
2501 Biel

Per E-Mail an: tp-secretariat@bakom.admin.ch
Unser Zeichen: 041.1-00011/mud/sca/std
Direktwahl: 058 466 34 10
Bern, 01.02.2022

041.1-00011: Vernehmlassungsverfahren zur Änderung der Verordnung über Fernmeldedienste (FDV) – Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten

Sehr geehrte Damen und Herren

Wir bedanken uns für die Einladung zur Stellungnahme im Rahmen des oben genannten Vernehmlassungsverfahrens.

Gerne teilen wir Ihnen hiermit mit, dass aus wettbewerblicher Sicht keine Bemerkungen hierzu angezeigt sind.

Freundliche Grüsse

Wettbewerbskommission

Prof. Dr. Andreas Heinemann
Präsident

Prof. Dr. Patrik Ducrey
Direktor

Wettbewerbskommission
Hallwylstrasse 4, CH-3003 Bern
Tel. +41 58 462 20 40, Fax +41 58 462 20 53
weko@weko.admin.ch
www.weko.admin.ch