Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt,
Verkehr, Energie und Kommunikation UVEK

Bern, den 16. November 2022

Revision der Verordnung über Fernmeldedienste (FDV)

Bericht über die Ergebnisse der Vernehmlassung (3. Dezember 2021 bis 18. März 2022)

Inhalt

1 Einleitung

Artikel 48*a* des Fernmeldegesetzes gibt dem Bundesrat die Kompetenz, die Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten zu regeln. Am 3. Dezember 2021 hat er eine Änderung der Verordnung über Fernmeldedienste (FDV) in die Vernehmlassung geschickt, mit der er diese Kompetenz umsetzen will. Die vorgeschlagenen Anpassungen betreffen die Meldung von Störungen, die Bekämpfung unbefugter Manipulationen von Fernmeldeanlagen sowie die Sicherheit der Mobilfunknetze der neusten Generation (5G). Die Kantone, die in der Bundesversammlung vertretenen politischen Parteien und die interessierten Kreise waren eingeladen, bis zum 18. März 2022 Stellung zu nehmen. Zur Vernehmlassungsvorlage sind 46 Stellungnahmen eingegangen. Im Anhang sind die einzelnen Teilnehmenden und das entsprechende Abkürzungsverzeichnis aufgeführt. Die Stellungnahmen können auf der Website des BAKOM eingesehen werden (www.bakom.admin.ch > Das BAKOM > Organisation > Rechtliche Grundlagen > Vernehmlassungen 2021).

Die Stellungnahme der **RK MZF** wurde von den Kantonen **BL, JU, AI, AR, LU, TG, NW, FR, BE, TI, GR, AG, OW, GE, GL** sowie von **IVR, KKPKS, KAPO AI, Gebäudeversicherung Kanton Zug, KKJPD** und **FKS** ganz, teilweise oder mit Änderungen übernommen.

Hinsichtlich der spezifischen Massnahmen für 5G-Mobilfunknetzbetreiberinnen verweist **SUISSEDIGITAL** in seiner Stellungnahme auf jene seines Mitglieds **Sunrise UPC.**

2 Allgemeine Bemerkungen

Die **WEKO** und die Kantone **UR, SH, BS, VS** sowie **SBV** und **SP** begrüssen oder unterstützen den in die Vernehmlassung gegebenen Verordnungsentwurf ohne weitere Kommentare oder Änderungsvorschläge.

RK MZF, die Kantone **JU, BL, TG, AI, AR, SO, SG, LU, NW, FR, BE, TI, ZG, GR, OW, GE, GL, VD, NE** sowie der **Internetverband für Rettungswesen, KKPKS, KAPO AI, Gebäudeversicherung Zug, Staatskanzlei ZH, KKJPD, asut, Sunrise UPC, Swisscom, SRG, digitalswitzerland, Salt, FER, FKS** und **economiesuisse** sind mit dem Verordnungsentwurf grundsätzlich einverstanden, haben aber Kommentare oder Anpassungsvorschläge angebracht.

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

Das Thema der Sicherheit von Informationen und Fernmeldeinfrastrukturen bildet bei **SUISSEDIGITAL** ein zentrales strategisches Verbandsthema. **SUISSEDIGITAL** meint, dass die vorgeschlagenen Massnahmen beim Betrieb von Fernmeldeinfrastrukturen und -diensten zwangsläufig mit höheren Investitionen und Betriebskosten ihrer Mitglieder verbunden sind, die am Ende auch die Kundinnen und Kunden ihrer Mitglieder betreffen.

Aus Sicht des **SBV** 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 von Nutzenden und Unternehmen in die Digitalisierung sowie die damit verbundenen Anwendungen fördern.

Das **Centre Patronal** befürwortet die vorgeschlagenen Anpassungen, überlässt jedoch die Beurteilung, ob die geforderten Anstrengungen praktikabel oder ausreichend sind, den betroffenen Fernmeldedienstanbieterinnen.

Asut begrüsst die vorgeschlagene Revision der FDV. Sie habe das Potenzial, das Vertrauen von Wirtschaft und Gesellschaft in die Sicherheit von Fernmeldenetzen als kritische Infrastruktur weiter zu stärken.

Gemäss **Sunrise UPC** wäre eigentlich eine Anpassung der rechtlichen Grundlagen nicht zwingend nötig. Mit verschiedenen etablierten Instrumenten sorge sie bereits heute für höchste Sicherheitsstandards und setze damit die meisten der vorgeschlagenen Massnahmen bereits um.

Swisscom teilt die Einschätzung des Bundesrates, dass der Sicherheit von Fernmeldenetzen und -diensten besondere Beachtung geschenkt werden muss und entsprechende Vorkehrungen zu treffen sind. Wichtig scheinen ihr ausreichende Umsetzungsfristen.

Wichtig ist aus Sicht der **SRG** zudem der Erlass des zweiten Massnahmenpakets, das die Stromversorgung gewährleisten soll.

3 Bemerkungen zu den Bestimmungen des Vorentwurfs

Art. 96 Störungsmeldung

IVR, KKPKS, KKJPD, FKS, GVZG, RK MZF, AG, AI, AR, BE, BL, FR, GE, GL, LU, NW, OW, SO, TG, TI, VD, ZG und **Kapo AI** regen an, dass die Alarmierungs- und Meldeprozesse bzw. die Rollen der einzelnen Akteure und Stellen detailliert beschrieben werden.

Absatz 1

RK MZF, IVR, KKPKS, KKJPD, FKS, Kapo AI, GVZG, BL, AI, AR, TG, SO, SG, LU, FR, NW, BE, TI, AG, OW, GL, GR, ZG und **GE** verlangen eine Herabsetzung der Schwellwerte einer meldepflichtigen Störung auf 1000 betroffene Kundinnen und Kunden während mindestens 15 Minuten bzw. 10 Minuten für den Kanton **JU**.

Swisscom will an den bestehenden Schwellenwerten von 30 000 betroffenen Kundinnen und Kunden und 1 Stunde festhalten.

IVR, KKPKS, KKJPD, FKS, SVP, GVZG, economiesuisse, Swisscom, SO, SG, BE, OW und **Kapo AI** fordern, dass der Schwellwert der betroffenen Kundinnen und Kunden weiterhin in den technischen und administrativen Vorschriften (TAV) und nicht auf Stufe FDV geregelt wird. Dies ermögliche eine rasche Anpassung an neue Gegebenheiten.

Swisscom und **Salt** stimmen der NAZ als Meldestelle zu.

IVR, KKPKS, KKJPD, FKS, GVZG, Kapo AI, SO, SG, BE, OW und **VD** äussern sich dahingehend, dass die Anbieterinnen von Fernmeldediensten die zuständigen kantonalen Notrufzentralen zu informieren haben, bevor die Meldungen an die NAZ oder weitere Organe abgesetzt werden.

Asut, Sunrise UPC, Digital Switzerland und **economiesuisse** betonen, dass die Zuständigkeiten der verschiedenen Amtsstellen, denen die FDA Vorfälle zu melden haben, zweifelsfrei definiert sein und ihre Anzahl so gering wie möglich gehalten werden müssen. Es wird auch vorgeschlagen, dass das NCSC statt die NAZ als Meldestelle festzulegen sei. Es sei wichtig, die Revision der FDV und die Anpassung des Informationssicherheitsgesetzes (ISG) zu koordinieren.

Absatz 2

IVR, KKPKS, KKJPD, FKS, SO, FR, TI, OW, GE, GL und **VD** stören sich daran, dass die FDV ausschliesslich die Information des BAKOM über die gemeldeten Störungen durch die NAZ regelt. Es seien beispielsweise auch das National Cyber Security Center (NCSC), die Melde- und Analysestelle Informationssicherung (MELANI) sowie die kantonalen Notrufzentralen von Polizei, Feuerwehr und Sanität einzubinden. **Swisscom** und **economiesuisse** unterstützen die Information von weiteren Behörden.

Salt fordert, dass die Daten der Störungsmeldungen nicht veröffentlicht werden. Diese könnten zu Falschdarstellungen in den Medien führen. Die gemeldeten Störungen seinen nur in aggregierter Form zu veröffentlichen.

Art. 96*a* Unbefugte Manipulation von Fernmeldeanlagen (Sicherheitsmassnahmen)

Absatz 1

IVR, KKPKS, KKJPD, BE, SG, OW, VD, KAPO AI, GVZG und **FKS** fordern, dass die Regelung nicht abschliessend auf DDoS-Angriffe zu beschränken sei. Derartige Angriffe seien vielmehr als Beispiel o. ä. aufzuführen. Zudem wird geltend gemacht, dass die Details von potenziellen Angriffsmechanismen nicht abschliessend in der FDV, sondern in den TAV zu regeln seien. Dies ermögliche ein adäquates Handeln und ein niederschwelliges Anpassen der zu berücksichtigenden Regelungen.

GE äussert sich dahingehend, dass die Betreiberinnen alle angemessenen technischen Mittel einsetzen sollten, um ihre Netze nach bewährten Sicherheitspraktiken zu konfigurieren, einschliesslich der Kontrolle gefälschter Adressierungsressourcen.

Economiesuisse macht geltend, es seien ausreichende Umsetzungsfristen und Vorlaufzeiten (mind. 6 Monate) vorzusehen und in den TAV zu definieren.

Absatz 2

Economiesuisse, **SVP** und **Swisscom** wünschen, den Anwendungsbereich klar einzugrenzen. Die Aktualisierung von Smartphones soll den Enduserinnen und -usern überlassen sein und nicht unter diese Bestimmung fallen. Gemäss **SUISSEDIGITAL** soll klargestellt werden, dass die Bestimmung ausschliesslich für die in der Rolle als IAP abgegebenen Geräte gilt.

Economiesuisse und **Swisscom** plädieren für ausreichende Umsetzungsfristen (mindestens 6 Monate).

Gemäss **economiesuisse** soll das CPE im Sinne eines Basis-Sicherheitsstandards reguliert werden. Zudem sollen die Anforderungen der Regulierung punktuell stärker an die technische Machbarkeit geknüpft werden.

Gemäss **FER** könne digitale Resilienz nur durch eine umfassende Betrachtung aller verschiedenen Facetten von Cyberrisiken erreicht werden.

Salt fordert «regelmässige» statt «unverzügliche» Aktualisierungen.

Der **SRG** gehen die Sicherheitsmassnahmen zu wenig weit, da sie auf CPE zugeschnitten sind und nur die IAP in die Pflicht nehmen. Das Ziel sollte der Schutz aller exponierten Endgeräte sein.

Swisscom möchte die Beurteilung, ob Fernmeldeanlagen aktualisiert werden müssen, den IAP überlassen.

Verschiedene Stellungnahmen äussern sich bereits zur konkreten technischen Umsetzung der vorliegenden Bestimmung. Teilweise nehmen sie explizit Bezug auf die im erläuternden Bericht aufgeführten Grundsätze für die TAV.

Gemäss **asut, digitalswitzerland** und **Sunrise UPC** sollte der TAV-Grundsatz zum *End of Life* von CPE umformuliert werden. Erst wenn das CPE nicht mehr mit kritisch eingestuften Sicherheitsupdates versorgt werde, sei es auszutauschen. **Swisscom** möchte die Beurteilung, ob Anlagen aus sicherheitsrelevanten Gründen auszutauschen seien, nicht den Herstellern allein überlassen. Die IAP seien einzubeziehen.

Asut und **Sunrise UPC** wünschen, den Grundsatz zu streichen, dass nicht benötigte Dienste auf dem CPE deaktiviert sein müssen. Gemäss **Swisscom** müssten gewisse Ports des CPE im Auslieferungszustand offen sein, damit es via Fernwartungssystem konfiguriert werden könne.

SUISSEDIGITAL und **Salt** wünschen, auf internationale Normen abzustellen.

Swisscom hält es für notwendig, dass sicherheitsspezifische Änderungen bei zeitlich und inhaltlich beschränkten Router-Zugängen im Rahmen des Supportprozesses vorgängig mit den IAP zu diskutieren und auf mögliche Alternativen zu prüfen sind. Allgemein sollen die TAV den betroffenen IAP vorgängig vorgelegt werden. Zudem sollen die Vorschriften nicht derart restriktiv sein, dass das Management des CPE durch die FDA unnötig erschwert oder gar verunmöglicht wird.

Absatz 3

FKS, Gebäudeversicherung Zug, BE, GE, OW, SO, SG, VD, Kapo AI, KKJPD, KKPKS und **IVR** fordern, dass Sperrungen oder Einschränkungen bei der Nutzung von Internetzugängen oder Adressierungselementen sehr selektiv erfolgen. Nur in Ausnahmefällen sollen sie dazu führen, dass über die betroffenen Anschlüsse keine Notrufnummern mehr gewählt werden können.

FKS, Gebäudeversicherung Zug, BE, OW, SO, Kapo AI, KKJPD, KKPKS und **IVR** beantragen, dass die betroffenen kantonalen Notrufzentralen informiert werden, falls durch die Einschränkungen mehr als 1000 Kundinnen und Kunden während mehr als 15 Minuten betroffen sein könnten.

AG, AI, AR, BL, GL, LU, NW, TI, TG, ZG und **RK MZF** fordern, dass bei Internetzugängen oder Adressierungselementen, von denen eine Gefährdung kritischer Infrastrukturen ausgeht, eine Pflicht zur Sperrung eingeführt wird.

Gemäss **BL** sollen die IAP verpflichtet werden, die von Sperrungen oder eingeschränkter Nutzung betroffenen Kundinnen und Kunden bei der Behebung des zugrundeliegenden Sicherheitsproblems zu unterstützen. Allgemein sollen die IAP die Internetzugänge so rasch wie möglich wiederherstellen.

TI fordert, dass Datenanalysen der IAP im Zusammenhang mit der Sperrung von Internetzugängen den Datenschutz nicht beeinträchtigt.

ZG wünscht, dass zur Vermeidung von Elektroschrott ergänzende Regelungen beim Verkauf und den Herstellern der Fernmeldeanlagen geprüft werden.

Swisscom stellt sich auf den Standpunkt, dass schädliche Aktivitäten auch von gemäss BÜPF überwachten Anschlüssen ausgehen könnten. Zum Schutz der Netze und Dienste sollten auch diese durch die IAP gesperrt werden können, insbesondere bei beträchtlicher Gefahr für Sicherheit und Stabilität der Kommunikationseinrichtungen. Zur Implementierung der Sicherheitsmassnahmen sowohl im Fest- als auch im Mobilfunknetz seien angemessene Umsetzungsfristen einzuräumen und die IAP bei der Umsetzung eng einzubeziehen. Bezüglich mobilen Internetzugängen müssten die technischen Möglichkeiten zur Sperrung erst noch geschaffen werden. Dabei komme den Betriebssystemen bzw. den Herstellern von mobilen Endgeräten eine entscheidende Rolle zu.

Art. 96*b* Unbefugte Manipulation von Fernmeldeanlagen (Meldestelle)

AG, AI, AR, BE, BL, FR, GE, GL, LU, NW, OW, SO, TG, TI, VD, ZH, FKS, Gebäudeversicherung ZG, IVR, KAPO AI, KKJPD, KKPKS, RK MZF und **SKS** fordern, dass die Rollen sämtlicher Stellen im Gesamtprozess von Meldung und Alarmierung im Cyberbereich im erläuternden Bericht detailliert aufzuführen sind. **SUISSEDIGITAL** und in diesem Sinne auch **asut** und **Sunrise UPC** wünschen, dass die Bestrebungen verwaltungsintern mit weiteren legislatorischen Projekten im Bereich Sicherheit abgestimmt und harmonisiert werden.

Economiesuisse beurteilt die Verpflichtung zum Betrieb einer Meldestelle kritisch, insbesondere da konkrete organisatorische Vorschriften gemacht werden, anstatt sich auf Handlungsgrundsätze zu beschränken. Die Organisation der Meldestelle sollte gemäss **Salt** in der Hand jeder einzelnen Anbieterin von Internetzugängen bleiben. Im Hinblick auf die Zusammenarbeit BAKOM / NCSC müsste gemäss **Swisscom** die vorliegende Meldestelle mit derjenigen zusammengelegt werden, die im Rahmen der Revision des ISG für kritische Infrastrukturen vorgesehen ist.

ZH erachtet eine genauere Bestimmung der Frist zur Ergreifung geeigneter Abwehrmassnahmen als wünschenswert.

Art. 96*c* Unbefugte Manipulation von Fernmeldeanlagen (Vollzug)

Salt fragt sich, worauf sich diese Vollzugsbestimmung bezieht. **Swisscom** wünschte eine Konsultation der betroffenen FDA, wenn in den TAV weitere Anforderungen definiert werden sollen.

Art. 96*d* Sicherheit von Netzen und Diensten, die von Mobilfunkkonzessionärinnen betrieben werden (Geltung)

ZG wünscht zu prüfen, ob die Massnahmen auf alle Mobilfunkdienste, und nicht nur auf die fünfte Generation, angewendet werden müssten.

ZH erachtet eine Beschränkung des Geltungsbereichs der Artikel 96*e*–96*g* auf die fünfte Mobilfunkgeneration ebenfalls als nicht sachgerecht. Aufgrund der Tatsache, dass die dritte und vierte Mobilfunkgeneration sowie WiFi-Hotspots von den Mobilfunkbetreiberinnen neben 5G für die nächsten Jahre weiterhin betrieben werden, sollten die Bestimmungen technologieneutral formuliert werden.

GE ist der Ansicht, dass dieser Artikel auf alle aktuellen und künftigen Mobilfunkgenerationen Anwendung finden sollte.

Auch **Salt** fragt sich, warum die betroffenen Artikel nicht grundsätzlich für die Mobilnetze und somit für alle Generationen gelten sollen.

Swisscom ihrerseits hält die Beschränkung auf 5G für verhältnismässig und angemessen.

Gemäss **FER** sei zu bedenken, dass 5G nur als Trägermedium diene: Entsprechend würde die Zahl der Datendiebstähle und Erpressungsfälle nur dann ansteigen, wenn die vernetzten Gegenstände fehleranfällig oder nicht korrekt konfiguriert seien, potenzielle Sicherheitslücken aufweisen oder angesichts des bekannten Risikos über ein unausgereiftes Sicherheitssystem verfügen würden. All dies komme erschwerend hinzu und zwinge den Gesetzgeber, auf die Kommunikationsmethoden, die Art der Verschlüsselung, den angemessenen Schutz und das erwartete Sicherheitsniveau aufmerksam zu machen. Es handle sich demnach um eine grosse Herausforderung, die klar über die Grenzen des Bundes, der IAP und anderer Intermediäre hinausgehe. Die Diskussionen darüber würden vielmehr auf der Ebene der Anbieterinnen von vernetzten Objekten und deren Pflichten stattfinden, was wiederum über übergeordnete Gremien wie die IETF und ihre Best Current Practice sowie die Abkommen der Welthandelsorganisation und der ENISA geschehe.

Art. 96*e* Sicherheit von Netzen und Diensten, die von Mobilfunkkonzessionärinnen betrieben werden (Sicherheitsmanagement)

Absatz 1

Sunrise und **Swisscom** haben bereits ein Sicherheitsmanagementsystem implementiert, und gemäss **Sunrise** soll die Sicherheit die Aufgabe jedes Akteurs sein und bleiben.

Salt kann nicht beurteilen, in welchem Umfang ein solches ISMS aufgebaut werden soll. Sie betreibt jedoch bereits ein Risikomanagementsystem, das ein Element des Managementsystems darstellt.

Asut und **Salt** sind der Meinung, eine vorgegebene Zertifizierung sei für kleinere Anbieterinnen mit grossem Aufwand und Kosten verbunden (einmalig und wiederkehrend). Eine konkrete Bestimmung würde einen schwerwiegenden Eingriff in die Wirtschaftsfreiheit bedeuten. Es sei deshalb unbedingt den Netzbetreiberinnen zu überlassen, wie sie das Sicherheitsmanagement umsetzen, und auf die Vorgabe von konkreten Standards in Verordnung und TAV sei zu verzichten. Das BAKOM solle erst bei Vorfällen aktiv werden und dann den Sachverhalt gemäss Artikel 96*g* untersuchen.

Absatz 3

FER und der Kanton **VS** unterstützen die Forderung, ein ISMS einzurichten, das auf ISO-Normen beruht. **Economiesuisse** ist der Meinung, dass das verlangte Managementsystem gemäss gängigen Standards und Zertifizierungen akzeptiert werden soll. Der Markt habe hier bereits ausreichende Grundlagen geschaffen, so dass eine schweizspezifische Regulierung nicht zielführend sei.

Swisscom, Sunrise und **FER** erwähnen die ISO-Norm ISO/IEC 27001 als Referenz für die Entwicklung eines Sicherheitsmanagementsystems, und **Swisscom, Salt, VS** und **FER** unterstützen das Kontinuitätsmanagementsystem und das Management von Sicherheitsvorfällen.

Sunrise betreibt ein Business Continuity Management System nach ISO/IEC 22301. **Swisscom** und **Sunrise** erwähnen auch diese Norm als Referenz für die Erstellung eines Kontinuitätsmanagementsystems.

Art. 96*f* Sicherheit von Netzen und Diensten, die von Mobilfunkkonzessionärinnen betrieben werden (Betrieb sicherheitskritischer Fernmeldeanlagen)

Absatz 1

Asut stimmt der Vorlage zu. Sie orientiere sich im Wesentlichen an Massnahmen, welche auch in anderen Ländern (insbesondere EU) implementiert würden und basiere auf international anerkannten Sicherheitsnormen und -initiativen (z. B. ENISA, NESAS, GSMA knowledge base, SCAS, 3GGP, ISO). Indem auf eine nationale Sonderlösung weitgehend verzichtet werde, könnten die Massnahmen effizient umgesetzt und die Sicherheitsstandards laufend den technischen Entwicklungen angepasst werden. Zudem orientierten sich auch die international tätigen Technologiefirmen sowie zunehmend auch die Schweizer Geschäftskunden an diesen Standards (z. B. Finanzbranche). Letzteres führe branchenübergreifend zu einer Erhöhung der Netzwerksicherheit und zeige zudem, dass Markt und Wettbewerb automatisch zu einer Steigerung des Sicherheitsniveaus führten.

Swisscom teilt mit, dass sie die einschlägigen, international etablierten Sicherheitsnormen bereits anwendeten.

Salt begrüsst die vorgeschlagene Zertifizierung nach anerkannten Sicherheitsnormen. Es gelte zu verhindern, dass hier schweizspezifische Normen geschaffen würden. Die Schweizer Mobilfunknetze würden vom Bundesamt für wirtschaftliche Landesversorgung (BWL) als systemrelevant und als kritische Infrastruktur eingestuft. Die entsprechenden Fernmeldeanlagen seien somit sicherheitskritisch. Salt ist deshalb nicht klar, was das BAKOM diesbezüglich genau definieren soll.

Absatz 2

Der vorgeschlagenen Standortpflicht bezüglich Netzwerk- und Sicherheitsbetriebszentren (Schweiz, EWR Vereinigtes Königreich) stimmen **IVR, KKPKS, KKJPD, SG, KAPO AI, GVZG, BE, OW, GE, GL, FKS, SO, VD, VS, ZH** und **Swisscom** zu. **Salt** möchte die Regelung auf Staaten mit angemessenem Datenschutz gemäss Liste des EDÖB ausdehnen. Neben ihrem Einverständnis zu einer Standortpflicht schlagen **IVR, KKPKS, KKJPD, SG, KAPO AI, GVZG, BE, OW, GE, GL, FKS, SO** und **VD** vor, auch einen Firmensitz oder Ableger in der Schweiz vorzuschreiben.

Art. 96*g* Sicherheit von Netzen und Diensten, die von Mobilfunkkonzessionärinnen betrieben werden (anwendbare Vorschriften und Aufsicht)

Absatz 1

Die **SVP** geht davon aus, dass die Ausgestaltung der untergeordneten TAV durch das BAKOM in enger Zusammenarbeit mit der Branche erfolge.

Gemäss **asut** seien spezielle Regelungen für die Schweiz zu vermeiden, da damit der technologische Fortschritt und die Innovationskraft gebremst werde. Dies gelte auch für die TAV.

Sunrise UPC und **digitalswitzerland** erachten es als richtig, dass sich die Vorlage im Wesentlichen an Massnahmen der EU und international anerkannten Sicherheitsnormen orientiert und keine nationale Sonderlösung vorsieht. Gemäss **Sunrise UPC** ist diese Stossrichtung auch bei den TAV beizubehalten.

SUISSEDIGITAL ist der Meinung, dass bei der Implementierung und Umsetzung von Sicherheitsmassnahmen auf die Expertise der Fernmeldedienstanbieterinnen abgestellt und auf ihre Tätigkeiten Rücksicht genommen werden soll.

Gemäss **Swisscom** wenden die Mobilfunkbetreiberinnen die etablierten Sicherheitsnormen bereits an. Spezifisch schweizerische Vorschriften seien aufgrund der Gefahr mangelnder internationaler Harmonisierung abzulehnen. Für künftige technische und administrative Vorschriften seien die betroffenen Anbieterinnen zu konsultieren und weitere Anwendungs- und Umsetzungsaspekte eng mit ihnen abzusprechen.

Salt beantragt die Streichung dieses Absatzes, da je nach Auswahl von Normen und zugehörigen Zertifizierungen insbesondere bei kleineren Anbietern ein grosser Aufwand und hohe Kosten resultieren könnten.

Absatz 2

Die **SVP, Swisscom** und **economiesuisse** schlagen vor, die Formulierung dieses Absatzes 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 könne (vgl. z. B. Art. 9 Abs. 1 des Geldwäschereigesetzes, Art. 5 VSoTr).

Salt findet, der Umfang eines möglichen Audits solle auf die vom Verdacht einer Rechtsverletzung betroffenen Fernmeldeanlagen beschränkt werden.

4 Weitere Bemerkungen und Vorschläge

RK MZF, BL, IVR, KKPKS, KKJPD, AR, TG, SG, KAPO AI, LU, NW, FR, GVZG, BE, TI, ZG, OW, FKS und **SO** schlagen vor, im Zusammenhang mit der Bedrohung von kritischen Infrastrukturen durch Cyber-Angriffe auch die Aufgaben der Armee aufzuzeigen und in die FDV zu integrieren.

IVR, KKPKS, KKJPD, SG, KAPO AI, GVZG, BE, OW, GE, GL, FKS, SO und **VD** sind der Meinung, die vorliegende Verordnungsrevision müsse auch die Notrufregulierung verbessern (Notrufdatenbank, LIS-Proxy, dynamische Leitweglenkung). Schliesslich wäre es gemäss **FR** wünschenswert, dass der Bundesrat zur Cybersicherheit eine globale Strategie vorlegen würde. Im Weiteren sei die vorgeschlagene Revision regelmässig zu evaluieren und wenn nötig um strengere staatliche Regeln zu ergänzen.

Anhang: Teilnehmerliste und Abkürzungsverzeichnis

Kantone

AG	Kanton Aargau
AI	Kanton Appenzell Innerrhoden
AR	Kanton Appenzell Ausserrhoden
BE	Kanton Bern
BL	Kanton Basel-Landschaft
BS	Kanton Basel-Stadt
FR	Kanton Freiburg
GE	Kanton Genf
GL	Kanton Glarus
GR	Kanton Graubünden
JU	Kanton Jura
LU	Kanton Luzern
NE	Kanton Neuenburg
NW	Kanton Nidwalden
OW	Kanton Obwalden
SG	Kanton St. Gallen
SH	Kanton Schaffhausen
SO	Kanton Solothurn
TG	Kanton Thurgau
TI	Kanton Tessin
UR	Kanton Uri
VD	Kanton Waadt
VS	Kanton Wallis
ZG	Kanton Zug
ZH	Kanton Zürich

In der Bundesversammlung vertretene politische Parteien

SPS / PSS	Sozialdemokratische Partei der Schweiz / Parti socialiste suisse
SVP / UDC	Schweizerische Volkspartei / Union Démocratique du Centre

Gesamtschweizerische Dachverbände

SBV	Schweizerischer Bauernverband
economiesuisse	

Weitere Teilnehmende

asut	Schweizerischer Verband der Telekommunikation / Association Suisse des télécommunications
Centre Patronal	
digitalswitzerland	
FER	Fédération des entreprises romandes Genève
FKS	Feuerwehr Koordination Schweiz
GVZG	Gebäudeversicherung ZUG
IVR	Internetverband für Rettungswesen

KAPO AI	KAPO Appenzell Innerrhoden
KKJPD / CCDJP	Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren / Conférence des directrices et directeurs des départements cantonaux de justice et police
KKPKS / CCPCS	Konferenz der kantonalen Polizeikommandanten der Schweiz / Conférence des commandants des polices cantonales de Suisse
RK MZF / CG-MPS	Regierungskonferenz Militär, Zivilschutz und Feuerwehr / Conférence gouvernementale des affaires militaires, de la protection civile et des sapeurs-pompiers
Salt Mobile AG	
SRG / SSR	Schweizerische Radio- und Fernsehgesellschaft / Société suisse de radiodiffusion et télévision
SUISSEDIGITAL	Verband für Kommunikationsnetze / Association de réseaux de communication
Sunrise	Sunrise UPC GmbH
Swisscom	Swisscom (Schweiz) AG
WEKO / COMCO	Wettbewerbskommission / Commission de la concurrence