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