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