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