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