Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK
Bundesamt für Kommunikation BAKOM

Bern, Dezember 2021

Änderung der Verordnung über Fernmeldedienste (FDV)

Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten

Erläuternder Bericht

Erläuternder Bericht

1 Ausgangslage

Die Änderung von Artikel 48*a* des Fernmeldegesetzes (FMG; SR 784.10) ist am 1. Januar 2021 in Kraft getreten (AS 2020 6159). Sie räumt dem Bundesrat erweiterte Kompetenzen im Bereich der Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten ein. Bis anhin regelte der Bundesrat gestützt auf den ehemaligen Artikel 48*a* FMG (AS 2007 921) einzig die Meldung von Störungen im Betrieb von Fernmeldenetzen und -diensten (vgl. Art. 96 Abs. 1 der Verordnung vom 9. März 2007 über Fernmeldedienste [FDV, SR 784.101.1]). Der vorliegende Entwurf zur Änderung der FDV will diese Bestimmung durch eine erste Reihe von Massnahmen ergänzen, mit denen die unbefugte Manipulation von Fernmeldeanlagen durch fernmeldetechnische Übertragungen bekämpft und ein hohes Sicherheitsniveau beim Betrieb von Mobilfunknetzen der neusten Generation (5G-Netze) sichergestellt werden soll. Sie werden in einer zweiten Etappe durch ein weiteres Massnahmenpaket vervollständigt, dessen Umfang noch zu prüfen ist, und bei dem insbesondere die Gewährleistung der Stromversorgung der Mobilfunknetze im Fokus stehen wird.

1.1 Handlungsbedarf und Ziele

1.1.1 Netzwerksicherheit von 5G-Mobilfunknetzen

Problematik

Gemäss Bundesamt für Statistik (BfS) stieg die mobile Internetnutzung in der Schweiz von 43% im Jahr 2010 auf 91% im Jahr 2019[1]. Gleichzeitig werden die Mobilfunknetze zunehmend auf die 5G-Technologie ausgerichtet. Gemäss Gartner machten Investitionen in 5G im Jahr 2020 weltweit bereits 21.3% der Investitionen in die Mobilfunkinfrastruktur aus[2]. Ericsson geht davon aus, dass ab 2026 die Hälfte des Mobilfunkverkehrs über 5G laufen wird[3]. In der EU sollen die besiedelten Gebiete im Jahr 2030 vollständig mit 5G erschlossen sein.[4] 5G wird potenziell auch neue oder verbesserte Anwendungen in sensiblen Bereichen wie Gesundheit und Energie ermöglichen[5] sowie eine zentrale Rolle spielen für das Internet der Dinge[6]. Ausserdem ist der Mobilfunk Teil der kritischen Infrastruktur Telekommunikation, von welcher wiederum andere kritische Teilsektoren abhängig sind.[7] Entsprechend wichtig ist die Gewährleistung sicherer 5G-Netze.
Mit der zunehmenden Verbreitung dieser Technologie haben Sicherheitsfragen auch in der aussenpolitischen Diskussion an Bedeutung gewonnen. Das amerikanische Aussendepartement erachtet die Absicherung von 5G als zentral.[8] In der EU wurde 2019 eine Risikoanalyse zu 5G durchgeführt, welche ihrerseits auf Risikoanalysen der Mitgliedsländer basiert[9]. Darin wird aufgezeigt, dass Verfügbarkeit, Vertraulichkeit und/oder Integrität der über 5G bedienten Daten durch verschiedene Akteure (u. a. einzelne Hacker, kriminelle Organisationen, staatliche oder durch Staaten unterstütze Organisationen) gefährdet sein können. Wichtig zur Gewährleistung der Sicherheit sind insbesondere die Funktionen im Kernnetz und das Management von virtualisierten Netzwerkfunktionen. Bezüglich Risikoszenarien gelten etwa Situationen als relevant, bei welchen Sicherheitsmassnahmen ungenügend oder Endnutzergeräte unsicher sind, oder wenn Lieferanten von bedrohlichen Akteuren unter Druck gesetzt werden.
Selbst wenn ein Szenario unwahrscheinlich ist, können die zu erwartenden Auswirkungen aufgrund der vorangehend beschriebenen, steigenden Bedeutung von 5G im Mobilfunk bedeutend sein. Die in der genannten Risikoanalyse beschriebenen Risikoszenarien sind zudem kaum landesspezifisch und entsprechend auf die Schweiz übertragbar. Die Schweiz unterscheidet sich jedoch insofern, als die aktuellen gesetzlichen

1 Bundesamt für Statistik (2020): *Mobile Internetnutzung* von https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft/gesamtindikatoren/haushalte-bevoelkerung/mobile-internetnutzung.html.
2 Gartner (2020): *Gartner Says Worldwide 5G Network Infrastructure* Spending to Almost Double in 2020 von https://www.gartner.com/en/newsroom/press-releases/gartner-says-worldwide-5g-network-infrastructure-spending-to-almost-double-in-2020.
3 Ericsson (2020): *More than 1 billion people will have access to 5G coverage by the end of 2020* von https://www.ericsson.com/en/press-releases/2020/11/more-than-1-billion-people-will-have-access-to-5g-coverage-by-the-end-of-2020.
4 Europäische Kommission (2021): *5G* von https://digital-strategy.ec.europa.eu/en/policies/5g.
5 BAKOM (2020): *Mobile Kommunikation: Auf dem Weg zu 5G* von https://www.bakom.admin.ch/bakom/de/home/telekommunikation/technologie/5g.html.
6 Oracle (2019): *How 5G Networking Will Unleash the Full Potential of IoT* von https://blogs.oracle.com/scm/how-5g-networking-will-unleash-the-full-potential-of-iot-v2.
7 BABS (2010): *Telekommunikation* von https://www.babs.admin.ch/de/aufgabenbabs/ski/kritisch.html.
8 US State Department (2021): *Department Press Briefing* von https://www.state.gov/briefings/department-press-briefing-february-22-2021/.
9 NIS Cooperation Group (2019): *EU coordinated risk assessment of the cybersecurity of 5G networks* von https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

Grundlagen auf absehbare Frist nur eingeschränktes staatliches Handeln zulassen. Kurzfristig möglich sind insbesondere Massnahmen auf technischer Ebene. Zu berücksichtigen ist weiter, dass bei den Mobilfunkkonzessionärinnen von einem gewissen Eigeninteresse an der Sicherheit ihrer 5G-Netze auszugehen ist. Eine vom BAKOM unter den drei Schweizer Mobilfunkkonzessionärinnen durchgeführte Umfrage[10] zeigt denn auch bedeutende Aktivitäten zur Ermöglichung sicherer 5G-Netze.

Ziele
Ziel ist ein allgemeines Mindestniveau an 5G-Netzwerksicherheit in der Schweiz, basierend insbesondere auf internationalen Standards.

1.1.2 Unbefugte Manipulation von Fernmeldeanlagen

Problematik
Cyberangriffe führen zu hohen volkswirtschaftlichen Schäden. Zwar gehen die Schätzungen weit auseinander, es herrscht jedoch Einigkeit, dass die Dimension der Schäden längst eine Grössenordnung in Milliardenhöhe erreicht. Der Schweizerische Versicherungsverband (SVV) hat beispielsweise 2018 die jährlichen Schäden auf 9.5 Mia CHF beziffert.[11] Die Zahl dürfte seither weiter gestiegen sein. Die Schäden betreffen nicht nur grosse Unternehmen oder einzelne Sektoren, sondern potentiell alle Unternehmen[12] sowie Privatpersonen. In einer repräsentativen Befragung der Geschäftsführenden von KMU wurde beispielsweise festgestellt, dass jedes dritte der ca. 38'000 KMU, welche bereits Opfer eines folgenschweren Cyberangriffs wurden, finanzielle Schäden erlitten hat.[13] Cyberangriffe haben aber nicht nur hohe wirtschaftliche Auswirkungen, sondern gefährden die Sicherheit des Landes, da sie zu Ausfällen oder fehlerhaftem Funktionieren von kritischen Infrastrukturen führen können. Es besteht daher ein sicherheits- und wirtschaftspolitisches Interesse daran, Massnahmen gegen Cyberangriffe umzusetzen.
Bei der Unterbindung der Cyberangriffe spielen die Anbieterinnen von Internetzugängen (IAP bzw. «Internet Access Provider») eine zentrale Rolle. Sie ermöglichen ihren Kundinnen und Kunden die Kommunikation mit dem Internet und stellen ihnen häufig auch direkt die dafür nötige Ausrüstung zur Verfügung. Dadurch sind sie in der Lage präventive oder reaktive Massnahmen mit direkter Auswirkung zu treffen. Solche Massnahmen sind für die Cybersicherheit der Schweiz von grosser Bedeutung. Ohne eine enge Einbindung der IAP wird es nicht gelingen, die Anzahl von Cyberangriffen signifikant zu reduzieren.
Weil die Bedrohung durch Cyberangriffe über die letzten Jahre kontinuierlich gestiegen ist und davon ausgegangen werden muss, dass dies weiter der Fall sein wird,[14] steigt der Handlungsbedarf für Schutzmassnahmen. Der Staat ist in der Pflicht solche zu prüfen. Das geschieht einerseits über die Unterstützung der Wirtschaft durch Anlaufstellen und Kompetenzzentren und durch den Ausbau der Strafverfolgung. Andererseits gehört aber auch dazu, dass der Staat regulative Rahmenbedingungen für eine angemessene Cybersicherheit schafft. Diese müssen sinnvoll aufeinander abgestimmt sein. Die Definition von Pflichten für IAP ist dabei ein sehr wichtiges Instrument. Es ist nicht sinnvoll, in vielen Wirtschaftssektoren strenge Schutzmassnahmen gegen Cyberangriffe einzuführen, wenn nicht gleichzeitig Vorgaben gemacht werden, welche die Rolle der IAP bei diesen Schutzbemühungen klären.
Diese Überlegungen haben dazu geführt, dass bei der Revision des FMG der Artikel 48a derart angepasst wurde, dass die Anbieterinnen neu verpflichtet werden, Cyberangriffe zu bekämpfen und ihnen zu diesem Zweck auch erlaubt, «Verbindungen umzuleiten oder zu verhindern sowie Informationen zu unterdrücken». Das FMG lässt aber offen, zu welchen Massnahmen die Anbieterinnen beim Schutz vor Cyberangriffen konkret verpflichtet sind. Die vorliegenden Massnahmen in der Verordnung über Fernmeldedienste wurden unter Federführung des BAKOM in Zusammenarbeit mit dem Nationalen Zentrum für Cybersicherheit (NCSC) erarbeitet.

10 BAKOM (2021): *Befragung zur 5G Toolbox (Antworten vertraulich)*.
11 Schweizerischer Versicherungsverband (2018): *Grundlagenpapier des SVV zu Cyber-Risiken* von https://www.svv.ch/sites/default/files/2018-04/Grundlagenpapier%20CyberRisiken_DE.pdf.
12 Gemäss Bundesamt für Statistik (2021): *IKT Infrastruktur in den Unternehmen* von https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft/gesamtindikatoren/unternehmen/ikt-infrastruktur.assetdetail.17784535.html verfügen 100% der Schweizer Unternehmen über einen Internetanschluss.
13 Gfs-zürich (2020): *Digitalisierung und Cyber-Sicherheit in kleinen Unternehmen* von https://kmu-transformation.ch/wp/wp-content/uploads/2020/12/Schlussbericht_Studienergebnisse_Digitalisierung_Transformation_Homeoffice_Cybersicherheit_KMU_2020_12.pdf.
14 Vgl. dazu die Trendeinschätzung des World Economic Forum (WEF) in Zusammenarbeit mit der Universität Oxford (2020): *Cybersecurity, emerging technology and systemic risk* von http://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf.

Ziel

Der vorliegende Regulierungsvorschlag betrifft in erster Linie die Umsetzung und Konkretisierung des bereits mit der Teilrevision des FMG beschlossenen staatlichen Handelns. Die Massnahmen dienen der Umsetzung des FMG mit dem Ziel, einheitliche und klare Regeln für die diversen Schweizer IAP aufzustellen. Diese Regeln sollen sodann zur Erhöhung des allgemeinen Schutzniveaus im Bereich der Cyber-Sicherheit beitragen.

1.2 Geprüfte Alternativen und gewählte Lösung

1.2.1 Netzwerksicherheit von 5G-Mobilfunknetzen

Folgendes sind die Eckpunkte der in der Vorlage enthaltenen Massnahmen:

- Die Fernmeldedienstanbieterinnen (FDA) werden verpflichtet, Störungen im Betrieb ihrer Fernmeldeanlagen und -dienste, welche mindestens 30'000 Kunden betreffen, unverzüglich zu melden.[15]
- Die Mobilfunkkonzessionärinnen werden verpflichtet, ein Managementsystem für die Informationssicherheit (ISMS) nach anerkannten Normen zu betreiben. Das System deckt auch Resilienz- und Kontinuitätspläne ab und regelt den Umgang mit Sicherheitsvorfällen.
- Die Mobilfunkkonzessionärinnen werden verpflichtet, nur sicherheitskritische Anlagen zu verwenden, welche nach anerkannten Normen zertifiziert sind.
- Die Mobilfunkkonzessionärinnen werden verpflichtet, ihre Network und Security Operations Centres in der Schweiz, im Europäischen Wirtschaftsraum oder im UK zu betreiben.
- Falls das BAKOM einen Rechtsverstoss vermutet und externe Unterstützung notwendig ist, kann es Mobilfunkkonzessionärinnen verpflichten, sich auf ihre Kosten einem Audit zu unterziehen und ihr Netz durch eine fachkundige Organisation testen zu lassen.

Eine Weiterführung des Status Quo wurde verworfen, um aufgrund der gestiegenen Bedeutung von Mobilfunkdiensten und dem raschen Ausbau mit 5G[16] ein gewisses Mindestmass an Netzwerksicherheit allgemein und verbindlich für die Schweiz festzuschreiben.

Massnahmen aus der 5G Toolbox[17] zur weitgehenden Risikoverminderung in der Lieferkette von Mobilfunkunternehmen (z. B. Ausschluss von risikobehafteten Lieferanten oder Vorgaben zur Diversifizierung von Lieferanten), Teil der sog. strategischen Massnahmen, kamen vorliegend nicht in Betracht. Das Fernmeldegesetz bietet die dafür erforderlichen rechtlichen Grundlagen nicht.

Teilweise beruhen die Massnahmen aus der 5G Toolbox auch auf Instrumenten aus rechtlichen Grundlagen, welche in der Schweiz nicht vorhanden sowie nicht fernmeldespezifisch sind. Ein Beispiel ist der 2020 in der EU vollständig in Kraft getretene Mechanismus zum Screening von ausländischen Direktinvestitionen (FDI).[18]

Massnahmen für einen besseren Schutz der Mobilfunknetze[19] vor Stromausfällen in besonderen oder ausserordentlichen Lagen sowie technologieneutrale Massnahmen zur Erhöhung der Netzwerksicherheit auch ausserhalb der 5G-Technologie werden aktuell vertieft geprüft und möglicherweise in eine zukünftige Vorlage integriert.

1.2.2 Unbefugte Manipulation von Fernmeldeanlagen

Bei der Prüfung von alternativen Handlungsoptionen gilt es entsprechend zu beachten, dass der Handlungsspielraum durch die beschlossene Teilrevision des FMG vorgegeben wird. In der Botschaft zur Teilrevision des FMG vom 6. September 2017[20] hat der Bundesrat diesen Handlungsspielraum bereits skizziert. Er hat dabei deutlich gemacht, dass sich die Pflicht zur Bekämpfung unbefugter Manipulationen von Fernmeldean-

15 Neu wird die Pflicht zur Störungsmeldung gemeinsam vom BAKOM mit der nationalen Alarmzentrale (NAZ) vollzogen. Durch den Beizug der auf ausserordentliche Ereignisse spezialisierten NAZ können Synergien genutzt werden (vgl. NAZ [2021]: *Die NAZ* von https://www.naz.ch/naz/index). Im Übrigen besteht bereits eine vergleichbare Regelung zu Störungsmeldungen in Art. 96 FDV bzw. bzgl. der Meldeschwelle von 30'000 Kunden in den technischen und administrativen Vorschriften des BAKOM (SR 784.101.113/1.8). Somit entstehen den FDA auf Verordnungsstufe im Vergleich mit dem Status Quo keine relevanten zusätzlichen Kosten. Nachfolgend wird deshalb in der RFA nicht näher auf diese Massnahme eingegangen.

16 Der Fortschritt des 5G-Ausbaus ist unter BAKOM (2021): *Antennenstandorte* von http://map.funksender.admin.ch/ sowie BAKOM und Mobilfunknetzbetreiberinnen (2021): *Breitbandatlas* von https://map.geo.admin.ch/?topic=nga ersichtlich.

17 NIS Cooperation Group (2020): *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures* von https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

18 EU (2019): *Screening of foreign direct investment* von http://trade.ec.europa.eu/doclib/press/index.cfm?id=2006.

19 Bundesrat (2020*): Besserer Schutz der Mobilfunknetze vor Stromausfällen* von https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-81445.html.

20 Bundesrat (2017): *Botschaft zur Revision des Fernmeldegesetzes* von https://www.fedlex.admin.ch/eli/fga/2017/1933/de.

lagen durch fernmeldetechnische Übertragungen z. B. auf die Verhinderung der Verteilung von Schadsoftware und auf die Blockierung von Angriffen auf die Verfügbarkeit von Web-Diensten (DDoS-Angriffe) bezieht und nicht auf physische Zugriffe oder die Verhinderung von Hintertüren («backdoors») in Hard- und Software.
Die vorgeschlagene Änderung der FDV hält sich folglich an die in der Botschaft skizzierte Absicht. Die Massnahmen und die Begründung, warum sie eingeführt werden sollen, werden in den folgenden Kapiteln dargestellt.

1.2.2.1 Massnahme 1: Pflicht der Anbieterinnen zur Filterung von IP-Paketen mit gefälschter Quell-IP-Adresse (Spoofing)

IP-Pakete mit gefälschter Quell-IP-Adresse sind zentrale Treiber von Angriffen auf die Verfügbarkeit von Webdiensten (DDoS-Angriffe). Solche Angriffe werden nach wie vor sehr häufig durchgeführt und generieren grosse Schäden. Die Sicherheitsspezialisten von NetScout haben für das Jahr 2020 global mehr als 10 Millionen DDoS-Angriffe festgestellt.[21] Schätzungen zu den Kosten solcher Attacken sind sehr schwierig, da sie stark davon abhängen, wie wichtig die Webdienste für die kommerziellen Tätigkeiten eines Unternehmen sind. Es ist jedoch klar, dass Angriffe auf die Verfügbarkeit erhebliche finanzielle Auswirkungen für die Opfer haben können. Betreffen die Angriffe die Verfügbarkeit von kritischen Infrastrukturen, gehen die potentiellen Konsequenzen weit über die möglichen finanziellen Schäden hinaus. Wenn beispielswiese die Verfügbarkeit von Spitälern oder Energieversorgungsunternehmen durch Cyberangriffe beeinträchtigt wird, sind auch Gefährdungen von Leib und Leben nicht ausgeschlossen.
Über die seit Jahren bekannten technischen Möglichkeiten zur Filterung gefälschter Quell-IP-Adressen, kann die Durchführung von DDoS-Angriffen deutlich erschwert werden.[22] Die Umsetzung der Filterung bleibt jedoch unzureichend.[23] Dies lässt sich auf das Problem der fehlenden ökonomischen Anreize zurückführen.[24] Bei der Umsetzung der Filterung entstehen den Anbieterinnen Kosten, die Schutzwirkung kann jedoch nicht internalisiert werden (sie besteht ja darin, dass DDoS-Angriffe generell schwieriger durchführbar werden).[25] Es besteht daher ein klassisches «Allmende»-Problem, auch wenn dieses durch den Umstand entschärft wird, dass die Kosten für die Umsetzung der Filter tendenziell sinken.[26] Mit der Einführung einer generellen Pflicht zur Filterung kann dieses Problem entschärft werden. Alle Anbieterinnen müssen dann dazu beitragen, dass es Angreifern erschwert wird, DDoS-Angriffe durchzuführen.

1.2.2.2 Massnahme 2: Pflicht der Anbieterinnen, die Sicherheit der von ihnen den Kunden zur Verfügung gestellten Geräte gemäss dem aktuellen Stand der Technik zu gewährleisten

Die von den Anbieterinnen ihren Kunden abgegebenen Endgeräte (CPE bzw. «Customer Premises Equipement») spielen auf Grund ihrer sehr starken Verbreitung eine grosse Rolle in der Cybersicherheit. Weisen diese CPE flächendeckend Schwachstellen auf, ermöglicht dies Angreifern unter Umständen den Zugriff auf tausende Geräte. Die Rechenleistung dieser Geräte können sie dann für Angriffe, z.B. für DDoS-Angriffe, nutzen.[27] Ein klassisches Beispiel für dieses Problem sind Router, welche mit Standardpasswort ausgeliefert werden. Die Problematik der sicheren Konfiguration von CPE wird mit der sehr rasch voranschreitenden Verbreitung von «Internet of Things»-Geräten noch wichtiger.[28] Wenn die CPE nicht sicher konfiguriert sind, bie-

21 Netscout (2021): *Crossing the 10 Million Mark: DDoS Attacks in 2020* von https://www.netscout.com/blog/asert/crossing-10-million-mark-ddos-attacks-2020.
22 Lone et al. (2020): *SAVing the Internet: Explaining the Adoption of Source Address Validation by Internet Service Providers* von https://weis2020.econinfosec.org/wp-content/uploads/sites/8/2020/06/weis20-final31.pdf.
23 Luckie et al. (2019): *Network hygiene, incentives, and regulation: Deployment of source address validation in the internet* von https://researchcommons.waikato.ac.nz/handle/10289/13176.
24 Bauer und Eeten (2009): *Cybersecurity: Stakeholder incentives, externalities, and policy options* von https://www.researchgate.net/publication/227426674_Cybersecurity_Stakeholder_incentives_externalities_and_policy_options.
25 Christin (2011): *Network Security Games: Combining Game Theory, Behavioral Economics, and Network Measurements* von https://link.springer.com/chapter/10.1007/978-3-642-25280-8_2.
26 McConachie (2014): *Anti-Spoofing, BCP 38, and the Tragedy of the Commons* von https://www.circleid.com/posts/20140801_anti_spoofing_bcp_38_and_the_tragedy_of_the_commons/.
27 Vixie et al. (2014): *Abuse of Customer Premise Equipment and Recommended Actions* von https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=312647.
28 Vlajic und Zhou (2018): *IoT as a Land of Opportunity for DDoS Hackers* von https://ieeexplore.ieee.org/abstract/document/8423144.

ten sie in der Masse ein sehr einfach zu manipulierendes Ziel für Angreifer. Diese nutzen dann die Rechenleistung dieser Geräte für ihre Angriffe aus.[29]
Eine rechtliche Verpflichtung der Anbieterinnen zur sicheren Konfiguration von CPE ist nötig, weil auch in diesem Fall die Kosten für die mangelnde Sicherheit nicht von jenen getragen werden, welche unsichere Geräte verteilen, sondern von der Allgemeinheit. Anbieterinnen möchten möglichst tiefe Kosten bei der Beschaffung und Auslieferung der Geräte. Die Sicherheitsvorschriften können diese jedoch verteuern. Damit jene Anbieterinnen, welche die Sicherheit hoch gewichten, nicht vom Markt bestraft werden, braucht es Minimalanforderungen für alle Anbieterinnen. Eine Regulierung entspricht auch der Absicht des Bundesrats im Bericht zum Po. 17.4295 Glättli, die Durchsetzung von Standards für die Sicherheit von IoT-Geräten über staatliche Massnahmen und Vorschriften zu unterstützen.[30]

1.2.2.3 Massnahme 3: Recht, Internetzugänge oder Adressierungselemente, von denen eine Gefährdung von Fernmeldeanlagen ausgeht, zu sperren oder deren Nutzung einzuschränken sowie Pflicht zur Information der Kunden

Art. 48a des FMG gibt den Anbieterinnen das Recht, Internetanschlüsse zu sperren oder deren Nutzung einzuschränken, wenn dies zum Schutz von Anlagen nötig ist. Dieses Recht gilt nur solange die Gefährdung anhält. Die Verordnung weist den Anbieterinnen in diesen Fällen die Pflicht zu, ihre Kunden über die Sperrung zu informieren. Diese Pflicht dient der Transparenz gegenüber den Nutzern und hilft mit, bei den Nutzern Verständnis für die Sicherheit und die nötigen Massnahmen zu erzeugen.

1.2.2.4 Massnahme 4: Pflicht der Anbieterinnen, eine Meldestelle für die Meldung von Manipulationen zu führen und auf Meldungen innerhalb einer angemessenen Frist mit geeigneten Abwehrmassnahmen zu reagieren

Die Cybersicherheit kann nur verbessert werden, wenn nationale und internationale Behörden, Fachstellen und Anbieterinnen von Internetanschlüssen aktiv zusammenarbeiten. Da es national und international eine Vielzahl von Akteuren gibt, ist es wichtig, dass die Kontaktstellen standardisiert bedient werden können. Deshalb sollen die Anbieterinnen verpflichtet werden, eine Meldestelle («Abuse Desk») zu führen und beim zuständigen Regional Internet Registry (RIR)[31] einen Kontakt zu hinterlegen. Es bleibt dabei den Anbieterinnen freigestellt, ob sie diese Meldestelle selber führen oder die Aufgabe Dritten übertragen.
Weil ein manipulierter Anschluss die Sicherheit vieler anderer Teilnehmer gefährdet, ist eine rasche Reaktion sehr wichtig. Die IAP müssen deshalb innert angemessener Frist Massnahmen einleiten. Es wird nicht erwartet, dass die Gefährdung in jedem Fall innerhalb dieser Frist bewältigt werden kann, es muss aber sichergestellt werden, dass eine Reaktion in diesem Zeitraum eingeleitet wurde.

1.2.2.5 Alternative Handlungsoptionen

Im Verhältnis zum Status Quo – welcher durch das revidierte FMG gegeben wird – führt die Änderung der FDV Konkretisierungen ein. Diese entsprechen den in der Botschaft zur Revision des FMG erläuterten Absichten. Ein Verzicht auf eine solche Konkretisierung über die Anpassung der FDV würde die aus FMG Art. 48a entstehende Pflicht der Anbieterinnen nicht aufheben, es bliebe aber unklar, was mit dieser Pflicht genau gemeint ist. Entsprechend entstünde Rechtsunsicherheit.
Als Alternative zum Status Quo besteht aufgrund der in der Vorlage beschriebenen, wenig restriktiven Massnahmen insbesondere die Möglichkeit einer weiter gehenden Konkretisierung. Gemäss Vorlage werden die Anbieterinnen nicht verpflichtet, Internetzugänge oder Adressierungselemente, von denen eine Gefährdung ausgeht, zu blockieren, sondern gibt ihnen nur das Recht dazu, dies zu tun. Auf eine Pflicht zur Blockierung wurde bewusst verzichtet. Die Anbieterinnen sollen weiterhin selber beurteilen können, in welchen Fällen eine Blockierung nötig ist. Es wird ihnen damit die Freiheit gelassen, die Sicherheit der von ihnen angebotenen Dienstleistungen mit den für sie geeignetsten Mitteln zu gewährleisten. Die Alternative dazu wäre, dass

29 Der prominenteste Fall ist das Mirai-Botnet, welches auf dem Höhepunkt 2016 bis zu 500'000 kompromittierte IoT-Geräte umfasste und für sehr mächtige DDoS-Angriffe verwendet wurde. Eine generelle Übersicht zur Rolle von IoT bei DDoS-Angriffen bietet Vingau, Khoury und Hallé (2019): *10 Years of IoT Malware: A Feature-Based Taxonomy* von https://ieeexplore.ieee.org/abstract/document/8859496.

30 Bundesrat (2020): *Sicherheitsstandards für Internet-of-Things-Geräte (IoT)* von https://www.efd.admin.ch/dam/efd/de/dokumente/home/dokumentation/berichte/internet-things.pdf.download.pdf/29042020%20Bericht%20IoT-d.pdf.

31 Iana (2021): *Number Resources* von https://www.iana.org/numbers.

die Blockierung vorgeschrieben wird oder durch Behörden angeordnet werden kann. Ebenfalls verzichtet wurde auf die Einführung einer Pflicht der Anbieterinnen für den Schutz ihrer Kundinnen von DDoS-Angriffen.[32] Dafür müssten die Anbieterinnen fähig sein, ein Vielfaches des üblichen Internetverkehrs auffangen zu können. Die dazu nötigen Instrumente sind relativ teuer. Zudem wird ein Schutz vor DDoS-Angriffen bereits heute auf dem Markt angeboten und kann von den Kundinnen erworben werden. Es ist deshalb nicht nötig, den Anbieterinnen vorzuschreiben alle ihre Kundinnen und Kunden vor solchen Angriffen zu schützen.

2 Grundzüge der Vorlage

2.1 Vorgeschlagene Regelung

Die vorgeschlagene Regelung sieht eine Änderung von Artikel 96 FDV vor, um die Zusammenarbeit zwischen dem BAKOM und der nationalen Alarmzentrale beim Empfang und bei der Bearbeitung von Meldungen über Störungen im Betrieb von Fernmeldenetzen und -diensten zu institutionalisieren. Weitere neue Bestimmungen umfassen Massnahmen zur Bekämpfung der unbefugten Manipulation von Fernmeldeanlagen durch fernmeldetechnische Übertragungen und zur Gewährleistung der Sicherheit von Mobilfunknetzen der fünften Generation.

2.2 Umsetzungsfragen

2.2.1 Netzwerksicherheit von 5G-Mobilfunknetzen

Die Vorlage beschränkt sich in grossen Teilen auf Massnahmen, welche auch in anderen Ländern, insbesondere der EU, implementiert werden[33]. Zudem beruhen sie teilweise auf internationalen Standards (z. B. 3GPP), an welchen auch die Mobilfunkindustrie mitwirkt[34]. Bezüglich der Audits nach Art. 96g sollen insbesondere die Einhaltung anerkannter Normen geprüft werden, wofür ebenfalls etablierte Prozesse bestehen.

2.2.2 Unbefugte Manipulation von Fernmeldeanlagen

Bei der Pflicht, IP-Pakete mit gefälschter Quell-IP-Adresse zu filtern (Massnahme 1) handelt es sich gemäss den Ausführungen unter Ziff. 1.2.2.1 um erprobte Verfahren, für welche die IAP bei Bedarf auf öffentlich verfügbare Umsetzungshilfen zurückgreifen können. Bei der Pflicht zur korrekten Konfiguration und Wartung von CPE (Massnahme 2) dürfte es in den meisten Fällen möglich sein, auf bestehende Lieferantenbeziehungen zurückzugreifen und diese nötigenfalls anzupassen. Für die Pflicht der IAP zur Information der Kunden gemäss Massnahme 3 kann von etablierten Kommunikationswegen zum Kunden ausgegangen werden. Bei Massnahme 4 muss eine IAP erst aktiv werden, wenn sie z. B. vom NCSC kontaktiert wird und erhält zur Einleitung der Abwehrmassnahmen eine angemessene Frist.

3 Kommentar zu den einzelnen Bestimmungen

Artikel 96 und folgende sind nach ihrem persönlichen Geltungsbereich in drei Abschnitte unterteilt. Der 3. Abschnitt (Störungsmeldung) betrifft wie bereits heute sämtliche Anbieterinnen von Fernmeldediensten. Die Bestimmungen zur unbefugten Manipulation von Fernmeldeanlagen (4. Abschnitt) gelten für alle Anbieterinnen von Internetzugängen. Der Kreis der Akteure, die vom 5. Abschnitt betroffen sind, beschränkt sich auf die Mobilfunkkonzessionärinnen, das heisst Salt, Sunrise UPC und Swisscom. Was den sachlichen Geltungsbereich anbelangt, gelten die Bestimmungen des 5. Abschnitts zudem nur für Mobilfunknetze der fünften Generation (vgl. Art. 96*d*).

32 Dies im Gegensatz etwa zu den Massnahmen 1 und 2, mit welchen nicht spezifisch die Kundinnen eines IAP, sondern allgemein die Adressaten des von den Kundinnen eines IAP generierten Internetverkehrs vor DDoS-Angriffen geschützt werden sollen.

33 NIS Cooperation Group (2020): *Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity* von https://digital-strategy.ec.europa.eu/en/library/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity.

34 3GPP (2021): *Partners* von https://www.3gpp.org/about-3gpp/partners.

3. Abschnitt Störungsmeldung (Art. 96)

Die Pflicht der FDA, dem BAKOM Störungen im Betrieb der Netze zu melden, wurde am 1. April 2007 im Artikel 96 FDV eingeführt. Die Einzelheiten der Meldung von Störungen werden in den technischen und administrativen Vorschriften des BAKOM betreffend die Meldung von Netzstörungen (SR 784.101.113/1.8) geregelt.
Störungen werden dem BAKOM mittels Webformular oder e-Mail gemeldet. Es gibt auch eine Reservelösung per Telefon. Die Meldungen werden während der Bürozeiten bearbeitet und an die mitinteressierten Stellen verteilt.
Um die Bearbeitung und Verteilung der eingegangenen Störungsmeldungen zu verbessern, ist es vorgesehen, in Zukunft mit der Nationalen Alarmzentrale (NAZ) zusammenzuarbeiten. Der Empfang solcher Meldungen ist eine Kernaufgabe der NAZ. Sie hat dafür eine sichere Informatikinfrastruktur und einen 24-Stunden-Betrieb. Die NAZ wird die Störungsmeldungen in Echtzeit bearbeiten und verteilen können. Damit steigt der Nutzen der Meldungen insbesondere hinsichtlich Krisenbewältigung.
Zum Teil stellen FDA Störungsmeldungen heute nicht nur dem BAKOM zu, sondern auch der NAZ. Durch die vorgesehene Zusammenarbeit zwischen dem BAKOM und der NAZ wird diese Doppelspurigkeit beseitigt und das Meldewesen vereinfacht.
Zur Umsetzung der vorstehenden Ausführungen wird Artikel 96 FDV dahingehend ergänzt, dass entsprechende Störungen der NAZ zu melden sind. Das BAKOM seinerseits wird von der NAZ über die gemeldeten Störungen informiert. Im Weiteren wurde der wichtigste Grund für die Pflicht zur Meldung einer Störung (potenzielle Betroffenheit von mindestens 30'000 Kundinnen und Kunden) aus den technischen und administrativen Vorschriften in die FDV verschoben.

4. Abschnitt Unbefugte Manipulation von Fernmeldeanlagen

Einleitend sei an dieser Stelle festgehalten, dass die Bestimmungen dieses Abschnitts einzig für Anbieterinnen von Internetzugängen gelten, da erfahrungsgemäss nur diese von unbefugten Manipulation von Fernmeldeanlagen betroffen sind.

Art. 96a Sicherheitsmassnahmen

Absatz 1 der vorliegenden Bestimmungen regelt die Bekämpfung von Angriffen auf die Verfügbarkeit von Internetdiensten durch eine Vielzahl von Anfragen (bekannt als «Distributed Denial of Service»-Angriffe, DDoS). Dieser Fall wird in der Botschaft zur Revision des FMG auch explizit erwähnt. Ein wichtiger Bestandteil im Kampf gegen DDoS ist die Verhinderung der Nutzung gefälschter IP-Adressen durch die Angreifer («Spoofing). Dadurch werden ausgehende DDoS-Angriffe, welche auf IP-Spoofing basieren, verunmöglicht. Zu diesem Zweck werden die Anbieterinnen von Internetzugängen verpflichtet, vernünftige technische Möglichkeiten zu nutzen, mit denen aus ihrem Netzwerk stammende IP-Pakete mit gefälschter Quell-IP-Adresse gefiltert werden können. Zur Einrichtung solcher Ingress-Filter müssen die Anbieterinnen eine aktuelle Liste der berechtigten Netze führen. Eine solche Liste lässt sich automatisch aus der Routingtabelle generieren. Die nötigen technischen Schritte beschreibt die Internet Engineering Task Force (IETF) in den «Best Current Practices» BCP38 für single-homed networks (Netzwerke, bei welchen jedes Gerät über eine IP-Adresse verfügt) und BCP84 für «multi-homed networks» (Netzwerke, bei welchen ein Gerät über mehrere IP-Adressen verfügt).
Die Anbieterinnen von Internetzugängen stellen ihren Kundinnen und Kunden häufig Geräte zur Verfügung (sogenanntes «Customer Premises Equipment», CPE). Diese spielen wegen ihrer sehr grossen Verbreitung bei der Bekämpfung von Cybervorfällen eine wichtige Rolle. Absatz 2 legt deshalb fest, dass die Sicherheitseigenschaften aller Fernmeldeanlagen, die den Kundinnen und Kunden zur Verfügung gestellt werden, gemäss den anerkannten Regeln der Technik zu konfigurieren und zeitnah zu aktualisieren sind, sofern die entsprechenden Anbieterinnen weiterhin die Kontrolle über diese Anlagen ausüben. Dies schliesst die Möglichkeit ein, Sicherheitslücken in solchen Geräten mittels pdates zu schliessen. Um die Risikoexposition bei solchen Geräten möglichst gering zu halten, wird das BAKOM technische und administrative Vorschriften erlassen. Die werden insbesondere folgende Grundsätze berücksichtigen müssen:

- Für den Zugriff auf CPE dürfen keine Standardzugangsdaten (Benutzername, Passwort) verwendet werden. Die Zugangsdaten müssen individuell pro Gerät vergeben werden. Falls dies technisch

nicht möglich ist, muss bei der Inbetriebnahme des Geräts einen Wechsel der Zugangsdaten erzwungen werden.
- Nicht benötigte Dienste auf dem CPE müssen deaktiviert sein.
- Ausgehender SMTP Traffic auf Port 25 muss standardmässig bei allen Kundenanschlüssen im Privatkundenbereich («Residential»-Anschlüsse, in der Regel dynamische IP-Adressen) gesperrt sein. Bei spezifischem Bedarf oder auf berechtigten Kundenwunsch ist eine Freischaltung denkbar.
- Im Auslieferungszustand eines CPE dürfen keine vom Internet her frei erreichbaren Ports offen sein. Für den Betrieb des CPE nötige offene Ports müssen durch technische Massnahmen (z.B. IP-Restriction) abgesichert werden.
- Die für die Fernwartung durch die Anbieterin verwendeten Ports müssen möglichst weit eingeschränkt werden (z.B. auf ein von der Anbieterin dafür verwendetes IP-Adress-Segment).
- Das für den Fernwartungszugriff verwendete Protokoll muss mit einer zeitgemässen Verschlüsselungstechnologie geschützt sein.
- 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.

Wenn Fernmeldeanlagen mit Malware infiziert sind, können sie weitere Fernmeldeanlagen, mit denen sie eine Verbindung aufbauen können, gefährden. Über die Verbindung kann die Malware weiterverbreitet werden, oder sie kann für andere schädliche Aktivitäten verwendet werden, beispielsweise den Versand von Spam, Phishing oder die Teilnahme an einer DDoS-Attacke. Aus diesem Grund ist es notwendig, in Absatz 3 Massnahmen gegen infizierte oder verwundbare Fernmeldeanlagen vorzusehen. Verschiedene Massnahmen sind vorstellbar. Bei schädlichen Aktivitäten kann der Internetanschluss gesperrt oder eingeschränkt werden, um die Aktivität zu unterbrechen. Eine Sperrung kann auch dann eingesetzt werden, wenn ein verwundbares Gerät über längere Zeit betrieben wird. Dies dient oft nicht nur dem Schutz der anderen Teilnehmer, sondern auch dem Schutz der betroffenen Person/Firma (Stichwort Ransomware Angriffe). Infizierte Geräte können sonst in einen Sandbox Modus («Walled Garden») versetzt werden, wobei der Internetanschluss zur Fernmeldedienstanbieterin aufrecht bleibt aber die Verbindung zum Internet stark eingeschränkt oder gesperrt wird. Damit stellt die Fernmeldeanlage keine Gefahr mehr für andere dar. Wenn schädliche Aktivitäten in Verbindung mit bestimmten Adressierungselementen (IP-Adressen oder Domain-Namen) stehen, können diese für Kundenzugriffe gesperrt werden.
Weil Nutzer von Sperrungen und Einschränkungen des Internetanschlusses stark getroffen werden, ist ihre zeitnahe Information durch die Anbieterinnen von Internetzugängen zwingend. Diese sollen die Nutzer daher transparent über die ihrerseits getroffenen Massnahmen informieren.
Die zur Sperrung oder Nutzungseinschränkung nach der vorliegenden Bestimmung berechtigten Anbieterinnen werden auf die entsprechenden Massnahmen verzichten oder sich zumindest mit dem Dienst Überwachung Post- und Fernmeldeverkehr ÜPF in Verbindung setzen müssen, wenn sie wissen, dass der entsprechende Internetzugang oder das entsprechende Adressierungselement Gegenstand einer Überwachungsanordnung ist. Dies dürfte bereits aus Artikel 26 Absatz 2 Buchstabe a des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF; SR 780.1) sowie Artikel 29 Absatz 2 und 3 der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF; SR 780.11) hervorgehen.

Art. 96b Meldestelle

Artikel 96b sieht vor, dass die Anbieterinnen von Internetzugängen eine spezialisierte Stelle zur Meldung unbefugter Manipulationen von Fernmeldeanlagen durch fernmeldetechnische Übertragungen (sogenanntes «Abuse Desk») betreiben, der Manipulationen von Fernmeldeanlagen gemeldet werden können. Den Anbieterinnen steht es frei, dieses «Abuse Desk» selber zu betreiben oder Dritte damit zu beauftragen. Das «Abuse Desk» kann nach den Bedürfnissen der Anbieterinnen ausgestaltet werden. Es ist jedoch sicherzustellen, dass innert angemessener Frist geeignete Abwehrmassnahmen eingeleitet werden können. Im Übrigen sind grundsätzlich folgende technischen und administrativen Anforderungen zu erfüllen:
- Bei der zuständigen «Regional Internet Registry» (RIR) ist grundsätzlich für jeden «Network Range» (IP-Adressblöcke) ein Kontakt (E-Mail-Adresse) zu hinterlegen («abuse-c»). Geschieht dies nicht, müssen die Anbieterinnen einen generellen Kontakt für technische Fragen («tech-c») hinterlegen. Sie müssen sicherstellen, dass dieser Kontakt die Funktion des «Abuse Desks» wahrnehmen kann.

- Die Anbieterinnen stellen sicher, dass Meldungen über Manipulationen über die hinterlegte Adresse gemeldet werden können und innerhalb der gesetzten Fristen auf die Meldung reagiert werden kann.
- Da Meldungen über Manipulationen oft Muster erhalten, die von Spamfilter aussortiert werden, müssten allfällige Filter sehr sorgfältig konfiguriert sein und es muss sichergestellt sein, dass die Nachricht in jedem Fall bearbeitet wird.

Sollte sich der Rechtsbegriff «innert angemessener Frist» als zu offen erweisen, könnte das BAKOM diesen in den technischen und administrativen Vorschriften allenfalls präzisieren, indem es z. B. eine konkrete Dauer vorsieht und/oder je nach Kategorie der meldenden Personen unterschiedliche Regelungen trifft.

Art. 96c Vollzug

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.

5. Abschnitt Sicherheit von Netzen und Diensten, die von Mobilfunkkonzessionärinnen betrieben werden

Art. 96d Geltung

Alle Bestimmungen zu den Sicherheitsfunktionen gelten sowohl für eigenständige (Standalone gemäss 3GPP TS 33.501) als auch für nicht eigenständige (Non Standalone) 5G-Netze. Die derzeitigen 5G-Netze verfügen nämlich über kein 5G-Kernnetz, sondern sind nicht eigenständige 5G-Netze mit 5G-Funkstationen, die auf der bestehenden Infrastruktur von 4G-Netzen und nicht auf einer reinen 5G-Infrastruktur betrieben werden (5G Standalone).
Die vom 3GPP (*3rd Generation Partnership Project*) standardisierten Sicherheitsfunktionen für 5G in den Bereichen Verschlüsselung des Datenverkehrs, Netzzugang und Authentifizierung (TS 33.501) bauen auf der Sicherheit von 4G-Netzen auf, was bedeutet, dass viele 5G-Sicherheitsfunktionen identisch mit jenen des 4G-Standards sind.
Die bei 5G neu hinzugekommenen Sicherheitsfunktionen (z. B. Spoofing-Schutz des Kernnetzes betreffend Roaming-Frauds, Schutz vor Webtracking, SIM-lose Authentifizierung von IoT-Geräten) setzen das Vorhandensein eines 5G-Kernnetzes voraus (logische Funktionen zur Verwaltung der neuen Zugänge und zur Kontrolle von 5G-Funkstationen). Folglich können die in der Norm TS 33.501 spezifizierten Sicherheitsfunktionen, die über 4G hinausgehen, technisch nicht vor der Einführung von 5G Standalone umgesetzt werden.

Art. 96e Sicherheitsmanagement

Die 5G-Mobilfunkinfrastruktur und die von ihr erzeugten und verarbeiteten Informationen sind wichtige Ressourcen, die umsichtig verwaltet werden müssen, um die Zuverlässigkeit und die Verfügbarkeit der Dienste zu gewährleisten.
Absatz 1 verlangt von den Mobilfunkkonzessionärinnen künftig die Entwicklung, Umsetzung und kontinuierliche Überprüfung eines Managementsystems für die Informationssicherheit (*Information Security Management System*, ISMS), wie dies von den meisten von ihnen bereits heute praktiziert wird.
Die Umsetzung eines ISMS erfordert eine Planungsphase, in der die potenziellen Risiken der betreffenden Organisation ermittelt und evaluiert werden. Diese erste Phase ermöglicht es, eine Sicherheitspolitik unter Einbezug der zu beachtenden Risiken zu definieren und danach die Zielsetzungen im Sicherheitsbereich ebenso wie den zu sichernden Bereich zu beschreiben. Auf dieser Grundlage legt die Organisation schliesslich die Kontrollen fest, die ihrer Sicherheitspolitik und den Risiken, vor denen sie sich schützen will, entsprechen.
Für den Bereich der Informations- und Kommunikationstechnologie wurden bereits ISMS in der Form von Normen entwickelt. Dazu zählt insbesondere die Normenreihe ISO/IEC 2700x (*ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements; ISO/IEC 27002:2005 Information technology – Code of practice for Information Security Management; ISO/IEC 27011:2008 Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*), auf die gemäss Absatz 3 dieses Artikels in den technischen und administrativen Vorschriften verwiesen werden soll.
Diese Normen betreffen vor allem Aspekte der physischen Sicherheit, der Zugangsverwaltung und der Softwaresicherheit. Das betriebliche Kontinuitätsmanagement und das Management von Sicherheitsvorfällen

sind zwar in der Regel ebenfalls in den ISMS enthalten, wie bei jenen, die in den Normen ISO/IEC 2700x beschrieben werden. Sie werden jedoch in Absatz 2 explizit erwähnt, weil es sich dabei um Elemente handelt, die bei der Erbringung von Dienstleistungen für die Allgemeinheit zwingend berücksichtigt werden müssen. Um die Anforderungen an das Kontinuitätsmanagement und das Management von Sicherheitsvorfällen zu präzisieren, ist vorgesehen, in den technischen und administrativen Vorschriften auf die Norm ISO 22301:2019 *Security and resilience – Business continuity management systems – Requirements* zu verweisen.
Ein ISMS richtet sich an Unternehmensleitungen, die für die Sicherheit verantwortlichen Mitarbeitenden und externe Evaluationsstellen. Eine unabhängige Evaluation durch eine akkreditierte Zertifizierungsstelle kann zu einer anerkannten Zertifizierung führen, die belegt, dass das betreffende Unternehmen das Sicherheitsmanagement beherrscht. Es ist derzeit nicht geplant, von Mobilfunkkonzessionärinnen eine solche Zertifizierung zu fordern. Das BAKOM kann jedoch im Rahmen seiner Aufsichtsaufgaben von der Konzessionärin Informationen über die Umsetzung des ISMS verlangen (vgl. Art. 96*g*).
Die Ausarbeitung eines ISMS wird von den Zielen, Bedürfnissen, Anforderungen und Risiken im Zusammenhang mit der Tätigkeit der betreffenden Organisation beeinflusst. Es hängt im Übrigen von den eingesetzten Technologien, der Kundschaft sowie der Grösse und Struktur der Organisation ab. Jegliche Veränderung dieser Kriterien muss eine Anpassung des Sicherheitsmanagementsystems nach sich ziehen. Der Aufwand für die Umsetzung eines ISMS hängt somit direkt mit der Organisation und den angebotenen Diensten zusammen.

Art. 96f Betrieb sicherheitskritischer Fernmeldeanlagen

Die Mobilfunkkonzessionärinnen müssen sicherstellen, dass die von ihnen betriebenen sicherheitskritischen Fernmeldeanlagen nach anerkannten Sicherheitsnormen zertifiziert sind. Das BAKOM definiert die sicherheitskritischen Fernmeldeanlagen, bei Bedarf in Zusammenarbeit mit der Branche. Die Liste der sicherheitskritischen Anlagen wird in den entsprechenden technischen und administrativen Vorschriften aufgeführt.
Auf europäischer Ebene und im Auftrag der Europäischen Kommission wird die ENISA (EU-Agentur für Cybersicherheit) ein neues Zertifizierungssystem für die Cybersicherheit von 5G-Netzen ausarbeiten. Diese Etappe schliesst an den Massnahmenkatalog der Europäischen Union für die Sicherheit von 5G-Netzen (5G-Toolbox) an und dürfte die Cybersicherheit von 5G-Netzen verbessern, da sie zur Eliminierung gewisser Risiken beiträgt.
Das neue System wird sich auf bereits bestehende Bestimmungen und Systeme zur Zertifizierung der Cybersicherheit sowie auf Erfahrungen der ENISA abstützen, welche die Agentur seit Beginn ihrer Arbeiten im Bereich der Zertifizierung der Cybersicherheit gesammelt hat. Das Programm ist aktuell noch nicht abgeschlossen, und im Frühsommer 2021 wurde ein Aufruf zur Interessensbekundung für Sachverständige lanciert. Sobald dieses Zertifizierungssystem für 5G eingeführt ist, wird das BAKOM die Möglichkeiten für seine Nutzung prüfen.
Es gibt jedoch bereits andere anerkannte Normen in diesem Bereich, wie beispielsweise das NESAS (*Network Equipment Security Assurance Scheme*[35]*)* der GSMA. GSMA NESAS ist eine freiwillige Initiative der Mobilfunkbranche zur Einführung eines Programms, mit dem die Sicherheit von Mobilnetzanlagen und -infrastrukturen kontinuierlich verbessert werden soll. Diese Norm betrifft Geräte, die vom 3GPP definierte Funktionen unterstützen und die von Mobilfunkbetreiberinnen in ihren Netzen eingesetzt werden. Die GSMA entwickelt weltweit anerkannte Sicherheitsstandards und Zertifizierungen, an denen sich die gesamte Telekommunikationsbranche beteiligt. Letztere setzt grosses Vertrauen in diese Spezifikationen, was gewährleistet, dass der technische Fortschritt nicht gebremst wird. Es ist darauf hinzuweisen, dass NESAS weder den Versand und die Bereitstellung von Netzausrüstung noch die Konfiguration und den Betrieb von Netzausrüstung in Mobilfunknetzen abdeckt.
Die GSMA hat die Sicherheitsanforderungen und -prozesse für NESAS in Zusammenarbeit mit 3GPP, Betreiberinnen und Geräteherstellerinnen entwickelt. Die Organisation führt eine aktuelle Liste von Geräteherstellerinnen, die am Programm beteiligt sind und deren Entwicklungs- und Life-Cycle-Prozesse sowie Netzwerkprodukte einer Sicherheitsbeurteilung unterzogen worden sind.
Die aktuelle Version der GSMA NESAS definiert die Elemente, die für die Entwicklung eines Zertifizierungssystems erforderlich sind:

35 https://www.gsma.com/security/network-equipment-security-assurance-scheme/.

- Ernennung einer Audit-Organisation
- Akkreditierung von Prüfstellen
- Sicherheitsanforderungen im Zusammenhang mit den Prozessen des Lieferanten und den Netzwerkprodukten sowie Methoden zur Evaluation der Prozesse des Lieferanten und der Produkte.

Gewisse Anbieterinnen von Mobilnetzausrüstung (vor allem aus China) haben die Entwicklungs- und Life-Cycle-Prozesse einiger ihrer Produkte von unabhängiger Seite bewerten und prüfen lassen («GSMA NESAS»-zertifizierte Prüfstellen), um die Integration der Sicherheit in ihre Design-, Entwicklungs-, Implementierungs- und Wartungsprozesse nachzuweisen (z. B. für die «5G gNodeB»-Produktelinien [Basisstationen]). Trotz zunehmender Möglichkeiten der Virtualisierung der Mobilfunknetze stellt die Präsenz von Infrastrukturen und Anlagen vor Ort oder in Ländern mit vergleichbaren Sicherheitsmassnahmen nach wie vor einen Sicherheitsvorteil dar. In diesem Sinne sieht Absatz 2 der vorliegenden Bestimmung vor, dass Netzwerk- und Sicherheitsbetriebszentren der Mobilfunkkonzessionärinnen in der Schweiz, im Europäischen Wirtschaftsraum oder im Vereinigten Königreich zu betreiben sind.
Gemäss Art. XIV^{bis} Absatz 1 Buchstabe b von Anhang 1B des Abkommens zur Errichtung der Welthandelsorganisation (General Agreement on Trade in Services; GATS) hindern dessen Bestimmungen ein Mitglied nicht daran, Massnahmen zu treffen, die nach seiner Auffassung zum Schutz seiner wesentlichen Sicherheitsinteressen notwendig sind. Ein Teil der Lehre vertritt die Auffassung, dass auch Cybersicherheit in den Anwendungsbereich dieser Bestimmung fallen könnte.
Davon scheint auch die Europäische Union auszugehen, geht aus dem Bericht der «NIS Cooperation Group» (Vertreter/-innen der EU-Mitgliedstaaten/EU-Kommission/ENISA) über die Fortschritte bei der Umsetzung der EU-Toolbox für 5G-Cybersicherheit doch hervor, dass 16 von 26 im Bericht berücksichtigte EU-Mitgliedstaaten bereits sichergestellt haben oder bis 2021 sicherstellen werden, dass die Mobilfunkbetreiberinnen ihre Network Operations Centres und Security Operations Centres vor Ort, innerhalb des Landes und/oder innerhalb der EU betreiben (Report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity | Shaping Europe's digital future; Veröffentlichung 24. Juli 2020; letztes Update: 8. März 2021).
Die erwähnte Toolbox stellt im Übrigen auch weitergehende Eingriffe, wie z. B. den gänzlichen Ausschluss bestimmter Akteure von Aktivitäten auf dem Territorium der Mitgliedstaaten, zur Auswahl und geht offensichtlich davon aus, dass auch diese durch das Recht der Welthandelsorganisation gedeckt wären.

Art. 96g Anwendbare Vorschriften und Aufsicht

Da Artikel 96*e* und 96*f* auf die anerkannten Sicherheitsnormen verweisen, obliegt es dem BAKOM, in seinen technischen und administrativen Vorschriften die Normen zu bezeichnen, die verbindlich anzuwenden sind (Abs. 1). Die Einhaltung dieser Normen kann von der betroffenen Anbieterin durch ein Zertifikat einer zuständigen Stelle gemäss dem schweizerischen Akkreditierungssystem (vgl. Verordnung vom 17. Juni 1996 über das schweizerische Akkreditierungssystem und die Bezeichnung von Prüf-, Konformitäts-, Anmelde- und Zulassungsstellen; SR 946.512) oder einem anderen Zertifizierungssystem (GSMA NESAS, Europäische Cybersicherheitssysteme[36)] nachgewiesen werden. Wurde das Sicherheitsmanagementsystem nicht auf freiwilliger Basis zertifiziert (Art. 96*e*) oder werden sicherheitskritische Fernmeldeanlagen betrieben, die nicht nach anerkannten Sicherheitsnormen zertifiziert sind (Art. 96*f*), kann eine Mobilfunkkonzessionärin im Rahmen der Aufsicht dazu verpflichtet werden, sich auf eigene Kosten bei einer qualifizierten Stelle einem Audit zu unterziehen oder ihre Fernmeldeanlagen prüfen zu lassen und dem BAKOM die Ergebnisse dieses Audits oder dieser Prüfung vorzulegen (Abs. 2). Eine solche Massnahme kann jedoch nur im Rahmen von Artikel 58 Absatz 2 FMG ergriffen werden, wenn der Verdacht besteht, dass die Konzessionärin die Anforderungen von Art. 96e und 96f nicht einhält und das BAKOM nicht in der Lage ist, den entsprechenden Sachverhalt selbst festzustellen. Sie ist jedoch dann ausgeschlossen, wenn kein solcher Verdacht besteht, insbesondere im Rahmen der generellen Überwachung im Sinne von Artikel 58 Absatz 1 FMG (Aufsichtskampagnen). Es muss auch sichergestellt werden, dass die qualifizierte Stelle die Informationen, zu denen sie Zugang hat, vertraulich behandelt, insbesondere solche, die sich auf eine mögliche Überwachungsmassnahme im Sinne des BÜPF beziehen.
Bei Telekommunikationsanlagen wird das BAKOM die grundlegenden fernmeldetechnischen Anforderungen,

36 Vgl. Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit), ABl. L 151/15.

die der Bundessrat in Artikel 96*f* festgelegt hat, gemäss Artikel 31 Absatz 2 Buchstabe b FMG konkretisieren. Dabei ist es für die Notifikationen im Rahmen der Welthandelsorganisation (WTO) und der Europäischen Freihandelsassoziation (EFTA) zuständig. Im Weiteren sind die einschlägigen Bestimmungen der Verordnung vom 25. November 2015 über Fernmeldeanlagen (FAV; SR 784.101.2) anwendbar. Insbesondere gilt Artikel 17 FAV für die Akkreditierung, Anerkennung oder Zulassung von Prüf- und Konformitätsbewertungsstellen. Wird eine bezeichnete technische Norm geändert, so muss das BAKOM festlegen, ab welchem Zeitpunkt die Vermutung der Konformität für konforme Funkanlagen nach der vorangehenden Fassung dahinfällt (vgl. Art. 8 Abs. 2 FAV).

4 Auswirkungen

4.1 Auswirkungen auf den Bund

4.1.1 Netzwerksicherheit von 5G-Mobilfunknetzen

Auswirkungen in finanzieller, personeller und anderer Hinsicht auf den Bund wurden geprüft und sind in einer ersten Phase nicht in relevantem Ausmass zu erwarten. Die Umsetzung und Kostentragung hat zunächst vorab durch die Unternehmen zu erfolgen. Für das BAKOM resultiert im Bereich der Normierung und der Aufsicht im Zusammenhang mit Sicherheitsbestrebungen zu 5G Mobilfunknetzen dennoch ein zusätzlicher Aufwand, der gegenwärtig schwer zu beziffern ist. In einer ersten Phase sollen denn auch die zusätzlichen Aufgaben im Bereich der Standardisierung und der Aufsicht in die bestehenden Arbeitsprozesse des BAKOM integriert werden. Die weitere Entwicklung ist diesbezüglich jedoch aufmerksam zu verfolgen.

4.1.2 Unbefugte Manipulation von Fernmeldeanlagen

Auswirkungen in finanzieller, personeller und anderer Hinsicht auf den Bund wurden geprüft und sind für den Bund insgesamt nicht in relevantem Ausmass zu erwarten. Das NCSC informiert bereits heute die Anbieterinnen über mögliche Cyberangriffe in oder aus ihrem Netz, da dies für die Cybersicherheit der Schweiz von grosser Bedeutung ist. Die in der Verordnung beschriebene Aufgabe des NCSC kann daher mit den bestehenden Ressourcen ausgeführt werden. Beim BAKOM führen die neuen Aufgaben im Bereich Cyber-Sicherheit und der gemeinsame Vollzug mit dem NCSC zu einem zusätzlichen Bedarf von ein bis zwei Stellen. Dafür verfügt das NCSC über einen Stellenpool. Das BAKOM hatte bereits in der Vergangenheit Bedarf geltend gemacht, wurde aber bisher nicht berücksichtigt. Mit den vorliegenden Bestimmungen ist der Bedarf nun ausreichend konkret. In der Gesamtsicht ergeben sich für den Bund keine relevanten Auswirkungen, da der Stellenpool bereits besteht.

4.2 Auswirkungen auf die Volkswirtschaft

4.2.1 Netzwerksicherheit von 5G-Mobilfunknetzen

Mit den vorgeschlagenen vier Massnahmen zur 5G-Sicherheit werden kostenseitig die drei in der Schweiz tätigen Mobilfunkkonzessionärinnen (MNO) adressiert.
Im Zeitraum zwischen Ende März und Mitte Mai 2021 hat das BAKOM bei den drei MNO eine Umfrage zu den von ihnen ergriffenen und geplanten technischen Massnahmen aus der 5G-Toolbox sowie deren Kosten durchgeführt.
Die Umfrage hat gezeigt, dass die Anbieterinnen bei ihren Informations-Sicherheits-Management-Systemen (ISMS) grossen Wert auf die ISO Norm 27001 legen. Auf diese und vergleichbare Normen sollen sich auch die konkretisierten Anforderungen in den technischen und administrativen Vorschriften beziehen. Für die MNO ist daher gegenüber dem Status Quo nicht mit grossen Änderungen und Kosten zu rechnen.
Aus den Eingaben lässt sich auch ableiten, dass die MNO eine Zertifizierung von Netzelementen grundsätzlich unterstützen und von ihren Lieferanten auch gewisse Sicherheitsanforderungen verlangen. Internationale Normen werden von ihnen in den Vordergrund gestellt, allen voran die GSMA NESAS. Es ist zu erwarten, dass mit einer Regelung in diesem Bereich nicht mit signifikanten zusätzlichen Kosten zu rechnen ist.
Die Pflicht Network Operation Centers (NOC) und Security Operation Centers (SOC) in der Schweiz, dem europäischen Wirtschaftsraum oder dem UK zu betreiben wird grundsätzlich bereits erfüllt.

Die MNO haben die von ihnen ergriffenen Massnahmen in unterschiedlichem Detailgrad beschrieben. Zu den konkreten mit den Massnahmen verbundenen Kosten haben sie grösstenteils keine oder nur wenige Angaben gemacht. Entsprechend können auch nur qualitative Aussagen zu Kosten vorgenommen werden. Weiter können den MNO durch allfällige Verpflichtungen zur Auditierung Kosten entstehen. Insbesondere bei einer hohen Konformität mit den relevanten Standards ist jedoch nicht von einem hohen Auditierungsrhythmus auszugehen, da eine Verpflichtung zur Auditierung auf Kosten der jeweiligen MNO nur im Rahmen von Art. 58 Abs. 2 FMG ergriffen werden darf, wenn der Verdacht besteht, dass eine Konzessionärin die Anforderungen von Art. 96e oder 96f nicht einhält und das BAKOM nicht in der Lage ist, die entsprechenden Tatsachen selbst festzustellen. Die Kosten eines einzelnen Audits sind dabei abhängig vom konkreten Umfang der Prüfung. Schätzungsweise liegen sie in den meisten Fällen im fünfstelligen Bereich.[37]
Der Nutzen für die Volkswirtschaft ergibt sich aus der Vermeidung von Kosten, welche den Haushalten, Unternehmen und weiteren gesellschaftlichen Gruppen im Falle von Risikoeintritten im Zusammenhang mit der Sicherheit von 5G-Netzen entstehen können. So haben Ausfälle in der Mobilfunkversorgung potenziell bedeutende Auswirkungen. Mobilfunk an[38] sich spielt bei Internetnutzerinnen und -nutzern[39] sowie bei den Unternehmen[40] eine immer grössere Rolle. Das BABS rechnet im Gefährdungsdossier «Ausfall Mobilfunk» bei einem dreitägigen Totalausfall eines grossen Mobilfunkproviders mit aggregierten Schäden in einem Bereich um rund neun Milliarden Franken. Ein solcher sehr unwahrscheinlicher[41,] aber aufgrund der genannten Schadenssumme dennoch relevanter Ausfall eines Netzes ist jedoch nur eine mögliche Auswirkung. Sicherheitslücken in Betrieb und Infrastruktur von 5G-Mobilfunknetzen können verschiedenste Arten von Cyber-Angriffen auf die über 5G bedienten Anwendungen und Daten erleichtern, etwa Datendiebstahl und Erpressung. Eine relativ aktuelle Studie zu kleinen und mittleren Unternehmen (KMU) zeigt, dass ein Viertel der befragten Schweizer KMU bereits Opfer eines Cyber-Angriffs wurden und zu rund einem Drittel finanzielle Schäden sowie in kleinerem Ausmass Kundendatenverlust und/oder einen Reputationsschaden erlitten[42.]
Eine Studie aus Österreich zeigt, dass selbst in der wirtschaftlich schwierigen Pandemiezeit beinahe drei Viertel der befragten Unternehmen ihr Budget für Cyber-Sicherheit erhöht haben.[43]
Wie beschrieben sind diese potenziellen nutzenseitigen Auswirkungen auf die Volkswirtschaft jedoch indirekt. Die Wahrscheinlichkeit z. B. eines Ausfalls lässt sich zudem kaum auf einzelne Sicherheitsmassnahmen herunterbrechen. Weiter ist das Schadenspotenzial von Cyber-Risiken an sich nur schwer messbar[44]. Entsprechend lässt sich der spezifische Nutzen aus den vorgeschlagenen Massnahmen nicht quantifizieren.

4.2.2 Unbefugte Manipulation von Fernmeldeanlagen

Der Nutzen für die Volkswirtschaft ergibt sich aus der Vermeidung von Kosten, welche den Haushalten, Unternehmen und weiteren gesellschaftlichen Gruppen aus Cyber-Angriffen entstehen können. Die unter den Ziff. 1.1.2 und 1.2.2 bzw. den ersten zwei RFA-Prüfpunkten beschriebenen volkswirtschaftlichen Kosten von Cyberangriffen sind hoch und stiegen über die letzten Jahre stark an. Sie lassen sich schwer berechnen, da

37 Basis für diese Schätzung bilden Richtwerte, welche von der Offert-Plattform gryps.ch für KMU mit 60 Mitarbeitenden ausgewiesen werden (GRYPS]2021]: *ISO Zertifizierung Kosten* von https://www.gryps.ch/produkte/iso-9001-zertifizierung-178/kosten/). Für ein Erstzertifizierungsaudit wird bspw. ein Richtwert von 16'000 CHF veranschlagt. Nun sind einerseits die MNO deutlich grösser, womit für ein Audit mit deutlich höheren Kosten zu rechnen wäre. Andererseits ist der zu prüfende Umfang in der Regel deutlich geringer als bei einem Erstzertifizierungsaudit, wodurch sich die zu veranschlagenden Kosten für ein Audit wiederum reduzieren. Aufgrund dieser gegenläufigen Effekte erscheint es wahrscheinlich, dass die resultierenden Kosten unter CHF 100'000 zu liegen kommen.

38 Wie unter Ziff. 1.1.1 beschrieben, wird Mobilfunk zunehmend über 5G geleistet.

39 Gemäss BfS (2020): *Mobile Internetnutzung* von https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft/gesamtindikatoren/haushalte-bevoelkerung/mobile-internetnutzung.assetdetail.12307308.html griffen im Jahr 2019 84% der Schweizer Internetnutzerinnen und –nutzer im Alter zwischen 16 und 74 Jahren auf Mobiltelefone zurück.

40 Gemäss BfS (2019): *IKT Infrastruktur in den Unternehmen* von https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft/gesamtindikatoren/unternehmen/ikt-infrastruktur.assetdetail.8486582.html nutzten im Jahr 2017 77% der Unternehmen mobile Breitbandanschlüsse.

41 Die Wahrscheinlichkeit eines solchen Ausfalls (Szenario 2 – gross) wird mit rund einmal in 30 Jahren angegeben. BABS (2020): *Ausfall Mobilfunk* von https://www.babs.admin.ch/de/aufgabenbabs/gefaehrdrisiken/natgefaehrdanalyse/gefaehrddossier.html. Die methodischen Grundlagen sind beschrieben in BABS (2020): *Methode zur nationalen Risikoanalyse* von https://www.babs.admin.ch/de/aufgabenbabs/gefaehrdrisiken/natgefaehrdanalyse.html.

42 Peter et al. (2020): *Digitalisierung, Home-Office und Cyber-Sicherheit in KMU* von https://www.fhnw.ch/de/die-fhnw/hochschulen/hsw/media-newsroom/news/digitalisierung-home-office-und-cyber-sicherheit/media/digitalisierung-home-office-cyber-sicherheit-kmu-2020-12.pdf bzw. *Schlussbericht von Gfs-zürich* (2020): Homeoffice-Welle in Schweizer KMU: Chancen wahrgenommen – Cyberrisiken unterschätzt von https://gfs-zh.ch/homeoffice-welle-in-schweizer-kmuchancen-wahrgenommen-cyberrisiken-unterschaetzt/.

43 KPMG (2021): *KPMG Studie: Cyberrisiken werden durch die Pandemie beschleunigt* von https://home.kpmg/at/de/home/media/press-releases/2021/04/kpmg-studie-cyberrisiken-werden-durch-die-pandemie-beschleunigt.html.

44 Biener et al. (2015): *Cyber Risk: Risikomanagement und Versicherbarkeit* von https://www.kessler.ch/fileadmin/09_PDFs/Cyber_Risk_Risikomanagement_und_Versicherbarkeit_de.pdf.

längst nicht alle Opfer eines Cyberangriffs diesen auch publik machen und es sehr schwierig ist, die indirekten Kosten von Cyberangriffen (z. B. Reputationsschäden, Vertrauensverluste, Kundenunzufriedenheit) adäquat zu messen. Die Nutzeneffekte lassen sich zudem kaum auf einzelne Sicherheitsmassnahmen herunterbrechen. Es ist jedoch unbestritten, dass die Schäden durch Cyberangriffe längst eine volkswirtschaftlich relevante Dimension erreicht haben. Massnahmen zur Reduktion dieser Kosten wirken sich daher unmittelbar positiv aus.
Es wird generell davon ausgegangen, dass sich die Cybersicherheit immer stärker zu einem Wettbewerbsfaktor bei der Digitalisierung entwickelt.[45] Damit die Schweiz ihre Standortvorteile auch in der digitalen Wirtschaft nutzen kann, müssen auch auf regulatorischer Ebene die nötigen Voraussetzungen geschaffen werden. Mindestanforderungen an die Anbieterinnen von Internetzugängen in Bezug auf die Sicherheit tragen dazu bei, dass das volkswirtschaftliche Potential der Digitalisierung genutzt werden kann.
Während sich damit die vorgeschlagenen Massnahmen gesamtwirtschaftlich und gesellschaftspolitisch (vgl. Ziff. 4.3.2) positiv auswirken werden, sind sie für die IAP mit Kosten verbunden. Es ist nicht möglich, die Kosten zu beziffern, da viele Faktoren, wie zum Beispiel das Ausmass der heute bereits umgesetzten Massnahmen durch die Anbieterinnen oder die Reduktion der Kosten durch technische Entwicklungen, nur sehr schwer zu erheben sind. In diesem Abschnitt wird deshalb eine qualitative Einschätzung zu den Kosten gemacht und jeweils spezifisch darauf eingegangen, welche Auswirkungen insbesondere auf kleinere Anbieterinnen zu erwarten sind. Zwar konzentrierten sich Stand 2019 gemessen an der Kundenzahl 86% der Marktanteile auf fünf grosse IAP. Gleichzeitig machen diese Unternehmen nur einen Bruchteil aller in der Schweiz tätigen IAP aus. Insgesamt sind rund 170 IAP in der Schweiz tätig. Davon haben ca. 60% zwischen 1 und 1’000 Internet-Kundinnen und Kunden, 25% der IAP haben zwischen 1’000 und 10’000 und 15% verfügen über mehr als 10'000 Kundinnen und Kunden.[46]

4.2.2.1 Kosten der Massnahme 1: Pflicht der Anbieterinnen, zur Filterung von IP-Paketen mit gefälschter Quell-IP-Adresse (Spoofing)

Die Einführung von Methoden zur Filterung von IP-Paketen mit gefälschter Quell-IP-Adresse führt zu einem technischen und administrativen Aufwand bei den Anbieterinnen. Sie müssen die Filter technisch implementieren und die berechtigten Netze identifizieren. Die Filter müssen zudem stets aktualisiert werden, damit keine legitimen IP-Pakete gefiltert werden. Da die Methodik der Ingress-Filterung jedoch bereits vor 20 Jahren entwickelt wurde, ist die Umsetzung heute sehr viel einfacher geworden. Es gibt zahlreiche frei zugängliche Hilfsmittel und Guidelines dazu[47] und technische Hindernisse für die Umsetzung der Filterung sind in den letzten Jahren stark gesunken.
Bei der Beurteilung der Kosten ist wichtig festzuhalten, dass die Kosten für kleinere Anbieterinnen deutlich tiefer sind als für grössere Anbieterinnen.[48] Die kleineren Anbieterinnen haben einen deutlich geringeren Aufwand bei der Feststellung, welche Netze berechtigt sind und werden auch beim Betrieb des Filters mit weniger komplexen Anforderungen konfrontiert. Zudem sollen ausgehende Verbindungen mit gefälschten Adressierungselementen nur dann verhindert werden, wenn dies für die IAP mit vertretbarem Aufwand technisch möglich ist.

4.2.2.2 Kosten der Massnahme 2: Pflicht der Anbieterinnen, die Sicherheit der von ihnen den Kunden zur Verfügung gestellten Geräte gemäss dem aktuellen Stand der Technik zu gewährleisten.

Die Massnahme 2 kann für die Anbieterinnen bei der Beschaffung und der Wartung von CPE zu höheren Preisen führen. Entscheidend sind die vertraglichen Vereinbarungen mit den Herstellern der CPE. Die technischen Anforderungen an die Geräte können von den Herstellern zu geringen Kosten erfüllt werden. Die Anbieterinnen müssen aber sicherstellen, dass die Hersteller vertraglich dazu verpflichtet werden. Sicherheitsmassnahmen bei der Fernwartung, das zeitnahe Einspielen von Sicherheitsupdates und der Ersatz der

45 Bundesamt für Sicherheit in der Informationstechnik (2016): *Cyber-Sicherheit als Wettbewerbsvorteil in der Digitalisierung* von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Cyber-Sicherheit_als_Wettbewerbsvorteil.pdf?__blob=publicationFile&v=3.
46 BAKOM (2021 auf Basis von Zahlen aus der Fernmeldestatistik des Jahres 2019). Siehe auch *Internet Service Provider* von https://www.bakom.admin.ch/bakom/de/home/telekommunikation/zahlen-und-fakten/sammlung-statisticher-daten/internet-service-provider.html.
47 MANRS (2016-2021): *Anti-Spoofing* von https://www.manrs.org/isps/guide/antispoofing/.
48 Lone et al. (2020): *SAVing the Internet: Explaining the Adoption of Source Address Validation by Internet Service Providers* von https://weis2020.econinfosec.org/wp-content/uploads/sites/8/2020/06/weis20-final31.pdf.

CPE bei Ende der Lebensdauer liegt in der Verantwortung der Anbieterinnen. Die Hersteller stellen jedoch die nötigen Updates zur Verfügung, so dass der Aufwand für die Anbieterinnen üblicherweise gering ist. Das Risiko und der Wartungsaufwand für unsichere oder veraltete CPE-Geräte ist über längere Dauer sehr wahrscheinlich kostspieliger als eine korrekte Konfiguration und Wartung der Geräte.
Auch die Massnahme 2 wird bei grösseren Anbieterinnen tendenziell zu höheren Kosten führen als bei kleineren Anbieterinnen. Letztere haben weniger CPE im Einsatz und können daher die sichere Konfiguration und Wartung mit geringerem Ressourcenaufwand sicherstellen.
Zu beachten ist, dass Art. 96a Abs. 3 nur den Fall regelt, in dem die Geräte den Kunden durch die IAP zur Verfügung gestellt werden. Bezieht der Kunde sein Gerät über eine Drittanbieterin, fallen keine Regulierungskosten an. Nach der Auslieferung der Geräte wiederum fallen allfällige Zusatzkosten bspw. beim Einspielen von Sicherheitsupdates nur an, falls die IAP weiterhin die Kontrolle über die Geräte innehaben.

4.2.2.3 Massnahme 3: Recht, Internetzugänge oder Adressierungselemente, von denen eine Gefährdung von Fernmeldeanlagen ausgeht, zu sperren oder deren Nutzung einzuschränken sowie Pflicht zur Information der Kunden

Da die Sperrung oder Einschränkung des Internetanschlusses im Ermessen der Anbieterinnen bleibt, generiert diese Massnahme nur dann Kosten, wenn sich die Anbieterinnen zur Sperrung oder Einschränkung entscheiden. Auch in diesem Fall liegen die Kosten tief und sind im Interesse der Anbieterin. Bezüglich Informationspflicht entstehen der Anbieterin mindestens gleichwertige Kosten, wie wenn sie die Kunden nicht aktiv über eine Sperrung oder Einschränkung ihrer Anschlüsse informiert, weil davon auszugehen ist, dass in einem solchen Fall die Kunden ihre Anbieterin mit hoher Wahrscheinlichkeit von sich aus kontaktieren würden. Beim Kundendienst entsteht damit so oder so Aufwand.

4.2.2.4 Massnahme 4: Pflicht der Anbieterinnen, eine Meldestelle für die Meldung von Manipulationen zu führen und auf Meldungen innerhalb einer angemessenen Frist mit geeigneten Abwehrmassnahmen zu reagieren.

Die Pflicht, eine Meldestelle zu bezeichnen, welche eine Reaktion auf Meldungen in den gegebenen Fristen sicherstellt, führt bei Anbieterinnen, welche noch nicht über eine solche Meldestelle verfügen zu Kosten. Die geforderte Reaktionszeit innerhalb einer angemessenen Frist verhindert aber, dass die Anbieterinnen einen Pikettdienst über Nacht oder über das Wochenende aufrechterhalten müssen. Es kann zudem mit dem NCSC Rücksprache genommen werden, ob die Meldung des NCSC auch über andere Kanäle erfolgen kann, womit den Anbieterinnen ermöglicht wird, die Reaktionsfähigkeit innert angemessener Frist zu möglichst geringen Kosten sicherzustellen. Den Kosten für die IAP steht ein hoher Nutzen beim Schutz der übrigen Anschlüsse gegenüber, da nur durch eine rasche Reaktion die Gefährdung der übrigen Anschlüsse reduziert werden kann. Die Kosten der Reaktion bzw. der Abwehrmassnahmen an sich sind schwierig zu beziffern, da sie in hohem Mass variieren je nach Anbieterin und vor allem je nach Gefährdung. Die möglichen Gefährdungen und die angemessenen Abwehrmassnahmen der IAP darauf entwickeln sich zudem laufend weiter.

4.3 Auswirkungen auf die Gesellschaft

4.3.1 Netzwerksicherheit von 5G-Mobilfunknetzen

Nutzenseitig lassen sich auch die Auswirkungen auf die Gesellschaft, insbesondere auf Gesundheit und Sicherheit, anführen. Etwa beschreibt das in Ziff. 4.2.1 (Auswirkungen auf die Volkswirtschaft) erwähnte Gefährdungsdossier des BABS auch Todesfälle, Verletzte und Einschränkungen in der Tätigkeit von Blaulichtorganisationen als mögliche Folgen eines Mobilfunkausfalls.

4.3.2 Unbefugte Manipulation von Fernmeldeanlagen

Die Digitalisierung hat grosse Auswirkungen auf die Gesellschaft, da sie den Alltag der Menschen direkt betrifft. Cybervorfälle verunsichern die Menschen bei der Nutzung digitaler Angebote. Es ist für das Vertrauen der Gesellschaft in die digitalen Technologien wichtig, dass diese einen Mindeststandard an Sicherheit erfüllen. Wenn die Konsumentinnen beim IAP ein Gerät beziehen, sollten sie daher davon ausgehen können, dass dieses gemäss Massnahme 2 so konfiguriert ist, dass es gegenüber Cyberangriffen minimal geschützt ist.

4.4 Auswirkungen in weiteren überprüften Bereichen

4.4.1 Netzwerksicherheit von 5G-Mobilfunknetzen

Mögliche Auswirkungen sowohl auf Kantone und Gemeinden sowie auf urbane Zentren, Agglomerationen und Berggebiete, auf die Umwelt als auch andere Auswirkungen wurden geprüft. Es ist potenziell mit indirekten, nutzenseitigen Auswirkungen in Folge sicherer 5G-Netze zu rechnen. Diese Auswirkungen sind jedoch unspezifisch und betreffen nicht bestimmte 5G-Anwendungen und –Nutzer. Deswegen wird für die genannten Bereiche nicht einzeln auf die Auswirkungen eingegangen. Der erwartete allgemeine Nutzen ist unter den Ziff. 4.2.1 (Auswirkungen auf die Volkswirtschaft) und 4.3.1 (Auswirkungen auf die Gesellschaft) beschrieben.

4.4.2 Unbefugte Manipulation von Fernmeldeanlagen

Mögliche Auswirkungen sowohl auf Kantone und Gemeinden sowie auf urbane Zentren, Agglomerationen und Berggebiete, auf die Umwelt als auch andere Auswirkungen wurden geprüft. Es ist potenziell mit indirekten, nutzenseitigen Auswirkungen in Folge eines erhöhten Schutzniveaus im Bereich der Cyber-Sicherheit zu rechnen. Diese Auswirkungen sind jedoch unspezifisch, weswegen für die genannten Bereiche nicht einzeln auf die Auswirkungen eingegangen wird. Der erwartete allgemeine Nutzen ist unter den Ziff. 4.2.2 (Auswirkungen auf die Volkswirtschaft) und 4.3.2 (Auswirkungen auf die Gesellschaft) beschrieben.

5 Rechtliche Aspekte

Mit den vorgeschlagenen Bestimmungen wird Artikel 48*a* FMG umgesetzt. Absatz 2 dieser Bestimmung überträgt dem Bundesrat weitreichende legislative Kompetenzen im Bereich der Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten. Gemäss Artikel 62 Absatz 2 FMG kann der Bundesrat dem BAKOM die Aufgabe übertragen, die notwendigen technischen und administrativen Vorschriften zu erlassen (siehe auch Art. 105 Abs. 1 FDV). Dabei muss das BAKOM die international geltenden Normen berücksichtigen. Insbesondere entwickelt die Europäische Union ein Zertifizierungssystem für die Cybersicherheit von 5G-Netzen (vgl. Kommentar zu Art. 96*g*), das in Bezug auf die Artikel 96*d* bis 96*g* so weit wie möglich als Modell dienen sollte.
Die in Artikel 96f Absatz 2 vorgesehene Standortplicht für Netzwerk- und Sicherheitsbetriebszentren ist mit Artikel XIV^{bis} Absatz 1 Buchstabe b von Anhang 1B des Abkommens zur Errichtung der Welthandelsorganisation (General Agreement on Trade in Services; GATS) kompatibel (vgl. Erläuterungen zu Art. 96*f* Abs. 2).

Abkürzungsverzeichnis

API	*Application Programming Interface*
BABS	Bundesamt für Bevölkerungsschutz
BAKOM	Bundesamt für Kommunikation
BCP	*Best Current Practices*
CPE	*Customer Premises Equipment*
DDoS	*Distributed Denial Of Service attack*
ENISA	*European Union Agency for Cybersecurity*
ETIS	*The Community for Telecom Professionals*
FDA	Fernmeldedienstanbieter
FDI	*Foreign Direct Investment*
FMG	Fernmeldegesetz
IAP	*Internet Access Provider*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
ISMS	*Managementsystem für die Informationssicherheit*
ISO	*International Organization for Standardization*
ITU	*International Telecommunication Union*
KMU	Kleine und mittlere Unternehmen
M3AAWG	*Messaging Malware Mobile Anti-Abuse Working Group*
MANRS	*Mutually Agreed Norms for Routing Security*
MNO	*Mobile Network Operator*
NAZ	Nationale Alarmzentrale
NCSC	Nationales Zentrum für Cybersicherheit
NOC	*Network Operation Center* - Netzwerkbetriebszentrum
RFA	Regulierungsfolgenabschätzung
RIR	*Regional Internet Registry*
SANS	*SysAdmin, Audit, Network, Security Institut*
SOC	*Security Operation Center* - Sicherheitsbetriebszentrum
SVV	Schweizerischer Versicherungsverband