Landeskanzlei
Rathausstrasse 2
4410 Liestal
T 061 552 50 06
landeskanzlei@bl.ch
www.bl.ch

BASEL LANDSCHAFT
REGIERUNGSRAT

Regierungsrat, Rathausstrasse 2, 4410 Liestal

Per E-Mail an:
tp-secretariat@bakom.admin.ch

Liestal, 15. Februar 2022

Stellungnahme zur Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit Schreiben vom 3. Dezember 2021 haben Sie den Regierungsrat des Kantons Basel-Landschaft eingeladen, im Rahmen der Vernehmlassung zur Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten) Stellung zu nehmen. Gerne lassen wir Ihnen diese Stellungnahme hiermit zukommen.

Der Regierungsrat begrüsst grundsätzlich den vorliegenden Entwurf der Verordnung über Fernmeldedienste (FDV). Mit dem vorliegenden Entwurf wird die unbefugte Manipulation von Fernmeldeanlagen durch fernmeldetechnische Übertragungen bekämpft. Insbesondere Massnahmen zur Schaffung eines Mindestniveaus an 5G-Netzwerksicherheit in der Schweiz erachtet der Regierungsrat als dringend erforderlich. Ein hohes Sicherheitsniveau beim Betrieb von Mobilfunknetzen der neusten Generation ist ebenso sicherzustellen.

Der Regierungsrat beantragt ausserdem folgende Ergänzungen:

1. Es ist darzulegen, wie die Blaulichtorganisationen und die Kritischen Infrastrukturen (KI) in die Alarmierungs- und Meldeprozesse einbezogen werden.

Begründung: Heute werden über 70 Prozent aller Notrufe über Mobiltelefone abgewickelt. Betriebsunterbrüche in den Mobilnetzen sind dadurch sensitiv. Sie haben direkte Auswirkungen auf das Notrufwesen und die Ereignisbewältigung durch die Blaulichtorganisationen, ebenso wie auf die Betreiber von KI, die auf einen zuverlässigen und sicheren Betrieb der neuen Generation von Mobilfunknetzen angewiesen sind.

2. Einführung einer Pflicht zur selektiven Blockierung von Internetzugängen oder Adressierungselementen, von denen eine Gefährdung im Zusammenhang mit KI ausgeht.

Begründung: Cyberangriffe haben nicht nur hohe wirtschaftliche Auswirkungen, sondern sie gefährden auch die Sicherheit des Landes, da sie zu Ausfällen oder fehlerhaftem Funktionieren von

KI führen können. Aus diesem Grund haben Anbieterinnen von Internetzugängen diese und Adressierungselemente zu blockieren, von denen eine Gefährdung für KI ausgeht. Nur so kann die Sicherheit der angebotenen Dienstleistungen gewährleistet werden.

3. Die Rollen der einzelnen Akteure und Stellen sind detailliert zu beschreiben.

Begründung: Um die Bearbeitung und Verteilung der eingegangenen Störungsmeldungen zu verbessern, sieht die revidierte Verordnung vor, die Rolle der Nationalen Alarmzentrale (NAZ) zu stärken, da sie eine sichere Informatikinfrastruktur und einen 24-Stunden-Betrieb unterhält (Art. 96). Cyberangriffe dagegen sind einer zu schaffenden Meldestelle gemäss Art. 96 b zu melden. Darüber hinaus bestehen weitere Organisationen, die sich um Cyberangriffe kümmern. So sind beispielsweise auch das National Cyber Security Center (NCSC), die Melde- und Analysestelle Informationssicherung (MELANI) sowie die kantonalen Notrufzentralen einzubinden. In diesem Zusammenhang kann es nicht sein, dass ausschliesslich das BAKOM von der NAZ über die gemeldeten Störungen informiert wird. Die Rollen sämtlicher Stellen im Gesamtprozess von Meldung und Alarmierung im Bereich Cyber sind im Erläuternden Bericht detailliert aufzuführen. Dabei ist die Schaffung eines Single Point of Contact (SPOC) grundsätzlich anzustreben, weil damit die Krisenbewältigung erleichtert wird.

4. Die Anbieterinnen sind zu verpflichten, Störungen im Betrieb ihrer Fernmeldeanlagen und Fernmeldedienste unverzüglich zu melden, wenn diese länger als 15 Minuten dauern und mindestens 1000 Kunden betreffen.

Begründung: Die in Art. 96 vorgesehene Zahl von 30'000 potenziell betroffenen Kunden entspricht dem Äquivalent einer Schweizer Stadt mittlerer Grösse. Eine Störung, die den gesamten Kanton Appenzell Innerhoden mit seinen 16'300 Einwohnern betreffen würde, würde gemäss vorliegendem Entwurf somit nicht gemeldet. Zudem ist es wichtig, dass die Dauer von Störungen abgeschätzt werden kann. Aktuell gehen die Notruforganisationen davon aus, dass Störungen relevant sind, welche voraussichtlich mehr als 15 Minuten dauern und mindestens 1000 Kundinnen und Kunden betreffen.

5. Im Zusammenhang mit der Bedrohung kritischer Infrastrukturen durch Cyber-Angriffe von staatlicher Seite und deren Abwehr sind die Aufgaben der Armee aufzuzeigen und in die FDV zu integrieren.

Begründung: Die klassische Machtpolitik erlebt seit einigen Jahren eine Renaissance. Bereits heute setzen einige Staaten ihre Cybermittel regelmässig im Sinne eines "Kalten" Cyber-Krieges ein. Im Falle eines bewaffneten Konflikts in Europa ist mit einer breiten Verwendung dieser Mittel zu rechnen. Davon dürften auch Staaten, die an den eigentlichen Kampfhandlungen nicht beteiligt sind, betroffen sein. Die Armee hat in den vergangenen Jahren Schritte unternommen, sich auf ein solches Szenario vorzubereiten. So ist die Führungsunterstützungsbasis (FUB) im Bereich Verteidigung für Aktionsplanung, Lageverfolgung, Ereignisbewältigung und Ausbildung der Mitarbeitenden und AdA im Cyber-Raum verantwortlich. Mit der Weiterentwicklung der Armee (WEA) wurde zur Unterstützung der Berufsorganisation der FUB eine Cyber-Kompanie gebildet. Ab 2022 werden sämtliche Cyber Formationen der Schweizer Armee in das neu gegründete Cyber Bataillon 42 integriert. Die Rolle der Armee ist in der revidierten FDV zu berücksichtigen und ihre Verwendung zu beschreiben.

6. Die Anbieterinnen sind zu verpflichten, den Kundinnen und Kunden bei der Behebung des kompromittierenden Systems Hilfe zur Selbsthilfe zu leisten bzw. diese zu instruieren.

Begründung: Gemäss Art. 96a Abs. 3 des Vorentwurfs (VE FDV) sind Internet Access Provider (IAP) berechtigt, Internetzugänge oder Adressierungselemente, die das ordnungsgemässe Funktionieren von Fernmeldeanlagen zu beeinträchtigen drohen, zu sperren oder deren Nutzung einzuschränken. Darüber hinaus haben sie ihre Kundinnen und Kunden, die Opfer unbefugter Manipulationen geworden sind oder werden könnten, unverzüglich über solche Sperrungen oder Einschränkungen zu informieren. Sie dürfen diese Massnahmen aufrechterhalten, solange die Bedrohung anhält. Diese Massnahme erscheint auf den ersten Blick effizient, da sie die Störung umgehend beseitigt. Im Endeffekt verlagert Art. 96 Abs. 3 VE FDV aber das Problem – und damit die Aufgabe – der Störungsbeseitigung auf den Endnutzer der kompromittierten Geräte und damit die Kunden der IAP. Diese werden mangels fachlichem Know-how in den wenigsten Fällen in der Lage sein, selbst die erforderlichen Massnahmen ergreifen zu können und ein System (meist ohne Back-ups) neu aufzusetzen. Zudem wird der Endbenutzer ohne Hilfe und Angaben zur zu beseitigenden Malware und zum infizierten System (mehrere Geräte sind im Internet der Dinge über einen WLAN-Router indirekt am Netz des IAP, z. B. Waschmaschine, Kühlschrank, Drucker, Staubsaugerroboter etc.) in den wenigsten Fällen zum Deblockieren des Anschlusses führen, da Massnahmen aufrechterhalten werden, solange die Bedrohung anhält.

7. Im Rahmen eines Sicherungselements sollten die Anbieterinnen verpflichtet werden, den Kundinnen und Kunden so rasch als möglich den Internetzugriff mittels Unterstützung wieder zu gewährleisten.

Begründung: Im Rahmen des im Entwurfes der Stellungnahme des Regierungsrates genannten Aufflammens der Machtpolitik ist zusätzlich zu beachten, dass sich das System des Art. 96 Abs. 3 VE FDV nicht gegen sich selbst richtet. Staatliche Akteure könnten durch eine gezielte Operation eine Vielzahl von Computersystemen in der Schweiz infizieren, deren Zugriff gestützt auf Art. 96 Abs. 3 FE FDV in der Folge blockiert würde. Als Konsequenz wäre die Kommunikation des Staates mit seinen Bürgern oder die Wirtschaft gezielt unterbunden bzw. destabilisiert.

Der Regierungsrat dankt Ihnen für die Gelegenheit zur Stellungnahme und für die Berücksichtigung unserer Anliegen.

Hochachtungsvoll

Thomas Weber
Regierungspräsident

Elisabeth Heer Dietrich
Landschreiberin