

Medienmitteilung

Vernehmlassung Bund: Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten

Ein wichtiger Schritt zur Erhöhung der schweizweiten Cyber-Resilienz

Bern/Zürich, 18.03.2022 – **In der zunehmend digitalisierten Gesellschaft ist Cybersecurity ein zentrales Thema geworden. Dies gilt besonders für den Schutz von kritischen Infrastrukturen. Hier will der Bundesrat nachbessern und führt deshalb zu gleich zwei Vorlagen eine Vernehmlassung durch. Die Einreichungsfrist der ersten, die gezielte Änderung der Verordnung über Fernmeldedienste (FDV) zum Schutz von Fernmeldeinfrastrukturen und -diensten, endet heute. Der Verein digitalswitzerland begrüsst die Revision und schlägt einzelne Anpassungen für eine klare und effiziente Umsetzung vor.**

Darum geht es

Heute endet die Vernehmlassung des Bundes zur «Änderung der Verordnung über Fernmeldedienste». Dank dieser soll die Sicherheit von Fernmeldeinfrastrukturen und -diensten weiter gestärkt werden. Der Bundesrat schlägt vier Massnahmen vor, um die unbefugte Manipulation von Fernmeldeanlagen zu bekämpfen und die Netzwerksicherheit von 5G-Mobilfunknetzen sicherzustellen. Namentlich sollen die Anbieterinnen von Internetzugängen (IAP) verpflichtet werden: 1. Spoofing-Versuche zu filtern; 2. die Sicherheit von Geräten, die sie ihren Kunden zur Verfügung stellen, bestmöglich zu gewährleisten; 3. ihre Kunden über die Sperrung von Internetzugängen oder Adressierungselementen zu informieren; sowie 4. unbefugte Manipulationen an Fernmeldeanlagen zu melden und in angemessener Frist Abwehrmassnahmen zu ergreifen.

Cyber-Resilienz ist das Gebot der Stunde

digitalswitzerland begrüsst die vorgeschlagene Revision der FDV ausdrücklich. Eine Stärkung der Sicherheit der Fernmeldenetze als kritische Infrastruktur von allen Seiten ist ein zentrales Element zur Erhöhung der schweizweiten Cyber-Resilienz.

Aus Sicht von digitalswitzerland sind die Prozesse im Interesse der Sicherheit möglichst klar und effizient zu gestalten. Es gilt Doppelspurigkeit zu vermeiden und Vorgaben auf internationalen Standards abzustimmen. Deshalb schlägt digitalswitzerland folgende punktuelle Anpassungen der Vorlage vor:

- Störungsmeldungen sollten künftig an das Nationale Zentrum für Cybersicherheit (NCSC) erfolgen. Denn im Rahmen des neuen Informationssicherheitsgesetzes (ISG), welches sich als zweite Vorlage zum Schutz von kritischen Infrastrukturen derzeit in der Vernehmlassung befindet, wird das NCSC als zentrale Meldestelle für Cybervorfälle bei kritischen Infrastrukturen definiert.
- Im Bericht wird festgehalten, welche Massnahmen für die Geräte vorgesehen sind, die Kunden zur Verfügung gestellt werden. Dies ist ein wichtiger Schritt. Allerdings gilt es, hier den Begriff «End of Life» einheitlich zu verwenden.

Weiter begrüsst digitalswitzerland, dass sich die Vorlage im Wesentlichen an Massnahmen orientiert, welche auch in der EU implementiert werden, und auf international anerkannten Sicherheitsnormen und -initiativen basiert (z.B. ENISA, NESAS, 3GGP, EU 5G Toolbox, ISO). Nun ist es wichtig, dass der Bund diesem Grundsatz auch bei den noch folgenden technischen Präzisierungen auf Stufe technischer und administrativer Vorschriften (TAV) treu bleibt.

Weitere Informationen zur Vernehmlassung FDV: [siehe vollständige Stellungnahme von digitalswitzerland](#)

Kontakt für weitere Auskünfte

Andreas W. Kaelin, digitalswitzerland | Geschäftsstelle Bern
Tel. +41 31 311 62 45 | andreas@digitalswitzerland.com

Über digitalswitzerland

digitalswitzerland ist eine schweizweite, branchenübergreifende Initiative, welche die Schweiz als weltweit führenden digitalen Innovationsstandort stärken und verankern will. Unter dem Dach von digitalswitzerland arbeiten an diesem Ziel mehr als 240 Organisationen, bestehend aus Vereinsmitgliedern und politisch neutralen Stiftungspartnern, transversal zusammen. digitalswitzerland ist Ansprechpartnerin in allen Digitalisierungsfragen und engagiert sich für die Lösung vielfältiger Herausforderungen.