Appenzell Ausserrhoden

Regierungsrat

Obstmarkt 3
9102 Herisau
Tel. +41 71 353 61 11
kantonskanzlei@ar.ch
www.ar.ch

Regierungsrat, 9102 Herisau

Dr. iur. Roger Nobs
Ratschreiber
Tel. +41 71 353 63 51
roger.nobs@ar.ch

Eidg. Departement für Umwelt, Verkehr,
Energie und Kommunikation

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

(PDF- und Wordversion)

Herisau, 4. März 2022

Eidg. Vernehmlassung; Änderung der Verordnung über Fernmeldedienste (Sicherheit von Informationen und Fernmeldeinfrastrukturen und –diensten); Stellungnahme des Regierungsrates von Appenzell Ausserrhoden

Sehr geehrte Damen und Herren

Mit Schreiben vom 3. Dezember 2021 unterbreitet das Eidg. Departement für Umwelt, Verkehr, Energie und Kommunikation einen Änderungsentwurf der Verordnung über Fernmeldedienste (FDV) bis zum 18. März 2022 zur Vernehmlassung.

Der Regierungsrat von Appenzell Ausserrhoden nimmt dazu wie folgt Stellung:

Er begrüsst den vorliegenden Entwurf im Grundsatz. Begrüsst wird insbesondere, dass mit der Vorlage die unbefugte Manipulation von Fernmeldeanlagen durch fernmeldetechnische Übertragungen bekämpft wird. 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 folgende Ergänzungen:

- Es ist darzulegen, wie die Blaulichtorganisationen und die kritischen Infrastrukturen (KI) in die Alarmierungs- und Meldeprozesse einbezogen werden. Da heute über 70 % aller Notrufe über Mobiltelefone abgewickelt werden, sind Betriebsunterbrüche in den Mobilnetzen aus diesen Gründen 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.
- Einführung einer Pflicht zur selektiven Blockierung von Internetzugängen oder Adressierungselementen, von denen eine Gefährdung im Zusammenhang mit KI ausgeht. 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 Anbieter von Internetzugängen diese und Adressierungselemente zu blockieren, von denen eine Gefährdung für KI ausgeht. Nur so kann die Sicherheit der angebotenen Dienstleistungen gewährleistet werden.

- Die Rollen der einzelnen Akteure und Stellen sind detailliert zu beschreiben. 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. 96b 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.
- Die Anbieter werden verpflichtet, unverzüglich Störungen im Betrieb ihrer Fernmeldeanlagen und Fernmeldedienste zu melden, wenn 1000 Kunden, die potentiell von einem Ausfall betroffen sind, der länger als 15 Minuten dauert. Die Zahl von 30'000 potenziell betroffenen Kunden entspricht dem Äquivalent einer Schweizer Stadt mittlerer Grösse. Eine Störung, die z. B. 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 davon betroffen sind.
- 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. 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 Angehörigen der Armee 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.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme.

Freundliche Grüsse

Im Auftrag des Regierungsrates

Dr. iur. Roger Nobs, Ratschreiber