Bundespräsidentin Viola Amherd
Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport VBS
Bundeshaus Ost
3003 Bern

Per E-Mail an: ncsc@ncsc.admin.ch

Bern, 13. September 2024

Stellungnahme zur Vernehmlassung Cybersicherheitsverordnung (CSV)

Sehr geehrter Frau Bundespräsidentin,
Sehr geehrte Damen und Herren

Wir nehmen Bezug auf die am 22. Mai 2024 eröffnete Vernehmlassung zur Cybersicherheitsverordnung (CSV) und danken Ihnen für die Einladung zur Stellungnahme. Der Schweizerische Verband der Telekommunikation (asut) vertritt die Interessen der Telekommunikations-, Netzwerk- und Datacenter-Branche und unsere Mitglieder sind direkt von den vorgeschlagenen Änderungen in der CSV betroffen. Gerne übermitteln wir Ihnen fristgerecht unsere Einschätzung dazu.

Einleitende Bemerkungen

Bereits das Fernmeldegeheimnis gemäss Art. 13 der Bundesverfassung hat bei den Telekommunikationsunternehmen zu einer hohen Sicherheitskultur zum Schutz der Daten und des Fernmeldeverkehrs geführt. Entsprechende rechtliche Vorgaben finden sich auch im Fernmeldegesetz und den dazugehörenden Verordnungen. Mit dem Internet und der zunehemenden Vernetzung nimmt die Bedeutung der Cybersicherheit weiter zu. Die Cybersicherheit ist daher ein zentrales Anliegen der Telekommunikationsunternehmen und viele unserer Mitglieder investieren substanzielle Ressourcen in den Aufbau und Betrieb sicherer Infrastrukturen und Prozesse. Die Telekommunikationsbranche begrüsst daher im Grundsatz den vorliegenden Entwurf der Cybersicherheitsverordnung und hat zu den folgenden Punkten ergänzende Anträge.

Nationale Cyberstrategie und Steuerungsausschuss

Art. 2 Nationale Cyberstrategie
Die Nationale Cyberstrategie (NCS) und die Umsetzung der Massnahmen haben direkte Auswirkungen auf Wirtschaft sowie auf Wissenschaft und die Zivilgesellschaft. Wir begrüssen daher, dass diese Stakeholder im Steuerungsausschuss vertreten sind. Darüber hinaus wäre es jedoch für die Akzeptanz der NCS wichtig, wenn diese Stakeholder – wie bereits die Kantone – bei der Festlegung der NCS einbezogen werden.

Art. 2 Nationale Cyberstrategie
[2] Sie wird in Abstimmung mit den Kantonen und unter Einbezug der Wirtschaft, der Wissenschaft und von Vertretern der Zivilgesellschaft festgelegt.

asut
Schweizerischer Verband der Telekommunikation
Hirschengraben 8
3011 Bern

+41 (0)31 560 66 66
info@asut.ch
www.asut.ch

Aufgaben des BACS

Art. 9 Koordinierte Offenlegung von Schwachstellen
Die koordinierte Offenlegung von Schwachstellen ist ein zentrales Element zur Bekämpfung von Cyberrisiken und zur Steigerung der Cybersicherheit. Wir begrüssen, dass sich das BACS dabei auf internationale Standards abstützt. Aufgrund der raschen Entwicklung im ICT- und Cyber-Bereich ist es jedoch denkbar, dass für neue Aspekte noch kein Standard vorliegt, sich aber bereits eine Best Practice etabliert hat. Das BACS soll daher in solchen Fällen in Ergänzung zu internationalen Standards auch Best Practice berücksichtigen dürfen.

Zudem soll die koordinierte Offenlegung erst nach Behebung einer Schwachstelle erfolgen. Ansonsten besteht die Gefahr, dass noch offene Schwachstellen breit bekannt gemacht werden mit entsprechenden Risiken für die betroffenen Systeme und deren Nutzerinnen und Nutzer.

Die vorgeschlagene Frist von 90 Tagen zur Behebung einer Schwachstelle mag für viele Situationen genügen. Angesichts der Vielfalt und Komplexität von ICT-Systemen ist jedoch absehbar, dass es Fälle gibt, die eine längere Behebungsfrist benötigen. Daher soll dem BACS die Möglichkeit gegeben werden, längere Fristen anzuordnen, wenn dies im Einzelfall zur Behebung der Schwachstelle notwendig ist.

Art. 9 Koordinierte Offenlegung von Schwachstellen
[1] Das BACS sorgt für die koordinierte Offenlegung der Schwachstellen nach deren Behebung nach international anerkannten Standards und Best Practices.
[2] Es setzt der Herstellerin der betroffenen Hard- oder Software eine angemessene Frist, jedoch mindestens ~~von~~ 90 Tage~~n~~, zur Behebung der Schwachstellen.

Bereits in unserer Stellungnahme zum Informationssicherheitsgesetz ISG vom 12. April 2022 haben wir darauf hingewiesen, dass die Abläufe und Informationsflüsse durch eine einzige zentrale Meldestelle vereinfacht und verbessert werden können. Leider sind immer noch unterschiedliche Meldeverfahren bei Störungen und Vorfällen vorgesehen. Wir regen daher an, bei der Umsetzung der CSV die diversen Meldeverfahren zu Harmonisieren. In diesem Sinne sind die Regelungen zur Koordination zwischen dem BACS und dem BAKOM in Art. 9 Abs. 7 und Abs. 8 der richtige Ansatz.

Informationsaustausch

Art. 11 Kommunikationssystem für den sicheren Informationsaustausch
Meldepflichtige Organisationen gemäss ISG Art. 74b können ihren Sitz auch im Ausland haben. Obwohl sich der Geltungsbereich des ISG auf die Schweiz beschränkt, soll die Möglichkeit geschaffen werden, dass sich solche Organisationen am Informationsaustausch beteiligen können. Dies jedoch nur gemäss festzulegenden Anforderungen durch das BACS. Durch den Einbezug dieser Unternehmen erhält das BACS eine bessere und umfassendere Sicht auf mögliche Gefährdungen.

Art. 11 Kommunikationssystem für den sicheren Informationsaustausch
[1] Zugang zum Kommunikationssystem des BACS für den sicheren Informationsaustausch (Artikel 74 Abs. 2 Buchstabe a) haben Organisationen und Behörden ~~mit Sitz in der Schweiz.~~, die entweder ihren Sitz in der Schweiz haben oder vom BACS zum Informationsaustausch zugelassen werden und die von ihm dafür festgelegten Anforderungen erfüllen.

Meldepflicht

Art. 18 Zu meldende Cyberangriffe
Von der Meldepflicht bei Cyberangriffen sind nur Betreiber einer kritischen Infrastruktur betroffen. Daher soll die Meldepflicht nur jene Vorfälle umfassen, welche auch direkte Auswirkungen auf den Betrieb der kritischen Infrastruktur haben können. Dies ist insbesondere dort zwingend, wo die ICT-Systeme der kritischen Infrastruktur stärker geschützt sind oder komplett getrennt von der restlichen ICT betrieben werden. Daher soll sich die Meldepflicht auf den Bereich der kritischen Infrastruktur beschränken.

Art. 18 Zu meldende Cyberangriffe
[1] Die Funktionsfähigkeit einer kritischen Infrastruktur gilt als gefährdet, wenn:
- *a. Mitarbeitende oder Dritte, welche den unmittelbaren Betrieb der kritischen Infrastruktur verantworten, von durch Cyberangriffen verursachten ~~von~~ Systemunterbrüchen betroffen sind und dadurch der stabile Betrieb der Infrastruktur unmittelbar gefährdet ist; oder*

b. die betroffene Organisation oder Behörde ihre Tätigkeiten nur noch mit Hilfe von Notfallplänen aufrechterhalten kann.

[2] Eine Manipulation oder ein Abfluss von Informationen liegt vor, wenn:

a. geschäftsrelevante Informationen, welche mit dem unmittelbaren Betrieb der kritischen Infrastruktur in Zusammenhang stehen, von Unbefugten verändert oder offengelegt werden; oder

b. eine Verletzung der Datensicherheit nach Artikel 24 des Datenschutzgesetzes vom 25. September 202012 vorliegt. (….)

Art. 19 Inhalt der Meldung
Die Meldung gemäss Art. 19 kann auch Personendaten umfassen, wobei das Informationssicherheitsgesetzt die Weitergabe von Personendaten ohne die Einwilligung der betreffenden Person nur unter definierten Voraussetzungen erlaubt. Da sich erst bei der vertieften Analyse der Meldung zeigen kann, ob diese Voraussetzungen zutreffen oder nicht, besteht bei jeder Meldung das Risiko einer Verletzung des Datenschutzgesetzes. Die Abläufe sollten daher so gestaltet werden, dass Personendaten nur bei gesicherten Vorfällen weitergegeben werden müssen.

Schlussbestimmungen

Art. 23
Die Anpassung der Unternehmensprozesse sowie allenfalls technischer Systeme an die neuen Anforderungen betreffend die Meldepflicht benötigen ausreichend Zeit und können nicht innert einiger weniger Wochen nach dem Entscheid des Bundesrates umgesetzt werden. Es ist daher eine Einführungsfrist von mindestens sechs Monaten vorzusehen.

Wir danken Ihnen bestens für die Berücksichtigung unserer Anliegen und stehen bei Fragen gerne mit unseren Expertinnen und Experten zur Verfügung.

Freundliche Grüsse

Peter Grütter
Präsident