KANTON
LUZERN

Justiz- und Sicherheitsdepartement
Bahnhofstrasse 15
Postfach 3768
6002 Luzern
Telefon 041 228 59 17
jsdds@lu.ch
www.lu.ch

Bundesamt für Cybersicherheit

per E-Mail
ncsc@ncsc.admin.ch

Luzern, 27. August 2024

Protokoll-Nr.: 902

Cybersicherheitsverordnung (CSV): Vernehmlassung

Sehr geehrte Damen und Herren

Für die Gelegenheit im Rahmen des oben genannten Vernehmlassungsverfahrens Stellung nehmen zu können, danken wir Ihnen. Im Namen und Auftrag des Regierungsrates erlauben wir uns die folgenden Bemerkungen.

1. Allgemeine Bemerkungen

Wir sind mit den Ausführungsbestimmungen zur Meldepflicht und den vorgesehenen Aufgaben des Bundesamtes für Cybersicherheit (BACS) einverstanden. Positiv werten wir, dass sämtliche Behörden und Unternehmen, welchen unklar ist, ob sie unter die Meldepflicht fallen, beim BACS Auskunft darüber verlangen können.

Es ist zu begrüssen, dass der Bund in Abstimmung mit den Kantonen eine Nationale Cyberstrategie (NCS) definiert und einen Steuerungsausschuss (StA NCS) für deren Umsetzung einsetzt. Ebenso ist es richtig, dass in dieser Strategie die Anstrengungen auf nationaler Ebene in enger Abstimmung mit den Kantonen festgelegt werden.

Wir vermissen im Verordnungsentwurf aber die Koordination der Strafverfolgungen bei Cybervorfällen, die dem BACS jedoch noch nicht den Strafverfolgungsbehörden gemeldet wurden. Dabei stützen wir uns auf die jüngsten Erfahrungen bei einem Fall von Ransomware, bei dem Daten gestohlen und im Darknet veröffentlicht wurden. Die Zuständigkeit für die Analyse der gestohlenen Daten und die Strafverfolgung war zwischen dem Bundesamt für Polizei (Fedpol), dem interkantonalen Netzwerk digitale Ermittlungsunterstützung Internetkriminalität (NEDIK) und dem BACS nicht koordiniert. Dies führte zu einer

Verzögerung der Cyber-Gefahrenabwehr, weil sich dadurch die Analyse der abgeflossenen Daten verzögerte.

Ebenfalls ist bei kritischen Infrastrukturen, die im kantonalen Kontext als solche eingestuft sind, in der Verordnung der Rückfluss der Informationen zu den kantonalen Behörden zu ergänzen. Ansonsten müsste mit einem erheblichen Mehraufwand kantonal ein Parallelprozess etabliert werden, obwohl die Informationen bereits bei den Bundesbehörden vorhanden sind.

Im Übrigen sollte im vorliegenden Verordnungsentwurf der Begriff des «grossen Schadenspotenzials», der im Zusammenhang mit der Bekämpfung der Cyberkriminalität als Element der Nationalen Cyberstrategie erwähnt wird, klarer definiert werden. Ein grosses Schadenspotenzial besteht unserer Meinung nach, wenn beispielsweise

- kritische Infrastrukturen in den Bereichen Versorgung, Sicherheit, Gesundheit, Wirtschaft (Finanzen), Logistik oder Produktion betroffen sind, und
- Reputationsschäden, rechtliche und regulatorische Konsequenzen, Datenverlust oder Datendiebstahl drohen.

Aus den Unterlagen ist nicht ersichtlich, welche finanziellen Auswirkungen die Einführung der Meldepflicht für die Kantone hat. Wir gehen davon aus, dass insbesondere Zusatzkosten für den Aufbau eines sogenannten Security Operations Center (SOC), für personelle Ressourcen und für Systeme zu erwarten sind. Den Kantonen sind die finanziellen Auswirkungen der Meldepflicht nachvollziehbar aufzuzeigen.

2. Bemerkungen zu den einzelnen Bestimmungen

Zu Artikel 18

Wir empfehlen die Einführung der folgenden Meldungskategorien, die je nach Auswirkungen des Ereignisses definiert werden. Dadurch soll sichergestellt werden, dass dem BACS nur Vorfälle gemeldet werden, die für andere Organisationen relevant oder nützlich sind:

- Minor-Vorfall: keine Meldung oder Meldung optional,
- Medium-Vorfall: zwingende Meldung innerhalb einer Woche,
- Major-Vorfall: zwingende Meldung innerhalb von 24 Stunden (gem. Art. 74e des geänderten Informationssicherheitsgesetzes). Anmerkung: Gemäss EU-Standard in der Datenschutz-Grundverordnung sind es 72 Stunden.

Zu Artikel 21

Es ist zu präzisieren, ob bei der erwähnten 14-tägigen Frist zur Ergänzung der Meldung Arbeitstage oder Wochentage gemeint sind.

Freundliche Grüsse

Ylfete Fanaj
Regierungsrätin

Kanton Obwalden

Der Vorsteher des Sicherheits- und Sozialdepartements SSD

CH-6060 Sarnen, Enetriederstrasse 1, SSD

Eidgenössisches Departement für
Verteidigung, Bevölkerungsschutz und Sport
VBS

per Mail an:
ncsc@ncsc.admin.ch

Referenz/Aktenzeichen: OWSTK.5024
Unser Zeichen: ks

Sarnen, 29. August 2024

**Cybersicherheitsverordnung (CSV);
Stellungnahme.**

Sehr geehrte Frau Bundesrätin

Für die Einladung zur Stellungnahme zur Cybersicherheitsverordnung (CSV) danken wir Ihnen.

Der Kanton Obwalden stimmt der neuen Verordnung zu und hat keine weiteren Anmerkungen oder Hinweise.

Freundliche Grüsse

Christoph Amstad
Regierungsrat

Kopie an:
- Kantonale Mitglieder der Bundesversammlung
- Kantonspolizei
- InformatikLeistungsZentrum OW/NW

Sicherheits- und Sozialdepartement SSD
Enetriederstrasse 1, 6060 Sarnen
Tel. +41 41 666 62 19
ssd@ow.ch
www.ow.ch

ASA | SVV

Schweizerischer Versicherungsverband
Association Suisse d'Assurances
Associazione Svizzera d'Assicurazioni
Swiss Insurance Association

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Manuel Suter, Stv. Direktor Bundesamt für
Cybersicherheit
Versand per E-Mail: ncsc@ncsc.admin.ch

Zürich, 30. August 2024

Vernehmlassungsverfahren zur Cybersicherheitsverordnung (CSV)

Sehr geehrter Herr Suter

Wir danken Ihnen für die Vernehmlassung zur Cybersicherheitsverordnung (CSV)**.** Gerne unterbreitet Ihnen der Schweizerische Versicherungsverband SVV nachstehend seine Anmerkungen und Anpassungsvorschläge zum Entwurf der Cybersicherheitsverordnung (E-CSV).

1 Einleitende Anmerkungen

Weitere Verbesserung der Koordination/Harmonisierung der verschiedenen Meldeverfahren notwendig
Die Versicherungsunternehmen als Betreiberinnen kritischer Infrastrukturen sind vom Vernehmlassungsverfahren zur CSV direkt betroffen. Die neue Meldepflicht des ISG, die mit der CSV ausgeführt wird, ergänzt die bereits bestehenden Meldepflichten der Versicherungsunternehmen gegenüber der FINMA und dem EDÖB (siehe FINMA-Aufsichtsmitteilung 05/2020 Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG und Art. 24 DSG).

Die neue ISG-Meldepflicht belastet Versicherungsunternehmen zusätzlich im Falle eines Cyberangriffes im kritischsten Moment und blockiert in den betroffenen Unternehmen Ressourcen, die besser zur Bewältigung des Cybervorfalls investiert werden. Die bestmögliche Koordination/Harmonisierung der verschiedenen Meldeverfahren bei Cyberangriffen ist deshalb ein zentrales Anliegen des SVV. Aus unserer Sicht ist der Bund bzw. die involvierten Bundesstellen (BACS, FINMA, EDÖB) hier in der Pflicht, eine optimale Koordination/Harmonisierung dieser Meldepflichten sicherzustellen.

Der SVV hat bei der Revision des ISG für einen One-Stop-Shop-Ansatz für alle Meldepflichten plädiert, um so den Meldeaufwand für die Unternehmen in der ausserordentlich schwierigen Situation eines Cyberangriffs in Grenzen zu halten und die Unternehmen nicht mit drei verschiedenen Meldeverfahren zu belasten.

Schweizerischer Versicherungsverband SVV
Conrad-Ferdinand-Meyer-Strasse 14 – CH-8002 Zürich – Zentrale +41 44 208 28 28 – svv.ch
Franziska Streich – franziska.streich@svv.ch – Direktwahl +41 44 208 28 63

Wir begrüssen daher, dass über das Meldeformular des BACS gleichzeitig die Erstmeldung/24 Stunden Meldung an die FINMA erfolgen kann (siehe Aufsichtsmitteilung FINMA 03/2024, Seite 8, wonach im Meldeformular des BACS die Option angewählt werden kann, die Meldung an die FINMA weiterzuleiten). Es besteht damit immerhin eine gewisse Koordination zwischen den Meldepflichten an das BACS und die FINMA. In diesem Zusammenhang begrüssen wir auch den neuen Absatz 5bis von Art. 24 DSG (im Rahmen der ISG-Revision eingeführt), welcher mit Einverständnis des meldenden Unternehmens die Weiterleitung der DSG-Meldung durch den EDÖB an das BACS zur Analyse des Vorfalls zulässt.

Eine weitere Verbesserung der Koordination/Harmonisierung der verschiedenen Meldeverfahren würde sehr begrüsst (soweit dies auf Stufe CSV möglich ist).

Zum Teil fehlende Grundlage im ISG
Bei der CSV handelt es sich um eine Ausführungsverordnung zur Konkretisierung des ISG. Die Art. 2 – 5 E-CSV zur nationalen Cyberstrategie des Bundesrates und zum Steuerungsausschuss Nationale Cyberstrategie knüpfen gemäss Erläuterungen zur CSV (Seite 6) an die Regelung in der aufgehobenen Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung an (Cyberrisikenverordnung, CyRV, Art. 5 und 9 CyRV).

Im ISG, dass der CSV zu Grunde liegt, finden sich weder für die nationale Cyberstrategie noch für den Steuerungsausschuss Bestimmungen oder eine Delegationsklauseln an den Bundesrat. Es scheint daher fraglich, ob diese beiden Punkte auf Verordnungsstufe (CSV) verankert werden können (siehe auch Art. 164 Abs. 1 Bundesverfassung, wonach «Wichtiges» wie die Organisation der Bundesbehörden ins Gesetz gehört).

Bundesamt für Cybersicherheit
Das Bundesamt für Cybersicherheit (BACS) hat seit dem 1. Januar 2024 das Nationale Zentrum für Cybersicherheit (NCSC) abgelöst. Diese Änderung hat im Schlussabstimmungstext der ISG-Revision vom 29. September 2023 noch keinen Eingang gefunden. Um Missverständnisse für die meldepflichtigen Unternehmen zu vermeiden, sollte diese Änderung im ISG baldmöglichst nachgeholt werden.

2 Anpassungsvorschläge und Anmerkungen zu einzelnen Bestimmungen des E-CSV

Art. 4 E-CSV Zusammensetzung Steuerungsausschuss Nationale Cyberstrategie
Das VBS hat gemäss Medienmitteilung des BACS vom 7. Juni 2024 den Steuerungsausschuss Nationale Cyberstrategie bereits eingesetzt. Die Wirtschaft ist hier gemäss Medienmitteilung durch die Akteure asut, futurae technologies und WiseStratEdge vertreten.

Zusätzlich zur Wirtschaft und den anderen Vertretern wäre es aus Sicht des SVV angebracht, dass auch explizit die Betreiberinnen kritischer Infrastrukturen als vom ISG betroffene Gesetzesadressaten gezielt in diesem

Steuerungsausschuss vertreten sind, wie z.B. die im Swiss Financial Sector Cyber Security Centre (Swiss FS-CSC) organsierte Versicherungs-/Finanzindustrie.

Art. 11 ff. E-CSV Informationsaustausch
Wichtig scheint uns, dass über die Meldungen an das BACS von diesem regelmässig eine detaillierte (anonymisierte) Berichterstattung erfolgt. Für die Versicherungsbranche ist es wichtig, dass Transparenz zu den Meldeverfahren herrscht. So kann sie einen Beitrag zu einer Erhöhung der Cyber-Resilienz der Schweizer Wirtschaft leisten und gleichzeitig die Versicherungsdurchdringung erhöhen.

Art. 18 E-CSV Zu meldende Cyberangriffe

Antrag (siehe rot markierter Änderungsvorschlag):
Art. 18 E-CSV
[1] Die Funktionsfähigkeit einer kritischen Infrastruktur gilt als gefährdet, wenn:
a. Mitarbeitende oder Dritte von absichtlich ausgelösten Systemunterbrüchen betroffen sind; oder (…).
[2] Eine Manipulation oder ein Abfluss von Informationen liegt vor, wenn:
a. geschäftsrelevante Informationen von Unbefugten verändert, ~~oder~~ offengelegt ~~werden~~, entwendet, zerstört, deaktiviert oder sonst wie bearbeitet werden, welche sich mittel- oder langfristig auf wesentliche Applikationen oder Systeme auswirken; oder
b. eine Verletzung der Datensicherheit nach Artikel 24 des Datenschutzgesetzes vom 25. September 2020 vorliegt, welche voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt.

Begründung:
Art. 18 Abs. 1 E-CSV:
Der Bundesrat konkretisiert in dieser Bestimmung Art. 74d ISG. Dabei muss bedacht werden, dass nur Cyberangriffe meldepflichtig sind. Cyberangriffe sind gemäss Legaldefinition von Art. 5 Bst. e ISG absichtlich ausgelöste Cybervorfälle.

Die vorgeschlagene Präzisierung ist aus unserer Sicht notwendig, um im Einklang mit dieser Legaldefinition klarzustellen, dass nur absichtlich ausgelöste Systemunterbrüche zu melden sind. Andere Vorfälle (z.B. unabsichtliche Fehlmanipulation von Mitarbeitenden) unterstehen keiner Meldepflicht. Ein Cyberangriff gilt als solcher, wenn er mit Absicht ausgelöst wird – unabhängig davon, ob es sich dabei um einen internen oder externen Cybervorfall handelt.

Art. 18 Abs. 2 E-CSV:
Geschäftsrelevante Informationen können von Unbefugten nicht nur verändert oder offengelegt werden, so dass die Tatbestände entsprechend erweitert werden sollten (wie vorgeschlagen). Jeglicher Abfluss von geschäftsrelevanten Informationen kann jedoch nicht zu einem meldenden Cyberangriff führen. Ein zu

meldender Cyberangriff aufgrund einer Manipulation oder eines Abflusses von Informationen kann erst dann vorliegen, wenn dies mittel- oder langfristig Auswirkungen auf wesentliche Applikationen oder Systeme hat und die Schutzziele (Verfügbarkeit, Integrität und Vertraulichkeit) beeinträchtigt wurden (siehe auch Erläuterungen zur CSV vom 22. Mai 2024, Seite 30, betreffend Schutzziele).

Eine Verletzung der Datensicherheit ist gemäss Art. 24 Abs. 1 DSG nur dann zu melden, wenn sie voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt. Da sich Art. 18 Abs. 2 Bst. b. E-CSV explizit auf das Datenschutzgesetz bezieht, sollte die Eintrittsschwelle einer ISG-Meldung mit der DSG-Meldung harmonisiert werden und gleich lauten.

Art. 23 E-CSV
Gemäss Art. 23 E-CSV/Erläuterungen (Seite 33) tritt die Verordnung gleichzeitig mit dem revidierten ISG am 1. Januar 2025 in Kraft.

Ein Inkrafttreten per 1. Januar 2025 ist zu früh. Das revidierte ISG mit dazugehöriger neuer Verordnung (CSV) verlangt bei den Betreiberinnen kritischer Infrastrukturen Anpassungen bei den unternehmensinternen Prozessen/IT-Änderungen. Zudem sind angemessene Testzeiträume einzuplanen, um sicherzustellen, dass die Prozesse/IT-Änderungen mit Inkraftsetzung des neuen Rechts zuverlässig live gehen können. Dies verlangt nach einer angemessenen Umsetzungsfrist. Für die Umsetzung des neuen Rechts muss zudem die Veröffentlichung der Endfassung der Verordnung (CSV) abgewartet werden. Dies ist bei der Festlegung des Inkraftsetzungstermins zu berücksichtigen. Für die Umsetzungsarbeiten in den Unternehmen erachten wir einen Zeitraum von mindestens einem Jahr, laufend ab Feststehen/Veröffentlichung der definitiven Fassung der CSV, als notwendig.

Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme bei der weiteren Behandlung der Vorlage. Gerne stehen wir Ihnen für Rückfragen zur Verfügung.

Freundliche Grüsse
Schweizerischer Versicherungsverband SVV

Sandra Kurmann
Leiterin Ressort Rahmenbedingungen

Franziska Streich
Fachverantwortliche Recht

KKJPD
CCDJP
CDDGP

Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren
Conférence des directrices et directeurs des départements cantonaux de justice et police
Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia

Per Mail an:
ncsc@ncsc.admin.ch

Bern, 27.08.2024
05.07 jäg

Cybersicherheitsverordnung

Sehr geehrte Damen und Herren

Die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) wurde eingeladen, zur oben erwähnten Vernehmlassung Stellung zu nehmen. Wir danken Ihnen dafür bestens.

Der Vorstand KKJPD hat in seiner Sitzung vom 28. Juni 2024 beschlossen, auf eine Stellungnahme im Namen der KKJPD zu verzichten und es den einzelnen Kantonen zu überlassen, sich zur Vorlage zu äussern.

Besten Dank für die Kenntnisnahme.

Mit freundlichen Grüssen

Sig. F. Düblin

Florian Düblin
Generalsekretär

Generalsekretariat KKJPD | Haus der Kantone. Speichergasse 6, Postfach, 3001 Bern | Tel. +41 31 318 15 05 | info@kkjpd.ch | www.kkjpd.ch

ETAT DE FRIBOURG
STAAT FREIBURG

Conseil d'Etat CE
Staatsrat SR

Route des Arsenaux 41, 1700 Fribourg

T +41 26 305 10 40
www.fr.ch/ce

Conseil d'Etat
Route des Arsenaux 41, 1700 Fribourg

PAR COURRIEL

Département fédéral de la défense, de la protection
de la population et des sports DDPS
3003 Bern

Courriel : ncsc@ncsc.admin.ch

Fribourg, le 2 septembre 2024

2024-777
Ordonnance sur la cybersécurité (OCyS) – Procédure de consultation

Madame la Présidente de la Confédération,

Par courrier du 22 mai dernier, vous nous avez consultés sur le projet cité en titre, et nous vous en remercions.

De manière générale, nous approuvons le projet d'ordonnance.

Nous nous permettons néanmoins de formuler les remarques suivantes :

> Ad art. 4 : Nous estimons que le CP CSN devrait obligatoirement comprendre un représentant du secteur énergétique, qui constitue une infrastructure critique majeure, et que l'ordonnance devrait le spécifier. A tout le moins, le rapport devrait le mentionner dans son commentaire de l'article 4.

> Ad art. 14 : Il conviendrait selon nous de parler de « fournisseurs de prestations de cybersécurité », comme dans le rapport, afin d'éviter toute confusion.

Nous vous prions de croire, Madame la Présidente de la Confédération, à l'assurance de nos sentiments les meilleurs.

Au nom du Conseil d'Etat :

Jean-Pierre Siggen, Président

Danielle Gagnaux-Morel, Chancelière d'Etat

Copie
—
à la Direction de la sécurité, de la justice et du sport, pour elle et la Police cantonale ;
à la Chancellerie d'Etat.

eAHV/IV – eAVS/AI
p.a. mundi consulting ag
Marktgasse 55
Postfach
3001 Bern
Mail info@eahv-iv.ch
Web www.eahv-iv.ch
Tf. +41 31 326 76 76

Geht an
Eidgenössisches Departement für
Verteidigung, Bevölkerungsschutz
und Sport VBS
Frau Bundespräsidentin
Viola Amherd

Via Mail an
ncsc@ncsc.admin.ch

Bern, 3. September 2024

Antwort zur Vernehmlassung: Cybersicherheitsverordnung (CSV)

Sehr geehrte Frau Bundespräsidentin Amherd
Sehr geehrte Damen und Herren

Wir danken Ihnen bestens für die Gelegenheit, uns zum erwähnten Verordnungsentwurf zu äussern. eAHV/IV koordiniert den Datenaustausch und Digitalisierung in der 1. Säule der Sozialversicherungen und Familienzulagen. Der Verein ist eine Fachorganisationen der Durchführungsstellen gemäss AHVG Art. 49a Abs. 3 und Art. 71 Abs. 4bis. Der sichere und zuverlässige Betrieb der Infrastrukturen bei den verschiedenen beteiligten Partnern ist ein zentrales gemeinsames Anliegen. Unsere Vereinsmitglieder sind die Konferenz der kantonalen Ausgleichskassen (KKAK), die Vereinigung der Verbandsausgleichskassen (VVAK), die IV-Stellen-Konferenz (IVSK) sowie die Zentrale Ausgleichsstelle (ZAS). Die drei Vereinigungen der Durchführungsstellen unterstützen die vorliegende Vernehmlassungsantwort.

Die vertretenen rund 110 Durchführungsstellen, deren IT-Dienstleister und der Verein selbst müssen die Meldepflicht umsetzen.

1. Im Grundsatz

Wir teilen die Einschätzung der grossen Wichtigkeit, die der Cybersicherheit zukommt. Wir sind überzeugt, dass Koordinations- und Unterstützungsmassnahmen des Bundesamts für Cybersicherheit (BACS) eine wichtige Ergänzung unserer eigenen Aktivitäten darstellen.

2. Aufwand für die initiale Meldung begrenzen

Die gesetzlichen Vorgaben bauen darauf auf, dass eine schnelle erste Meldung an das BACS gemacht werden muss. Gleichzeitig bestehen für Cybersecurityvorfälle in der ersten Säule bereits eine Meldepflicht gegenüber dem BSV (gemäss AHVV Art. 141septies) und dem EDÖB. Weiter haben kantonale Ausgleichskassen Meldepflichten gegenüber kantonalen Stellen. Aus unserer Sicht muss die Priorität bei einem Cybersicherheitsvorfall auf der Schadensbegrenzung und die Wiederherstellung der Systeme liegen können und deshalb der Aufwand für Meldungen an verschiedene Stellen begrenzt werden.

Die Verbände haben sich mit Hinweis auf die Bestimmungen des Informationssicherheitsgesetz gegen die zusätzliche Meldepflicht an das BSV ausgesprochen. Wir sehen im Rahmen der Umsetzung der Meldepflicht (Art. 11 ff CSV) die Möglichkeit, dass das BACS eine Drehscheibenfunktion übernimmt im Sinne des

once-only-Prinzips und die Meldung des Vorfalles an weitere Stellen in der Bundesverwaltung und an kantonale Stellen übermittelt. Nach Art. 15 CSV wäre dann spezifisch zu bestimmen, dass das BACS die Meldung zum Vorfall mit der Einwilligung der Organisation an weitere definierte Behörden in Bund und Kantonen weiterleitet.

3. Rolle des BACS bei einem Vorfall klarer definieren

Die Rolle des BASC bei einem Sicherheitsvorfall müsste unserer Meinung nach klarer gefasst werden. In dieser Situation muss der Fokus auf Unterstützung der betroffenen Organisation bei der Bewältigung liegen. So sollte in Art. 21 CSV zur Geltung kommen, dass die Sammlung von weiteren Informationen, die ggf. nicht unmittelbar erhoben werden können, im Austausch und mit der Unterstützung des BACS erfolgt. Dabei kommt auch Art. 8 der vorgeschlagenen Verordnung in Bezug auf Priorisierung zur Geltung.
Im erläuternden Bericht zu Art. 7 Abs. 1 müsste verständlicher beschrieben werden, wie, wann und zu welchen Bedingungen einer Soforthilfe vom BACS im Falle eines Notfalles erfolgt.

Abschliessend möchten wir nochmals betonen, dass eine zweckmässige Ausgestaltung der Meldepflicht im Sinne der Akteure der 1. Säule ist und die verbesserte Information und Koordination durch das BACS einen Beitrag zum zuverlässigen Funktionieren der 1. Säule leisten kann.

Wir danken Ihnen für die Kenntnisnahme unserer Anregungen und bitten um deren Berücksichtigung.

Freundliche Grüsse

Christian Zeuggin
Präsident eAHV/IV

Natalia Weideli
Präsidentin der Konferenz der Kantonalen Ausgleichskassen

Barbara Ghirardin
Präsidentin der Schweizerischen Vereinigung der Verbandsausgleichskassen

Martin Schilt
Präsident der IV-Stellen-Konferenz

Regierungsrat des Kantons Schwyz

6431 Schwyz, Postfach 1260

per E-Mail
Eidgenössisches Departement für
Verteidigung, Bevölkerungsschutz und
Sport VBS
3003 Bern
ncsc@ncsc.admin.ch

Schwyz, 27. August 2024

Verordnung über die Cybersicherheit (Cybersicherheitsverordnung, CSV)
Vernehmlassung des Kantons Schwyz

Sehr geehrte Frau Bundesrätin

Mit Schreiben vom 22. Mai 2024 hat das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport VBS den Kantonsregierungen die Unterlagen zum Erlass der Verordnung über die Cybersicherheit zur Vernehmlassung bis 13. September 2024 unterbreitet.

Mit der Änderung des Bundesgesetzes über die Informationssicherheit vom 18.Dezember 2020 (Informationssicherheitsgesetz, ISG, SR 128) hat das Eidgenössische Parlament am 29. September 2023 die Einführung einer Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen beschlossen. Mit der Verordnung über die Cybersicherheit legt der Bundesrat die Ausführungsbestimmungen zu dieser Gesetzesänderung vor.

Der Kanton Schwyz stimmt der Verordnung grundsätzlich zu. Kritsch ist der Kanton Schwyz bezüglich der Ausnahme von der Meldepflicht gemäss Art. 16 Abs. 1 Bst. a E-CSV. Gemäss Art. 74b Abs. 1 Bst. b und c ISG gilt die grundsätzliche Meldepflicht für Bundes-, Kantons- und Gemeindebehörden sowie interkantonale, kantonale und interkommunale Organisationen (Bst. b) und für Organisationen mit öffentlich-rechtlichen Aufgaben in den Bereichen Sicherheit und Rettung, Trinkwasserversorgung, Abwasseraufbereitung und Abfallentsorgung (Bst. c). Dass die E-CSV hier eine Ausnahme von der Meldepflicht vorsieht, sofern weniger als 1000 Einwohnerinnen und Einwohner betroffen sind, ist nicht nachvollziehbar. Durch den hohen Vernetzungsgrad zwischen Behörden auf den verschiedenen föderalen Stufen ist ein Verzicht auf diese Ausnahmeregelung zu prüfen. Kleinere Gemeinden sind durchaus auch mit dem Kantonsnetz verbunden. Ein Cyberangriff auf eine der entsprechenden Stellen könnte somit auch negative Auswirkungen auf die kantonale Infrastruktur haben. Eine Meldepflicht wäre somit auch hier angezeigt. Selbstverständlich muss sichergestellt werden, dass im Falle einer Meldung einer kommunalen Behörde an das Nationale Zentrum für Cybersicherheit (NCSC) gewährleitet ist, dass die Informationen auch zu den zuständigen kantonalen Stellen gelangen.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und versichern Sie, Frau Bundesrätin, unserer vorzüglichen Hochachtung.

Im Namen des Regierungsrates:

Regierungsrat Kanton Schwyz

Michael Stähli
Landammann

Dr. Mathias E. Brun
Staatsschreiber

Regierung des Kantons St.Gallen

Regierung des Kantons St.Gallen, Regierungsgebäude, 9001 St.Gallen

Eidgenössisches Departement für
Verteidigung, Bevölkerungsschutz und
Sport
Bundeshaus Ost
3003 Bern

Regierung des Kantons St.Gallen
Regierungsgebäude
9001 St.Gallen
T +41 58 229 89 42
info.sk@sg.ch

St.Gallen, 2. September 2024

Cybersicherheitsverordnung; Vernehmlassungsantwort

Sehr geehrte Frau Bundesrätin

Mit Schreiben vom 22. Mai 2024 laden Sie uns zur Vernehmlassung zur Cybersicherheitsverordnung ein.

Wir danken für diese Gelegenheit und können Ihnen mitteilen, dass wir mit dem vorgeschlagenen Verordnungsentwurf einverstanden sind.

Im Namen der Regierung

Susanne Hartmann
Präsidentin

Dr. Benedikt van Spyk
Staatssekretär

Zustellung auch per E-Mail (pdf- und Word-Version) an:
ncsc@ncsc.admin.ch

Département fédéral de la défense, de la protection de la population et des sports
Madame Viola Amherd
Présidente de la Confédération
Palais fédéral est
Bundesgasse 3
3003 Berne

Concerne : Consultation relative à l'ordonnance sur la cybersécurité (OCyS)

Madame la Présidente de la Confédération,

Votre courrier du 22 mai 2024 relatif à l'objet cité en titre nous est bien parvenu et a retenu toute notre attention. Nous vous remercions de nous avoir consultés.

Nous saluons et accueillons favorablement ce projet d'ordonnance, qui va permettre de clarifier un certain nombre de dispositions de la loi fédérale sur la sécurité de l'information (LSI), en complément des ordonnances déjà en vigueur.

Vous trouverez toutefois, en annexe, quelques suggestions visant à clarifier ou préciser certains articles de l'ordonnance afin de favoriser sa mise en œuvre.

Nous vous remercions par avance pour la prise en compte de ces suggestions et vous prions de croire, Madame la Présidente de la Confédération, à l'assurance de notre haute considération.

AU NOM DU CONSEIL D'ÉTAT

La chancelière : Michèle Righetti-El Zayadi

La présidente : Nathalie Fontanet

Annexe : mentionnée

Copie à (*format Word et pdf*) : ncsc@ncsc.admin.ch

ANNEXE
Observations particulières

Cette annexe présente des observations ou propositions d'ajouts article par article.

Art. 4, al. 1 et 3

Il est proposé de compléter "société" par "civile", pour mieux refléter en français l'intention de représenter les intérêts des citoyennes et des citoyens.

Art 5, let. a

Il est suggéré de remplacer "contrôle" par "audite", dénotant ainsi une revue plus détaillée et précise.

Art 6

La reformulation suivante est proposée: "L'OFCS peut, afin d'avertir les autorités, les organisations ou les personnes visées par une cybermenace, imminente ou en cours, requérir les coordonnées des titulaires de noms de domaine auprès du registre des noms de domaine relevant de la compétence de la Confédération.

Art. 7, al. 1

De plus, le "qui" pouvant se référer à l'équipe, au CERT ou à l'OFCS, il est suggéré de le remplacer par "laquelle".

Art. 8, al. 1

Il serait utile d'inclure les critères pour la gestion des priorités, par exemple une référence de standards communs.

Il serait pertinent d'ajouter un alinéa 3, « Il communique alors aux parties concernées les priorités définies », sinon elles restent dans l'expectative.

Art. 13

Plutôt que le terme « enregistrement », il faudrait privilégier « enrôlement » et « s'enrôler ». L'enregistrement a plusieurs sens en français et peut être ambigu.

Art. 13, al. 2, let. c [nouveau]

En application de l'art. 86 al. 3 LSI, il est suggéré d'ajouter une lettre supplémentaire, précisant « les coordonnées de l'unité chargée de la cybersécurité au sein de l'organisation ou de l'autorité ».

Par analogie, on peut estimer que toutes les autres infrastructures critiques sont soumises à la même contrainte.

Art. 14, al. 1

Compte tenu des données sensibles échangées, il semble opportun de préciser qu'une analyse des fournisseurs sera effectuée par l'OFCS.

Art. 16, al. 1, let. b

Il n'est pas clair si les deux conditions sont cumulatives ou alternatives.

Art. 18, al. 1, let. a

Il serait judicieux de préciser ce qui est entendu par « part importante » dans le rapport explicatif en ajoutant des informations quantitatives, que ce soit un pourcentage de personnes touchées, une durée minimale d'interruption des systèmes ou d'une violation des dispositions contractuelles en matière de disponibilité.

Art. 18, al. 4

Remplacer "d'actes" par "des actes"

Art. 19, al. 1, let. e

En adéquation avec le rapport explicatif, ajouter "lorsqu'elles sont disponibles" en fin de paragraphe.

Art. 19, al. 2

Il est proposé une nouvelle formulation pour faciliter la compréhension de l'alinéa: "…des informations sur l'éventualité ou la réalité d'un chantage, ainsi que d'une dénonciation pénale".

Art. 19, al. 3

Pour faire suite à l'article 18, il faudrait aussi préciser dans le rapport explicatif les informations relatives à la proportion de personnes touchées.

Art. 19, al. 4, let. c [nouveau]

En application de l'art. 86 al. 3 LSI, il est suggéré d'ajouter une lettre supplémentaire, précisant « les coordonnées de l'unité chargée de la cybersécurité au sein de l'organisation ou de l'autorité ».

Kanton Zürich Regierungsrat
staatskanzlei@sk.zh.ch
Tel. +41 43 259 20 02
Neumühlequai 10
8090 Zürich
zh.ch

Elektronisch an ncsc@ncsc.admin.ch

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport
3003 Bern

4. September 2024 (RRB Nr. 908/2024)
Verordnung über die Cybersicherheit (Vernehmlassung)

Sehr geehrte Frau Bundespräsidentin

Mit Schreiben vom 22. Mai 2024 haben Sie uns eingeladen, zum Entwurf zur Verordnung über die Cybersicherheit (Cybersicherheitsverordnung) Stellung zu nehmen. Wir danken Ihnen für diese Gelegenheit und äussern uns wie folgt:

Wir unterstützen die vorgeschlagene Verordnung. Sie sollte mit einem angemessenen Mehrwert für die beteiligten Akteurinnen und Akteure verbunden sein. Mit den nachstehenden Bemerkungen möchten wir die Entwicklung in diesem Sinne unterstützen.

I. Allgemeine Bemerkungen

Mit RRB Nr. 541/2022 haben wir bereits zur Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen Stellung genommen. Wir unterstützen den Entwurf zur Cybersicherheitsverordnung und deren Beitrag zu einer nationalen Betrachtungsweise der Cybersicherheit. Durch die Cybersicherheitsverordnung wird eine Stärkung der kantonalen Cyberresilienz angestrebt, namentlich durch die Definition einer Nationalen Cyberstrategie in Abstimmung mit den Kantonen (Art. 2 und 4) und die Unterstützung der kantonalen Behörden durch das Bundesamt für Cybersicherheit (BACS; Art. 7 und 10).
In Bezug auf die Meldepflicht der kantonalen Behörden regen wir an, den Begriff der kritischen Infrastrukturen von Behörden (Art. 5 Bst. c Informationssicherheitsgesetz [ISG; SR 128] in Verbindung mit Art. 74b Abs. 1 Bst. b ISG) in der Cybersicherheitsverordnung zu konkretisieren. Eine Qualifikation sämtlicher Organisationseinheiten als «Betreiber kritischer Infrastrukturen» erscheint nicht als zielführend, da die Kritikalität der jeweiligen Dienste damit ausser Acht gelassen wird.
Durch die neue Meldepflicht erhält eine Bundesbehörde Kenntnis von strafbaren Handlungen, weshalb wir die Institutionalisierung der Zusammenarbeit des BACS mit den kantonalen Strafverfolgungsbehörden in der Cybersicherheitsverordnung empfehlen. Das BACS

hat keine strafrechtlichen Kompetenzen oder Aufgaben, da es sich nur indirekt mit Cyberkriminalität befasst. Zur wirksamen Bekämpfung von Cyberkriminalität ist indessen die zeitnahe Einbindung der Strafverfolgungsbehörden erfolgskritisch, namentlich in Bezug auf die Beweissicherung. Angesichts der zeitlichen Dringlichkeit bei der Strafverfolgung von Cyberkriminalität ist es zweckdienlich, bei einer Meldung an das BACS gleichzeitig Strafanzeige bei der zuständigen Strafverfolgungsbehörde einzureichen.
Daher empfehlen wir, mit einer Anzeigepflicht des BACS sicherzustellen, dass Meldungen an die zuständigen Strafverfolgungsbehörden weitergeleitet werden (vgl. auch Bemerkungen zu Art. 7 und 15).

Sodann würden wir eine stärkere Berücksichtigung der Lieferkette in der Cybersicherheitsverordnung begrüssen, zumal sich diese als primäres Angriffstor für Cyberangriffe erweist. Namentlich regen wir an, den betroffenen Dienstleister als Meldeinhalt aufzunehmen (vgl. Bemerkung zu Art. 19). Zudem schlagen wir differenziertere Regelungen für Angriffe auf die Lieferkette vor:

– Bei Cyberangriffen auf Betreiberinnen von Informatikinfrastrukturen mit Auswirkungen auf eine grosse Zahl verschiedener meldepflichtiger Organisationen und Behörden (insbesondere Hyperscaler und Betreiberinnen von Rechenzentren) schlagen wir vor, dass anstelle der gleichzeitigen Meldung durch alle Meldepflichtigen in einem ersten Schritt nur die Betreiberin der Informatikinfrastruktur eine Meldung gegenüber dem BACS absetzt. Damit könnte das BACS seine Ressourcen zielgerichtet für die Behandlung des Cyberangriffs einsetzen, ohne dass diese zusätzlich oder gar vorrangig durch die Administration einer Vielzahl von Meldungen gebunden sind. Die weiteren betroffenen meldepflichtigen Organisationen sollten ihre eigenen Meldungen zeitverzögert absetzen können.
– Es wäre klarzustellen, dass die Frist von 24 Stunden für meldepflichtige Organisationen und Behörden erst mit der eigenen Kenntnisnahme des Cyberangriffs zu laufen beginnt. In diesem Zusammenhang wäre die Verankerung einer Mitteilungspflicht von Dienstleistern an meldepflichtige Organisationen und Behörden in der Cybersicherheitsverordnung begrüssenswert.

II. Bemerkungen zu einzelnen Bestimmungen

1. Cybersicherheitsverordnung

Art. 2 Nationale Cyberstrategie

Die koordinierte Definition einer Nationalen Cyberstrategie ist zu begrüssen, da sie den Kantonen eine frühzeitige Anpassung und Ergänzung eigener Cybersicherheitsstrategien erlaubt.
Namentlich beim Aspekt der «Bekämpfung der Cyberkriminalität» muss indessen der Beizug von Staatsanwaltschaft und Polizei als fachkompetente Behörden sichergestellt werden, und zwar unabhängig von deren Vertretung im Rahmen des Steuerungsausschusses Nationale Cyberstrategie. Es ist festzuhalten, dass die Strategie und die Befugnisse zur strafrechtlichen Verfolgung von Cybervorfällen bei den Strafverfolgungsbehörden verbleiben und dass deren Weisungsfreiheit durch Festlegungen in der Nationalen Cyberstrategie nicht berührt werden.

Art. 7 Technische Analyse von Cybervorfällen und Cyberbedrohungen

Zulässige Gegenmassnahmen

Mit Bezug auf die Zulässigkeit von Gegenmassnahmen bei einem Cyberangriff bestehen unterschiedliche Auffassungen und ein rechtlich enger Rahmen. Demgegenüber sind technisch viele Gegenmassnahmen möglich. Es ist zu definieren, was das Computer Emergency Response Team (CERT) unter Präventiv- und Gegenmassnahmen versteht. Je nach Verständnis und Umfang sind erweiterte gesetzliche Grundlagen für Massnahmen erforderlich, die in der Regel nur den Strafverfolgungsbehörden gemäss der Schweizerischen Strafprozessordnung (SR 312.0) oder dem Nachrichtendienst gemäss dem Nachrichtendienstgesetz (SR 121) offenstehen.
Wir empfehlen daher, Gegenstand, Wirkungsziele und Umfang der «Gegenmassnahmen» zu definieren und die dafür nötigen Kompetenzen des CERT zu umschreiben.

Zusammenarbeit mit den Strafverfolgungsbehörden

Bei Cyberangriffen besteht für die Strafverfolgungsbehörden üblicherweise Gefahr im Verzug hinsichtlich der Sicherung der nötigen Beweise. Zudem können Sicherungsmassnahmen der Betroffenen oder des CERT die forensische Erhebung von Beweismitteln vereiteln, da die Daten durch die vorgängig vorgenommenen Manipulationen kompromittiert werden. Dies kann einen faktischen oder rechtlichen Beweisverlust zur Folge haben.
Wir regen daher die Formalisierung und Institutionalisierung der Zusammenarbeit mit der Staatsanwaltschaft und der Polizei an. Insbesondere schlagen wir vor, dass das BACS bzw. das CERT diese informieren und in die technische Analyse miteinbeziehen soll.

Art. 15 Übermittlung und Nutzung der Informationen

Gemäss Art. 15 soll das BACS über die Weitergabe der Informationen frei entscheiden können. Diese Regelung steht in einem Spannungsverhältnis zum Informationsbedarf der Strafverfolgungsbehörden. Es ist anzuerkennen, dass ein vertrauensbasierter Informationsaustausch mit den Informationslieferantinnen und -lieferanten schützenswert ist.
Eine effektive Strafverfolgung ist aber ohne rasche Informationen nicht möglich. Im Ergebnis und angesichts der betroffenen Rechtsgüter sind öffentliche Interessen, namentlich Strafverfolgungsinteressen, höher zu gewichten als die Ermessensfreiheit des BACS. Immerhin sind die Informationen bei den Strafverfolgungsbehörden auch durch das Amtsgeheimnis geschützt und werden nur zweckgebunden verwendet.
Daher regen wir an, dass das BACS verpflichtet wird, Meldungen über Cyberangriffe gemäss Art. 18 zur strafrechtlichen Beurteilung an die zuständigen Strafverfolgungsbehörden weiterzuleiten.
Sobald am Informationssystem angeschlossene Strafverfolgungsbehörden von einem Offizialdelikt erfahren, sind sie gesetzlich verpflichtet, die Ermittlungen aufzunehmen. Das BACS hat aus diesem Grund sicherzustellen, dass bei den veröffentlichten Informationen die angegriffene Betreiberin kritischer Infrastruktur nicht ersichtlich bzw. nicht ermittelbar ist.
Allgemein sollte in der Verordnung genauer festgelegt werden, wie das BACS bzw. die Strafverfolgungsbehörden mit den strafrechtlich relevanten Informationen umzugehen haben, die sie über das Informationssystem erhalten (vgl. Art. 76 Abs. 3 Satz 2 ISG).

Art. 18 Zu meldende Cyberangriffe

Art. 18 Abs. 3 geht von einem längeren Zeitraum aus, wenn nach der Entdeckung festgestellt wird, dass der Cyberangriff bereits vor mehr als 90 Tagen erfolgt ist. Dies kann beispielsweise durch die Auswertung von Logdaten geschehen. Die Datenschutzstellen wiederum verlangen eine möglichst kurze Aufbewahrung von Logdaten. Daher wäre eine grundsätzliche Regelung wünschenswert, die sich darüber ausspricht, welche Logdaten wie lange aufbewahrt werden dürfen.

Art. 19 Inhalt der Meldung

Zur Berücksichtigung von Angriffen auf die Lieferkette und zur angemessenen Beurteilung der nationalen Bedrohungslage durch das BACS empfehlen wir, den Inhalt der Meldung um «involvierte Dienstleister oder andere Dritte» zu ergänzen, um Erkenntnisse über den Angriffsweg auf die betroffene Organisation oder Behörde sicherzustellen.
Die Meldung sollte auch die Information enthalten, bei welcher Behörde Strafanzeige erstattet wurde, damit das BACS mit dieser bei einer entsprechenden Datenfreigabe Informationen austauschen kann.
Zudem sollte festgehalten werden, dass die Meldungen auf dem jeweiligen Wissensstand zum Zeitpunkt der Meldung beruhen und auf der Grundlage neuer Erkenntnisse nachgeführt werden können und sollen.

2. Organisationsverordnung für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport

Es wird weder in der vorgeschlagenen Regelung von Art. 15a Abs. 2 Bst. h der Organisationsverordnung für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (SR 172.214.1) noch in den Erläuterungen dazu umschrieben, ob und inwieweit das BACS ausschliesslich zur Vertretung der Schweiz in internationalen Gremien berechtigt sein soll. Die Polizei nimmt im Bereich der Cyberbedrohungen ähnliche Aufgaben wahr, und auch die Staatsanwaltschaften bewältigen Cybervorfälle. Ein nationaler und internationaler Austausch zwischen den Strafverfolgungsbehörden ist längst etabliert. Entsprechend regen wir an, den Umfang, in dem das BACS in den Gremien mitwirkt, genauer zu umschreiben und auf den Bereich Cybersicherheit zu beschränken. Der nationale und internationale Austausch der Strafverfolgungsbehörden zum präventiven Schutz vor Cyberbedrohungen und zur repressiven Bewältigung von Cybervorfällen darf durch diese Bestimmung nicht eingeschränkt werden.

Freundliche Grüsse

Im Namen des Regierungsrates

Die Präsidentin: Die Staatsschreiberin:

Natalie Rickli Dr. Kathrin Arioli

Kanton Zürich Regierungsrat
staatskanzlei@sk.zh.ch
Tel. +41 43 259 20 02
Neumühlequai 10
8090 Zürich
zh.ch

Elektronisch an ncsc@ncsc.admin.ch

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport
3003 Bern

4. September 2024 (RRB Nr. 908/2024)
Verordnung über die Cybersicherheit (Vernehmlassung)

Sehr geehrte Frau Bundespräsidentin

Mit Schreiben vom 22. Mai 2024 haben Sie uns eingeladen, zum Entwurf zur Verordnung über die Cybersicherheit (Cybersicherheitsverordnung) Stellung zu nehmen. Wir danken Ihnen für diese Gelegenheit und äussern uns wie folgt:

Wir unterstützen die vorgeschlagene Verordnung. Sie sollte mit einem angemessenen Mehrwert für die beteiligten Akteurinnen und Akteure verbunden sein. Mit den nachstehenden Bemerkungen möchten wir die Entwicklung in diesem Sinne unterstützen.

I. Allgemeine Bemerkungen

Mit RRB Nr. 541/2022 haben wir bereits zur Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen Stellung genommen. Wir unterstützen den Entwurf zur Cybersicherheitsverordnung und deren Beitrag zu einer nationalen Betrachtungsweise der Cybersicherheit. Durch die Cybersicherheitsverordnung wird eine Stärkung der kantonalen Cyberresilienz angestrebt, namentlich durch die Definition einer Nationalen Cyberstrategie in Abstimmung mit den Kantonen (Art. 2 und 4) und die Unterstützung der kantonalen Behörden durch das Bundesamt für Cybersicherheit (BACS; Art. 7 und 10).
In Bezug auf die Meldepflicht der kantonalen Behörden regen wir an, den Begriff der kritischen Infrastrukturen von Behörden (Art. 5 Bst. c Informationssicherheitsgesetz [ISG; SR 128] in Verbindung mit Art. 74b Abs. 1 Bst. b ISG) in der Cybersicherheitsverordnung zu konkretisieren. Eine Qualifikation sämtlicher Organisationseinheiten als «Betreiber kritischer Infrastrukturen» erscheint nicht als zielführend, da die Kritikalität der jeweiligen Dienste damit ausser Acht gelassen wird.
Durch die neue Meldepflicht erhält eine Bundesbehörde Kenntnis von strafbaren Handlungen, weshalb wir die Institutionalisierung der Zusammenarbeit des BACS mit den kantonalen Strafverfolgungsbehörden in der Cybersicherheitsverordnung empfehlen. Das BACS

hat keine strafrechtlichen Kompetenzen oder Aufgaben, da es sich nur indirekt mit Cyberkriminalität befasst. Zur wirksamen Bekämpfung von Cyberkriminalität ist indessen die zeitnahe Einbindung der Strafverfolgungsbehörden erfolgskritisch, namentlich in Bezug auf die Beweissicherung. Angesichts der zeitlichen Dringlichkeit bei der Strafverfolgung von Cyberkriminalität ist es zweckdienlich, bei einer Meldung an das BACS gleichzeitig Strafanzeige bei der zuständigen Strafverfolgungsbehörde einzureichen.
Daher empfehlen wir, mit einer Anzeigepflicht des BACS sicherzustellen, dass Meldungen an die zuständigen Strafverfolgungsbehörden weitergeleitet werden (vgl. auch Bemerkungen zu Art. 7 und 15).

Sodann würden wir eine stärkere Berücksichtigung der Lieferkette in der Cybersicherheitsverordnung begrüssen, zumal sich diese als primäres Angriffstor für Cyberangriffe erweist. Namentlich regen wir an, den betroffenen Dienstleister als Meldeinhalt aufzunehmen (vgl. Bemerkung zu Art. 19). Zudem schlagen wir differenziertere Regelungen für Angriffe auf die Lieferkette vor:

– Bei Cyberangriffen auf Betreiberinnen von Informatikinfrastrukturen mit Auswirkungen auf eine grosse Zahl verschiedener meldepflichtiger Organisationen und Behörden (insbesondere Hyperscaler und Betreiberinnen von Rechenzentren) schlagen wir vor, dass anstelle der gleichzeitigen Meldung durch alle Meldepflichtigen in einem ersten Schritt nur die Betreiberin der Informatikinfrastruktur eine Meldung gegenüber dem BACS absetzt. Damit könnte das BACS seine Ressourcen zielgerichtet für die Behandlung des Cyberangriffs einsetzen, ohne dass diese zusätzlich oder gar vorrangig durch die Administration einer Vielzahl von Meldungen gebunden sind. Die weiteren betroffenen meldepflichtigen Organisationen sollten ihre eigenen Meldungen zeitverzögert absetzen können.
– Es wäre klarzustellen, dass die Frist von 24 Stunden für meldepflichtige Organisationen und Behörden erst mit der eigenen Kenntnisnahme des Cyberangriffs zu laufen beginnt. In diesem Zusammenhang wäre die Verankerung einer Mitteilungspflicht von Dienstleistern an meldepflichtige Organisationen und Behörden in der Cybersicherheitsverordnung begrüssenswert.

II. Bemerkungen zu einzelnen Bestimmungen

1. Cybersicherheitsverordnung

Art. 2 Nationale Cyberstrategie

Die koordinierte Definition einer Nationalen Cyberstrategie ist zu begrüssen, da sie den Kantonen eine frühzeitige Anpassung und Ergänzung eigener Cybersicherheitsstrategien erlaubt.
Namentlich beim Aspekt der «Bekämpfung der Cyberkriminalität» muss indessen der Beizug von Staatsanwaltschaft und Polizei als fachkompetente Behörden sichergestellt werden, und zwar unabhängig von deren Vertretung im Rahmen des Steuerungsausschusses Nationale Cyberstrategie. Es ist festzuhalten, dass die Strategie und die Befugnisse zur strafrechtlichen Verfolgung von Cybervorfällen bei den Strafverfolgungsbehörden verbleiben und dass deren Weisungsfreiheit durch Festlegungen in der Nationalen Cyberstrategie nicht berührt werden.

Art. 7 Technische Analyse von Cybervorfällen und Cyberbedrohungen

Zulässige Gegenmassnahmen

Mit Bezug auf die Zulässigkeit von Gegenmassnahmen bei einem Cyberangriff bestehen unterschiedliche Auffassungen und ein rechtlich enger Rahmen. Demgegenüber sind technisch viele Gegenmassnahmen möglich. Es ist zu definieren, was das Computer Emergency Response Team (CERT) unter Präventiv- und Gegenmassnahmen versteht. Je nach Verständnis und Umfang sind erweiterte gesetzliche Grundlagen für Massnahmen erforderlich, die in der Regel nur den Strafverfolgungsbehörden gemäss der Schweizerischen Strafprozessordnung (SR 312.0) oder dem Nachrichtendienst gemäss dem Nachrichtendienstgesetz (SR 121) offenstehen.
Wir empfehlen daher, Gegenstand, Wirkungsziele und Umfang der «Gegenmassnahmen» zu definieren und die dafür nötigen Kompetenzen des CERT zu umschreiben.

Zusammenarbeit mit den Strafverfolgungsbehörden

Bei Cyberangriffen besteht für die Strafverfolgungsbehörden üblicherweise Gefahr im Verzug hinsichtlich der Sicherung der nötigen Beweise. Zudem können Sicherungsmassnahmen der Betroffenen oder des CERT die forensische Erhebung von Beweismitteln vereiteln, da die Daten durch die vorgängig vorgenommenen Manipulationen kompromittiert werden. Dies kann einen faktischen oder rechtlichen Beweisverlust zur Folge haben.
Wir regen daher die Formalisierung und Institutionalisierung der Zusammenarbeit mit der Staatsanwaltschaft und der Polizei an. Insbesondere schlagen wir vor, dass das BACS bzw. das CERT diese informieren und in die technische Analyse miteinbeziehen soll.

Art. 15 Übermittlung und Nutzung der Informationen

Gemäss Art. 15 soll das BACS über die Weitergabe der Informationen frei entscheiden können. Diese Regelung steht in einem Spannungsverhältnis zum Informationsbedarf der Strafverfolgungsbehörden. Es ist anzuerkennen, dass ein vertrauensbasierter Informationsaustausch mit den Informationslieferantinnen und -lieferanten schützenswert ist.
Eine effektive Strafverfolgung ist aber ohne rasche Informationen nicht möglich. Im Ergebnis und angesichts der betroffenen Rechtsgüter sind öffentliche Interessen, namentlich Strafverfolgungsinteressen, höher zu gewichten als die Ermessensfreiheit des BACS. Immerhin sind die Informationen bei den Strafverfolgungsbehörden auch durch das Amtsgeheimnis geschützt und werden nur zweckgebunden verwendet.
Daher regen wir an, dass das BACS verpflichtet wird, Meldungen über Cyberangriffe gemäss Art. 18 zur strafrechtlichen Beurteilung an die zuständigen Strafverfolgungsbehörden weiterzuleiten.
Sobald am Informationssystem angeschlossene Strafverfolgungsbehörden von einem Offizialdelikt erfahren, sind sie gesetzlich verpflichtet, die Ermittlungen aufzunehmen. Das BACS hat aus diesem Grund sicherzustellen, dass bei den veröffentlichten Informationen die angegriffene Betreiberin kritischer Infrastruktur nicht ersichtlich bzw. nicht ermittelbar ist.
Allgemein sollte in der Verordnung genauer festgelegt werden, wie das BACS bzw. die Strafverfolgungsbehörden mit den strafrechtlich relevanten Informationen umzugehen haben, die sie über das Informationssystem erhalten (vgl. Art. 76 Abs. 3 Satz 2 ISG).

Art. 18 Zu meldende Cyberangriffe

Art. 18 Abs. 3 geht von einem längeren Zeitraum aus, wenn nach der Entdeckung festgestellt wird, dass der Cyberangriff bereits vor mehr als 90 Tagen erfolgt ist. Dies kann beispielsweise durch die Auswertung von Logdaten geschehen. Die Datenschutzstellen wiederum verlangen eine möglichst kurze Aufbewahrung von Logdaten. Daher wäre eine grundsätzliche Regelung wünschenswert, die sich darüber ausspricht, welche Logdaten wie lange aufbewahrt werden dürfen.

Art. 19 Inhalt der Meldung

Zur Berücksichtigung von Angriffen auf die Lieferkette und zur angemessenen Beurteilung der nationalen Bedrohungslage durch das BACS empfehlen wir, den Inhalt der Meldung um «involvierte Dienstleister oder andere Dritte» zu ergänzen, um Erkenntnisse über den Angriffsweg auf die betroffene Organisation oder Behörde sicherzustellen.
Die Meldung sollte auch die Information enthalten, bei welcher Behörde Strafanzeige erstattet wurde, damit das BACS mit dieser bei einer entsprechenden Datenfreigabe Informationen austauschen kann.
Zudem sollte festgehalten werden, dass die Meldungen auf dem jeweiligen Wissensstand zum Zeitpunkt der Meldung beruhen und auf der Grundlage neuer Erkenntnisse nachgeführt werden können und sollen.

2. Organisationsverordnung für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport

Es wird weder in der vorgeschlagenen Regelung von Art. 15a Abs. 2 Bst. h der Organisationsverordnung für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (SR 172.214.1) noch in den Erläuterungen dazu umschrieben, ob und inwieweit das BACS ausschliesslich zur Vertretung der Schweiz in internationalen Gremien berechtigt sein soll. Die Polizei nimmt im Bereich der Cyberbedrohungen ähnliche Aufgaben wahr, und auch die Staatsanwaltschaften bewältigen Cybervorfälle. Ein nationaler und internationaler Austausch zwischen den Strafverfolgungsbehörden ist längst etabliert. Entsprechend regen wir an, den Umfang, in dem das BACS in den Gremien mitwirkt, genauer zu umschreiben und auf den Bereich Cybersicherheit zu beschränken. Der nationale und internationale Austausch der Strafverfolgungsbehörden zum präventiven Schutz vor Cyberbedrohungen und zur repressiven Bewältigung von Cybervorfällen darf durch diese Bestimmung nicht eingeschränkt werden.

Freundliche Grüsse

Im Namen des Regierungsrates

Die Präsidentin: Die Staatsschreiberin:

Natalie Rickli Dr. Kathrin Arioli

Kanton Schaffhausen
Departement des Innern
Mühlentalstrasse 105
CH-8200 Schaffhausen
www.sh.ch

T +41 52 632 74 61
sekretariat.di@sh.ch

Departement des Innern

Eidgenössisches Departement für
Verteidigung, Bevölkerungsschutz
und Sport VBS
Bundeshaus Ost
3003 Bern

Schaffhausen, 4. September 2024

Vernehmlassung Cybersicherheitsverordnung (CSV)

Sehr geehrte Damen und Herren

Mit Schreiben vom 22. Mai 2024 wurde der Kanton Schaffhausen zu einer Vernehmlassung in eingangs erwähnter Angelegenheit eingeladen. Dieses Geschäft wurde zuständigkeitshalber an das Departement des Innern weitergeleitet. Wir bedanken uns für die Möglichkeit zur Stellungnahme und lassen uns wie folgt vernehmen:

Cyberrisiken sind zu einer der wichtigsten Bedrohungen der Sicherheit und der Wirtschaft der Schweiz geworden. Die Professionalisierung der Cyberkriminalität schreitet weiter voran und erreicht 2024, angetrieben durch den Aufstieg der KI und innovativer Technologien, einen neuen Höhepunkt. Sei es, um ihren Unmut kundzutun, ihre Überzeugungen zu vertreten oder die angespannte Lage zu ihrem finanziellen Vorteil auszunutzen – Cyberkriminelle und Hacktivisten machen sich die unruhigen Zeiten für ihre Zwecke zunutze. Mit einem rasanten Anstieg von Zwischenfällen und Disinformation-as-a-Service (DaaS) hat sich die digitale Bedrohungslage zu einem komplexen Schlachtfeld entwickelt. Das beispiellose Ausmass an Cyberbedrohungen macht vor keiner Branche Halt, wobei das Risiko für den öffentlichen Sektor und kritische Infrastrukturen besonders hoch ist. Cyberkriminelle wissen nur zu gut, dass sie durch das Spiel mit den menschlichen Emotionen ihre Erfolgschancen maximieren – Social Engineering ist nicht ohne Grund der gemeinsame Nenner aller Angriffstaktiken. Die Professionalisierung der Cyberkriminalität und der Aufstieg der Künstlichen Intelligenz ermöglichen Cyberkriminellen, komplexe Social-Engineering-Angriffe überzeugend und erschreckend realitätsnah aufzusetzen. Zwischen echten und trügerischen Nachrichten zu unterscheiden, wird in Zukunft deutlich schwerer, während sich Bedrohungen über immer mehr digitale Kommunikationskanäle schneller verbreiten denn je. Die beunruhigenden Entwicklungen der letzten Jahre sind erst die

Spitze des Eisbergs, denn Cyberkriminelle werden auch in Zukunft ihre Methoden weiter perfektionieren. Hier gilt es mit vereinten Kräften das gesammelte Wissen zusammenzulegen.

Der Kanton Schaffhausen schätzt die Bedrohungslage als akut ein und hat entsprechend den Erlass des Bundesgesetzes über die Informationssicherheit begrüsst. Die nun vorliegenden Ausführungsbestimmungen konkretisieren, welche Cyberangriffe meldepflichtig sind, und definieren das Verfahren zur Erfüllung der Meldepflicht. Dadurch wird klar, welche Organisationen und Behörden welche Art von Cyberangriffen wie und innerhalb welcher Frist zu melden haben. Zusätzlich regelt die Verordnung, die Aufgaben des Bundesamts für Cybersicherheit (BACS) den Informationsaustausch des BACS mit Behörden und Organisationen zum Schutz vor Cybervorfällen und Cyberbedrohungen sowie die Strukturen für die strategische Steuerung der Cybersicherheit in der Schweiz.

Ein wichtiges Element dabei ist die in Art. 6 festgeschriebene Befugnis des BACS Domainhalter abfragen zu dürfen. Zentral ist daneben auch die Beratung und Unterstützung durch technische Analysen und Auskünfte zu technischen und organisatorischen Massnahmen (Art. 8) sowie die Offenlegung von Schwachstellen, welche darauf abzielt, eine möglichst hohe Transparenz über Schwachstellen zu ermöglichen, ohne Sicherheitsrisiken zu erzeugen. Dabei soll den Herstellern genügend Zeit eingeräumt werden zur Behebung der Schwachstelle, bevor diese öffentlich gemacht wird.

Da Angreifer oftmals die gleichen Methoden und Mittel verwenden, um bei möglichst vielen Opfern erfolgreiche Attacken durchzuführen, kann durch die Offenlegung von Schwachstellen innerhalb des geplanten Kommunikationssystems in Art. 11 eine breitflächige Abwehr erfolgen. Dies ermöglicht es den registrierten Organisationen und Behörden, schneller auf Bedrohungen zu reagieren und Gegenmassnahmen zu ergreifen, da Angreifer oftmals die gleichen und jeweils nur leicht modifizierten Methoden und Mittel verwenden, um bei möglichst vielen Opfern Angriffe durchzuführen. Indem die Betroffenen anderen Organisationen und Behörden ihre Erkenntnisse aus Cybervorfällen und Cyberbedrohungen rasch mitteilen können, sollte deren Zahl deutlich verringert werden können. Aus datenschutzrechtlicher Sicht ist dies sicherheitstechnisch zu begrüssen. Wie der Austausch der Informationen genau aussehen soll, muss sich wohl noch weisen. Diesbezüglich gilt es zu beachten, dass es bei einem Austausch von Informationen über Methoden und Mittel solcher Angriffe zum besseren Schutz der kritischen Infrastruktur bleiben und damit kein Zugriff auf Fremdsysteme zu Analysezwecken angestrebt werden soll. Weiter sollten Informationen möglichst anonymisiert weitergegeben werden und die Aufbewahrungsdauer allfällig mitgeteilter Daten beschränkt werden.

Zu Art. 12 ff.

Der Informationsaustausch ist von zentraler Bedeutung. In der Verordnung bleibt jedoch unklar, wie dieser Austausch zwischen allen Beteiligten erfolgen soll. Es ist unerlässlich, präzise Regelungen zu treffen bezüglich der Art und Weise des Austauschs der Meldungen sowie der Benachrichtigungen. Es stellt sich die Frage, ob eine aktive Benachrichtigung erfolgen soll oder ob eine Einsichtnahme in eine Liste erforderlich ist.

Die blosse Meldepflicht reicht nicht aus; es bedarf einer Kategorisierung, die festlegt, ab wann sofortige Massnahmen erforderlich sind, um Systeme zu überprüfen oder anzupassen. Der bisherige Informationskanal ist nicht ausreichend definiert. Es muss klargestellt werden, ab wann alle Beteiligten gewarnt werden sollen.

Ein spezialisierter Kanal für besonders kritische Meldungen ist notwendig. Eine klare Weisung an die Registrierten, wie bei einer Meldung vorzugehen ist, würde die Regelungen wesentlich effektiver gestalten. Dies würde gewährleisten, dass notwendige Massnahmen umgehend und ordnungsgemäss getroffen werden.

Darüber hinaus ist nicht eindeutig geregelt, ab wann eine Meldung erfolgen soll. Die Schwelle für die Meldepflicht sollte festgelegt werden, damit die Kriterien schnell und effizient eingeschätzt werden können, da die zeitliche Dringlichkeit für Meldungen von grosser Bedeutung ist.

Generell fehlt eine Regelung zu Massnahmen und der Zusammenarbeit mit Strafverfolgungsbehörden. Wenn ein Angriff mehrere Akteure betrifft, sollte die Erhebung einer Strafanzeige koordiniert werden. Die Zuständigkeit könnte in solchen Fällen bei der Fedpol anstatt bei der kantonalen Polizei liegen. Es wäre sinnvoll, den geplanten Ausschuss mit weitreichenden Kompetenzen auszustatten, um Angriffe effektiv einzudämmen. Das blosse Auflisten von Meldungen reicht hierfür nicht aus.

Zu Art. 13:

Bei kritischen Meldungen dürfen Benachrichtigungen nicht nur an einzelne Personen erfolgen. Es besteht die Gefahr, dass diese Personen abwesend sind. Es muss daher möglich sein, mehrere Personen zu registrieren, um die Kontinuität der Informationskette sicherzustellen.

Zu Art. 15:

Es wird erwartet, dass nicht nur eine Filterung der Meldungen erfolgt, sondern auch eine Kategorisierung durch ein spezialisiertes Supportteam. Eine zentrale Behörde mit explizitem Fachwissen sollte auf nationaler Ebene beratend tätig sein. Die einzelnen registrierten

Unternehmen verfügen oft nicht über ausreichende Ressourcen und wären zudem uneinheitlich in der Kategorisierung von Cyberattacken. Eine zentrale Bundesbehörde zum Schutz der nationalen Sicherheit, die Cyberattacken behandelt und erforderliche Massnahmen verordnet, ist notwendig.

Zu Art. 18:
Art. 18 scheint zu kurz formuliert. Nur in der Marginalie steht, dass eine Meldung zu erfolgen hat. Im Abs. 1 und 2 stehen die Definitionen, nicht aber die Pflicht selber. Ausserdem ist die Formulierung im Text sehr offen. Es müsste demnach, wenn man es wirklich wörtlich nimmt, jeder einzelne Virenfund in einem einzelnen Clientdevice gemeldet werden. Das geht sehr weit. Es wäre sinnvoll, eine Schwelle zu definieren. Der Datendiebstahl ohne Veränderung oder Offenlegung ist leider nicht umfasst. Auch dieser Aspekt sollte in den Artikel aufgenommen werden, um eine umfassende Meldepflicht sicherzustellen.

Schlussbemerkung:
Mit der Cybersicherheitsverordnung werden wesentliche Elemente der Cybersicherheit und Abwehr in der Schweiz endlich festgelegt. Ob dieses Cyberrisiko-Management mit dem anberaumten Prozess der Erkennung, Priorisierung, Verwaltung und Überwachung der Risiken für Informationssysteme genügt, wird sich zeigen. Wünschenswert wäre aber sicher, dass um möglichen Cyberangriffen und anderen digitalen und physischen Bedrohungen vorzugreifen, eine flexible Lösung notwendig ist. In der Verordnung sollte daher eine Notbestimmung aufgenommen werden, dass der Steuerungsausschuss der Nationalen Cyberstrategie (StA NCS) nicht nur Empfehlungen und Pläne machen kann (Art. 5 lit.a VO), sondern bei Dringlichkeit die Befugnis erhält, umgehend geeignete Massnahmen zu treffen. Als Voraussetzung kann statuiert werden, dass der StA NCS davon ausgehen muss, dass die Massnahmen von den zuständigen Gremien gutgeheissen würden. Diese Flexibilität braucht eine effiziente Cyberabwehr, da die Cyberkriminellen immer dreister werden und dem System einen Schritt voraus sind. Denkbar wäre auch eine Erweiterung der Halterabfrage-Befugnis in Art. 6 auf Sperrung der kriminellen Domains, statt potenziell betroffene Parteien von akuten Cyberbedrohungen oder Cyberangriffen lediglich zu warnen und Gegenmassnahmen vorzuschlagen. Die Sperrung wäre zu befristen im Rahmen der Verhältnismässigkeit (Erforderlichkeit und Geeignetheit).

Abschliessend möchten wir nochmals verdeutlichen, dass der Kanton Schaffhausen die eidgenössischen Bestrebungen und auch den Steuerungsausschuss unter Einbezug der Kantone ausdrücklich begrüsst. Die Bedrohung durch Cyberattacken ist eine ernste und zunehmende Gefahr, die einen zentralen, einheitlichen Zusammenhalt und ein koordiniertes

Vorgehen erfordert. Der Schutz unserer Informationsinfrastruktur und kritischer Systeme darf nicht durch fragmentierte kantonale Regelungen und Organisationen beeinträchtigt werden.

Es ist von grösster Wichtigkeit, dass der Bund die Verantwortung für die nationale Cybersicherheit übernimmt und einheitliche Massnahmen implementiert, ähnlich wie es im Bereich der Bundespolizei gehandhabt wird. Nur durch eine zentrale und koordinierte Vorgehensweise kann den komplexen und dynamischen Herausforderungen der Cyberkriminalität wirksam begegnet werden. Kantonale Regelungen und Organisationen wären nicht in der Lage, die umfassenden und hoch spezialisierten Anforderungen zur Abwehr von Cyberbedrohungen und zum Schutz der nationalen Sicherheit angemessen zu erfüllen.

Daher soll sich der Bund nicht scheuen, diese Verantwortung auf nationaler Ebene zu übernehmen und klare, verbindliche Vorgaben und Strukturen zu schaffen, die für alle Kantone gelten. Nur so kann gewährleistet werden, dass die Schweiz als Ganzes effektiv vor den Gefahren aus dem Cyberspace geschützt wird sowie eine resiliente und sichere digitale Infrastruktur aufrechterhalten bleibt.

Für die Berücksichtigung unserer Stellungnahme und Ihre Bemühungen danken wir bestens.

Freundliche Grüsse
Der Departementssekretär

Christoph Aeschbacher

canton de vaud
LIBERTÉ ET PATRIE

CONSEIL D'ÉTAT

Château cantonal
1014 Lausanne

Madame la Conseillère fédérale
Viola Amherd
Cheffe du Département fédéral de la défense, de la protection de la population et des sports DDPS
Palais fédéral Est
3003 Berne

Par courriel (en Word et PDF) :
ncsc@ncsc.admin.ch

Réf. : 24_COU_4066

Lausanne, le 4 septembre 2024

Modification de l'ordonnance sur la cybersécurité (OCyS) : procédure de consultation

Madame la Conseillère fédérale,

Le Conseil d'Etat du Canton de Vaud vous remercie d'avoir sollicité son avis dans le cadre de la procédure de consultation relative à la modification de l'ordonnance sur la cybersécurité (OcyS).

Il a pris connaissance du nouveau projet d'ordonnance et note positivement l'éclaircissement des tâches du nouvel Office fédéral de la cybersécurité (OFCS) et de la cyberstratégie nationale, avec son comité de pilotage. Cette démarche offre ainsi une meilleure compréhension, fortement appréciée, de la vision du Conseil fédéral sur ce sujet.

Le Conseil d'Etat partage aussi l'avis que le renforcement des infrastructures critiques contre les cyberattaques contribue indéniablement à l'amélioration de la protection de la population. L'obligation pour ces infrastructures de signaler les cyberattaques dont elles sont victimes y contribue selon notre appréciation.

Cependant, le Conseil d'Etat vaudois tient à exprimer ses réserves concernant l'exclusion des petites communes et entreprises de l'obligation de signalement. Cette limitation nous semble en effet contre-productive par rapport à l'objectif visé, sachant que ces petites infrastructures sont souvent les plus vulnérables et les plus touchées. Il souhaite par ailleurs souligner le fait que cette obligation ne doit pas se substituer à la déclaration aux autorités pénales. Le Conseil d'État recommande aussi l'inclusion d'un représentant des communes au sein du comité de pilotage de la cyberstratégie nationale.

Pour compléter les informations qui ont nourri sa prise de position, le Conseil d'Etat vous adresse, en annexe de ce courrier, diverses remarques et observations sur certains articles de l'ordonnance.

En conclusion, le Conseil d'Etat peut soutenir la proposition de modification de l'ordonnance mise en consultation.

Nous vous prions de croire, Madame la Conseillère fédérale, à l'assurance de notre considération distinguée.

AU NOM DU CONSEIL D'ETAT

LA PRESIDENTE	LE CHANCELIER.
Christelle Luisier Brodard	Michel Staffoni

Annexe mentionnée

Copies

- Secrétariat général du Département de la culture, des infrastructures et des ressources humaines
- Direction générale du numérique et des systèmes d'information
- Office des affaires extérieures

Annexe : remarques et propositions d'amendement sur l'ordonnance sur les services de télécommunications (OST)

Art. 16, Alinéa 1 let. a :
L'exemption à l'obligation de signaler des autorités fédérales, cantonales et communales et les organisations intercantonales, cantonales et intercommunales (art. 74b, al. 1, let. b, LSI) responsables de moins de 1000 résidents est contre-productive à la finalité d'annonce. Ces petites infrastructures sont les plus exposées aux cyberattaques en raison de leur manque de ressources pour investir dans des solutions de sécurité adéquates. Les exempter de cette obligation envoie un message inapproprié, minimisant l'importance de la cybersécurité pour ces entités. De plus, la charge de travail supplémentaire générée par la déclaration d'une cyberattaque est minime, puisqu'il s'agit essentiellement d'un simple courriel.

Proposition d'amendement :
Suppression de l'exemption à l'obligation de signaler des autorités fédérales, cantonales et communales et les organisations intercantonales, cantonales et intercommunales (art. 74b, al. 1, let. b, LSI) responsables de moins de 1000 résidents.

Art. 16, Alinéa 2 :
L'exemption à l'obligation de signaler des entreprises qui emploient moins de 50 personnes dans le domaine concerné et dont le chiffre d'affaires annuel ou la somme inscrite au bilan annuel ne dépasse pas 10 millions de francs dans le domaine concerné est contre-productive à la finalité d'annonce. Ces petites entreprises sont les plus exposées aux cyberattaques en raison de leur manque de ressources pour investir dans des solutions de sécurité adéquates. Les exempter de cette obligation envoie un message inapproprié, minimisant l'importance de la cybersécurité pour ces entités. De plus, la charge de travail supplémentaire générée par la déclaration d'une cyberattaque est minime, puisqu'il s'agit essentiellement d'un simple courriel.

Proposition d'amendement :
Suppression de l'exemption à l'obligation de signaler des entreprises qui emploient moins de 50 personnes dans le domaine concerné et dont le chiffre d'affaires annuel ou la somme inscrite au bilan annuel ne dépasse pas 10 millions de francs dans le domaine concerné.

Autres remarques :

- L'obligation d'annonce ne doit en aucun cas se substituer à l'annonce auprès des autorités de poursuite pénale.
- La composition du comité de pilotage de la cyberstratégie nationale devrait comprendre un représentant des communes par l'entremise de l'Association des Communes suisses (ACS), par exemple.

Switch

Frau Bundespräsidentin Viola Amherd
Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport, VBS

Herr Manuel Suter / Herr Rino Siffert
Bundesamt für Cybersicherheit, BACS

ausschliesslich per E-Mail:
ncsc@ncsc.admin.ch

Ihre Kontaktpersonen
Martin Leuthold
Head of Security and Network
Nora Zinsli
General Counsel
T +41 44 268 15 15
martin.leuthold@switch.ch
nora.zinsli@switch.ch

Zürich, den 6. September 2024

Stellungnahme zum Entwurf der Cybersicherheitsverordnung (CSV)

Sehr geehrte Frau Bundespräsidentin,
Sehr geehrte Herren Suter und Siffert,
Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit zum oben genannten Geschäft Stellung beziehen zu können und nehmen diese hiermit gerne fristgerecht wahr.

Switch wurde 1987 von der Schweizerischen Eidgenossenschaft gemeinsam mit den damals acht Universitätskantonen als privatrechtliche Stiftung errichtet. Entsprechend dem Stiftungszweck erbringt Switch im Wesentlichen Informatikdienstleistungen gegenüber kantonalen Universitäten, Eidgenössischen Technischen Hochschulen, Fachhochschulen und pädagogischen Hochschulen sowie anderen Organisationen der öffentlichen Hand und kritischen Infrastrukturen in der Schweiz.

Switch selbst betreibt drei kritische Infrastrukturen für die Schweiz: das Domain Name System (DNS) für die ccTLD .ch, das Nationale Netzwerk für Forschung und Lehre (NREN) der Schweiz und das Multisektor-CERT Switch-CERT, neben dem GovCERT im NCSC das zweite nationale CERT für die Schweiz. Dieses erbringt in enger Zusammenarbeit mit dem GovCERT operative Sicherheits-Dienstleistungen für sämtliche oben erwähnte Hochschulen (entspricht allen Organisationen des Teilsektors gemäss Art. 74b lit. a ISG) sowie relevante Unternehmen der KI-Sektoren Banken, Energie sowie Industrie und Logistik. Zudem erbringt es auch Leistungen zur Erhöhung der Internetsicherheit und zur Bekämpfung von Domain-Missbrauch im Rahmen des Domain Registry Auftrags des BAKOM.

Begrüssung einer Meldepflicht

Switch beschäftigt sich als Betreiberin von kritischen Infrastrukturen täglich mit der Cybersicherheit ihres eigenen Unternehmens und leistet als Multisektor-CERT einen relevanten Beitrag an die Cybersicherheit kritischer Infrastrukturen, insbesondere aufgrund der Bedrohungslage des immer wichtiger werdenden Bereichs der Vorfallbewältigung sowie durch die Erarbeitung national relevanter Threat Intelligence aber auch mit Aktivitäten im Bereich der Security Awareness auch präventiv.

Im Rahmen des Vernehmlassungsverfahren zum Entwurf des Bundesgesetzes über die Informationssicherheit beim Bund durfte Switch bereits Stellung nehmen. Mit der Änderung des vorgenannten Gesetzes vom 29. September 2023 wurde dann die Einführung einer Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen beschlossen.

Switch begrüsst somit die Konkretisierung und Präzisierung der wesentlichen Elemente der Cybersicherheit in der Schweiz sowie die Festlegung einer gemeinsamen Grundlage für eine Umsetzung der Meldepflicht für Cyberangriffe in der Verordnung für die Cybersicherheit.

Zu den einzelnen Bestimmungen

Nationale Cyberstrategie (Art. 2 E-CSV)

Laut Art. 2 E-CSV legt die Nationale Cyberstrategie (nachstehend: NCS) den Rahmen für Prävention, Früherkennung, Reaktionsmöglichkeiten, Resilienz sowie Bekämpfung und koordiniert die Anstrengungen auf nationaler Ebene in enger Abstimmung mit den Kantonen. Switch würde es begrüssen, wenn die nationale NCS nicht nur mit den Kantonen, sondern auch unter Einbezug der Wirtschaft, der Wissenschaft und von Vertretern der Zivilgesellschaft festgelegt wird. Unserer Meinung nach ermöglicht die vorgeschlagene Anpassung einen grösseren Kreis von wichtigen Akteuren einzubeziehen und dadurch eine breitere Verankerung und Abstimmung für die NCS zu erreichen.

Demzufolge schlägt Switch vor, Art. 2 E-CSV wie folgt anzupassen:

Art. 2 Nationale Cyberstrategie	**Anpassungsvorschlag (in grün)**
[1] Die Nationale Cyberstrategie (NCS) legt den strategischen Rahmen für die Prävention im Bereich der Cybersicherheit, die Früherkennung von Cyberbedrohungen, die Reaktionsmöglichkeiten und die Resilienz bei Vorfällen sowie die Bekämpfung der Cyberkriminalität fest.	
[2] Sie wird in Abstimmung mit den Kantonen festgelegt.	[2] Sie wird in Abstimmung mit den Kantonen und unter Einbezug der Wirtschaft, der Wissenschaft und von Vertretern der Zivilgesellschaft festgelegt.

Technische Analyse von Cybervorfällen und Cyberbedrohungen (Art. 7 E-CSV)

Das BACS betreibt das nationale Computer Emergency Response Team (nachstehend: CERT), das eine zentrale Rolle bei der Bewältigung von Cybervorfällen und Cyberbedrohungen in der Schweiz spielt. In den Erläuterungen ist ferner festgestellt, dass das CERT sich eng mit Spezialistinnen und Spezialisten aus den Sicherheitsteams der Privatwirtschaft und anderer Länder austauscht. Switch würde es begrüssen, wenn der in den Erläuterungen vorgesehene Austausch ausdrücklich in der Verordnung verankert würde. Eine explizite Verankerung würde der generellen Zusammenarbeit GovCert-Switch, aber auch mit anderen Organisationen wie z.B. Swiss FS-CSC oder Rail-ISAC oder Switch für die Hochschulen und Forschungsorganisationen direkt legitimieren.

Demzufolge schlägt Switch vor, Art. 7 E-CSV wie folgt anzupassen:

Art. 7 Technische Analyse von Cybervorfällen und Cyberbedrohungen	**Anpassungsvorschlag (in grün)**
[1] Das BACS betreibt das nationale Einsatzteam für Computersicherheit *(Computer Emergency Response Team [CERT])*, das insbesondere die folgenden Aufgaben wahrnimmt: a. technische Vorfallbewältigung; b. Analyse technischer Fragestellungen; c. Identifikation und Beurteilung von Cyberbedrohungen. [2] Es betreibt für die Analyse der Cybervorfälle und Cyberbedrohungen eine resiliente Infrastruktur; diese muss unabhängig von der restlichen Bundesinformatik funktionieren.	[3] Für die Erfüllung seiner Aufgaben tauscht sich das CERT mit nationalen und internationalen Kompetenzzentren sowie Spezialistinnen und Spezialisten aus den Sicherheitsteams der Privatwirtschaft aus.

Priorisierung der Beratung und Unterstützung bei Cyberangriffen (Art. 8 E-CSV)

Art. 8 E-CSV stützt sich auf Art. 74 Abs. 3 und Art. 74a Abs. 3 ISG. Aus Art. 74 Abs. 3 ISG ergibt sich unserem Verständnis nach die Subsidiarität des BACS in gewissen Fälle. Wenn es sich um eine private Betreiberin handelt, ist vorgesehen, dass das BACS berät und unterstützt, sofern die Funktionsfähigkeit der betreffenden kritischen Infrastruktur gefährdet ist und es nicht möglich ist, rechtzeitig eine gleichwertige Unterstützung auf dem Markt zu erhalten. Darüber hinaus entscheiden die Betroffenen, wie in den Erläuterungen dargelegt, selbst, ob sie die Unterstützung des BACS in Anspruch nehmen wollen.

Mit Blick auf die Subsidiarität des BACS in bestimmten Fällen empfehlen wir, Art. 8 E-CSV entsprechend anzupassen respektive zu konkretisieren. Zudem wäre ein zusätzlicher Absatz, der der

Grundsatz der Eigenverantwortung von private Bertreiberinnen für Cybersicherheit klar festschreibt (siehe hierzu Art. 716a OR), wünschenswert.

Demzufolge schlägt Switch vor, Art. 8 E-CSV wie folgt anzupassen:

Art. 8 Priorisierung der Beratung und Unterstützung bei Cyberangriffen	**Anpassungsvorschlag (in grün)**
[1] Übersteigt die Nachfrage nach Beratung und Unterstützung bei einem Cyberangriff die Kapazitäten des BACS, so kann es die Bearbeitung in Bezug auf den Zeitpunkt und den Umfang der Beratung und Unterstützung priorisieren. [2] Es berücksichtigt dabei die öffentliche Sicherheit und Ordnung, das Wohlergehen der Bevölkerung und das Funktionieren der Wirtschaft.	[3] Private Betreiberinnen beachten der Grundsatz der Eigenverantwortung für Cybersicherheit. [4] Private Betreiberinnen beauftragen notwendige Beratungs- und Unterstützungsleistungen grundsätzlich auf dem privaten Markt.

Ausnahmen von der Meldepflicht (Art. 16 E-CSV)

Diese Bestimmung stützt sich auf Art. 74c ISG, wonach der Bundesrat Organisationen und Behörden von der Meldepflicht nach Art. 74b ISG ausnimmt, wenn durch Cyberangriffe ausgelöste Funktionsstörungen nur geringe Auswirkungen auf die öffentliche Ordnung, die Sicherheit, das Wohlergehen der Bevölkerung oder das Funktionieren der Wirtschaft haben.

Die für Switch relevante Kategorien (d.h. Hochschulen gemäss Art. 74b Abs. 1 Bst. a ISG, Anbieterinnen von Fernmeldediensten gemäss Art. 74 Abs. 1 Bst. q ISG sowie Registerbetreiberinnen und Registrare von Internet-Domains gemäss Art. 74 Abs. 1 Bst. r ISG) sind weder im Abs. 1 noch im Abs. 2 von Art. 16 E-CSV aufgeführt, womit keine Ausnahmeregelung vorgesehen ist. Anbieterinnen und Betreiberinnen von Cloudcomputing, digitalen Sicherheits- und Vertrauensdiensten gemäss Art. 74b Abs. 1 Bst. t ISG sind zwar in Art. 16 Abs. 1 Bst. e E-CSV aufgeführt. Die vorgesehene Einschränkung trifft jedoch auf Switch nicht zu.

Nach unserem Verständnis sind nicht nur die Hochschulen, die Registrare, sondern auch Switch als Anbieterin von Fernmeldediensten, Cloud Service und Domain Registry somit vollständig meldepflichtig. Angesicht der Kategorien für welche Ausnahmen gelten und welche Verwaltungen, Blaulichtorganisationen, Organisationen der Grundversorgung (Energie, Wasser, etc.) und weitere umfassen, welche bei Ausfall einen limitierten Schaden verursachen (z.B. bei Gemeinden mit weniger als 1000 Einwohnern, etc.) erachten wir diese Bestimmung für die Hochschulen und die Registrare als unverhältnismässig und aus Sicht der Interessen des BACS und des Bundes als nicht sinnvoll und zielführend.

Deswegen schlägt Switch vor, die Hochschulen und Registrare in gewisse Fälle von der im Art. 74b ISG vorgesehene Meldepflicht auszunehmen und dahingehend Art. 16 E-CSV wie folgt anzupassen:

Art. 16 Ausnahmen von der Meldepflicht	**Ergänzungsvorschlag (in grün)**
[1] Die folgenden Behörden und Organisationen sind unter den nachstehenden Voraussetzungen von der Meldepflicht ausgenommen: a. Stellen nach Artikel 74*b* Absatz 1 Buchstaben b und c ISG: sofern sie für weniger als 1000 Einwohnerinnen und Einwohner zuständig sind; massgeblich ist die ständige Wohnbevölkerung; b. Unternehmen nach Artikel 74*b* Absatz 1 Buchstabe d ISG, sofern sie: 1. als Netzbetreiber, Elektrizitätserzeuger, Elektrizitätsspeicherbetreiber oder Dienstleister im Elektrizitätsbereich gemäss Artikel 5*a* Absatz 1 und Anhang 1*a* der Stromversorgungsverordnung vom 14. März 20084 weder das Schutzniveau A noch das Schutzniveau B einhalten müssen, 2. als Betreiber von Gasleitungen nach Artikel 2 Absatz 3 der Rohrleitungssicherheitsverordnung vom 4. Juni 2021 im Durchschnitt der letzten fünf Jahre eine transportierte Energie von weniger als 400 GWh/Jahr aufweisen; c. Unternehmen nach Art. 74*b* Absatz 1 Buchstabe n ISG, sofern sie: 1. kein Information Security Management System nach den Artikeln 2 und 4 und dem Anhang II der Verordnung (EU) 2023/2036 oder nach Artikel 2 und dem Anhang II der Verordnung (EU) 2022/16457 einrichten müssen, 2. die Vorgaben nach Punkt 1.7 des Anhangs der Verordnung (EU) 2015/19988 in ihrem Security-Programm nach Artikel 2, 12, 13 oder 14 der Verordnung (EG) 300/20089 nicht umsetzen müssen; d. Eisenbahnunternehmen sowie Seilbahn-, Trolleybus-, Autobus- und Schifffahrtsunternehmen nach Artikel 74*b* Absatz 1 Buchstabe m ISG, sofern sie: 1. nicht mit Systemaufgaben (Art. 37 des Eisenbahngesetzes vom 20. Dezember 195710 [EBG]) beauftragt sind,	

2. über eine Personenbeförderungskonzession nach Artikel 6 des Personenbeförderungsgesetzes vom 20. März 200911 (PBG) verfügen, aber keine durch Bund und Kantone gemeinsam bestellten Angebote erbringen (Art. 28–31*c* PBG), 3. sie über eine Infrastrukturkonzession nach Artikel 5 EBG verfügen, diese aber nicht erteilt wurde, weil ein öffentliches Interesse am Bau und Betrieb der Infrastruktur besteht (Art. 6 Abs. 1 Bst. a EBG); e. Anbieterinnen und Betreiberinnen nach Artikel 74*b* Absatz 1 Buchstabe t ISG: sofern sie einen Sitz in der Schweiz haben und ihre Leistungen weder teilweise noch vollumfänglich gegen Entgelt für Dritte erbringen. [2] Unternehmen nach Artikel 74*b* Absatz 1 Buchstaben f, g, h, l und p ISG, für die Absatz 1 nicht anwendbar ist, sind von der Meldepflicht ausgenommen, sofern sie im betroffenen Bereich weniger als 50 Personen beschäftigen und ihr Jahresumsatz beziehungsweise ihre Jahresbilanzsumme im betroffenen Bereich 10 Millionen Franken nicht übersteigt.	f. Hochschulen nach Artikel 74b Absatz 1 Buchstabe a ISG, sofern sie für weniger als 2000 Studierende zuständig sind; massgeblich ist die aktuelle Statistik des BFS. g. Registrare nach Artikel 74b Absatz 1 Buchstabe r ISG, sofern weniger als 50 Personen beschäftigen und ihr Jahresumsatz beziehungsweise ihre Jahresbilanzsumme im betroffenen Bereich 10 Millionen Franken nicht übersteigt.

Zu meldende Cyberangriffe (Art. 18 E-CSV)

Laut Art. 18 Abs. 1 Bst. a. E-CSV gilt die Funktionsfähigkeit einer kritischen Infrastruktur u.a. als gefährdet, wenn Mitarbeitenden oder Dritte von Systembrüche betroffen sind. Unser Meinung nach wäre es zweckmässig, diese Bestimmung in mehrfacher Hinsicht zu konkretisieren. Insbesondere erscheint es uns notwendig, nicht nur eine zeitliche Grenze, sondern auch eine Grenze der Anzahl betroffener Personen festzulegen. Wird die Grenze zeitlich und/oder personell unterschritten, ist die Auswirkung nicht relevant oder gering, weshalb eine Meldung nicht notwendig wäre und das BACS damit nur überlastet würde. Darüber hinaus ist es möglicherweise sinnvoll, zwischen den betroffenen

Personen (z.B. Mitarbeitende, Forschende, Dozierende, Studierende) und der Relevanz für das Kerngeschäft zu unterscheiden.

Unseren Vorschlag können wir wie folgt veranschaulichen: DDoS-Angriffe auf eine unbedeutende Webplattform einer Hochschule, welche nur kurze Zeit nicht zugreifbar ist, es nur Mitarbeitende betrifft und weder Studierende noch Forschende noch Dozierende.

Switch begrüsst zudem den Wortlaut von Art. 18 Abs. 1 Bst. b. E-CSV, aus welchem hervorgeht, dass alles, was als normaler Incident behandelt werden kann, nicht gemeldet werden muss. Ebenso begrüsst Switch den Wortlaut von Art. 18 Abs. 2 Bst. a. E-CSV, weil er unserer Meinung nach genug Interpretationsspielraum lässt.

Inhalt der Meldung (Art. 19 E-CSV)

Die Meldung nach Art. 19 Abs. 1 E-CSV muss unter anderem Angaben zum Verursacher enthalten. Solche Angaben können allerdings Personendaten bilden (z.B. IP-Adressen). Art. 75 Abs. 2 ISG erlaubt eine Herausgabe solcher Daten nur unter gewissen Voraussetzungen ohne Einwilligung der betroffenen Personen. Es besteht also die Gefahr, dass bei unmittelbarer Meldung eines Vorfalls eine genauere Analyse durch das BACS ergibt, dass die Meldung nicht relevant ist. Damit stünde die übereilte Weitergabe personenbezogener Daten unter Umständen im Konflikt zum Datenschutzgesetz. Aus den genannten Gründen regen wir daher an, das Meldevorgehen so zu anpassen, dass eine Behörde oder Organisation personenbezogen Daten nur aufgrund eines gesicherten Vorfalls an das BACS weitergibt.

Um unseren Vorschlag zu veranschaulichen, folgt ein Beispiel: Die Behörde oder Organisation meldet Informationen zum Cyberangriffe (Datum und Uhrzeit der Feststellung des Angriffs, Datum und Uhrzeit des Angriffs, Art des Angriffs und Angriffsmethode) und erwähnt gleichzeitig, ob sie Angaben zum Verursacher besitzt. Das BACS bitten dann die meldende Behörde oder Organisation um die Aushändigung der Informationen, sofern sich nach der Erstanalyse ein berechtigter Anspruch ergibt.

Übermittlung der Meldung (Art. 20 E-CSV)

Unsere Meinung nach sollte die Möglichkeit bestehen, dass sich ein Unternehmen oder mehrere Unternehmen gemeinsam entscheiden können, Meldungen über eine spezialisierte Drittorganisation zu melden, welche auch die Incident Response unterstützt, z.B. einen MSSP (Managed Security Service Provider), ein Branchen-CERT, ein Branchen-ISAC, eine kantonale Meldestelle, etc..

Demzufolge schlägt Switch vor, der Art. 20 E-CSV wie folgt zu ergänzen:

Art. 20 Übermittlung der Meldung	**Ergänzungsvorschlag (in grün)**
[1] Falls die Meldung nicht über das Kommunikationssystem des BACS erfolgt, informiert dieses die Kontaktperson nach Artikel 13 Absatz 2 Buchstabe b über den Eingang und den Inhalt der Meldung.	[2] Eine oder mehrere meldepflichtige Behörden oder Organisationen können sich entscheiden den Meldevorgang individuell oder gemeinsam an eine spezialisierte Drittorganisation auszulagern.

Frist zur Erfassung der Meldung (Art. 21 E-CSV)

Dieser Artikel statuiert die Frist zur Erfassung der Meldung. Es wird klargestellt, dass die Behörde oder Organisation, die von einem Cyberangriff betroffen ist, die bekannten Informationen innerhalb von 24 Stunden melden muss. Obwohl wir uns bewusst sind, dass es für die Prävention und Frühwarnung von entscheidender Bedeutung ist, Cyberangriffe sofort nach ihrer Entdeckung zu melden, erachten wir die Frist von 24 Stunden vor allem für kleinere Organisation als einen unverhältnismässigen Aufwand in Vergleich zum Mehrwert beim BACS. Dies gilt umso mehr, als weder im Entwurf der Verordnung noch in ihren Erläuterungen definiert ist, innerhalb welcher Frist das BACS und das Gov-CERT auf die Meldung reagieren werden. Was würde also die Meldung an Feiertagen und ausserhalb Bürozeiten bringen? Wir würden es demzufolge begrüssen, wenn sich die 24 Stunden Frist auf Arbeitswochen und Bürozeiten bezieht und Art. 21 Abs. 1 E-CSV dahingehend angepasst würde. Eine Meldung beim BACS müsste jedoch weiterhin rund um die Uhr möglich sein.

Wir bedanken uns für die Möglichkeit einer Stellungnahme und hoffen, dass unsere Anliegen soweit als möglich berücksichtigt werden können.

Bei Fragen stehen wir Ihnen jederzeit gerne zur Verfügung.

Freundliche Grüsse

Martin Leuthold
Head of Security & Network

Nora Zinsli
General Counsel

Per Mail:
ncsc@ncsc.admin.ch

Olivier Schneider
T +41 61 415 44 68
O.Schneider@primeo-energie.ch

Münchenstein, 06.09.2024

Stellungnahme zur Vernehmlassung der Cybersicherheitsverordnung (CSV)

Sehr geehrte Frau Bundesrätin Amherd,
sehr geehrte Damen und Herren

Besten Dank für die Möglichkeit, zur Cybersicherheitsverordnung (CSV) Stellung nehmen zu können. Primeo Energie nimmt diese Gelegenheit gerne wahr.

Wir unterstützen das Ansinnen des Bundesrates, eine Meldepflicht von Betreiberinnen und Betreiber kritischer Infrastrukturen für Cyberangriffe einzuführen. Demzufolge sind wir mit dem Inhalt der Vorlage einverstanden.

Wir erachten es jedoch als wichtig, folgende Präzisierung (folgend in roter Schrift) von Art. 4 Abs. 3 vorzunehmen.

- Er ernennt aus dem kreis der Vertreterinnen und Vertreter der Wirschaft, der Gesellschaft, der kritischen Infrastruktur und der Hochschulen die vorsitzende Person

Bei der Zusammensetzung ist es unabdingbar, spezifisch auf Vertreterinnen und Vertreter der kritischen Infrastruktur hinzuweisen, da diese eine aktive Rolle in der Vorlage einnehmen.

Weiter sollte unter Art. 19 (Inhalt der Meldung) als zusätzlicher Punkt der Meldepflicht aufgeführt werden, welcher OT-Bereich von einem Angriff betroffen ist (z. B. welche Produkte). Dadurch können wichtige Schlussfolgerungen hinsichtlich eines zukünftigen besseren Schutzes von Cyberangriffen gemacht werden, in dem z. B. Empfehlungen an die Geschädigten ausgesprochen oder neue Methoden für einen besseren Schutz entwickelt werden.

Besten Dank für die Kenntnisnahme und die wohlwollende Prüfung unserer Anliegen. Für Fragen stehen wir Ihnen gerne zur weiteren Verfügung.

Freundliche Grüsse

Im Namen der **Primeo Energie AG** und der gesamten **Primeo Energie-Gruppe**

Primeo Management AG

Dominik Baier
General Counsel / Corporate Secretary

Olivier Schneider
Public Affairs

Bundesamt für Cybersicherheit (BACS)
Schwarztorstrasse 59
3003 Bern

Cybersicherheitsversordnung (CSV); Vernehmlassung

Sehr geehrte Frau Bundespräsidentin Viola Amherd
Sehr geehrte Damen und Herren

Der Bundesrat hat am 22. Mai 2024 das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) beauftragt, bei den Kantonen ein Vernehmlassungsverfahren zur Cybersicherheitsverordnung durchzuführen.

Der Regierungsrat betrachtet Cyberrisiken wie der Bund als eine der wichtigsten Bedrohungen der Sicherheit von Bürgern, Wirtschaft und Verwaltung. Eine schweizweite Einschätzung der Bedrohungslage kann durch eine Meldepflicht von Cyberangriffen mit höherer Qualität gestaltet werden. Die CSV legt nun konkret fest, welche Ausnahmen von der Meldepflicht gelten und konkretisiert, welche Cyberangriffe meldepflichtig sind. Zudem wird das Verfahren zur Erfüllung der Meldepflicht definiert. Dadurch wird klar, welche Organisationen und Behörden welche Art von Cyberangriffen wie und innerhalb welcher Frist zu melden haben. Zusätzlich regelt die Verordnung, wie das BACS die sich aus dem ISG ergebenden Aufgaben erfüllen soll und definiert die Strukturen für die strategische Steuerung der Cybersicherheit in der Schweiz.

Der Kanton Uri ist seit 2014 Mitglied des geschlossenen Kundenkreises des BACS/NCSC/Melani und schätzt die Arbeit dessen sehr. Die Konkretisierung der Meldepflicht in der CSV ist notwendig und wird befürwortet.

Der Kanton Uri nimmt zu einzelnen Artikeln der CSV wie folgt Stellung:

Artikel 2 Der Bund hat für die Zusammenarbeit mit den Kantonen im Bereich der Cybersicherheit die Organisation Sicherheitsverbund Schweiz (SVS) vor über zehn Jahren ins Leben gerufen. Anlässlich von 1 bis 2 Workshops pro Jahr wurden in sogenannten Landsgemeinden die Grundlagen für die heutige Cyberstrategie gelegt. Eine breite Teilnehmerschaft aus Kantonen, Bund, Hochschulen und Privaten konnten sich aktiv beteiligen und die Strategie stetig weiterentwickeln. Aus Kantonssicht wäre es wünschenswert, wenn dieses Gremium weiterhin massgeblich an der zukünftigen NCS-Gestaltung und Massnahmenumsetzung mitarbeiten könnte.

Artikel 5 a Die NCS wird mindestens alle fünf Jahre überprüft und angepasst. Wir beurteilen diese Zeitspanne als zu lange und schlagen vor, die NCS mindestens alle drei Jahre zu überprüfen.

Artikel 8 Die meldepflichtigen Unternehmen und Organisationen würden hier optimalerweise nach Funktionen (Energie; Ernährung; Logistik; Gesundheit; Sicherheit-Polizei-Militär-Zivilschutz; Finanzwesen; Medien; Verwaltung; usw.) vorbereitend priorisiert.

Artikel 10 Uns stellt sich in diesem Artikel die Frage, wie die Gemeinden in den Gesamtprozess eingebunden werden sollen.

Artikel 16 Einwohnermässig kleinere Gemeinden sind im Kanton Uri in einen der zwei Rechenzentrumsverbunde eingebunden. Diese sollten nicht von einer Meldepflicht enthoben werden, da sich ein Sicherheitsereignis im schlimmsten Falle auf weitere Gemeinden ausweiten könnte.

Artikel 21 Wir stellen uns die Frage, welche Sanktionen vorgesehen sind, wenn eine betroffene Behörde die erforderlichen Informationen nicht macht und der Meldepflicht ans BACS nicht nachkommt.

Sehr geehrte Frau Bundespräsidentin, sehr geehrte Damen und Herren, wir bedanken uns für die Möglichkeit zur Stellungnahme und grüssen Sie freundlich.

Altdorf, 10. September 2024

Im Namen des Regierungsrats
Der Landammann: Christian Arnold
Der Kanzleidirektor: Roman Balli

Schweizerischer Pensionskassenverband
Association suisse des Institutions de prévoyance
Associazione svizzera delle Istituzioni di previdenza
Kreuzstrasse 26
8008 Zürich

Telefon 043 243 74 15/16
Telefax 043 243 74 17
E-Mail info@asip.ch
Website www.asip.ch

Bundesamt für Cybersicherheit BACS
Schwarztorstrasse 59

3003 Bern

info@ncsc.admin.ch

Zürich, 09.09.2024

Stellungnahme zur Vernehmlassung zur Cybersicherheitsverordnung

Sehr geehrte Damen und Herren

Gerne nehmen wir zur Vernehmlassung zur Cybersicherheitsverordnung Stellung.

Der Schweizerische Pensionskassenverband ASIP mit Sitz in Zürich ist der Dachverband für über 900 Pensionskassen. Er vertritt über die Mitglieder rund zwei Drittel der Versicherten in der beruflichen Vorsorge sowie ein Vorsorgevermögen von gegen CHF 650 Mia. Der ASIP bezweckt die Erhaltung und Förderung der sozialpartnerschaftlich geführten beruflichen Vorsorge auf freiheitlicher und dezentraler Basis und setzt sich für das Drei-Säulen-Konzept in ausgewogener Gewichtung ein. Er positioniert sich als Ansprechpartner für alle Akteure im Umfeld der beruflichen Vorsorge. Die Exponenten unseres Verbandes vertreten die Interessen der Pensionskassen in verschiedenen Gremien sowie gegenüber der Politik und der Öffentlichkeit.

Im Fokus der Vernehmlassung steht die Ausnahme von der Meldepflicht gemäss nArt. 16 Abs. 1 der Verordnung über die Cybersicherheit (Cybersicherheitsverordnung, CSV). Gemäss Erläuterungen zur Verordnung über die Cybersicherheit (Cybersicherheitsverordnung, CSV) vom Mai 2024, S. 22, ist „zu beachten, dass es meldepflichtige Behörden und Organisationen gibt, für die keine Ausnahmen von der

Meldepflicht gemäss den nachfolgend erläuterten Absätzen 1 und 2 bestehen", wozu „Organisationen [gehören], die Leistungen zur Absicherung gegen die Folgen von Krankheit, Unfall, Arbeits- und Erwerbsunfähigkeit, Alter, Invalidität und Hilflosigkeit erbringen (Art. 74b Abs. 1 Bst. i ISG)".

In unserer Vernehmlassungsantwort vom 14. April 2022 betreffend die nArt. 74a und 74b ISG hatten wir die eingeschränkte Meldepflicht für Vorsorgeeinrichtungen begrüsst. Im Erläuterungsbericht zur Änderung des ISG vom 12. Januar 2022, S. 18f., wird die eingeschränkte Meldepflicht (damals noch lit. j, jetzt lit. i) wie folgt beschrieben: „[…] Es wurde auf die Aufzählung einzelner Gesetze (z.B. IVG, AHVG) verzichtet, um nicht nur gesetzliche, sondern auch überobligatorische Leistungen, beispielsweise der beruflichen Vorsorge oder der Zusatzversicherung zur obligatorischen Krankenkasse, abzudecken. Bei der beruflichen Vorsorge werden alle registrierten und nicht registrierten Vorsorge- und Freizügigkeitseinrichtungen erfasst, jedoch nicht die gebundene oder freiwillige Selbstvorsorge (Säule 3a und 3b). Diese letztgenannten Vorsorgemöglichkeiten werden in aller Regel von Banken und Versicherungen angeboten, die ihrerseits der Meldepflicht unterstehen."

Gemäss nArt. 74c ISG kann der Bundesrat auf Verordnungsstufe „bestimmte Kategorien von Betreiberinnen von kritischen Infrastrukturen von der Meldepflicht ausnehmen, wenn durch Cyberangriffe auf ihre Infrastrukturen ausgelöste Funktionsausfälle oder Fehlfunktionen: a. unwahrscheinlich sind, insbesondere wegen einer geringen Abhängigkeit von Informatikmitteln; oder b. nur geringe Auswirkungen auf das Funktionieren der Wirtschaft beziehungsweise das Wohlergehen der Bevölkerung haben, insbesondere, weil sie:
1. nur eine geringe Anzahl Personen betreffen,
2. von anderen kritischen Infrastrukturen aufgefangen werden, oder
3. nur ein geringes volkswirtschaftliches Schadenspotenzial haben."

So könnte der Bundesrat den Adressatenkreis der meldepflichtigen Vorsorgeeinrichtungen durch geeignete Kriterien einschränken.

Da die Verantwortlichkeit für Cybersicherheit beim obersten Organ der Vorsorgeeinrichtung (Überwachung von Geschäftsrisiken: Risikomanagement) liegt und nicht unnötigerweise durch gesetzliche Bestimmungen eingeschränkt werden sollte, beantragen wir eine Erweiterung von nArt. 16 CSV i.S. einer Befreiung von der Meldepflicht für sämtliche registrierten und nicht registrierten Vorsorgeeinrichtungen (mit und ohne reglementarische Leistungen) bis zur Grösse von 30'000 Versicherten (inkl. Rentnerinnen und Rentner).

Wir danken Ihnen für die Beachtung unserer Hinweise. Gerne stehen wir Ihnen zur Beantwortung allfälliger weiterer Fragen zur Verfügung.

Mit freundlichen Grüssen

A S I P

Schweizerischer Pensionskassenverband

Dr. Lukas Müller-Brunner

Direktor ASIP

Dr. Michael Lauener

Leiter Recht

Flughafen Zürich

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Bundeshaus Ost
CH-3003 Bern

Per Email an
ncsc@ncsc.admin.ch

Zürich-Flughafen, 10. September 2024

Vernehmlassung zum Erlass der Cybersicherheitsverordnung – Stellungnahme Flughafen Zürich AG

Sehr geehrter Herr Suter, sehr geehrter Herr Siffert

Mit Schreiben vom 22. Mai 2024 hat Frau Bundesrätin Viola Amherd interessierte Kreise zur Teilnahme an der erwähnten Vernehmlassung eingeladen. Gerne nehmen wir die Gelegenheit wahr, unsere Anliegen zur geplanten Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe zu äussern. Die Flughafen Zürich AG ist Eigentümerin und Betreiberin des grössten Landesflughafens mit über 30 Millionen Passagieren im Jahr. Gemäss der vom Bundesrat definierten nationalen Strategie «Spektrum der kritischen Infrastrukturen» fällt auch der Flughafen Zürich unter die Definition einer kritischen Infrastruktur. Zudem bestätigt Artikel 74b Bst. n des Informationssicherheitsgesetzes, dass die Meldepflicht von Cyberangriffen für «die Landeflughäfen gemäss Sachplan Infrastruktur Luftfahrt» gilt. Insofern überrascht es, dass weder der Dachverband der Luftfahrt Aerosuisse noch die Landesflughäfen als direkt betroffene Akteure eingeladen wurden, zumal sich alle beim Vernehmlassungsverfahren zum Informationssicherheitsgesetz eingegeben hatten.

Die Flughafen Zürich AG anerkennt, dass Cyberrisiken zu einer wichtigen Bedrohung für die Schweiz und für Unternehmen geworden sind. Dazu gehören namentlich auch die Betreiberinnen von kritischen Infrastrukturen, zu denen die Flughafen Zürich AG als Konzessionärin des Bundes gehört und bereits heute für Vorfälle meldepflichtig ist, die potenzielle Auswirkungen auf die Sicherheit haben. Das beinhaltet die Meldung von erfolgreichen Cyber-Angriffen an das BAZL. Die Flughafen Zürich AG begrüsst deshalb die Stossrichtung des Informationssicherheitsgesetzes sowie der Cybersicherheitsverordnung als wirksame Mittel für die Harmonisierung und Koordination der Meldepflicht auf Bundesebene und damit die Förderung des Informationsaustauschs zwischen den Sektoren. Die Flughafen Zürich AG hat sich dabei als privatwirtschaftlich geführte kritische Infrastruktur

andrew.karim@zurich-airport.com | T +41 43 816 71 29 | M +41 77 529 13 93
Flughafen Zürich AG | Postfach | CH-8058 Zürich-Flughafen | flughafen-zuerich.ch

intensiv in die politischen Diskussionen eingebracht. Die verschiedenen Sichtweisen aus Verwaltung, Kantonen, Wirtschaft, Gesellschaft und Hochschulen helfen, die Herausforderungen im Bereich der Cybersicherheit und Cyberbedrohungen ganzheitlich anzugehen und in Zusammenarbeit aller Akteure sinnvolle, geeignete und verhältnismässige Massnahmen zu treffen. Die Flughafen Zürich AG begrüsst daher die Schaffung eines Steuerungsausschusses Nationale Cyberstrategie, wie in den Artikeln 3 - 5 vorgeschlagen wird, und besonders, dass auch der Einbezug der Wirtschaft vorgesehen ist. Als börsenkotierte und privatwirtschaftlich geführte Betreiberin einer kritischen Infrastruktur sehen wir uns in der Pflicht, Verantwortung zu übernehmen. Die Flughafen Zürich AG stellt sich daher gerne als Vertretung der Wirtschaft für den Steuerungsausschuss Nationale Cyberstrategie zur Verfügung.

Antrag 1: Steuerungsausschuss Nationale Cyberstrategie

Wir begrüssen es, wenn die Flughafen Zürich AG als Vertretung der Wirtschaft in den Steuerungsausschuss Nationale Cyberstrategie aufgenommen wird.

Die Informationstechnologiebranche ist sehr schnelllebig und einem steten Wandel unterworfen. Heute geltende Ansätze, Informationen sowie Technologielösungen können bereits morgen veraltet sein. Eine Strategie muss jeweils die Entwicklungen berücksichtigen können und gleichzeitig genug übergeordnet sein, um nicht ständig überprüft und nötigenfalls angepasst zu werden. In diesem Spannungsfeld erachten wir es als richtig und wichtig, eine regelmässige Überprüfung vorzusehen. Dazu würden wir angesichts der Dynamik im IT- und Cyberbereich eine Überprüfung bestenfalls alle drei Jahre, mindestens aber alle vier Jahre vorsehen.

Antrag 2: Anpassung in Art. 5

Der StA NCS hat folgende Aufgaben:

a. Er überprüft die NCS mindestens alle *vier* ~~fünf~~ Jahre, wirkt bei ihrer Weiterentwicklung mit und erarbeitet bei Bedarf Anpassungsvorschläge.

Der Meldung von Cyberangriffen und dem damit verbundenen Austausch von zum Teil hochsensitiven und betriebskritischen Daten kommt ein besonderer Schutzbedarf zu. Eine Meldung an eine zentrale staatliche Stelle setzt voraus, dass das Sicherheitssystem dieser Behörde absolut bzw. bestmöglich geschützt ist. Lecks sollten zu jeder Zeit komplett ausgeschlossen und bei Auftreten jederzeit und unverzüglich geschlossen werden können. Es wäre sehr heikel, wenn Informationen von kritischen Infrastrukturen in der Schweiz in die Hände von Personen oder Organisationen mit unlauteren oder kriminellen Absichten gelangen würden. Die vorgeschlagene Regelung in Artikel 7 Absatz 2, dass das NSCS für die Analyse von Cybervorfällen und Cyberbedrohungen eine resiliente Infrastruktur betreibt, die unabhängig von der restlichen Bundesinformatik funktionieren muss, ist deshalb besonders zu begrüssen. Hier gälte es allerdings einen Schritt weiterzugehen und diese nicht nur unabhängig von der restlichen Bundesinformatik zu betreiben, sondern mit einem erhöhten Schutzstatus auszustatten. Das

Ziel sollte deshalb sein, dass die betreffende Infrastruktur ein mindestens gleich hohes, wenn nicht sogar höheres Schutzlevel als die Bundesverwaltung aufweist.

Antrag 3: Ergänzung in Art. 7 Abs. 2

2 Es betreibt für die Analyse der Cybervorfälle und Cyberbedrohungen eine resiliente Infrastruktur; diese muss unabhängig von der restlichen Bundesinformatik funktionieren. *Dabei ist ein höheres Schutzlevel als bei der Bundesverwaltung anzustreben.*

Kritische Infrastrukturen haben ein immanentes Interesse, ihre Infrastrukturen vor Cyberangriffen bestmöglich zu schützen, denn der Cyberbereich ist grenzenlos und die Bedrohungen stammen aus aller Welt. Koordinierte Massnahmen, die diesen Schutz erhöhen, sind daher zu begrüssen. In Art. 9 Abs. 5 wird vorgeschlagen, dass wenn dem BACS eine Schwachstelle bekannt ist, dieses die Betreiberinnen kritischer Infrastrukturen bereits vor der Behebung oder der Offenlegung über Schwachstellen, die für andere kritische Infrastrukturen eine akute Cyberbedrohung darstellen, informieren kann. Dies sollte nicht als Möglichkeit im Sinne einer Kann-Formulierung gelten, sondern zwingend stattfinden. Nur so können die Betreiberinnen kritischer Infrastrukturen frühzeitig über potenzielle Sicherheitsrisiken informiert werden. Sie können somit rechtzeitig angemessene Massnahmen zum Schutz ihrer Systeme ergreifen. Wie im erläuternden Bericht erwähnt, kann damit ein Beitrag geleistet werden, potenzielle Angriffe auf kritische Infrastrukturen zu verhindern oder abzuschwächen.

Antrag 4: Anpassung in Art. 9 Abs. 5

5 *Hat das BACS Kenntnis von Schwachstellen gemäss Absatz 3,* ~~Es~~ ~~kann~~ *muss* es die Betreiberinnen kritischer Infrastrukturen *innert 72 Stunden* informieren. *Dies* hat ~~bereits~~ vor der Behebung oder Offenlegung über Schwachstellen *zu erfolgen*. *Das BACS soll nach Möglichkeit den Betreiberinnen kritischer Infrastrukturen Empfehlungen zum Umgang mit der Schwachstelle geben.*

Wie bereits in Antrag 3 erwähnt, unterliegt der Informationsaustausch über Cyberangriffe und Cyberbedrohungen bei kritischen Infrastrukturen und betriebskritischen Daten einem besonderen Schutz. Deshalb soll in Artikel 12 auch das Schutzniveau nach oben angepasst werden und das BACS nach höchsten Sicherheitsstandards streben.

Antrag 5: Ergänzung in Art. 12 Abs. 2

2 Das BACS ist für die Sicherheit der Informationssysteme und die Rechtmässigkeit der Bearbeitung der Daten verantwortlich. *Das BACS strebt dabei nach höchsten Sicherheitsstandards.*

Die freiwillige Teilnahme von kritischen Infrastrukturen am Informationsaustausch begrüssen wir. Allerdings sieht der erläuternde Bericht die Registrierung auch für „meldepflichtige Behörden und Organisationen [als] nicht zwingend“. Wir entnehmen hier jedoch, dass die Meldepflicht für Cyberangriffe idealerweise über den gleichen Kanal zu laufen hat. Aus unserer Sicht sollte die Registrierung für die Nutzung des Kommunikationssystems für kritische Infrastrukturen bereits bei Einführung des Informationssicherheitsgesetzes verpflichtend sein. Damit wird sichergestellt, dass ein Cyberangriff einerseits auch auf diesem Weg gemeldet wird und andererseits nicht vergessen wird, weil z.B. eine kritische Infrastruktur (noch) nicht registriert ist. Zudem bedeutet – wie im erläuternden Bericht erwähnt – eine frühzeitige Registrierung eine Zeitersparnis im Falle eines meldepflichtigen Cyberangriffs. Idealerweise gibt es für die Meldung von Cyberangriffen bei kritischen Infrastrukturen nur einen einzigen Informationskanal. Das Ziel sollte es deshalb sein, dass alle meldepflichtigen kritischen Infrastrukturen sich innert 90 Tagen nach Inkrafttreten des Informationssicherheitsgesetzes für den Informationskanal anmelden müssen und Cyberangriffe ausschliesslich auf diesem melden. Die Teilnahme am Informationsaustausch soll jedoch weiterhin freiwillig als zusätzliche Option mit Beratung seitens BACS wählbar sein.

Antrag 6: Anpassungen in Art. 13

1 Die Organisationen und Behörden *gemäss Art. 74b* müssen sich für die *Meldung eines Cyberangriffs für das* Kommunikationssystem~~s~~ registrieren. Sie müssen Änderungen von Angaben unverzüglich melden. *Die Registrierung hat innert 90 Tagen nach Inkrafttreten des Gesetzes zu erfolgen.*

2 Die Registrierung muss mindestens folgende Informationen enthalten: a. Firma, Name oder Bezeichnung und Adresse; b. *Angaben zu einer oder mehreren Kontaktpersonen* ~~Kontaktangaben der gemeldeten Person.~~

3 *Die Teilnahme am Informationsaustausch ist freiwillig.*

Oberstes Ziel des Informationssicherheitsgesetzes sind die frühzeitige Erkennung und die wirksame Bekämpfung von Cyberangriffen durch die Förderung der Zusammenarbeit und des Informationsaustauschs der kritischen Infrastrukturen mit dem BACS und untereinander sowie durch gegenseitige Schulungen und Unterstützung. Insofern besteht schon naturgemäss ein hohes Eigeninteresse der kritischen Infrastrukturen an diesem Austausch. Mit der Teilnahme wird – analog zur Safety-Kultur in der Luftfahrt – eine positive Fehlerkultur gestärkt, die dazu führt, dass gemeinsam aus Fehlern gelernt wird, Prozesse verbessert werden und letztlich die Sicherheit erhöht werden kann. Dabei muss die Datenhoheit weiterhin bei den kritischen Infrastrukturen bleiben. Insofern sollten die kritischen Infrastrukturen nicht nur entscheiden, an wen (neben dem BACS) sie Informationen gemäss Art. 15 liefern, sondern vor allem welche. Beispielsweise unterliegen gewisse Informationen einem erhöhten Schutz und sollten deshalb nur einem sehr eingeschränkten Kreis zugänglich gemacht werden können (closed user group). Wie im erläuternden Bericht erwähnt, soll deshalb der Informationslieferant bestimmen können, wie mit den geteilten Informationen umgegangen wird.

Antrag 7: Art. 15 Abs. 1

1 Registrierte Unternehmen und Behörden übermitteln Informationen dem BACS und bestimmen dabei, ob, *welche* und an wen dieses die Informationen weitergegeben darf, soweit eine Weitergabe der Informationen nicht gesetzlich vorgesehen ist.

Das Kernelement des Informationssicherheitsgesetzes ist die Meldung eines erfolgreichen Cyberangriffs, wenn er die Tatbestände gemäss Art. 74d erfüllt. Dazu zählt mit Blick auf Art. 18 insbesondere die Gefährdung der Funktionsfähigkeit der betroffenen kritischen Infrastruktur. Es ist deshalb zentral, die Verordnung im Sinne des Gesetzesgebers dahingehend zu präzisieren, dass lediglich erfolgreiche Cyberangriffe mit funktionalen Konsequenzen der Meldepflicht unterliegen. Nur so kann sichergestellt werden, dass nicht jede erfolgreiche Phishing-Attacke, die jedoch schadenfrei bleibt, gemeldet werden müsste. Hier gilt es, die Verhältnismässigkeit zu wahren und keinen administrativen Mehraufwand ohne Mehrwert zu generieren. Gleichzeitig gilt es, den Begriff „Systemunterbruch" enger zu fassen. Stand jetzt müsste jeder Systemunterbruch gemeldet werden, zum Beispiel im Zuge von Wartungsarbeiten. Ebenso ist der Begriff „Dritter" einzugrenzen. Auch wenn ein Informatiksystem temporär nicht verfügbar ist, bedeutet dies noch keine systemrelevante Gefährdung der Funktionsfähigkeit der kritischen Infrastruktur. Fällt beispielsweise das GPS eines Taxifahrers am Flughafen aus, hat dies deutlich geringere Konsequenzen, als wenn das GPS für die Flugzeuge ausfällt. Insofern ist auch hier ein Systemunterbruch bei Dritten auf die Systemrelevanz abzuwägen.

Antrag 8: Art. 18 Abs. 1

1 Die Funktionsfähigkeit einer kritischen Infrastruktur gilt *durch einen Cyberangriff* als gefährdet, wenn:

a. *gleichzeitig mehrere* Mitarbeitende oder *systemrelevante* Dritte von *durch den Cyberangriff verursachten* Systemunterbrüchen betroffen sind und diese Auswirkungen auf funktionsrelevante Mittel der kritischen Infrastruktur haben; oder

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

Auch für Artikel 18 Absatz 2 ist eine enger gefasste Definition anzustreben. Der erläuternde Bericht erwähnt den unbefugten Zugriff auf «sensible» Daten. Jedoch findet sich diese Einschränkung im Verordnungstext nicht. Nicht alle geschäftsrelevanten Daten sind auch sensible Daten und nicht alle sensiblen Daten sind für die betroffene kritische Infrastruktur funktionsrelevant. Wenn beispielsweise auf der Homepage der Flughafen Zürich AG die Anzahl Mitarbeitende verändert wird, hat dies keinen Einfluss auf den Betrieb des Flughafens Zürich als kritische Infrastruktur. Hingegen weist eine Manipulation der Software der Gepäcksortieranlage oder anderer systemrelevanter Informatiksysteme ein deutliches Sicherheitsrisiko auf.

Antrag 9: Art. 18 Abs. 2

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

a. *sensible* geschäftsrelevante *und funktionsrelevante* Informationen von Unbefugten verändert oder offengelegt werden; oder

Wie im erläuternden Bericht erwähnt, stellen über einen längeren Zeitraum unentdeckte Cyberangriffe eine ernsthafte Bedrohung für kritische Infrastrukturen dar. Es ist deshalb richtig und wichtig, dass insbesondere diese gemeldet werden müssen. Dabei ist unerheblich, wie lange der Angriff zurückliegt. Für die Sicherheit ist es jedoch entscheidend, dass ein erfolgreicher Angriff zeitnah nach dem Entdecken gemeldet wird. Wir schlagen eine Meldepflicht innert 7 Tagen vor.

Antrag 10: Art. 18 Abs. 3

3 Ein *erfolgreicher* Cyberangriff*, der* ~~gilt als~~ über einen längeren Zeitraum unentdeckt *bleibt*, *muss innerhalb von 7 Tagen gemeldet werden.* ~~wenn der Vorfall mehr als 90 Tage zurückliegt~~.

Gemäss Artikel 18 Absatz 4 sind auch Cyberangriffe verbunden mit Erpressung, Drohung oder Nötigung gegen ehemalige Verantwortliche und Mitarbeitende einer kritischen Infrastruktur von der Verordnung erfasst. Während im öffentlichen Dienst stehende Personen auch nach Beendigung des Amtes öffentliche Personen bleiben, erlischt im privatwirtschaftlichen Umfeld der Zugriff auf Daten und Systeme mit der Beendigung des Arbeitsverhältnisses, so dass ab dann kein direkter Zusammenhang mehr zwischen der Person und der kritischen Infrastruktur besteht. Wir schlagen eine Präzisierung vor, dass als Mitarbeitende nur diejenigen zählen, die über Login-Daten verfügen (inkl. externe Mitarbeitende) bzw. auf der Payroll des Unternehmens.

Antrag 11: Art. 18 Abs. 4

4 Ein Cyberangriff gilt als mit Erpressung, Drohung oder Nötigung verbunden, wenn sich diese Handlungen gegen die meldepflichtige Behörde oder Organisation oder gegen deren Verantwortliche oder Mitarbeitende, einschliesslich *scheidender* ~~ehemaliger~~ Verantwortlicher oder Mitarbeitender, oder gegen für die meldepflichtige Behörde oder Organisation tätige Personen richten.

Als börsenkotierte und privatwirtschaftliche kritische Infrastruktur verfügt die Flughafen Zürich AG über verschiedene Anspruchsgruppen. Bei einem Cyberangriff gilt es in erster Linie die Sicherheit des Flughafens Zürich und des Flugbetriebs sicherzustellen und gleichzeitig geeignete Massnahmen zu treffen, um den Schaden möglichst klein zu halten. In zweiter Instanz gilt es, den Unternehmenswert hochzuhalten. Aus diesem Grund ist es für uns entscheidend, dass die Informationen gemäss Artikel 19 Absatz 2 nicht ohne das Einverständnis der meldenden Stelle an andere Behörden ausserhalb des BACS weiter gemeldet werden. Damit soll verhindert werden, dass polizeiliche Ermittlungs- und Beweissicherungsmassnahmen die Funktionsfähigkeit der kritischen Infrastruktur nicht noch zusätzlich gefährden oder stören. Die Behebung eines Cyberangriffs und die Ergreifung allfälliger schadenminimierender Massnahmen, wie z.B. eine ganze oder teilweise Betriebsunterbrechung bei

Privaten, muss zwingend der kritischen Infrastruktur überlassen werden – diese kann zur Entscheidung Behörden hinzuziehen. Falls nötig, ist dies zu präziseren.

Antrag 12: Art. 19 Abs. 2

2 Sie muss zudem die Information enthalten, ob der Angriff mit Erpressung, Drohung oder Nötigung verbunden war und ob Strafanzeige erstattet wurde. Das BACS gibt diese Informationen nicht ohne Zustimmung der meldepflichtigen Behörde oder Organisation an Strafverfolgungsbehörden und weitere Behörden bekannt.

Gemäss Artikel 19 Absatz 3 Buchstabe a muss die Meldung eines Cyberangriffs die Auswirkungen auf «betroffene Einheiten» enthalten. Der Bezug auf die Einheiten eines Unternehmens erscheint uns aufgrund der vielfältigen Organisationsformen in der Privatwirtschaft und der unterschiedlichen IT-Systeme als nur schwer vergleichbar. Der Betrieb eines Flughafens und einer Bank lassen sich nicht vergleichen, obschon beide in der Einheit «Operations» stattfinden. Wertvoller könnte die damit verbundene Funktion innerhalb der Einheit sein, die eine Vergleichbarkeit erhöht. Zum Beispiel weist eine Gepäcksortieranlage des Flughafens eine Ähnlichkeit mit einer Briefsortieranlage der Post auf, diese Anlagen müssen aber nicht zwingend in derselben Einheit angesiedelt sein.

Antrag 13: Art. 19 Abs. 3

3 Sie muss folgende Informationen zu den Auswirkungen des Cyberangriffs enthalten:

a. betroffene Einheiten *und deren Funktion* der Organisation oder Behörde;

Wie oben erwähnt, soll für meldepflichtige Organisationen der Kommunikationskanal des BACS die einzige Möglichkeit zur Meldung sein. Damit wird sowohl die Datensicherheit gewahrt als auch eine schnelle Verbreitung der Information an die kritischen Infrastrukturen, damit sich diese bestmöglich schützen können. Gleichzeitig soll die Meldung von Cyberangriffen auch nicht meldepflichtigen Organisationen und Behörden offenstehen. In diesem Fall soll die Meldung ausserhalb des Kommunikationskanals möglich sein.

Antrag 14: Art. 19 Abs. 4

4 *Die Meldung hat für Behörden und Organisationen gemäss Art. 74b ISG über das Kommunikationssystem des BACS zu erfolgen. Nicht meldepflichtige Unternehmen können ebenfalls einen Cyberangriff an das BACS melden.* Erfolgt die Meldung nicht über das Kommunikationssystem des BACS, so muss sie zusätzlich folgende Informationen zur meldepflichtigen Behörde oder Organisation enthalten:

Abschliessend möchten wir nochmals hervorheben, dass wir eine Harmonisierung und Koordination der Meldepflicht auf Bundesebene und damit die Förderung des Informationsaustauschs zwischen den

Sektoren sehr begrüssen. Ebenfalls begrüssenswert ist, dass die Meldepflicht wie im erläuternden Bericht zur Vernehmlassung des ISG bereits dargelegt «einen möglichst geringen Mehraufwand» bedeuten soll. Trotz dieser Fortschritte sehen wir uns auch künftig bei einem Cyberangriff mit unterschiedlichen Meldepflichten konfrontiert. Es ist deshalb eine Harmonisierung der Meldepflichten anzustreben, sodass Unternehmen lediglich einen Angriff nur noch an einer Stelle melden müssen. Hier bietet es sich an, dem BACS diese Kompetenz zu übertragen. Gerade bei einem Cyberangriff ist es unerlässlich, die Zeit und Ressourcen für die Abwehr und mitigierende Massnahmen zu bündeln und die Meldepflichten auf ein Minimum zu reduzieren. Mit einer Meldung an das BACS sollen somit automatisch die weiteren Meldeplichten, z.B. solche an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten und an das BAZL, aufgehoben werden. Damit einhergehend ist eine Plicht des BACS als zentrale Koordinationsstelle zur Information der relevanten Bundesstellen nach Eingang einer Meldung in den Verordnungstext aufzunehmen. In der Konsequenz muss zwingend das BACS als Kompetenzzentrum die verschiedenen Anfragen der Behörden koordinieren, sodass einzig das BACS als direkter Ansprechpartner einer von einem Cyberangriff getroffenen kritischen Infrastrukturen fungiert.

Antrag 15: Art. 22

Eine Meldung an das BACS hebt automatisch alle anderen Meldepflichten im Falle eines Cyberangriffs auf. Das BACS informiert nach Eingang einer Meldung die relevanten Bundesstellen und koordiniert die Anfragen der Behörden.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Michael Hofmeier
Leiter Information & Communication Technology

Andrew Karim
Stv. Leiter Public Affairs

Schweizerischer Städteverband
Union des villes suisses
Unione delle città svizzere

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
3003 Bern

Per Mail: ncsc@ncsc.admin.ch

Bern, 10.09.2024

Cybersicherheitsverordnung (CSV)
Vernehmlassung

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Wir danken Ihnen bestens für die Gelegenheit, zur Cybersicherheitsverordnung Stellung nehmen zu können. Der Schweizerische Städteverband vertritt die Städte, städtischen Gemeinden und Agglomerationen in der Schweiz und damit gut drei Viertel der Schweizer Bevölkerung.

Allgemeine Einschätzung

Mit der Änderung des Informationssicherheitsgesetzes vom 29. September 2023 hat das Parlament die Einführung einer Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen beschlossen. Die Meldepflicht soll es dem Bundesamt für Cybersicherheit (BACS) ermöglichen, eine verbesserte Übersicht über Cyberangriffe in der Schweiz zu gewinnen, Betroffene bei der Bewältigung von Cyberangriffen zu unterstützen und Betreiberinnen kritischer Infrastrukturen zu warnen.

Mit der Cybersicherheitsverordnung (CSV) legt der Bundesrat die Ausführungsbestimmungen zu dieser Gesetzesänderung vor. Die Verordnung legt fest, welche Ausnahmen von der Meldepflicht gelten und konkretisiert, welche Cyberangriffe meldepflichtig sind. Zudem wird das Verfahren zur Erfüllung der Meldepflicht definiert. Dadurch wird klar, welche Organisationen und Behörden welche Art von Cyberangriffen wie und innerhalb welcher Frist zu melden haben. Zusätzlich regelt die Verordnung, wie das BACS die sich aus dem ISG ergebenden Aufgaben erfüllen soll und definiert die Strukturen für die strategische Steuerung der Cybersicherheit in der Schweiz.

Die verbindliche Regelung wird von unseren Mitgliedern grundsätzlich begrüsst. Die CSV schafft Transparenz und Klarheit für alle involvierten Stellen (Bund, Kantone, Städte**,** Gemeinden, Wirtschaft und Wissenschaft). Die Verordnung ist bezüglich Qualität und Quantität gut gestaltet und nicht zu umfangreich. Die Ausführungsbestimmungen sind angemessen und ausgewogen gestaltet. Einzig die fehlende Nichtberücksichtigung der Städte und Gemeinden bei der nationalen Cyberstrategie und dem Steuerungsausschuss ist für uns nicht nachvollziehbar.

Monbijoustrasse 8, Postfach, 3001 Bern
Telefon +41 31 356 32 32
info@staedteverband.ch, www.staedteverband.ch

Rückmeldungen zu einzelnen Artikeln der Verordnung

- Art. 2 Abs. 2
  Die nationale Cyberstrategie wird nur in Abstimmung des Bundes mit den Kantonen festgelegt. Der Einbezug der grösseren Städte/Gemeinden fehlt aus unserer Sicht.
- Art. 4
  In der Zusammensetzung des Steuerungsausschusses sind die Städte/Gemeinde nicht vertreten. Ein Einsitz der Städte/Gemeinden im Steuerungsausschuss wäre wünschenswert, um eine umfassende Betrachtung verschiedener Aspekte der Cybersicherheit zu gewährleisten und eine koordinierte Zusammenarbeit zwischen den verschiedenen Akteuren auf nationaler Ebene zu garantieren.
- Art. 16 Abs. 1
  Ist eine Ergänzung der «Allgemeinen Geschäftsbedingungen für IKT-Leistungen» vorgesehen, die von der Digitalen Verwaltung Schweiz DVS bereitgestellt werden und von vielen Verwaltungen für den Abschluss von Verträgen mit Dritten verwendet werden?
- Art. 19
  In welchem Umfang müssen die genannten Informationen von den Behörden bereitgestellt werden und welche Konsequenzen ergeben sich, wenn bestimmte Informationen nicht bekannt sind?

Rückmeldungen zum erläuternden Bericht

- Art. 16 Abs. 1 Bst. c
  Der erläuternde Bericht ist hier eher schwer verständlich formuliert, der letzte Satz im ersten Punkt der Aufzählung scheint zudem nicht vollständig ausformuliert zu sein.
- Art. 19
  Die Übernahme der relevanten Teile des Formulars der FINMA betreffend Kommentare zu Erläuterungen zur CSV wird ausdrücklich begrüsst.
- Art. 19 Abs. 1 Bst. d
  Es stellt sich die Frage, ob hier die Nennung von Angriffsmethoden im Sinne einer Kategorisierung gemeint ist.
- Art. 19 Abs. 3 Bst. b
  Es stellt sich hier die Frage nach dem Unterschied zwischen «hoch» und «schwerwiegend». Allenfalls könnte statt «schwerwiegend» auch «sehr hoch» verwendet werden. Alternativ könnte man auch 3 Stufen verwenden («gering», «mittel», «hoch»).

Wir danken Ihnen für die Berücksichtigung unserer Anliegen.

Schweizerischer Städteverband
Union des villes suisses
Unione delle città svizzere

Freundliche Grüsse
Schweizerischer Städteverband

Präsident	Direktor
Anders Stokholm	Martin Flügel
Stadtpräsident Frauenfeld	

Kopie: Schweizerischer Gemeindeverband

Schweizerischer Gemeindeverband
Association des Communes Suisses
Associazione dei Comuni Svizzeri
Associaziun da las Vischnancas Svizras

Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Bundeshaus Ost
3003 Bern

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

Bern, 10. September 2024

Vernehmlassung über die Cybersicherheitsverordnung (CSV).
Stellungnahme des Schweizerischen Gemeindeverbandes

Sehr geehrte Frau Bundesrätin,
Sehr geehrte Damen und Herren

Mit Schreiben vom 22. Mai 2024 hat das Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport VBS im Auftrag des Bundesrats dem Schweizerischen Gemeindeverband (SGV) das oben erwähnte Geschäft zur Stellungnahme unterbreitet. Für die Gelegenheit, uns aus Sicht der rund 1'500 dem SGV angeschlossenen Gemeinden äussern zu können, danken wir Ihnen bestens.

I. Einleitende Bemerkungen

Mit der Cybersicherheitsverordnung soll die vom Parlament am 29. September 2023 beschlossene Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen im Detail geregelt werden und zusammen mit dem 5. Kapitel des revidierten Informationssicherheitsgesetzes auf den 1. Januar 2025 in Kraft treten. Die Cybersicherheit stellt eine zentrale Herausforderung für Behörden, Wirtschaft und Gesellschaft dar. Da heute praktisch alle Lebensbereiche digital verwaltet werden, sind die Folgen einer erfolgreichen Cyberattacke vielfältig. Sie reichen von finanziellen Schäden über den Verlust vertraulicher Daten bis hin zum Ausfall ganzer Systeme. Der SGV setzt sich seit längerem aktiv ein für die Cybersicherheit in den Gemeinden und weist diese auf die entsprechenden Angebote des BACS resp. des früheren NCSC hin. Der SGV unterstützt die Einführung einer Meldepflicht, weil sie einen Beitrag zur Erhöhung der Cybersicherheit in der Schweiz leistet. Cyberangriffe können so frühzeitig entdeckt, Angriffsmuster analysiert und Betreiberinnen kritischer Infrastrukturen rechtzeitig gewarnt werden. Die vorliegenden Ausführungsbestimmungen zur Meldepflicht sind aus Sicht des SGV grundsätzlich zielführend und bieten eine ausgewogene Balance zwischen den notwendigen Anstrengungen zur Erreichung des angestrebten Zieles und der Beschränkung des bürokratischen Aufwandes.

Kritisch beurteilen wir jedoch den fehlenden Einbezug der dritten föderalen Staatsebene.
Die Gemeinden sind ebenso wie Bund und Kantone von Cyberangriffen betroffen. Zusätzlich sind sie möglicherweise mit anderen Herausforderungen in Zusammenhang mit Cyberangriffen konfrontiert. Eine Koordination über alle Staatsebenen hinweg ist daher unabdingbar. Es ist somit zentral, dass die

Gemeinden resp. die Dachverbände der Gemeinden bei der Erarbeitung der Nationalen Cyberstrategie (NCS) eingebunden werden und Einsitz in den Steuerungsausschuss Nationale Cyberstrategie (StA NCS) erhalten.

II. Bemerkungen zu den einzelnen Bestimmungen

Nationale Cyberstrategie und Steuerungsausschuss (Art. 2 – 5)

Der SGV begrüsst, dass eine Nationale Cyberstrategie definiert und ein Steuerungsausschuss (StA NCS) für deren Umsetzung vom Bundesrat eingesetzt werden soll (Art. 3. Abs.1). Dies verleiht dem Gremium das notwendige politische Gewicht. Auch begrüsst er die breite Beteiligung verschiedenster Akteure, welche im StA NCS angestrebt wird. Für eine umfassende Betrachtung der verschiedenen Aspekte der Cybersicherheit und der angestrebten koordinierten Zusammenarbeit sind neben den Kantonen aber auch Vertretungen der kommunalen Ebene einzubeziehen. Der SGV beantragt daher folgenden Änderungen im Verordnungstext:

Nationale Cyberstrategie
Art. 2 Abs. 2
Sie wird in Abstimmung mit den Kantonen und Vertretungen der Gemeinden oder deren Dachorganisationen festgelegt.

Zusammensetzung des StA NCS
Art. 4 Abs. 1
Der StA NCS setzt sich aus Vertreterinnen und Vertretern der Departemente, der Bundeskanzlei, der Kantone, der Gemeinden oder deren Dachorganisationen, der Wirtschaft, der Gesellschaft und der Hochschulen zusammen.

Art. 4 Abs. 2
Der Bundesrat bestimmt alle fünf Jahre die Mitglieder des StA NCS, mit Ausnahme der Vertreterinnen und Vertreter der Kantone; diese werden von der Konferenz der Kantonsregierungen bestimmt, sowie mit Ausnahme der Vertreterinnen und Vertreter der Gemeinden; diese werden von den Dachorganisationen der Gemeinden bestimmt.

Informationsaustausch (Art. 11 - 15)

Ein sicherer Informationsaustausch zu Cybervorfällen und -bedrohungen ist wichtig, um deren Zahl und Auswirkungen zu verringen. Der SGV begrüsst daher ausdrücklich die Bestrebungen des Bundes, Erkenntnisse aus anderen Organisationen und Behörden rasch weiterleiten zu können. Unabdingbar ist dabei, dass die Registrierung für die Teilnahme am Informationsaustausch möglichst einfach und unbürokratisch möglich ist und der Zugang zum Informationsaustausch in der Praxis unkompliziert ist. Dies ermöglicht es allen Gemeinden, daran teilzunehmen und von den Erkenntnissen zu profitieren. Der SGV ersucht das BACS daher, in der praktischen Umsetzung der Verordnung für eine leichte Zugänglichkeit zu sorgen.
Meldepflicht (Art. 16)

Holzikofenweg 8 | Postfach | 3001 Bern | T +41 (0)31 380 70 00 | verband@chgemeinden.ch | www.chgemeinden.ch

Der SGV begrüsst es grundsätzlich, dass Gemeinden mit weniger als 1000 Einwohnern von der Meldepflicht für Cyberangriffe ausgenommen werden sollen (Abs. 1 lit. a). Damit wird der bürokratische Aufwand für Gemeinden, welche nicht über die entsprechenden Ressourcen verfügen, verringert. Unabhängig davon ist aber sicherzustellen, dass alle Gemeinden Cybervorfälle melden können und zeitnah technische Unterstützung vom BACS erhalten, wenn sie dies wollen, resp. als notwendig erachten. Wichtig dabei ist, dass es eine zentrale Anlaufstelle für die Meldung von Cybervorfällen gibt. Es ist denkbar, dass manche Vorfälle für Gemeinden spezifische Herausforderungen mit sich bringen, beispielsweise für Schul- oder Sozialbehörden oder bei der Durchführung von Abstimmungen und Wahlen. Es ist daher wichtig, dass Cyberangriffe unbürokratisch gemeldet werden können. Die entsprechenden Formularentwürfe, welche dieser Vernehmlassung beigefügt sind, gehen aus unserer Sicht in die richtige Richtung. Der SGV wird seine Mitgliedsgemeinden unabhängig ihrer Grösse dazu ermutigen, Cyberangriffe zu melden und das BACS um technische Unterstützung zu ersuchen, wenn sie dies als notwendig erachten.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen.

Freundliche Grüsse

Schweizerischer Gemeindeverband

Präsident Direktorin

Mathias Zopfi
Ständerat

Claudia Kratochvil-Hametner

Kopie an:

- Schweizerischer Städteverband SSV
- Schweizerische Arbeitsgemeinschaft für die Berggebiete SAB

Holzikofenweg 8 | Postfach | 3001 Bern | T +41 (0)31 380 70 00 | verband@chgemeinden.ch | www.chgemeinden.ch

Per Mail: ncsc@ncsc.admin.ch

Bern, 11. September 2024

Vernehmlassung: Erlass der Cybersicherheitsverordnung (CSV)

Sehr geehrte Damen und Herren

Sie haben uns eingeladen, zur obengenannten Vernehmlassungsvorlage Stellung zu nehmen. Für diese Gelegenheit zur Meinungsäusserung danken wir Ihnen bestens.

Die Cybersicherheitsverordnung (CSV) erlässt die Ausführungsbestimmungen zur Änderung des Informationssicherheitsgesetzes vom 29. September 2023, welche eine Meldepflicht für Cyberangriffe auf kritische Infrastrukturen eingeführt hatte. Die Verordnung enthält Bestimmungen zur Nationalen Cyberstrategie und zu deren Steuerungsausschuss, zu den Aufgaben des Bundesamtes für Cybersicherheit (BACS), zum Informationsaustausch des BACS mit Behörden und Organisationen zum Schutz vor Cybervorfällen und Cyberbedrohungen sowie zur Meldepflicht für Cyberangriffe.

Die Mitte will starke nationale Strukturen im Kampf gegen Cyberangriffe

Die Schweiz verzeichnet eine stetige Zunahme an Cyberangriffen. Sowohl die Anzahl der Vorfälle wie auch das Schadensausmass nehmen ein besorgniserregendes Ausmass an. Angreifende machen dabei weder vor Kantons- noch vor Landesgrenzen halt. Es ist daher aus Sicht der Mitte unerlässlich, auf Bundesebene wirksame Strukturen zu etablieren, welche dieser Entwicklung angemessen entgegentreten können. Die Cybersicherheitsverordnung, welche sich der Umsetzung dieses Erfordernisses widmet, wird deshalb von der Mitte grundsätzlich unterstützt.

Die Aufgaben des Bundesamtes für Cybersicherheit in Bezug auf die Offenlegung von Schwachstellen, der Behördenunterstützung oder der Bereitstellung des sicheren Kommunikationssystems erachtet Die Mitte als angemessen und für die Zielerreichung notwendig.

Die Mitte begrüsst weiter die breite Zusammensetzung des Steuerungsausschusses für die Nationale Cyberstrategie (NCS), welche eine landesweit koordinierte Problembehandlung ermöglichen will. In Bezug auf die NCS fehlt der Mitte jedoch der Aspekt der ständigen Antizipation von Risiken technischer Evolutionen und die daraus abgeleitete kontinuierliche Anpassung der Strategie. Die rasante Entwicklung im Cyberbereich – bspw. im Hinblick auf die Künstliche Intelligenz oder die Fortschritte beim Quantencomputing – bedingen eine adaptive Kultur. Eine Revision der NCS «mindestens alle fünf Jahre» (Art. 5 Bst. a) wird diesem Anspruch aus Sicht der Mitte nicht genügend gerecht.

Bezüglich der Meldepflicht für Cyberangriffe hält Die Mitte fest, dass der Adressatenkreis eine ausreichende Grösse haben muss, damit die Meldepflicht ihre volle Wirkung entfalten kann. Die Mitte würde es daher begrüssen, wenn die Schwellenwerte für die Ausnahmen innerhalb eines geeigneten Zeitintervalls vom Bundesrat überprüft und gegebenenfalls mit Bezug auf neue Gegebenheiten und Erkenntnisse aktualisiert würden.

Die Mitte
Schweiz

Seilerstrasse 8a
Postfach
CH-3001 Bern

T 031 357 33 33
info@die-mitte.ch
die-mitte.ch

Wir danken Ihnen für die Möglichkeit zur Stellungnahme und verbleiben mit freundlichen Grüssen.

Die Mitte

Sig. Gerhard Pfister
Präsident Die Mitte Schweiz

Sig. Gianna Luzio
Generalsekretärin Die Mitte Schweiz

KANTON AARGAU

REGIERUNGSRAT

Regierungsgebäude, 5001 Aarau
Telefon zentral 062 835 12 40
Fax 062 835 12 50
regierungsrat@ag.ch
www.ag.ch/regierungsrat

Per E-Mail
Bundesamt für Cybersicherheit
ncsc@ncsc.admin.ch

11. September 2024

Cybersicherheitsverordnung (CSV); Vernehmlassung

Sehr geehrte Damen und Herren

Die Kantonsregierungen wurden mit Schreiben vom 22. Mai 2024 eingeladen, im Rahmen des Vernehmlassungsverfahrens zur Cybersicherheitsverordnung (CSV) Stellung zu nehmen. Der Regierungsrat des Kantons Aargau bedankt sich für diese Möglichkeit.

Der Regierungsrat stimmt dem Entwurf zur Verordnung über die Cybersicherheit (Cybersicherheitsverordnung, CSV) unter Vorbehalt der unten vorgebrachten Anmerkungen zu. Die Verordnung unterstützt den kantonalen Auftrag zur Erhöhung der Resilienz und die Prozesse der Verteidigung auf der Ebene der Cybersicherheit. Der Kanton Aargau wird von den in der Verordnung vorgesehen Regelungen und Prozessen profitieren können.

Anmerkungen zu Art. 16 CSV:

Art. 16 Abs. 1 Bst. a

Der Regierungsrat erachtet eine Ausnahme von der Meldepflicht aufgrund einer kleinen Wohnbevölkerung als nicht sinnvoll. Die Begründung, dass der Aufwand für kleine Gemeinden höher ist, ist aufgrund des marginalen Aufwands nicht nachvollziehbar und steht der Sinnhaftigkeit der in Art. 18 aufgelisteten Kriterien zur Meldepflicht entgegen.

Die Gründe für die Meldepflicht haben für den Regierungsrat unabhängig der Grösse der Gemeinde oder der kritischen Infrastruktur dieselben Auswirkungen. Insbesondere der beabsichtigte Effekt der Frühwarnung ist wichtig, damit zuständige Behörden einen Vorfall nicht erst aus den Medien erfahren und frühzeitig Gegenmassnahmen wie Monitoring initiieren können. Kleinere Gemeinden sind gegenüber Cyberangriffen aufgrund ihrer geringeren Abwehrressourcen exponierter und stellen damit eine grössere Gefahr für die kantonale Infrastruktur sowie diejenige des Bundes dar. Darüber hinaus sind die Daten der Anzahl Einwohnerinnen und Einwohner von mehr als 1'000 nicht weniger sensitiv als diejenigen geringer 1'000.

Wir danken Ihnen für die Berücksichtigung unserer Vernehmlassung.

Freundliche Grüsse

Im Namen des Regierungsrats

Dr. Markus Dieth	Joana Filippi
Landammann	Staatsschreiberin

Regierungsrat des Kantons Basel-Stadt

Rathaus, Marktplatz 9
CH-4001 Basel

Tel: +41 61 267 85 62
E-Mail: staatskanzlei@bs.ch
www.regierungsrat.bs.ch

per Email an: ncsc@ncsc.admin.ch

Basel, den 10. September 2024

P240734

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS; Cybersicherheitsverordnung (CSV); Vernehmlassung; Stellungnahme des Kantons Basel-Stadt

Sehr geehrte Damen und Herren

Mit Schreiben vom 22. Mai 2024 haben Sie uns die Vernehmlassungsunterlagen zur Cybersicherheitsverordnung (CSV) zu kommen lassen. Wir danken für die Gelegenheit zur Stellungnahme und teilen gerne mit, dass der Kanton Basel-Stadt die Verordnung begrüsst und keine Einbringen hat.

Wir danken für die Kenntnisnahme. Für Fragen steht Ihnen Miriam Gantner, akademische Mitarbeiterin des Finanzdepartementes, miriam.gantner@bs.ch, Tel. 061 267 67 08, gerne zur Verfügung.

Freundliche Grüsse
Im Namen des Regierungsrates des Kantons Basel-Stadt

Dr. Conradin Cramer
Regierungspräsident

Barbara Schüpbach-Guggenbühl
Staatsschreiberin

Kanton Bern
Canton de Berne

Regierungsrat

Postgasse 68
Postfach
3000 Bern 8
info.regierungsrat@be.ch
www.be.ch/rr

Staatskanzlei, Postfach, 3000 Bern 8

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport (VBS)
Per E-Mail (PDF/Word) an: ncsc@ncsc.admin.ch

11. September 2024

Unser Zeichen: 2024.FINGS.141

RRB Nr.: 932/2024
Direktion: Finanzdirektion
Klassifizierung: Nicht klassifiziert

Vernehmlassung zur Cybersicherheitsverordnung (CSV).
Stellungnahme des Kantons Bern

Sehr geehrte Frau Bundespräsidentin
Sehr geehrte Damen und Herren

Der Regierungsrat des Kantons Bern dankt Ihnen für die Gelegenheit zur Stellungnahme zu dieser Vorlage.

1. Grundsätzliches

Wir unterstützen weiterhin die vom Parlament beschlossene Ergänzung des Informationssicherheitsgesetzes (ISG) betreffend die Meldepflichten kritischer Infrastrukturen sowie anderer Organisationen und Behörden. Täglich zeigt sich, dass Cyberangriffe zu den grössten Bedrohungen der Sicherheit und der Wirtschaft der Schweiz gehören. Wir begrüssen es daher, dass der Bund beim Schutz des Landes vor dieser Bedrohung die Führung übernommen hat und die Betroffenen bei der Bewältigung dieses Risikos unterstützt.

Mit unserer damaligen Stellungnahme vom 16. März 2022 zum Entwurf des ISG stellten wir aber fest, dass die Liste der kritischen Infrastrukturen in Art. 74b E-ISG sehr weit gefasst ist: Neben Infrastrukturunternehmen im klassischen Sinne umfasst sie auch alle Kantons- und Gemeindebehörden, Hochschulen, Spitäler sowie eine Vielzahl von Privatunternehmen, deren Leistungen von nationaler Bedeutung sind. Diese breite Meldepflicht ist u.E. zwar gerechtfertigt, weil eine wirksame Bekämpfung von Cyberangriffen ihre frühe Erkennung voraussetzt. Wir erwarteten aber, dass der Bundesrat von seiner Kompetenz zum Erlass von Ausnahmen von der Meldepflicht (Art. 74c EISG) so Gebrauch macht, dass der Aufwand für die Meldepflicht in einer nationalen Gesamtsicht verhältnismässig bleibt.

Mit der nun vorgelegten Verordnung hat der Bundesrat dieses Anliegen aufgenommen und sachgerecht umgesetzt.

So sind nach Art. 16 Abs. 1 Bst. a E-CSV insbesondere auch die Gemeinden mit weniger als 1'000 ständigen Einwohnerinnen und Einwohnern – inkl. deren Betriebe zur Ver- und Entsorgung – von der Meldepflicht ausgenommen. Zwar sind insbesondere solche kleinen Verwaltungseinheiten beliebte Ziele von Cyberangriffen. Das Schadenspotenzial jedoch bleibt einigermassen begrenzt, obwohl auch kleine Gemeinden (inkl. Kirch- und Burgergemeinden) des Kantons Bern an dessen Netzwerk angeschlossen sind.

Ebenso begrüssen wir die genaue Beschreibung der meldepflichtigen Vorfälle sowie des Inhalts der Meldungen in Art. 18 ff. E-CSV, welche uns auch als Grundlage für die vertraglichen Meldepflichten unserer Auftragsdatenbearbeiter dienen werden.

Im Einzelnen bitten wir Sie, die nachfolgenden Anträge zu berücksichtigen.

2. Anträge

2.1 Antrag zu Art. 1 Bst. b, Aufgaben des BACS

Die CSV regelt nicht die Aufgaben des BACS schlechthin, sondern nur jene im Rahmen dieser Verordnung. Die generellen Aufgaben sind in Art. 43 ISV geregelt.

Dies ist zu präzisieren.

2.2 Antrag zu Art. 9 Abs. 1, Koordinierte Offenlegung von Schwachstellen

Der Absatz ist wie folgt zu formulieren, analog zum Titel des Artikels:

«Das BACS sorgt für die koordinierte Offenlegung von Schwachstellen ...».

2.3 Antrag zu Art. 9 Abs. 3, Information vor Behebung oder Veröffentlichung

Zur besseren Verständlichkeit ist der Absatz wie folgt zu formulieren (in Anlehnung an den Erläuternden Bericht):

«Ist dem BACS eine Schwachstelle bekannt, die für einzelne kritische Infrastrukturen eine akute Cyberbedrohung darstellt, informiert es umgehende deren Betreiberinnen, noch bevor die Schwachstelle veröffentlicht oder behoben wurde.».

2.4 Anträge zu Art. 11 und 12 E-CSV

2.4.1 Verdeutlichung der Abgrenzung der Systeme nach Art. 11 und Art. 12 E-CSV

Der Zweck und der Unterschied zwischen dem Kommunikationssystem für den sicheren Informationsaustausch (Art. 11 E-CSV) und dem Informationssystem für den automatischen Austausch (Art. 12 E-CSV) ist in der Verordnung zu verdeutlichen.

Begründung:

Weder aus den Normen noch aus dem Erläuternden Bericht geht die Abgrenzung beider Systeme, die unterschiedlichen Nutzungsvorgaben und Zwecke klar verständlich hervor.

2.4.2 Korrekter und vollständiger Gesetzesverweis in Art. 11 E-CSV

Der Gesetzesverweis in Klammer ist anzupassen:

«Zugang zum Kommunikationssystem des BACS für den sicheren Informationsaustausch (Art.~~ikel~~ 74 Abs. 2 Bst.~~uchstabe~~ a ISG) haben Organisationen und Behörden mit Sitz in der Schweiz.».

2.4.3 Registrierung

Den gemäss Art. 74b ISG meldepflichtigen Organisationen und Behörden sowie Betreiberinnen kritischer Infrastrukturen ist eine Registrierungspflicht auf dem Kommunikationssystem für den sicheren Informationsaustausch bzw. den Informationssystemen für den automatischen Austausch aufzuerlegen.

Begründung:

Den in Art. 74b ISG genannten Meldepflichtigen ist zuzumuten, dass sie aufgrund ihrer Bedeutung ihren Melde- und Austauschpflichten in standardisierter und kontrollierter Form nachkommen. Dies vereinfacht einerseits die Arbeit des BACS und hilft den Meldepflichtigen beim Erfüllen ihrer Aufgaben. Dies wiederum entlastet auch die kantonalen Sicherheitsorgane, da auch sie mit weniger Fragen zur Meldepflicht konfrontiert sein werden.

Zudem wird damit auch namentlich klargestellt, welches Organ bzw. welche Person die Meldepflichtigen befugt und – ausschliesslich – verantwortlich für das Meldewesen ist. Auch hiermit wird einerseits dem BACS geholfen, indem sich eine Meldepraxis pro Meldepflichtigen etablieren kann. Und andererseits hilft dies den Meldepflichtigen, das unkoordinierte Absetzen von Meldungen zu vermeiden.

2.5 Antrag zu Art. 16 E-CSV, Ausnahmen von der Meldepflicht

Abs. 1 ist wie folgt zu ergänzen:

Die folgenden Behörden, Organisationen und Betreiberinnen von kritischen Infrastrukturen sind unter den nachstehenden Voraussetzungen von der Meldepflicht ausgenommen:

Begründung

Sowohl das ISG als auch die E-CSV unterscheiden zwischen Betreiberinnen kritischer Infrastrukturen sowie Behörden und Organisationen. Nicht jede Betreiberin einer kritischen Infrastruktur ist eine Behörde oder Organisation und umgekehrt. Art. 74b ISG bezeichnet unabhängig davon einfach die Meldepflichtigen, Art. 16 E-CSV die davon Ausgenommenen. Die Ergänzung stellt zudem klar, dass grundsätzlich alle Behörden von der Meldepflicht erfasst sind, unabhängig davon, ob sie kritische Infrastrukturen betreiben.

2.6 Anträge zu Art. 18 E-CSV, Zu meldende Cyberangriffe

2.6.1 Absatz 4, Erpressung, Drohung oder Nötigung

Antrag 1

Entweder ist die Meldepflicht bei Erpressung, Drohung oder Nötigung direkt auf die ehemaligen Verantwortlichen oder Mitarbeitenden der Meldepflichtigen auszudehnen, oder auf diese Personengruppe ist ganz zu verzichten.

Begründung

Wir können uns nicht vorstellen, wie eine meldepflichtige Behörde ihre Pflicht zur Meldung von Erpressungen, Drohungen oder Nötigungen gegen ehemalige Verantwortliche oder Mitarbeitende wahrnehmen kann. Dies funktioniert nur, wenn die Ehemaligen von sich aus aktiv werden und den Meldepflichtigen über ihre Bedrohung Meldung erstatten. Dieser Umweg ist jedoch zu vermeiden, so dass sie entweder selbst dem BACS Meldung erstatten oder aber dieses auf solche Meldungen verzichtet.

Antrag 2

Es ist an dieser Stelle der E-CSV (oder andernorts) der Informationsaustausch mit den Strafverfolgungsbehörden des Bundes und der Kantone bei Verdacht auf ein Offizialdelikt verbindlich zu regeln. Dabei sind auch der Abgrenzung zwischen der Cyberabwehr (grundsätzlich Bund) und der Cyberstrafverfolgung (grundsätzlich Kantone) Rechnung zu tragen.

Begründung

Es ist davon auszugehen, dass die Meldepflichtigen aufgrund des recht einfachen Meldewesens viel eher eine Meldung beim BACS als eine Anzeige bei der Polizei oder der Staatsanwaltschaft deponieren. Das BACS verfügt zudem meistens über weitergehende Informationen, so dass klar sein muss, dass dieses bei Verdacht auf ein Offizialdelikt bei der zuständigen Strafverfolgungsbehörde Anzeige machen muss.

2.7 Antrag zu Art. 19, Inhalt der Meldung

Abs. 1 Bst. e: Angaben zum ~~Verursacher~~ Angreifer.

Begründung:

In den Buchstaben a bis d ist konsequent vom «Angriff» die Rede, der von einem Angreifer durchgeführt wird.

Der Regierungsrat dankt Ihnen für die Berücksichtigung seiner Anliegen.

Freundliche Grüsse

Im Namen des Regierungsrates

Evi Allemann
Regierungspräsidentin

Christoph Auer
Staatsschreiber

Sozialdemokratische Partei der Schweiz

Zentralsekretariat
Theaterplatz 4
3011 Berne

Tel. 031 329 69 69
Fax 031 329 69 70

info@spschweiz.ch

Eidgenössisches Departement für
Verteidigung, Bevölkerungsschutz und Sport
(VBS)

Per Mail an: ncsc@ncsc.admin.ch

11. September 2024

SP-Stellungnahme zur Cybersicherheitsverordnung

Sehr geehrte Frau Bundespräsidentin Amherd,
sehr geehrte Damen und Herren,

Wir bedanken uns für die Gelegenheit zur Stellungnahme, die wir gerne nutzen.

Die SP Schweiz begrüsst die Einführung der Cybersicherheitsverordnung. Wir unterstützen die präzise Regelung der Meldepflicht für Cyberangriffe auf kritische Infrastrukturen und die klare Definition der Aufgaben des Bundesamtes für Cybersicherheit (BACS). Diese Massnahmen sind entscheidend, um die Sicherheit und Stabilität unserer kritischen Infrastrukturen zu gewährleisten und die Resilienz der Schweiz gegenüber Cyberbedrohungen zu stärken. Die Verordnung stellt sicher, dass relevante Informationen zeitnah ausgetauscht und Schutzmassnahmen effektiv koordiniert werden können. Die SP Schweiz sieht dies als wichtigen Schritt zur Erhöhung der nationalen Cybersicherheit und zur Verbesserung des Schutzes unserer Gesellschaft vor digitalen Risiken.

Insbesondere begrüssen wir die Regelung in Art. 9 Abs. 1: „Das BACS sorgt für die koordinierte Offenlegung der Schwachstellen nach international anerkannten Standards.» Diese Praxisänderung stellt eine klare Verbesserung im Vergleich zum Status Quo dar.

Wir danken Ihnen, geschätzte Damen und Herren, für die Berücksichtigung unserer Anliegen und verbleiben mit freundlichen Grüssen

Sozialdemokratische Partei der Schweiz

Mattea Meyer
Co-Präsidentin

Cédric Wermuth
Co-Präsident

Severin Meier
Politischer Fachreferent

-

Sozialdemokratische Partei der Schweiz
Theaterplatz 4
Case postale · 3001 Berne
Tel. 031 329 69 69
Fax 031 329 69 70
info@spschweiz.ch
www.spschweiz.ch

KANTON NIDWALDEN
LANDAMMANN UND REGIERUNGSRAT
Dorfplatz 2, Postfach 1246, 6371 Stans
Telefon 041 618 79 02, www.nw.ch

CH-6371 Stans, Dorfplatz 2, Postfach 1246, STK

PER E-MAIL
Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS
Frau Bundespräsidentin Viola Amherd
Bundeshaus Ost
3003 Bern

Telefon 041 618 79 02
staatskanzlei@nw.ch
Stans, 10. September 2024

Cybersicherheitsverordnung (CSV). Stellungnahme

Sehr geehrte Frau Bundespräsidentin

Mit Schreiben vom 22. Mai 2024 eröffnete das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport VBS unter anderem bei den Kantonen das Vernehmlassungsverfahren in Sachen Cybersicherheitsverordnung (CSV). Für die Möglichkeit zur Stellungnahme bedanken wir uns.

Der Regierungsrat des Kantons Nidwalden befürwortet die Verordnung ohne Vorbehalte.

1 Einleitung

Der Regierungsrat des Kantons Nidwalden begrüsst ausdrücklich die Einführung der Verordnung über die Cybersicherheit (CSV), wie sie vom Bundesrat vorgeschlagen wird. Diese Verordnung stellt einen wesentlichen Schritt dar, um die nationale Sicherheit und die Widerstandsfähigkeit gegenüber Cyberbedrohungen zu stärken. Als Kanton, der die Bedeutung der Cybersicherheit in unserer zunehmend digitalisierten Welt erkennt, sehen wir die Notwendigkeit einer starken und koordinierten Antwort auf die Herausforderungen im Cyberraum.

2 Aufgaben des Bundesamtes für Cybersicherheit (BACS)

Wir unterstützen die präzise Definition der Rollen und Aufgaben des Bundesamtes für Cybersicherheit (BACS). Durch die klare Zuweisung von Verantwortlichkeiten und Befugnissen an das BACS wird eine effiziente und zielgerichtete Reaktion auf Cyberbedrohungen ermöglicht. Dies trägt wesentlich dazu bei, das Vertrauen der Bürger und Unternehmen in die digitale Infrastruktur unseres Landes zu stärken.
Die klaren Zuständigkeiten und Aufgaben des BACS, wie sie in der Verordnung beschrieben sind, tragen wesentlich zur Stärkung der nationalen Cybersicherheit bei. Wir begrüssen die technische Expertise und die koordinierende Rolle des BACS, insbesondere bei der Unterstützung von Behörden und Betreibern kritischer Infrastrukturen. Dies ermöglicht eine

schnelle und gezielte Reaktion auf Cybervorfälle und verbessert die Widerstandsfähigkeit gegenüber Bedrohungen.

3 Meldepflicht für Cyberangriffe

Die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen ist ein wichtiger Schritt zur Erhöhung der Transparenz und Reaktionsfähigkeit. Der Kanton Nidwalden unterstützt diese Massnahme, da sie dazu beiträgt, frühzeitig auf Bedrohungen zu reagieren und die Sicherheit der gesamten Infrastruktur zu gewährleisten. Die klare Definition der Meldeprozesse und Fristen stellt sicher, dass Informationen schnell und effizient weitergeleitet werden.

4 Informationsaustausch und Kooperation

Die vorgeschlagene nationale Cyberstrategie und der entsprechende Steuerungsausschuss bieten eine hervorragende Plattform für die Zusammenarbeit zwischen Bund, Kantonen und weiteren relevanten Akteuren. Wir schätzten insbesondere die integrative Gestaltung des Ausschusses, der sicherstellt, dass auch die Kantone aktiv an der Entwicklung und Implementierung der Strategie beteiligt sind. Diese kooperative Herangehensweise ist entscheidend, um eine umfassende und effektive Umsetzung der nationalen Cyberstrategie zu gewährleisten.

5 Fazit

Der Kanton Nidwalden unterstützt die Massnahmen der Cybersicherheitsverordnung in vollem Umfang. Wir sind überzeugt, dass die Verordnung die Sicherheit und Resilienz der Schweiz im Cyberraum deutlich stärken wird.

Der Regierungsrat Nidwalden bedankt sich für die Möglichkeit zur Stellungnahme und spricht sich für die Änderung der Cybersicherheitsverordnung (CSV) aus.

Freundliche Grüsse
NAMENS DES REGIERUNGSRATES

Res Schmid	lic. iur. Armin Eberli
Landammann	Landschreiber

Geht an:
- aemterkonsultation-uepf@isc-ejpd.admin.ch

UZH / UNIL

Consultation 2024/35 : adoption de l'Ordonnance sur la cybersécurité (OCyS)

Dans ce rapport, des membres du projet *L'éthique et le droit pour promouvoir la confiance en la cybersécurité* (projet PNR 77 n°197425) transmettent leur prise de position concernant la consultation 2024/35 relative à l'adoption de l'ordonnance sur la cybersécurité. Le projet fait partie du programme national de recherche 77 *transformation numérique*.

Dieser Bericht beinhaltet die Überlegungen des Teams des Projekts *Mit Ethik und Recht das Vertrauen in die Cybersicherheit fördern* (Projekt NFP 77 Nr°197425) zur Vernehmlassung 202024/35 "Erlass der Cybersicherheitsverordnung (CSV)". Das Projekt ist Teil des Nationalen Forschungsprogramms 77 *Digitale Transformation*.

Version: Version du 12 septembre 2024 (version finale).

Auteurs : Pauline Meyer et Sylvain Métille

Distribution : Département fédéral de la défense, de la protection de la population et des sports / Par courriel : ncsc@ncsc.admin.ch

Prise de position

Tout d'abord, l'adoption de l'Ordonnance sur la cybersécurité (OCyS) est bienvenue et nécessaire. En effet, la Loi sur la sécurité de l'information au sein de la Confédération (Loi sur la sécurité de l'information, LSI) constitue la loi principale pour la cybersécurité en Suisse et plusieurs dispositions de la version révisée de la loi nécessitent d'être précisées dans une ordonnance. En outre, plusieurs dispositions figurant dans l'ancienne Ordonnance sur la protection contre les cyberrisques dans l'administration fédérale (Ordonnance sur les cyberrisques, aOPCy), abrogée lors de l'entrée en vigueur de la LSI, ne figuraient plus dans le cadre légal.

De manière générale :

- On peut regretter l'absence d'une définition légale de la cybersécurité.
- Nous saluons en revanche la clarification de différents aspects de la LSI dans l'OCyS, à l'instar des exemptions de l'obligation de signaler les cyberattaques ou de la pratique de l'OFCS, notamment concernant la priorité dans les affaires l'occupant.

Concernant ensuite la section 2 P-OCyS :

- Art. 5 P-OCyS : il est judicieux d'ajouter à la liste de compétences du Comité de pilotage de la Cyberstratégie nationale (CP CSN) que ce dernier est compétent pour veiller à la cohérence de la CSN et de sa mise en œuvre. Cette tâche se concrétise d'une part avec la compétence du CP CSN de veiller à ce que les différents acteurs impliqués dans la CSN adoptent une approche coordonnée dans la mise en œuvre des mesures prévues dans la stratégie. D'autre part, il doit veiller à ce que la CSN et sa mise en œuvre soient coordonnées des autres stratégies nationales

connexes, à l'instar de la stratégie nationale de protection des infrastructures critiques. L'art. 9 al. 4 aOPCy, qui prévoyait les tâches du Comité de pilotage de la stratégie nationale de protection de la Suisse contre les cyberrisques (CP SNPC) prévoyait ces tâches. Si ces informations ne figurent pas dans l'ordonnance, elles devraient à tout le moins être présentes dans le rapport explicatif.

- Il est également judicieux de clarifier l'organigramme de l'OFCS ainsi que son statut. Dans la mesure où le mandat de GovCERT est précisé dans l'ordonnance, il convient de se poser la question de savoir si d'autres services devraient voir leurs compétences spécifiées dans l'ordonnance.

Au sujet de la section 3 :

- Art. 9 P-OCyS : un alinéa devrait être ajouté pour concrétiser les conséquences lorsqu'un fabricant n'élimine pas la vulnérabilité dans le délai fixé (en particulier concernant la transmission d'informations par l'OFCS dans le cadre des sanctions relatives aux marchés publics).

Pour la section 4 :

- Art. 11 P-OCyS : il n'est pas clair si toute autorité et organisation dont le siège est en Suisse a accès au système de communication de l'OFCS ou si seules les infrastructures critiques sont concernées. Dans la mesure où un renvoi est effectué à l'art. 74 al. 2 let. a LSI, il semble s'agir uniquement des exploitants d'infrastructures critiques. Cependant, l'art. 12 P-OCyS mentionne expressément la notion d'exploitants d'infrastructures critiques. Partant, la mention explicite d'exploitants d'infrastructures critiques devrait aussi figurer à l'art. 11 P-OCyS si seuls ces derniers sont concernés. Si la volonté est de permettre également à d'autres organisations (non critiques) d'avoir accès à ce système, le renvoi à l'art. 74 LSI au sein de la disposition est incorrect.
- Art 15 P-OCyS :
    - Art. 15 al. 1 P-OCyS : dans la mesure où le commentaire de l'OCyS renvoie au Protocole TLP, la disposition devrait davantage préciser que les entreprises et les autorités transmettant des informations doivent indiquer si et à quelles catégories de destinataires elles peuvent être retransmises, afin d'éviter aux organisations la charge de lister précisément et, à la place, que celles-ci listent des catégories en se basant sur le Protocole TLP.
    - Art. 15 al. 2 P-OCyS : le fait que l'OFCS décide de la publication d'informations risque d'entrer en conflit avec l'art. 15 al. 1 P-OCyS, selon lequel les entreprises et autorités enregistrées lui indiquent si et à qui les informations peuvent être transmises. Ce point devrait donc être clarifié dans l'ordonnance. La disposition devrait en outre préciser que l'OFCS ne peut publier ces informations que lorsque c'est nécessaire pour la protection des infrastructures critiques ou de la Suisse contre les cybermenaces.

Pour la section 5 :

- Art- 17 P-OCyS : la formulation du titre de la disposition manque de clarté du moins en français par l'utilisation du terme "documenter". Une autre formulation serait préférable, à l'instar de "Obligation de mettre à disposition des informations", "Obligation de collaborer" ou encore "Obligation d'information", avec un texte de disposition prévoyant d'une part que les informations pertinentes à l'assujettissement doivent être collectées et conservées par les organisations et d'autre part qu'elles doivent être transmises à l'OFCS sur sa demande pour fournir des informations quant à l'assujettissement de l'organisation à l'obligation de signaler les cyberattaques.

- Art. 18 P-OCyS :
    - les différents alinéas ne mentionnent pas de termes à l'instar de "notamment", formulation nécessitant d'être ajoutée. L'illusion de l'exhaustivité au sein de cette disposition peut être problématique lorsque de nouvelles situations seront découvertes, raison pour laquelle il est important que les cas de figure décrits ne soient pas exhaustifs.
    - Art. 18 al. 1 lit. a P-OCyS : la mention d'une durée d'interruption serait plus sûre, afin d'éviter que ne tombent dans ces cyberattaques les interruptions de quelques minutes s'il n'y a pas plus de gravité.
    - Art. 18 al. 2 lit. b P-OCyS : le renvoi à la LPD n'est pas idéal. En effet, la LPD prévoit des obligations d'annonce (et non de signalement) en cas de violations également non intentionnelles de la sécurité des données (par exemple l'erreur d'un collaborateur qui engendrer la destruction de dossiers). Certaines violations de la sécurité des données ne sont donc pas constitutives de cyberattaques.
- Art. 19 P-OCyS :
    - al. 1 : une lettre doit être ajoutée pour rappeler que parmi les informations devant être transmises à l'OFCS doivent figurer les mesures prises et, lorsqu'elles sont connues, les mesures prévues ;
    - al. 1 let. e : il est plus juste de parler des "données sur l'attaquant" (à la place de "l'agresseur") ;
    - al. 3 : il est judicieux d'ajouter une lettre pour que l'exploitant soumis à l'obligation de signaler transmette également des informations sur les effets plus larges qu'uniquement sur le fonctionnement des unités touchées (par exemple pour la clientèle, éventuellement une partie de la population, pour l'environnement etc.). La seule mention dans les commentaires concernant l'ordonnance n'est pas suffisante et ces informations permettent en effet d'évaluer la cyberattaque ainsi qu'à la mise en garde d'éventuelles victimes (ce qui revient aux objectifs du signalement).
- Art. 21 al. 1 P-OCyS : il devrait être reprécisé "dans les 24 heures suivant la détection de la cyberattaque" pour faciliter la compréhension aux autorités et organisations assujetties (surtout si l'ordonnance ne renvoie pas aux dispositions de la LSI).
- La question de la plateforme de signalement commune à l'OFCS et aux autres autorités à l'instar du PFPDT n'est pas traitée au niveau du projet de l'ordonnance, ce qui est regrettable.

En vous remerciant pour la bonne réception de la présente prise de position, nous restons à disposition pour de plus amples informations.

Veuillez croire en l'expression de nos meilleurs sentiments,

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS
Direktionsstab
Schwarztorstrasse 59
3003 Bern

ncsc@ncsc.admin.ch

Bern, 12.09.2024

Vernehmlassung ISSS zur Cybersicherheitsverordnung

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, uns zur Vernehmlassung zur Cybersicherheitsverordnung (CSV) äussern zu können.

Vorstellung Taskforce Cybersicherheitsverordnung ISSS

Die Information Security Society Switzerland (ISSS) http://www.isss.ch ist der führende Fachverband in der Schweiz auf dem Gebiet der ICT-Sicherheit, welchem heute mehr als 1'100 Einzel- und Firmenmitglieder aus Wirtschaft, Verwaltung und Wissenschaft angehören. ISSS setzt sich mit den technischen, wirtschaftlichen, regulatorischen und gesellschaftspolitischen Aspekten von ICT-Sicherheit und Informationsschutz auseinander.

ISSS wurde 1993 als Verein gegründet und ist Mitglied von Digitalswitzerland sowie offizieller Security Fachpartner von SwissICT sowie ASUT. Mit unseren Mitgliedern arbeiten wir in Taskforces, um Fachexpertise gezielt abzuholen und der Öffentlichkeit zur Verfügung zu stellen. Auch vorliegende Stellungnahme wurde in einer Taskforce erarbeitet.

Taskforce Lead ISSS

Dario Walder	Vizepräsident ISSS
Andrea Michel	Geschäftsleiterin ISSS

Organisationen & Fachexperten

Fridel Rickenbacher	Swiss IT Security AG
Bettina Löw	Wirtschaftsprüferin
Christoph Pfister	atrete AG
Michael Schläpfer	Fort IT
Valmir Gashi	CyberSinn
Alexander Heuzeroth	Swiss Infosec AG
Dario Stöckli	CISO Aebi Schmidt Group
Felix Burri	Burri Consulting GmbH

Die positive Zusammenarbeit der Bundesverwaltung und besonders des BACS (früher NCSC) mit der Privatwirtschaft, auch im Kontext der Cybersicherheitsverordnung, wird von uns begrüsst. Gerne geben wir untenstehend unsere Überlegungen zum Vernehmlassungsentwurf der Cybersicherheitsverordnung bekannt:

Art. 2, Nationale Cyberstrategie
Die hier vorliegende Definition lässt unseres Erachtens die angestrebte führende Rolle in der internationalen Zusammenarbeit aussen vor. Diese Rolle hat mit 3 (von 17) Massnahmen in der aktuellen Nationalen Cybersicherheitsstrategie ein vergleichsweises hohes Gewicht, ist in der vorliegenden Verordnung jedoch nirgends festgehalten.

Art. 3, Abs f Steuerungsausschuss
Wir unterstützen es, einen Steuerungsausschuss Nationale Cyberstrategie (StA NCS) einzusetzen. Das ist aus unserer Sicht eine sinnvolle Massnahme. Wir schlagen jedoch vor, bei der Zusammensetzung dieses Steuerungsausschusses auch Vertreterinnen und Vertreter von kritischen Infrastrukturen zu berücksichtigen. Deren Einbindung ist unabdinglich. Die Formulierung «Vertreter der Wirtschaft» ist diesbezüglich zu wenig klar.

Art. 5, Abs a Aufgaben des StA NCS
Der Artikel schreibt vor, dass der Steuerungsausschuss die NCS alle 5 Jahre überprüft. In einem dynamischen und sich stets wandelnden Umfeld sollte jedoch zusätzlich risikobasiert und bei besonderen Herausforderungen eine Kurskorrektur durchgeführt werden können.

Art 6, Halterabfragen
Hier fehlt unserer Ansicht nach die Kompetenz im Nachgang zu Angriffen (zum Bsp. Art. 7 1b), Halteranfragen zu machen sowie historische Halterinformationen zu beziehen.

Art. 7, Technische Analyse von Cybervorfällen und Cyberbedrohungen
Dieser Artikel regelt unserer Ansicht nach nicht, wem das CERT zur Verfügung steht. Das ist zwar implizit geregelt, respektive andernorts beschrieben, wir empfinden es dennoch als Mangel das in der Verordnung nicht zu erwähnen.

Absatz 1a und 1b legen Wert auf den technischen Fokus der Arbeit des CERT, Absatz 1c besitzt diesen Fokus nicht und gerade Bedrohungen sind nicht notwendigerweise technischer Natur, noch ist die Technik zwingend das definierende Element einer Bedrohung. Der Artikel ist also gegebenenfalls nochmals zu überdenken.

Was in unseren Augen fehlt, ist die Vorgabe die erarbeiteten Analysen im Regelfall zu publizieren. Gegebenenfalls in gekürzter Fassung, aber Transparenz und Öffentlichkeit scheint uns bei der Positionierung als nationales CERT wichtig.

Art 8, Priorisierung der Beratung und Unterstützung bei Cyberangriffen
Es ist in der Verordnung nicht vorgesehen, dass das CERT sich bei Cyberangriffen extern verstärken kann. Eine solche Verstärkung wäre gegebenenfalls anzudenken. Überhaupt ist die Zusammenarbeit mit den kritischen Infrastrukturen und die Abgrenzung in der Verordnung kaum geregelt. Der begleitende Bericht beschreibt diese Zusammenarbeit zwar und wir würden es begrüssen, dies in der Verordnung zu regeln.

Art. 19 Inhalt der Meldung
Abs. 1, 2, 3 umschreiben den Inhalt einer Meldung. Wir sind der Meinung, dass zwischen dem Inhalt der Erstmeldung und je nach Klassifizierung des Vorfalls zwischen weiteren Inhalten unterschieden werden sollte. Art. 21 nimmt diesen Punkt indirekt auf, es wäre jedoch einfacher zwischen einer

Erstmeldung und einer umfassenden Aufarbeitung zu unterscheiden. Dadurch könnte viel administrativer Aufwand vermieden werden. Wir möchten dadurch verhindern, dass beispielsweise kurze Systemausfälle bei einem eingeschränkten Personenkreis gemeldet werden müssen.

Generell ist bezüglich Meldepflichten zu evaluieren, ob diese mit europäischen Regularien, wie z.B. NIS-2[1], DORA[2], CRA[3] harmonisiert werden könnten, um hier u. a. den Organisationen und Unternehmen mit Europabezug nicht unnötig Aufwand zu generieren.

Ziel muss sein, dass meldepflichtige Akteure jeweils nur eine Meldung an eine Behörde machen. Wir sehen das BACS in einer zentralen, koordinativen Rolle, was die Meldepflicht betrifft. Wir regen an, dass das BACS sämtliche meldepflichtigen Vorfälle entgegennimmt und diese dann mit weiteren relevanten Behördenstellen koordiniert. Eine einzige Meldestelle verhindert Mehraufwand und Doppelspurigkeiten. Zusätzlich können wir uns auch vorstellen, dass sich Behörden, an welche gemeldet werden muss (FINMA, EDÖB, BACS) untereinander koordinieren.

Im Rahmen der Meldung müssen auch Angaben zum Verursacher der Cyberattacke gemacht werden. Dies bedingt aufwändige forensische Verfahren und ist äusserst komplex. Aus unserer Sicht sollen die Unternehmen nicht Aufgaben im Bereich der Strafverfolgung übernehmen müssen - dies müsste zumindest freiwilliger Natur sein.

Inputs zum erläuternden Bericht zur Eröffnung des Vernehmlassungsverfahrens

- Art. 9 Abs. 5 umschreibt die Bekanntgabe der Schwachstelle vor Behebung oder Veröffentlichung. In diesem Zusammenhang würde uns interessieren, wie die Interessensabwägung funktioniert und was die ausschlaggebenden Faktoren sind, ab wann die Informationen weitergegeben werden.
- Art. 15 Abs 3 erläutert die Übermittlung und Nutzung der Informationen. Gibt es in diesem Zusammenhang Voraussetzungen oder Prüfungen, die ein Informationsempfänger erfüllen muss, um am Informationsaustausch teilnehmen zu dürfen?[4]

Wir hoffen, dass wir mit unserer Stellungnahme einen Beitrag zur Förderung der ICT-Sicherheit, dem Informationsschutz und dem konstruktiven Dialog in unserem Lande leisten können und danken Ihnen für die Berücksichtigung unserer Anregungen.

Mit freundlichen Grüssen

Dario Walder

ISSS Vize Präsident
Information Security Society Switzerland (ISSS)
Zentweg 13
3006 Bern
E-Mail: vicepresident@isss.ch

[1] European Union – EUR Lex - https://eur-lex.europa.eu/eli/dir/2022/2555

[2] Digital Operational Resilience Act (DORA) - https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

[3] European Commission – EU Cyber Resilience Act - https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[4] Hier möchten wir insbesondere auf die NIS-2 Richtlinie hinweisen: NIS-2 (RICHTLINIE (EU) 2022/2555) Art. 9 Abs. 5 CSV. Koordination der Offenlegung von Schwachstellen: NIS-2: Art. 12 Tätigkeit der mit der Koordination beauftragten Behörde: NIS-2: Art. 11.

SBB CFF FFS

Public Affairs und Regulation · Hilfikerstrasse 1 · CH-3000 Bern 65

Bundesamt für Cybersicherheit BACS
3003 Bern

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

Bern, 12. September 2024

Cybersicherheitsverordnung

Sehr geehrte Damen und Herren

Die SBB bedankt sich für die Möglichkeit, im Rahmen der Vernehmlassung zur Cybersicherheitsverordnung Stellung nehmen zu können. Vor dem Hintergrund der rasant zunehmenden Cyberangriffen begrüssen wir die Einführung einer Meldepflicht im Grundsatz. Damit die Meldepflicht jedoch ihren Zweck erfüllen kann, müssen die Bestimmungen dazu für die Betreiberinnen kritischer Infrastrukturen klar verständlich und einfach umsetzbar sein.

Allgemeine Bemerkungen
Die Verordnung ist komplex und teilweise schwer verständlich. Wir beantragen daher, relevante Definitionen zu präzisieren, die Struktur der Verordnung zu verbessern sowie eine bessere Abstimmung mit übergeordneten Regelwerken vorzunehmen. Wir beantragen ebenfalls eine Klärung der Definition von Systemaufgaben und der Rolle des BAV. Da die Verordnung das Verständnis von ISG erfordert, empfehlen wir zudem einen direkten Bezug oder eine Integration von ISG in die Verordnung.

Nachfolgend finden Sie unsere Anträge zu den einzelnen Bestimmungen:

Art. 2 Nationale Cyberstrategie
Wir bitten, die Identifikation von Bedrohungen («Identity») in die Aufzählung unter Ziffer 1 aufzunehmen, um alle fünf Funktionen des NIST Cybersecurity Framework (Identity, Protect, Detect, Respond und Recover) abzudecken.

SBB AG
Public Affairs und Regulation
Hilfikerstrasse 1· 3000 Bern 65 · Schweiz
luca.arnold@sbb.ch / www.sbb.ch

Antrag: Artikel 2 Ziffer 1 ist wie folgt zu ergänzen (unterstrichen)

Die Nationale Cyberstrategie (NCS) legt den strategischen Rahmen für die Prävention im Bereich der Cybersicherheit, die Früherkennung von Cyberbedrohungen, die Identifikation von Bedrohungen «Identity», die Reaktionsmöglichkeiten und die Resilienz bei Vorfällen sowie die Bekämpfung der Cyberkriminalität fest.

Art. 4 Zusammensetzung des StA NCS

Die Angaben zu Grösse und Zusammensetzung des Steuerungsausschusses sind unzureichend. Begriffe wie «Wirtschaft» sind zu generisch und müssen aus Sicht der SBB zwingen präzisiert werden, damit auch sichergestellt werden kann, dass die betroffenen Branchen im Steuerungsausschuss adäquat vertreten sind. Nur so kann garantiert werden, dass der generierte Output den Bedürfnissen aller relevanten Akteure entspricht.

Antrag: Wir beantragen, die Angaben zu Grösse und Zusammensetzung des StA in der Verordnung zu präzisieren.

Art. 5 Aufgaben des StA NCS

Gemäss Verordnung soll die Strategie mindestens alle fünf Jahre überprüft werden. Aus Sicht der SBB ist dies zu selten. Wir beantragen eine jährliche Überprüfung, wobei eine ausführliche Überprüfung nur alle zwei Jahre durchgeführt werden soll.

Antrag: Artikel 5a ist wie folgt zu ändern (kursiv unterstrichen)

Er überprüft die NCS mindestens ~~alle fünf Jahre~~ *jährlich*, wirkt bei ihrer Weiterentwicklung mit und erarbeitet bei Bedarf Anpassungsvorschläge.

Art. 8 Priorisierung der Beratung und Unterstützung bei Cyberangriffen

Wir beantragen bei Art.8 Abs.2 eine klare Priorisierung. Aus Sicht der SBB muss bei einem Engpass der Kapazitäten des BACS in erster Linie die öffentliche Sicherheit und Ordnung sichergestellt werden, gefolgt vom Wohlergehen der Bevölkerung und zuletzt vom Funktionieren der Wirtschaft.

Wie regen zusätzlich an, noch einen Bezug zu Artikel 18 herzustellen. Damit soll geklärt werden, ob eine Meldung automatisch eine Unterstützungsanforderung auslöst oder ob diese explizit verlangt werden muss.

Antrag:
1. Wir beantragen eine Klärung des beschriebenen Sachverhalts in Bezug auf die Unterstützungsanforderungen.

2. Artikel 8 Absatz 2 ist wie folgt zu ergänzen (unterstrichen)
Es berücksichtigt dabei in folgender Priorisierung: die öffentliche Ordnung, das Wohlergehen der Bevölkerung und das Funktionieren der Wirtschaft.

Artikel 9 Koordinierte Offenlegung von Schwachstellen
Die SBB beantragt folgende Klärungen bzw. Präzisierungen:

- Wir beantragen eine Klärung bezüglich der Fristen zur Behebung von Schwachstellen durch Hersteller und der Kommunikation zwischen BACS und BAV zu Zulassung und Patching.
- Es besteht Unsicherheit über die Abgrenzung der Meldepflicht und Kommunikation von Schwachstellen zwischen Herstellern und Betreibern. Konkret fordern wir eine Klarstellung, a) ob das ausschliesslich Schweizer Hersteller oder solche mit Hauptsitz in der Schweiz betrifft, b) ob dies ausschliesslich Schwachstellen, welche über die Meldepflicht an das BACS gemeldet wurden, betrifft und c) ob dies die entdeckende Firma/Organisation davon entbindet, die Schwachstelle einem Anbieter zu melden.
- Es ist uns ferner nicht klar, wie die Verknüpfung von Hersteller und Betreiber stattfindet. Müssen die Betreiber von kritischen Infrastrukturen Meldepflichten von Schwachstellen wiederum mit den relevanten Herstellern regeln, da nur die Betreiber über ein Inventar der eingesetzten Systeme verfügen, oder bekommen die Betreiber kritischer Infrastrukturen über den in Kapitel 4 definierten Informationsaustausch vorab Informationen über alle vorhandenen Schwachstellen und prüfen selbst, ob sie betroffen sind?
- Zuletzt bitten wir um eine präzise Definition des Begriffs «Schwachstelle» im Kontext dieser Verordnung.

Antrag: Wir bitten um eine Klärung der aufgelisteten Fragen.

Artikel 11 Kommunikationssystem für den sicheren Informationsaustausch
Aus den Verordnungsunterlagen ist nicht ersichtlich, wer genau neue, für die Benutzenden relevante Bedrohungen auf der Kommunikationsplattform des BACS überwacht. Die Verordnung gibt zudem keine Auskunft darüber, wer Zugriff darauf hat und von wo aus dieser erfolgt. Diese Verantwortlichkeiten müssen zwingend geklärt werden, da

insbesondere die Meldung und das Hinzufügen von Dienstleistern dazu führen könnten, dass gewisse Informationen nicht mehr über die Plattform geteilt werden, wenn das nötige Vertrauen aufgrund unklarer Verantwortlichkeiten fehlt.

Antrag: Wir bitten um eine Klärung der Verantwortlichkeiten und Zugriffrechte auf die Kommunikationsplattform des BACS.

Artikel 12 Informationssysteme für den automatischen Austausch
Aus den Verordnungsunterlagen geht nicht klar hervor, wie solche Informationen gehandhabt werden dürfen. Konkret bitten wir um die Klärung der folgenden Fragen:

- Wie werden Cloudumgebungen verwaltet?
- Wann und unter welchen Bedingungen dürfen Informationen in Cloud Environments ausserhalb der Schweiz gespeichert werden?

Antrag: Wir bitten um eine Klärung der aufgelisteten Fragen.

Artikel 16 Ausnahmen von der Meldepflicht
Wir beantragen, die vorgesehenen Ausnahmen von der Meldepflicht für kleinere Bahnen, Betreiber von Gasleitungen und Elektrizitätswerken zu überdenken. Auch diese Akteure können von Angriffen betroffen sein, die schnell sicherheitsrelevant werden können. Eine Meldepflicht auch für kleinere Unternehmen erachten wir als sinnvoll und wichtig. Dadurch könnten Angriffe frühzeitig erkannt und eine Koordination durch das BACS erleichtert werden.
Weiter beantragen wir, bei der Ausnahme einer Meldepflicht auf eine mögliche Vernetzung zu meldepflichtigen Infrastrukturen zu achten.

Antrag: Wir beantragen auf die Ausnahmen von der Meldepflicht gemäss unseren Ausführungen zu verzichten.

Artikel 18 zu meldende Cyberangriffe
Wir erachten die Formulierungen hinsichtlich der Gefährdung der Funktionsfähigkeit kritischer Infrastrukturen als zu generisch und zu umfassend. Gemäss der aktuellen Formulierung wären bspw. auch Mitarbeitende betroffen, die in einem unkritischen Bereich (bspw. Parkplatzverwaltung) tätig sind. Wir beantragen daher, Artikel 18 Absatz 1 zu präzisieren und den Anwendungsbereich einzugrenzen. Dasselbe gilt für die Zeitdauer und das Ausmass eines Unterbruchs. In der aktuellen Formulierung wäre auch ein kurzfristiger Ausfall meldepflichtig

Bei den zu meldenden Cyberangriffen ist es unklar, wie ein Lieferantenverhältnis abgebildet ist und wer in welchem Fall meldepflichtig ist. Dies ist insbesondere bei hoch integrierten Systemen der Fall, bei denen auch eine Betriebsleistung an einen externen Lieferanten ausgelagert ist. Wie wird das Verhältnis rechtlich geregelt, wenn der Zulieferer den rechtlichen Sitz nicht in der Schweiz hat und/oder der kritischen Infrastruktur einen Angriff meldet, der eine Auswirkung gemäss Art 18 zur Folge hat, aber nicht bei der kritischen Infrastruktur selbst passiert ist?
Wir beantragen zuletzt die Reichweite von Absatz 4 einzugrenzen damit nur jene Cyberangriffe, die mit Erpressung, Drohung und Nötigung verbunden sind, gemeldet werden müssen, die auch strafrechtlich relevant sowie glaubwürdig sind. Ohne entsprechende Eingrenzung müssten auch Angriffe in Form von Fake Sextortion / We have hacked you etc. gemeldet werden.

Antrag:
1. Wir beantragen eine Präzisierung und Eingrenzung von Artikel 18 Absatz a gemäss unseren Bemerkungen.
2. Wir beantragen eine Klärung des Verhältnisses zwischen einem Betreiber kritischer Infrastrukturen und den Lieferanten in Bezug auf Rolle und Verantwortung bei zu meldenden Cyberangriffen.
3. Artikel 18 Absatz 4 ist zudem folgendermassen zu ergänzen (unterstrichen):
«…oder gegen die für meldepflichtige Behörde oder Organisation tätige Person meldet, wenn der Cyberangriff strafrechtlich relevant und glaubwürdig ist.»

Artikel 19 Inhalt der Meldung
Die unter Ziffer 1a bis e zu liefernden Informationen erachten wir als unpraktikabel und unrealistisch. Es ist denkbar, dass zum Zeitpunkt der Meldung noch nicht alle geforderten Informationen vorliegen. Wir beantragen daher, den Artikel so anzupassen, dass eine Meldung auch ohne Vorhandensein aller Angaben gemacht werden kann.
In diesem Zusammenhang sehen wir die Forderung nach Angaben zum Verursacher als problematisch (Ziffer 1e). Diese Forderung beinhaltet eigentlich eine Attribuierung, welche viele Organisationen überfordern dürfte und zum Zeitpunkt der Meldung ohnehin unklar sein dürfte.
Weiter beantragen wir, dass zusätzlich zur Uhrzeit auch die Zeitzonen angegeben werden müssen, dies ist vor allem für global tätige Unternehmen zentral.

Antrag: Wir beantragen Artikel 19 Absatz 1 wie folgt zu ändern (unterstrichen)

SBB CFF FFS

1 Die Meldung muss folgende Informationen zum Cyberangriff enthalten, sofern diese zum Zeitpunkt der Meldung bekannt sind.
a. Datum, Uhrzeit und Zeitzone…
b. Datum, Uhrzeit und Zeitzone…

Wir bedanken uns für die Berücksichtigung unserer Anliegen. Für Fragen steht Ihnen Jean-Luc Nottaris (jean-luc.nottaris@sbb.ch; 076 372 17 33) zur Verfügung.

Freundliche Grüsse

Luca Arnold
Leiter Regulation und Internationales

Marcus Griesser
Leiter Konzernsicherheit

Kopie an:

- Gery Balmer, Abteilungschef Politik, Stellvertretender Direktor, BAV
- Manuel Suter, Stellvertretender Direktor, BACS

Swiss Banking

FS-CSC Swiss Financial Sector Cyber Security Centre

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport
Bundesamt für Cybersicherheit BACS
Schwarztorstrasse 59
CH-3003 Bern

Per Mail zugestellt an: ncsc@ncsc.admin.ch

Basel, 12. September 2024
AAR / +41 58 330 62 32

Cybersicherheitsverordnung
Vernehmlassung – unsere Stellungnahme

Sehr geehrte Frau Bundesrätin Amherd
Sehr geehrter Herr Schütz
Sehr geehrte Damen und Herren

Mit Schreiben vom 22. Mai 2024 haben Sie die Vernehmlassung zur Cybersicherheitsverordnung (CSV) eröffnet. Gerne äussern wir uns zu Ihrem Entwurf nachfolgend. Wir unterstützen den Entwurf mit nachstehenden Anpassungsvorschlägen.

Zusammenfassung

Die Schweizerische Bankiervereinigung (SBVg) und das Swiss Financial Sector Cyber Security Centre (Swiss FS-CSC) unterstützen den Entwurf der Cybersicherheitsverordnung (E-CSV), sofern die nachstehend begründeten Anpassungsvorschläge Berücksichtigung finden.

Wichtige Anliegen unserer Verbände sind:

- die Zulassung aller in der Schweiz tätigen und meldepflichtigen Unternehmen zum Informationsaustausch, unabhängig von einem schweizerischen Sitz (also z.B. der Zweigniederlassungen ausländischer Finanzinstitute mit FINMA-Bewilligung) (Art. 11 Abs. 1 E-CSV);

Schweizerische Bankiervereinigung
und Swiss Financial Sector Cyber
Security Centre (Swiss FS-CSC)

Aeschenplatz 7
Postfach 4182
CH-4002 Basel

office@sba.ch
info@fscsc.ch
www.swissbanking.ch
www.fscsc.ch

- eine juristische Regelung und technische Ausgestaltung der Meldepflicht, die gewährleistet, dass in einer Sammelmeldung an verschiedene Behörden jede Behörde nur den sie betreffenden Teil der Meldung einsehen kann (Art. 15 E-CSV);
- die Schaffung von De-minimis-Ausnahmen von der Meldepflicht auch für Finanzinstitute, ggf. ergänzt durch eine FINMA-Verordnung oder eine Selbstregulierung der Verbände (Art. 16 E-CSV);
- die Notwendigkeit einer stringenten Verwendung von Begriffen und deren Definition in der gesamten Verordnung zur Gewährleistung der Rechtssicherheit.

Diese Vorschläge dienen der Wahrung der Verhältnismässigkeit (Art. 5 Abs. 2 und 36 Abs. 3 BV), was auch für unsere ergänzenden Vorschläge zu Art. 18 und 19 E-CSV gilt.

Schliesslich erscheint uns eine ausreichende Übergangsfrist von zwei Jahren, mindestens aber einem Jahr ab Veröffentlichung des finalen Verordnungstextes, unabdingbar (Art. 23 E-CSV).

Weitere Anliegen betreffen insbesondere eine möglichst saubere, verständliche Terminologie, wozu wir Ihnen ebenfalls Vorschläge unterbreiten.

1. Allgemeines

Das Swiss FS-CSC wurde im April 2022 – unter federführender Mitwirkung der Schweizerischen Bankiervereinigung (SBVg) und des Schweizerischen Versicherungsverbands (SVV) – von Banken, Versicherungen, ihren Verbänden, SIX und der Schweizerischen Nationalbank (SNB) gegründet und setzt sich für die Stärkung der Widerstandsfähigkeit des Finanzsektors gegen Cyberrisiken – der sogenannten Cyberresilienz – ein. Dabei haben die Bundesbehörden von Anfang an mitgewirkt, insbesondere das Bundesamt für Cybersicherheit (BACS, ursprünglich Nationales Zentrum für Cybersicherheit NCSC), aber auch die SNB, die FINMA und das Staatssekretariat für Internationale Finanzfragen (SIF), die heute alle im Verein mitarbeiten. Im Rahmen einer Public-Private Partnership mit dem Bund leistet das Swiss FS-CSC einen wichtigen Beitrag zur Stärkung der Cyberresilienz und fördert die Kooperation zwischen den Finanzinstituten und mit den Behörden.

Ein Kernelement der Verordnung – und schon der vorangegangenen Revision des Informationssicherheitsgesetzes (ISG) – ist die Meldepflicht bei Cyberangriffen. Sie stellt einen wichtigen Schritt auf dem Weg der Umsetzung dieser gemeinsamen Bemühungen dar – einen Schritt, der notwendigerweise dem Gesetzgeber, also der staatlichen Seite der Public-Private Partnership, zukommt.

Wir unterstützen Sie dabei und äussern uns nachstehend zu einzelnen Gesichtspunkten, insbesondere dort, wo wir noch Verbesserungsbedarf sehen.

Schweizerische Bankiervereinigung
und Swiss Financial Sector Cyber Security Centre (Swiss FS-CSC)
Aeschenplatz 7
Postfach 4182
CH-4002 Basel
office@sba.ch
info@fscsc.ch
www.swissbanking.ch
www.fscsc.ch

2. Bemerkungen zu einzelnen Bestimmungen des Entwurfs

2.1 Hauptanliegen

Art. 11 Abs. 1 E-CSV: Kommunikationssystem für den sicheren Informationsaustausch

Aufgrund der bisherigen Erfahrungen mit dem Informationsaustausch über den Cyber Security Hub (CSH) des BACS erscheint uns der jetzige Formulierungsvorschlag zu restriktiv und damit kontraproduktiv. Die notwendige Stärkung der Cyberresilienz auf dem Wirtschaftsstandort Schweiz bedingt, dass alle im Land tätigen «Betreiberinnen kritischer Infrastrukturen» (Art. 74 rev. ISG)[1] – nicht nur jene mit Sitz in der Schweiz – am Informationsaustausch teilnehmen können. Globale Unternehmen oder Unternehmensgruppen sind darauf angewiesen, Informationen über die Landesgrenze hinweg teilen zu können. So ist es für den Finanzplatz schon heute durch das BACS geregelt: Auch Zweigniederlassungen ausländischer Finanzinstitute, die in der Schweiz über eine Bewilligung der FINMA verfügen, sind zum CSH zugelassen. Nur so lässt sich die Cyberresilienz auf dem Wirtschaftsstandort Schweiz wirksam stärken. An diese Regelung ist für die Ausgestaltung von Art. 11 Abs. 1 E-CSV anzuknüpfen. Alle meldepflichtigen Unternehmen sollten zur Teilnahme am Informationsaustausch zugelassen sein.

Vorschlag

Wir schlagen deshalb vor, die Worte «Organisationen und Behörden mit Sitz in der Schweiz» in Art. 11 Abs. 1 E-CSV zu ersetzen durch: «Meldepflichtige Organisationen und Behörden».

Art. 15 E-CSV: Übermittlung und Nutzung der Informationen

Hier ist es aus unserer Sicht unerlässlich, die seitens der Wirtschaft in das Gesetz eingebrachte Regelung von Art. 74*f* rev. ISG und damit die Modalitäten der Übermittlung von Meldungen an das BACS zu konkretisieren. Es ist zur Aufwandminimierung gerade für kleinere Unternehmen wichtig, die Meldung eines Cyberangriffs – abhängig von dessen Art und Wirkung – technisch und rechtskonform in einem einzigen Formular melden zu können, auch wenn der Angriff womöglich mehrere Bundesstellen betrifft (das BACS, bei Betroffenheit von Personendaten überdies den EDÖB und bei einem Cyberangriff gegen einen Finanzdienstleister zusätzlich die FINMA). Bei Meldungen an das BACS stehen andere Informationen im Vordergrund (Art und Funktionsweise des Cyberangriffs) als bei Meldungen an den EDÖB (Schutz von Personendaten) oder die FINMA (Stabilität und Funktionsfähigkeit des Finanzdienstleisters, Schutz der Bankkundinnen und -kunden). Deshalb lässt Art. 74*f* Abs. 2 rev. ISG eine Meldung an mehrere Behörden gleichzeitig zu.

Die unterschiedlichen Meldeinhalte je Behörde setzen voraus, dass jede Behörde nur jene Daten erhält bzw. einsehen kann, für deren Bearbeitung sie zuständig ist (das entspricht auch dem DSG-Grundsatz der Datensparsamkeit). Ein breiter ausgreifender Einblick in die verschiedenen Datensätze wäre ein Verstoss gegen die Datensparsamkeit und könnte je nach Inhalt weitere Gesetzesverstösse beinhalten, z.B. einen Verstoss gegen das Bankkundengeheimnis. Deshalb muss bei einer Sammelmeldung an verschiedene

[1] Darunter sind für den Finanzbereich u.E. alle in Art. 74b Abs. 1 Bst. e rev. ISG genannten Finanzinstitute, also Banken, Versicherungen und Finanzmarktinfrastrukturen, zu verstehen.

Behörden sichergestellt sein, dass jede Behörde nur den an sie adressierten Teil der Meldung lesen kann. Für gesonderte Meldungen an die verschiedenen Behörden verlangt Art. 74*f* Abs. 3 rev. ISG dies ausdrücklich:

«[3] Sind zur Erfüllung einer Meldepflicht gegenüber weiterten Behörden Informationen erforderlich, die über Artikel 74*e* hinausgehen, so muss das System den meldepflichtigen Behörden und Organisationen ermöglichen, diese Informationen direkt an die betreffenden Behörden zu übermitteln, ohne dass das NCSC darauf Zugriff hat.»

Konsequenterweise muss dies nicht nur bei gesonderten Meldungen, sondern ebenso bei einer Sammelmeldung gelten, da die Geheimhaltungsregeln der einschlägigen Gesetze materiell dieselben sind.

Einen zusätzlichen Grund für eine Regelung in diesem Sinne bietet auch Art. 4 Abs. 1[bis] rev. ISG, der die Anwendbarkeit des Öffentlichkeitsgesetzes für gemeldete Daten explizit ausschliesst:

«[1 bis] Informationen Dritter, von denen das Nationale Zentrum für Cybersicherheit (NCSC) durch die Entgegennahme und Analyse von Meldungen gemäss dem 5. Kapitel Kenntnis erhält, dürfen nicht nach dem BGÖ zugänglich gemacht werden. Nicht als Dritte gelten Behörden, Organisationen und Personen nach Artikel 3 Absatz 1 BGÖ.»

Die Anforderung muss deshalb technisch so umgesetzt werden, dass innerhalb einer einzigen Meldung, die an verschiedene Behörden geht, jeder einzelne Abschnitt technisch entsprechend gekennzeichnet werden kann, z.B. «an BACS, EDÖB und FINMA» oder «nur an BACS», «nur an EDÖB», «nur an FINMA».

Dies sieht Art. 15 E-CSV aktuell nicht vor, im Gegenteil: Der jetzige Wortlaut von Art. 15 Abs. 1 und 2 E-CSV legt vielmehr den Schluss nahe, dass die Meldung gesamthaft dem BACS zugestellt werden müsse (was soweit noch akzeptabel wäre), das BACS dann aber im eigenen Ermessen entschiede, welche Teile allenfalls an andere Behörden weiterzuleiten wären (was nach dem Gesagten unzulässig wäre), oder sogar welche Teile publiziert würden (was erst recht nicht zulässig wäre).

Nötig ist hier aus unserer Sicht eine Plattform, die vom BACS betrieben wird und Meldungen zulässt, deren Inhalt von der meldenden Organisation so unterteilt werden kann, dass die einzelnen Teile unterschiedlichen Behörden zugewiesen sind und jede Behörde nur die ihr zugewiesenen Inhalte einsehen kann.

Vorschlag

Entsprechend ist der Wortlaut von Art. 15 E-CSV zu überarbeiten und im abschliessenden Erläuterungsbericht wie erwähnt zu begründen. Wir schlagen folgende Ergänzung von Art. 15 E-CSV vor:

«[1 bis] Das vom BACS zur Übermittlung von Meldungen zur Verfügung gestellte System ist so auszugestalten, dass alle angeschlossenen Behörden nur die von der meldenden Organisation für sie bestimmten Inhalte lesen und verarbeiten können.

[1 ter] Für jene Meldungsinhalte, die auf diesem Weg mit dem BACS geteilt werden, entscheidet das BACS über die Veröffentlichung ... [weiter nach Art. 15 Abs. 2]»

Zur Wahrung des Datenschutzes empfehlen wir dem BACS als Betreiberin der Meldeplattform, eine selbstbindende Erklärung zu verfassen, welche den Plattformnutzenden die Einsicht des BACS nur in die an sie adressierten Inhalte gegenüber den Plattformnutzenden garantiert.

Wir bitten Sie, gerade mit Blick auf die vorstehend skizzierten Eckpfeiler des Meldeprozesses, einschliesslich des Meldeformulars, die Wirtschaft in die Erarbeitung sowohl des Formulars wie auch des dazugehörigen technischen Prozesses einzubeziehen.

Art. 16 E-CSV: Ausnahmen von der Meldepflicht

Grundlage für diese Bestimmung ist Art. 74*c* rev. ISG, welcher den Bundesrat verpflichtet, Ausnahmen von der Meldepflicht vorzusehen, «wenn durch Cyberangriffe ausgelöste Funktionsstörungen nur geringe Auswirkungen auf das Funktionieren der Wirtschaft oder das Wohlergehen der Bevölkerung haben.» Diese Ausnahmen sind im Vorschlag zu Art. 16 E-CSV enthalten. Doch es fehlt eine Ausnahmebestimmung für Finanzinstitute i.S.v. Art. 74*b* Abs. 1 Bst. e rev. ISG (Banken, Versicherungen und Finanzmarktinfrastrukturen). In unserer Vernehmlassung vom 13.04.2022 zur Revision des ISG haben wir auf Seite 5 eine solche Regelung in Art. 74*d* rev. ISG vorgeschlagen, die in Anlehnung an die FINMA-Aufsichtsmitteilung 05/2020 bspw. wie folgt lauten könnte:

«Zu melden sind Cyberangriffe mit erheblichen Auswirkungen auf die Geschäftstätigkeit des Unternehmens, insbesondere erfolgreiche oder teilweise erfolgreiche Angriffe auf kritische Funktionen, deren Ausfall oder Störung den Schutz der Kundinnen und Kunden oder das Funktionieren der Märkte stark beeinträchtigen würde.»

Eine solche Bestimmung entspräche dem Grundsatz der Verhältnismässigkeit (Art. 5 Abs. 2 und 36 Abs. 3 BV).

Denn es ist sinnvoll, die Anzahl meldepflichtiger Unternehmen mit De minimis-Regeln und qualitativen Kriterien einzugrenzen, umso mehr, als Cyberangriffe gegen «kleine» oder gesamtwirtschaftlich «unkritische» Unternehmen typischerweise mit einfacherer Technik bereits erfolgreich sein können und deshalb zur Cyberabwehr grösserer und systemrelevanter Opfer keine oder höchstens marginale Schlüsse zulassen.

Vorschlag

Wir schlagen vor, den Ausnahmekatalog in Art. 16 E-CSV durch eine Bestimmung für Finanzinstitute gemäss Art. 74 Abs. 1 Bst. e rev. ISG (Banken, Versicherungen und Finanzmarktinfrastrukturen) im Sinne unseres oben erwähnten Vorschlags zu ergänzen. Diese könnte als Abs. 1 Bst. d^{bis} wie folgt lauten:

«d ^{bis}. Unternehmen nach Artikel 74*b* Absatz 1 Buchstabe e ISG, wenn Cyberangriffe nur geringfügige Auswirkungen auf die Geschäftstätigkeit des Unternehmens haben, insbesondere keine erfolgreichen oder teilweise erfolgreichen Angriffe auf kritische Funktionen sind, deren Ausfall oder Störung den Schutz der Kundinnen und Kunden oder das Funktionieren der Märkte stark beeinträchtigen würde. Diese Bestimmung kann durch eine Verordnung der FINMA oder eine Selbstregulierung der zuständigen Verbände konkretisiert werden»

Des Weiteren können Cyberangriffe auch nur kurzzeitige Systemunterbrüche zur Folge haben, welche gemäss dem aktuell vorgesehenen Verordnungstext ebenfalls meldepflichtig wären. Dies erweist sich jedoch als wenig praktikabel für die meldepflichtigen Institute und für das BACS als Verwaltungsinstanz der Meldeplattform. Daher ist eine Präzisierung der Verordnung im erwähnten Sinn erforderlich.

Zudem schlagen wir vor, direkte Verweise auf EU-Gesetzgebungen (siehe hierzu Art. 16 Abs. 1 Bst. c Ziff. 1 und 2 E-CSV) zu vermeiden, da diese häufig angepasst werden und Verweise dann ins Leere zielen, was in der Konsequenz zu Rechtsunsicherheit führt.

Art. 18 E-CSV: Zu meldende Cyberangriffe

Die vorgeschlagenen Regelungen gehen in die richtige Richtung, sollten sich aber – entsprechend der Zuständigkeit und Aufgabe des BACS – inhaltlich konsequent auf Cyberangriffe beschränken und weitere Aspekte wie namentlich den Datenschutz weglassen. Nur so lassen sich die notwendigen klaren Abgrenzungen bei der Meldepflicht schaffen (vgl. oben unsere Bemerkungen zu Art. 15 E-CSV).

Vorschlag

Folgende konkreten Eingrenzungen schlagen wir vor, wobei diese alternativ (nicht kumulativ) zur Anwendung kommen müssen:

(1) Bei Abs. 1 Ingress: «Die Funktionsfähigkeit einer kritischen Infrastruktur gilt als durch einen Cyberangriff gefährdet, wenn: …»

(2) Bei Abs. 1 Bst. a: «Mitarbeitende oder Dritte von Unterbrüchen kritischer Systeme betroffen sind …»

(3) Bei Abs. 2 Verzicht auf die Buchstabengliederung und Ersetzung durch folgenden Wortlaut: «Eine Manipulation oder ein Abfluss von Informationen liegt vor, wenn kritische geschäftsrelevante Informationen von unbefugten Dritten verändert oder offengelegt werden.»

Eventualvorschlag

Sollte dies nicht wie vorgeschlagen in Erwägung gezogen werden, ist stattdessen Art. 18 Abs. 2 E-CSV wie folgt anzupassen: Einfügung eines zusätzlichen Bst. zwischen Bst. a und b in Abs. 2 mit folgendem Wortlaut: «die Integrität kritischer Geschäftsprozesse beeinträchtigt ist, oder»

Bei Abs. 2 Bst. b (neu dann Abs. 2 Bst. c) sollen folgende Anpassung vorgenommen werden: «Infolge eines Cyberangriffs eine meldepflichtige Verletzung der Datensicherheit …»

Art. 19 E-CSV: Inhalt der Meldung

(1) Zum Inhalt der Meldung

Der Schweregrad des zu meldenden Cyberangriffs wird im Entwurf sehr detailliert umschrieben, was wiederum die Entscheidung, ob eine Meldung zu erstatten ist und – wenn ja – den dafür erforderlichen Aufwand unnötig erschwert. Im Rahmen der Meldung muss es genügen, wenn der Schweregrad des Angriffs pauschal mit leicht, mittel oder schwer qualifiziert wird. Entsprechend dem Fokus des ISG (kritische Angriffe auf kritische Strukturen) sollten hinsichtlich des Schweregrads als leicht qualifizierte Cyberangriffe sachlogisch auch nicht meldepflichtig sein.

Auch die übrigen Kriterien wären zumindest dahingehend zu flexibilisieren, dass auf das Wissen, welches vernünftigerweise überhaupt vorhanden sein kann, abgestellt wird. Über «Methode» und «Verursacher» des Cyberangriffs liegen i.d.R. keine sofortigen und klaren Kenntnisse vor.

(2) Frist der Meldung

Mit Blick auf die gesetzlich zur Verfügung gestellte Möglichkeit, eine Meldung zu erstatten, welche je nachdem auch Teile enthält, die (nur) für den EDÖB oder die FINMA bestimmt sind (vgl. oben unsere Bemerkungen zu Art. 15 E-CSV), müssen auch die zeitlichen Anforderungen koordiniert werden. Andernfalls läuft das zur Verfügung gestellte, kombinierte Formular ins Leere.

Zielführend erscheint eine zwischen ISG/CSV, Datenschutzgesetz und Bankengesetz harmonisierte, kurze Frist für die Erstmeldung, ergänzt durch eine ebenfalls harmonisierte, längere Frist von z.B. 14 Tagen für die Nachmeldung, diese ergänzt um nachträglich eruierte Details.

Vorschlag

Wir schlagen folgende Ergänzung von Art. 19 Abs. 1–3 E-CSV vor:

«[1] Die Meldung muss, soweit innert der Meldefrist schon vorhanden, folgende Informationen zum Cyberangriff enthalten […].

[2] Sie muss zudem die Information enthalten, ob der Angriff nach vorläufiger Einschätzung voraussichtlich mit Erpressung, Drohung oder Nötigung verbunden war und ob Strafanzeige erstattet wurde.

[3] Sie muss folgende Informationen zu den Auswirkungen des Cyberangriffs enthalten […]:

b. voraussichtlicher Schweregrad der Beeinträchtigung der Verfügbarkeit, Integrität und Vertraulichkeit der eigenen Informationen und der Informationen von Dritten nach vorläufiger Einschätzung (leicht, mittel oder schwer) […]»

Art. 23 E-CSV: Inkrafttreten

Ein Inkrafttreten per 1. Januar 2025 erscheint uns weder sachgerecht noch objektiv überhaupt möglich.

Der finale Wortlaut der Regelung liegt erst mit der endgültigen Publikation der Verordnung vor. Dies wird wohl erst wenige Wochen oder sogar nur Tage vor dem 1. Januar 2025 der Fall sein. Vorher wissen zahlreiche Unternehmen weder, ob sie der Regelung überhaupt unterstehen, noch in welcher Form und innert welcher Frist gegebenenfalls eine Meldung zu erstatten wäre. Auch das in Aussicht gestellte Meldeformular liegt womöglich bis Ende 2024 noch nicht finalisiert vor.

Erst gestützt auf den finalen Wortlaut der Verordnung und die technische Umsetzung des Meldeprozesses einschliesslich Meldeformular weiss jede Unternehmung, ob sie der Regelung untersteht, welche technischen Vorgaben sie einhalten muss und wie der Meldeprozess von statten geht. Dann erst kann eine Detailanalyse erfolgen, das entsprechende Budget beantragt und gestützt darauf wiederum die Detailspezifikation zur technischen Umsetzung gemacht werden. Dazu gehört die interne Koordination mit den bestehenden Meldeprozessen unter Datenschutz- und Bankengesetz, wie auch die entsprechende Anpassung der gesamten Governance. Eine seriöse Umsetzung erfasst schliesslich verschiedene Tests der vor-finalen Prozesse, damit der gesamte Ablauf sowohl intern als auch koordiniert mit dem vom BACS zur Verfügung gestellten Meldeprozess und -formular einwandfrei funktioniert. Zu berücksichtigen ist zudem, dass Verletzungen der Meldepflicht sanktioniert sind.

Vorschlag

Aus all diesen Gründen bedarf es zwischen dem Vorliegen des finalen Wortlauts der Verordnung und ihrem Inkrafttreten einer Übergangsfrist von mindestens einem Jahr, erfahrungsgemäss aber besser zwei Jahren. Auch für das BACS ist es zielführender, wenn ausreichend Zeit zur Verfügung steht, um qualitativ gute Systeme und Prozesse zu schaffen, statt derart wichtige Meldungen erzwungenermassen «hand-made» zu erhalten. Nur so erhält das BACS seriöse Informationen, welche effizient, zielführend und gewinnbringend ausgewertet werden können.

2.2 Weitere Vorschläge

Art. 4 Abs. 1 und 2 E-CSV: Zusammensetzung des StA NCS

Was bei der Zusammensetzung des Steuerungsausschusses «Nationale Cyberstrategie» unter «Gesellschaft» zu verstehen ist und nicht schon durch Wirtschaft und Hochschulen abgedeckt wäre, ist unklar. Es fragt sich auch, ob es in diesem stark auf die Cyberresilienz und ihre Anforderungen fokussierten Bereich der Politik einen so breit zusammengesetzten Steuerungsausschuss braucht und nicht stattdessen gezielt Erfahrungen oder Kenntnisse im Cyberbereich zu verlangen wären.

Vorschlag

Wir schlagen deshalb vor, die Worte «der Gesellschaft» zu streichen und Abs. 2 durch den Satz zu ergänzen: «Bei der Bestimmung der Mitglieder des Steuerungsausschusses ist auf angemessene Erfahrungen oder Kenntnisse im Cyberbereich zu achten.»

Ausserdem schlagen wir vor, die bisherige Zusammensetzung des StA NCS (vgl. Medienmitteilung des BACS vom 7. Juni 2024) durch eine Vertretung der Betreiberinnen kritischer Infrastrukturen zu ergänzen, wie z.B. der im Swiss FS-CSC organisierte Banken- und Versicherungsbranche.

Art. 7 Abs. 1 Bst. a E-CSV: Technische Analyse von Cybervorfällen und Cyberbedrohungen

Uns erscheint wichtig, dass eine technische Vorfallbewältigung auch auf Anfrage von anderen Behörden und Organisationen unterstützt wird.

Vorschlag

Wir schlagen deshalb vor, Art. 7 Abs. 1 Bst. a E-CSV zu ergänzen durch den Nebensatz: «dies bei Bedarf auch auf Anfrage von anderen Behörden und Organisationen.»

Art. 9 zusätzlicher Absatz E-CSV: Koordinierte Offenlegung von Schwachstellen

Der Begriff der «Schwachstelle» ist weder im Gesetz noch im Verordnungsentwurf ausreichend definiert. Die Ergänzenden Erläuterungen zum E-CSV verweisen dafür auf die ISO/IEC-Norm 29147:2018-10. Eine entsprechende Präzisierung in der Verordnung scheint uns aus rechtsstaatlichen Gründen unerlässlich.

Vorschlag

Wir schlagen deshalb vor, beispielsweise die Definition des CVE-Programms des National Cybersecurity Federally Funded Research and Development Center (FFRDC) zu übernehmen:

«Eine oder mehrere Sicherheitslücken in einem Produkt, die ausgenutzt werden können, um die Vertraulichkeit, Integrität oder Verfügbarkeit zu beeinträchtigen; eine Reihe von Bedingungen oder Verhaltensweisen, die die Verletzung einer expliziten oder impliziten Sicherheitsrichtlinie ermöglichen.»

Art. 14 E-CSV: Dienstleister

Bei den «Dienstleistern kritischer Infrastrukturen» gemäss Art. 14 Abs. 1 E-CSV handelt es sich um Unterakkordanten von Unternehmen, welche für diese – meist aufgrund eines Outsourcings – Dienstleistungen im Zusammenhang mit der eigenen Geschäftstätigkeit erbringen. Unter «kritischen Infrastrukturen» sind u.E. die meldepflichtigen Organisationen und Behörden i.S.v. Art. 74b rev. ISG zu verstehen.

Solche Dienstleister – bspw. IT-Provider – sind schon gemäss der heutigen Praxis des BACS und des Swiss FS-CSC zur Teilnahme am Informationsaustausch der auslagernden Organisation auf dem CSH zugelassen, wenn sie die Anforderungen des BACS erfüllen (z.B. ein auf diese Situation zugeschnittenes Non-Disclosure Agreement unterzeichnen). Art. 14 E-CSV hält diese Praxis nun verbindlich fest.

Vorschlag

Wir schlagen vor, Art. 14 E-CSV wie folgt zu präzisieren: «Die Betreiberinnen kritischer Infrastrukturen können dem BACS Dienstleister melden, die für sie Dienstleistungen im Rahmen ihrer Geschäftstätigkeit erbringen (z.B. im Rahmen eines Outsourcings) und deshalb zusammen mit ihnen am Informationsaustausch teilnehmen wollen.»

Wir bitten Sie um die wohlwollende Prüfung unserer vorstehend geschilderten Anliegen und stehen auf Ihren Wunsch für deren gesprächsweise Erläuterung gerne zur Verfügung.

Freundliche Grüsse

August Benz
Leiter Geschäftsbereich International & Transformation
und stellvertretender CEO der Geschäftsstelle
Schweizerische Bankiervereinigung

Alexandra Arni
Geschäftsführerin
Swiss FS-CSC

FDP
Die Liberalen

FDP.Die Liberalen, Postfach, 3001 Bern

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport (VBS)

Bern, 12. März 2025 / SO
VL_CSV_d

Elektronischer Versand: ncsc@ncsc.admin.ch

Cybersicherheitsverordnung (CSV)
Vernehmlassungsantwort der FDP.Die Liberalen

Sehr geehrte Damen und Herren

Für Ihre Einladung zur Vernehmlassung oben genannter Vorlage danken wir Ihnen. Gerne geben wir Ihnen im Folgenden von unserer Position Kenntnis.

Obwohl die FDP Schweiz die Meldepflicht von Cyberangriffen grundsätzlich befürwortet, da sie zu mehr Sicherheit beiträgt, darf diese Pflicht aber nicht zu einer übermässigen administrativen Belastung der betroffenen Unternehmen führen. Es muss somit eine wirtschaftlich verträgliche Lösung gefunden werden.

Allein schon kleine und mittlere Unternehmen (KMUs) müssten für die Umsetzung der Meldepflicht gemäss CSV erhebliche finanzielle Ressourcen aufwenden (geschätzt zwischen 500 Mio. und 1 Mia. CHF) oder eine ausserordentlich gut ausgestattete IT-Abteilung besitzen, um die geforderten Informationen im geplanten Umfang und innerhalb der vorgesehenen Fristen melden zu können. Die geplante Einführung der Verordnung auf Anfang 2025 lässt den Unternehmen zudem keine Zeit, sich ausreichend auf diese neue Verpflichtung vorzubereiten. Wir fordern daher für die Einführung der Meldepflicht eine Übergangsfrist von mindestens 12 Monaten, vorzugsweise 24 Monate, um den Unternehmen eine faire Chance zu geben, die notwendigen internen Prozesse zu erarbeiten und einzuführen, Personal zu rekrutieren sowie Schulungen durchzuführen und Systemanpassungen vorzunehmen.

Die Einführung spezifischer Prozesse und Systeme für die Umsetzung der geplanten Meldepflicht von Cyberangriffen ist nicht trivial und stellt eine erhebliche bürokratische Belastung für die betroffenen Unternehmen dar. Der detaillierte Informationskatalog, der innerhalb von 24 Stunden bzw. innerhalb von 2 Wochen nach einem Cyberangriff ausgefüllt werden muss, ist aus unserer Sicht inhaltlich zu umfangreich und schwer verständlich.

Die FDP Schweiz weist darauf hin, dass im Rahmen der Meldepflicht sensible Unternehmensdaten an staatliche Stellen übermittelt werden müssen. Dies stellt eine erhebliche Gefahr für den Informationsschutz, den Datenschutz sowie für die Wahrung von Geschäftsgeheimnissen dar.

Die FDP appelliert deshalb an eine Datensparsamkeit. Es sollte klar definiert werden, welche Daten tatsächlich zur Erhöhung der Sicherheit notwendig sind. Daten, die keinen direkten Beitrag zur Cybersicherheit leisten, sollten nicht gemeldet werden müssen. Zudem sollte das Bundesamt für Cybersicherheit (BACS) Schulungen und Veranstaltungen für meldepflichtige

Unternehmen organisieren, um diese auf die neuen Pflichten rechtzeitig vorzubereiten. Auch vor diesem Hintergrund ist die Einführung der Meldepflicht per Anfang 2025 nicht realistisch.

Wir möchten betonen, dass wir uns für die Belange der Unternehmen und insbesondere auch der KMUs einsetzen. Es ist uns deshalb ein Anliegen, dass diese Verordnung so ausgestaltet wird, dass sie die Sicherheit erhöht, ohne aber die Unternehmen übermässig zu belasten. Aus all diesen Gründen erachten wir eine gründliche Überarbeitung der Verordnung in Zusammenarbeit mit der Wirtschaft und den Wirtschaftsverbänden als unerlässlich.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und für die Berücksichtigung unserer Überlegungen.

Freundliche Grüsse

FDP.Die Liberalen

Der Präsident

Der Generalsekretär

Thierry Burkart
Ständerat

Jonas Projer

Numero			Bellinzona
4380	fr	0	11 settembre 2024

Consiglio di Stato
Piazza Governo 6
Casella postale 2170
6501 Bellinzona
telefono +41 91 814 41 11
fax +41 91 814 44 35
e-mail can@ti.ch
web www.ti.ch

Repubblica e Cantone
Ticino

Il Consiglio di Stato

Onorevole Consigliera federale
Viola Amherd
Direttrice DDPS
3003 Berna

ncsc@ncsc.admin.ch

Procedura di consultazione
Ordinanza sulla cibersicurezza (OCS)

Signora Consigliera federale,
gentili signore, egregi signori,

vi ringraziamo per essere stati coinvolti nella procedura di consultazione sull'Ordinanza sulla cibersicurezza, in scadenza il prossimo 13 settembre.

Salutiamo con favore l'Ordinanza che considera gli elementi essenziali della cibersicurezza in Svizzera, ponendo le basi per un'attuazione mirata dell'obbligo di segnalare ciberattacchi. Sulla stessa non abbiamo particolari osservazioni.

Vogliate gradire, signora Consigliera Federale, gentili signore, egregi signori, i sensi della nostra massima stima.

PER IL CONSIGLIO DI STATO

Il Presidente — Il Cancelliere

Christian Vitta — Arnoldo Coduri

Copia a:
- Dipartimento finanze ed economia (dfe-dir@ti.ch)
- Dipartimento delle istituzioni (di-dir@ti.ch)
- Divisione delle risorse (dfe-dr@ti.ch)
- Centro dei sistemi informativi (dfe-csi@ti.ch)
- Deputazione ticinese alle Camere federali (can-relazioniesterne@ti.ch)
- Pubblicazione in internet

per Email: ncsc@ncsc.admin.ch

und A-Post

Departement für Verteidigung, Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS
Schwarztorstrasse 59
CH-3003 Bern

Zürich, 12. September 2024

Entwurf der Verordnung über die Cybersicherheit (Cybersicherheitsverordnung, CSV)

Eingabe der *swissICT* zur laufenden Vernehmlassung

Sehr geehrte Damen und Herren

Wir nehmen Bezug auf die Einladung zur Vernehmlassung zum Entwurf der Verordnung über die Cybersicherheit (Cybersicherheitsverordnung, CSV). Namens der *swissICT* reichen wir hiermit unsere Positionen zum Vorschlag, insbesondere betreffend Art. 9 und Art. 16 ff., des Entwurfs, ein und bedanken uns für die Gelegenheit zur Stellungnahme.

1. Legitimation und Betroffenheit

1 *swissICT* ist ein im Jahr 2000 durch die Fusion zweier Verbände – Schweizerische Vereinigung für Datenverarbeitung (SVD, gegründet 1968) und Wirtschaftsinformatik-Fachverband (WIF, gegründet 1955) – gegründeter Verband und vertritt ICT-Anbieter, -Anwender sowie -Fachkräfte in der Schweiz. Mit fast 2'500 Mitgliedern ist *swissICT* der primäre Repräsentant des ICT-Werkplatzes Schweiz und der grösste Fachverband der Branche.

2 Viele *swissICT* Mitglieder sind von der CSV und namentlich der Meldepflicht direkt betroffen, sei es als Anwender oder als Anbieter von ICT-Dienstleistungen an Unternehmen, die sich als kritische Infrastruktur qualifizieren.

3 Die Stellungnahme beschränkt sich entsprechend auf jene Punkte, welche für alle betroffenen Mitglieder von *swissICT* relevant und kritisch sind, also sowohl für Anbieter wie für Anwender.

2. Vernehmlassung

2.1. Formelles

4 Selbst für Personen mit juristischem Hintergrund ist es aufwändig und schwierig zu evaluieren, ob eine Gesetzesbestimmung in der Verordnung konkretisiert wird bzw. auf welche Gesetzesbestimmung sich die Versordnung jeweils bezieht. Für die bessere Allgemeinverständlichkeit und bessere Anwendbarkeit der CSV regen wir dringend an, bei allen Bestimmungen der CSV zu erwähnen, welche Gesetzesbestimmung sie ausführen, ergänzen, vervollständigen oder konkretisieren. Die CSV sollte unseres Erachtens auch für IT-Fachleute ohne Beizug von Juristen verständlich sein.

2.2. Zu Art. 9 CSV (Offenlegung von Schwachstellen)

5 Die geplante koordinierte Offenlegung gemäss Art. 9 Abs. 1 CSV bringt für Hersteller eine zusätzliche Belastung mit sich, da die Zusammenarbeit mit dem BACS sowie die Einhaltung der Normen und Fristen erhebliche administrative und technische Ressourcen erfordern, die dann für die eigentliche Fehlerbehebung fehlen. Besonders kleinere Unternehmen dürften stärker betroffen sein.

6 Zudem bestehen Bedenken hinsichtlich der Vertraulichkeit geschäftskritischer Informationen bei der Offenlegung von Schwachstellen, da dies das Vertrauen der Kunden in die Sicherheit der Softwareprodukte untergraben und bei negativer Berichterstattung den Ruf der Hersteller schädigen kann. Geschäftsgeheimnisse, die bei der Offenlegung von Schwachstellen betroffen sein können, sind zudem strafrechtlich und zivilrechtlich geschützt. Immerhin sieht Art. 73c Abs. 2 des revidierten ISG vor, dass Angaben zur betroffenen Hard- oder Software nur mit Einwilligung der Herstellerin gemacht werden dürfen, es sei denn, die Frist zur Behebung von Schwachstellen ist nicht eingehalten worden.

7 Die Fristsetzung zur Behebung von Schwachstellen ist im revidierten ISG in Art. 73b Abs. 3 vorgesehen, allerdings ohne genaue Angaben zur Dauer. Eine Frist von 90 Tagen gemäss Art. 9 Abs. 2 CSV wird aus unserer Sicht als vertretbar angesehen, wobei unklar ist, um wie viel diese Frist gemäss Art. 9 Abs. 3 CSV maximal verkürzt werden kann. Die Festlegung dieser Details in der Verordnung würde zur Rechtssicherheit beitragen.

8 Besorgnis besteht auch darüber, dass Informationen über Schwachstellen durch die Offenlegung gegenüber Betreiberinnen gemäss Art. 9 Abs. 5 CSV vor deren Behebung bekannt werden können, was das Risiko von Cyberangriffen erhöht und das Vertrauen der Kunden sowie den Ruf der Hersteller schädigen kann. Alle diese Auswirkungen wären kontraproduktiv. Unbefriedigend erscheint uns zudem die Einschränkung auf die Herstellerin in Art. 9 Abs. 2 CSV. In vielen Fällen wird nicht mehr die Herstellerin, sondern vielmehr nur noch die Nutzerin oder Betreiberin eine Schwachstelle beheben können (z.B. bei Individualentwicklung von Software nach Go-Live). Entsprechend sollte die Betreiberin als potenziell Behebungspflichtige ergänzt werden.

2.3. Zu Art. 16 (Ausnahmen Meldepflicht)

9 Art. 16 CSV regelt die Ausnahmen von der Meldepflicht. Gemäss Art. 74c ISG sollen Ausnahmen dann gelten, “wenn durch Cyberangriffe ausgelöste Funktionsstörungen nur geringe Auswirkungen auf das Funktionieren der Wirtschaft oder das Wohlergehen der Bevölkerung haben.” Gemäss Art. 74a Abs. 4 ISG dient die Meldepflicht ausschliesslich dazu, “dass das NCSC Angriffsmuster auf kritische Infrastrukturen frühzeitig erkennen und dadurch mögliche Betroffene warnen und ihnen geeignete Präventions- und Abwehrmassnahmen empfehlen kann.”

10 Einzelne der Ausnahmen knüpfen an die Grösse einer potenziell meldepflichtigen Organisation an, namentlich Art. 16 Abs. 1 Bst. a CSV (Einwohnerzahl einer Gemeinde) und Art. 16 Abs. 2 CSV (Mitarbeiterzahl und Umsatz eines Unternehmens). Dadurch werden kleinere Gemeinden und Unternehmen von der Meldepflicht ausgenommen. Dies erscheint insbesondere unter dem zuvor erwähnten Aspekt der Früherkennung und -warnung als fragwürdig, nehmen Cyberkriminelle doch regelmässig zunächst kleinere Ziele als Angriffsobjekte ins Visier, da diese meist weniger resilient und entsprechend leichter angreifbar sind. Entsprechend müsste der Fokus der Früherkennung und -warnung gerade auf den kleineren Institutionen liegen.

11 Während Mindestaufgreifschwellen häufig sinnvoll sind, um KMU und kleinere Organisationen von administrativem Ballast zu verschonen, würden Sinn und Zweck der Meldepflicht durch eine solche Ausnahmeregelung letztlich vereitelt oder jedenfalls gefährdet. Bei der Meldepflicht besteht auch kein spezifischer Bedarf nach einer solchen Entlastung, ist der damit verbundene Zusatzaufwand (Ausfüllen des Meldeformulars) doch sehr überschaubar. Wir empfehlen daher, die Ausnahmen von Art. 16 Abs. 1 Bst. a und Art. 16 Abs. 2 CSV zu streichen.

2.4. Zu meldende Cyberangriffe (Art. 18 CSV)

12 Für die Verständlichkeit sollte ergänzt werden, dass sich Art. 18 CSV auf die Pflicht zur Meldung von Cyberangriffen auf kritische Infrastrukturen gemäss Art. 74d ISG bezieht.

13 Cyberangriffe müssen gemäss Art. 74c ISG gemeldet werden, wenn die Funktionsfähigkeit der kritischen Infrastruktur gefährdet ist. Art. 18 Abs. 1 Bst. a CSV sieht nun die Funktionsfähigkeit bereits dann gefährdet, wenn ein Systemunterbruch vorliegt und Mitarbeitende oder Dritte vom Systemunterbruch betroffen sind. Da bei praktisch jedem Systemausfall Mitarbeitende betroffen sind, wäre im Ergebnis praktisch jeder Systemunterbruch ein meldepflichtiges Ereignis.

14 Diese Definition von Art. 18 Abs. 1 Bst. a CSV scheint uns etwas ausufernd. Wir sind der Ansicht, dass nicht jeder Unterbruch eines IT Systems nach einem Angriff die Funktionsfähigkeit der kritischen Infrastruktur im Sinne des gesetzlichen Schutzziels gefährdet. Nicht jeder Systemunterbruch bedeutet eine Gefahr für das «Wohlergehen der Wirtschaft und Bevölkerung» gemäss Art. 5 ISG.

15 Ausserdem kann die Kopplung der Meldepflicht an einen Systemunterbruch falsche Anreize setzen. Ein Systemunterbruch kann eine wirksame Massnahme zur Verhinderung der weiteren Ausbreitung eines Angriffes sein und sollte daher nicht zur Vermeidung einer Meldepflicht unterlassen werden.

16 Wir regen daher an, eine Gewichtung vorzunehmen und die Bestimmung so einzuschränken, dass sie nur greift, wenn eine Gefahr für das Wohlergehen der Wirtschaft und Bevölkerung besteht. Beispielsweise durch Beschränkung auf Unterbrüche von systemkritischen Teilen kritischer Infrastruktur, durch Abstellen auf einen Betriebsunterbruch (statt Systemunterbruch), auf eine längere Dauer eines Systemunterbruches oder durch das Einfügen einer kumulativen Verknüpfung von Bst. a und Bst. b.

2.5. Inhalt und Übermittlung der Meldung (Art. 19 - 21 CSV)

17 Die Meldepflicht gemäss CSV enthält zwingende Informationen, die mitgeteilt werden müssen. Die Aufzählungen im ISG und in der CSV sind nicht klar abgegrenzt: Teilweise enthält die CSV erweiterte Informationen, teilweise wiederholt die CSV (Art. 19 ff.) den Katalog gemäss ISG. Dies ist zu bereinigen oder aber klar darauf hinzuweisen.

18 Hinweise, ob der Angriff mit Erpressungsversuchen oder Lösegeldzahlungen einher geht, sollten nicht als Pflicht in die CSV aufgenommen werden. Solche Informationen sind für den Verlauf der Meldung nicht zwingend, können aber für Unternehmen eine weitreichende Auswirkung haben, wenn dies publik wird. Ergo ist Art. 19 Abs. 2 CSV ersatzlos zu streichen. Im Meldeformular können solche Informationen fakultativ abgefragt werden.

19 Sind bei der Erstmeldung noch nicht alle Informationen erfasst, sollten diese so rasch als möglich nachgereicht werden (sobald verfügbar). Die vorgesehene 14-tägige Frist ist (zu) spät (vgl. Art. 21 Abs. 1 CSV); sinnvoller wäre die Ergänzung, die Informationen sobald verfügbar mitzuteilen. Ebenso sollte ergänzt werden, was das BACS mit den Informationen tut resp. zu tun hat, da weitere Schritte, Austausche etc. in der CSV nicht weiter beschrieben sind. Der Mehrwert der Meldepflicht erschliesst sich deshalb hier nicht.

2.6. Entwurf Meldeformular

20 Mit der Vernehmlassungsvorlage zur CSV wurde auch der Entwurf eines Meldeformulars für Cyberangriffe publiziert. Wir begrüssen grundsätzlich das Vorgehen, für die Erfüllung der Meldepflicht ein entsprechendes Formular bereitzustellen.

21 Zum Entwurf des Meldeformulars bringen wir die Bemerkung an, dass ein Eingabefeld zur eigentlichen Beschreibung des Cyberangriffs nicht vorgesehen ist. Dies mag insoweit folgerichtig sein, als auch Art. 74e ISG hierzu keine Informationen verlangt, was aber möglicherweise ein gesetzgeberisches Versehen darstellt. Daher sollte diese für das Verständnis eines Cyberangriffs wichtige Information zumindest auf freiwilliger Basis (Ausgestaltung als optionales Eingabefeld) erhoben werden.

22 Unklar bleibt beim Meldeformular sodann der Nutzen bzw. Mehrwert der Option, eine Meldung zugleich an den EDÖB abzusetzen, wenn mit einer solchen Meldung die Meldepflicht im Falle einer Verletzung der Datensicherheit nach DSG nicht erfüllt werden kann. Für die meldepflichtige Organisation resultieren keine Synergien, und der EDÖB erhält in unterschiedlichen Zeitintervallen (24 Stunden vs so rasch als möglich) unterschiedliche Meldungen zum selben Vorfall, was wenig sinnvoll erscheint.

23 Die Meldepflicht des ISG resp. der CSV ist bekanntlich eine von mehreren (sich häufenden) Meldepflichten wie jener nach der entsprechenden FINMA Aufsichtsmitteilung oder die Meldung von Datensicherheitsverletzungen gemäss DSG. Hinzu kommen häufig Meldepflichten nach europäischem Recht, die für Unternehmen insgesamt den administrativen Aufwand massiv erhöhen und damit wichtige Ressourcen im Fall eines Cybersecurity-Vorfalls binden. Die Vorgaben der CSV sollten wenigstens hinsichtlich schweizerischer Meldepflichten harmonisiert und nach dem Prinzip des *Single Point of Contact* behandelt werden: Geht die Meldung bei einer Behörde ein, so gilt sie auch den übrigen als zugestellt; die zuständigen Behörden sollten es ermöglichen, dass eine Eingabe gleichzeitig an verschiedene Ämter und Stellen zugestellt werden kann und dass damit die Meldepflicht als erfüllt gelten kann.

Wir danken Ihnen im Namen unserer Mitglieder im Voraus dafür, dass Sie unsere Anregungen in geeigneter Weise bei der definitiven Formulierung der CSV berücksichtigen.

Gerne stehen wir Ihnen für Rückfragen und weitere Diskussionen zur Verfügung.

Freundliche Grüsse

Kathy Riklin
Vorstandsmitglied swissICT
Alt-Nationalrätin
Leiterin der Politik-Kommission swissICT

Christian Hunziker
Geschäftsführer swissICT

Dachorganisation der Schweizer KMU
Organisation faîtière des PME suisses
Organizzazione mantello delle PMI svizzere
Umbrella organization of Swiss SME

Madame la Conseillère fédérale Amherd
Département fédéral de la défense,
de la protection de la population et des sports DDPS
Bundeshaus Ost
3003 Berne

ncsc@ncsc.admin.ch

Berne, le 12 septembre 2024 usam-MH/zh

Réponse à la procédure de consultation :
Adoption de l'ordonnance sur la cybersécurité (OCyS)

Madame la Conseillère fédérale Amherd,
Madame, Monsieur,

Plus grande organisation faîtière de l'économie suisse, l'Union suisse des arts et métiers usam représente plus de 230 associations et plus de 600 000 PME, soit 99,8% des entreprises de notre pays. La plus grande organisation faîtière de l'économie suisse s'engage sans répit pour l'aménagement d'un environnement économique et politique favorable au développement des petites et moyennes entreprises.

Le 22 mai 2024, le Département fédéral des finances nous a convié à prendre position dans le cadre de la procédure de consultation sur l'Adoption de l'ordonnance sur la cybersécurité (OCyS).

L'usam demande à être représentée directement dans le comité de pilotage pour la Cyberstratégie nationale. L'usam exige par ailleurs quelques précisions sur les cas de cyberattaques à annoncer, sinon les entreprises concernées resteront dans une situation d'incertitude juridique.

I. Contexte

L'ordonnance sur la cybersécurité (OCyS) a pour but de renforcer la protection des infrastructures critiques en Suisse contre les cyberattaques, en imposant notamment une obligation de signaler les incidents de cybersécurité. Elle s'inscrit dans la révision de la Loi sur la sécurité de l'information (LSI), qui a été approuvée en 2023 et qui entrera en vigueur le 1er janvier 2025. Cette révision prévoit la mise en place d'un cadre légal pour signaler les cyberattaques qui visent les infrastructures critiques, telles que l'énergie, les transports ou les services financiers.

L'Office fédéral de la cybersécurité (OFCS), créé récemment au sein du Département fédéral de la défense, de la protection de la population et des sports (DDPS), succède au Centre national pour la cybersécurité. Cet office aura pour mission de collecter et d'analyser les signalements, de faciliter l'échange d'informations entre les autorités et les entités concernées, et de fournir un soutien en cas

d'incident. Il jouera un rôle central dans la gestion des cyberattaques et des menaces à l'échelle nationale.

L'ordonnance introduit également un système de communication sécurisé pour améliorer la détection des cybermenaces et la coordination des réponses. Ce système permettra aux infrastructures critiques de recevoir des informations actualisées sur les menaces et de réagir rapidement. Un comité de pilotage pour la Cyberstratégie nationale, composé de représentants des départements fédéraux, des cantons, de l'économie et des universités, sera responsable de la mise en œuvre de la stratégie de cybersécurité.

Enfin, l'OCyS prévoit la gestion et la divulgation coordonnée des vulnérabilités dans les systèmes informatiques, en collaboration avec les fabricants et les autorités compétentes. Ces mesures visent à mieux protéger les infrastructures critiques et à renforcer la résilience du pays face aux cyberattaques.

II. Appréciation de l'usam

Pour l'usam, il est important de ne pas conduire à des sanctions des entreprises touchées, mais à trouver des solutions basées sur la coopération entre la Confédération et l'économie privée.

L'usam a ainsi deux demandes de précisions pour réduire les incertitudes dans la mise en œuvre de cette ordonnance. Il s'agit de l'art. 18, alinéas 1 et 2 ; les propositions de modification ainsi que les justifications sont visibles en vert. L'arrière-plan de l'ajustement souhaité est la crainte que la formulation actuelle n'oblige potentiellement à signaler chaque compromission d'un système.

Art. 18 Cyberattaques à signaler

1. La fonctionnalité d'une infrastructure critique est considérée comme menacée lorsque :

   1.1 . les employés ou des tiers sont affectés par des interruptions de système ; ou

   1.2. l'organisation ou l'autorité concernée ne peut plus maintenir ses activités qu'à l'aide de plans d'urgence.

Explication du rapport explicatif : *La fonctionnalité d'une infrastructure critique peut être menacée par une cyberattaque si les systèmes informatiques, réseaux ou systèmes de contrôle essentiels au fonctionnement de l'infrastructure sont compromis de telle manière qu'il en résulte des interruptions de système pour les employés et des tiers (art. 18, al. 1, let. a de cette ordonnance) ou que l'organisation ou l'autorité concernée ne peut plus maintenir ses activités qu'à l'aide de plans d'urgence (art. 18, al. 1, let. b de cette ordonnance).*
Une interruption de système se produit lorsque les employés ou des tiers ne peuvent plus exécuter des étapes importantes de leur travail en raison de l'indisponibilité des moyens informatiques nécessaires. Les plans d'urgence comprennent toutes les mesures techniques ou organisationnelles qui doivent être prises lorsque les moyens informatiques habituellement utilisés ne sont plus disponibles de manière imprévue et temporaire.

L'usam a des doutes sur ce que signifie exactement "essentiels au fonctionnement". Par exemple, le poste de travail d'un ingénieur télécom compromis par un malware entre-t-il dans le cadre de cette réglementation, dans la mesure où, pendant le nettoyage de son poste de travail, il ne pourrait plus exécuter certaines étapes importantes de son travail ?

L'usam demande de préciser cette règle, par exemple ainsi : "Les employés ou des tiers, qui sont directement responsables du fonctionnement immédiat de l'infrastructure critique, sont affectés par des interruptions de système causées par des cyberattaques, mettant ainsi directement en danger la stabilité du fonctionnement de l'infrastructure."

2. Une manipulation ou une fuite d'informations se produit lorsque :

   2.1 des informations pertinentes pour l'activité sont modifiées ou divulguées par des personnes non autorisées ; ou

   2.2 une violation de la sécurité des données au sens de l'article 24 de la loi fédérale sur la protection des données du 25 septembre 2020 se produit.

Pour l'usam, il serait nécessaire de préciser ce que l'on entend exactement par "informations pertinentes pour l'activité". Par exemple, si une application Web de l'entreprise XY, fournissant un service sans lien direct avec l'exploitation d'une infrastructure critique, est compromise, cela doit-il être signalé ?

L'usam demande d'ajouter une formulation du type : "des informations pertinentes pour l'activité, liées au fonctionnement immédiat de l'infrastructure critique".

Nous vous remercions de l'attention portée à notre prise de position et vous présentons, Madame, Monsieur, nos respectueuses salutations.

Union suisse des arts et métiers usam

Urs Furrer
Directeur

Mikael Huber
Responsable du dossier

KANTON
APPENZELL INNERRHODEN

Landammann und Standeskommission

Sekretariat Ratskanzlei
Marktgasse 2
9050 Appenzell
Telefon +41 71 788 93 11
info@rk.ai.ch
www.ai.ch

Ratskanzlei, Marktgasse 2, 9050 Appenzell

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

Appenzell, 12. September 2024

Cybersicherheitsverordnung (CSV)
Stellungnahme Kanton Appenzell I.Rh.

Sehr geehrte Damen und Herren

Mit Schreiben vom 22. Mai 2024 haben Sie uns die Vernehmlassungsunterlagen zur Cybersicherheitsverordnung zukommen lassen.

Die Standeskommission hat die Unterlagen geprüft. Die Zusammenarbeit mit kompetenten Partnern im Bereich der Cybersicherheit ist für den Kanton Appenzell I.Rh. von elementarer Bedeutung, da die Ressourcen in diesem Bereich sehr begrenzt sind. Nur durch eine solche Zusammenarbeit können wir eine angemessene Gewährleistung der Sicherheit unserer kritischen Infrastrukturen sicherstellen.

Die Einführung einer Meldepflicht für Cyberangriffe ist ein entscheidender Schritt, um das Bundesamt für Cybersicherheit (BACS) in die Lage zu versetzen, eine umfassende Übersicht über Cyberangriffe in der Schweiz zu erhalten und die betroffenen Parteien effektiv zu unterstützen. Die klaren Richtlinien und Fristen für die Meldung von Cyberangriffen, wie sie in der Verordnung festgelegt sind, werden die Effizienz und Effektivität der Reaktion auf solche Bedrohungen erheblich verbessern.

Wir begrüssen die Bestrebungen des Bundes, die strategische Steuerung der Cybersicherheit in der Schweiz zu verbessern und die Aufgaben, die sich aus dem Informationssicherheitsgesetz ergeben, klar zu definieren. Diese Massnahmen sind entscheidend, um die Cybersicherheit in der Schweiz zu stärken und eine zielgerichtete Umsetzung der Meldepflicht zu gewährleisten.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme und grüssen Sie freundlich.

Im Auftrage von Landammann und Standeskommission
Der Ratschreiber:

Markus Dörig

Zur Kenntnis an:
- Finanzdepartement, Amt für Informatik Appenzell I.Rh., Hauptgasse 51, 9050 Appenzell
- Ständerat Daniel Fässler, Weissbadstrasse 3a, 9050 Appenzell
- Nationalrat Thomas Rechsteiner (thomas.rechsteiner@parl.ch)

piratenpartei
www.piratenpartei.ch

Piratenpartei Schweiz, 3000 Bern

Stellungnahme der Piratenpartei Schweiz zur Verordnung über die Cybersicherheit (CSV)

Sehr geehrte Frau Bundesrätin Amherd

Sehr geehrte Damen und Herren

Bezugnehmend auf die Vernehmlassungseröffnung vom 22.05.2024 nehmen wir gerne Stellung.
Im Weiteren finden wir Piraten es sehr bedenklich, dass Sie für die Stellungnahme auf eine proprietäre Software verweisen (Word der Firma Microsoft), obwohl es heutzutage zahlreiche offene und freie Dateiformate gibt. Wir entsprechen ihrem Wunsch mit einer docx-Datei, welche auch in neueren Word Versionen geöffnet werden kann.
Die Piratenpartei Schweiz setzt sich seit Jahren für eine humanistische, liberale und progressive Gesellschaft ein. Dazu gehören die Privatsphäre der Bürger, die Transparenz des Staatswesens, inklusive dem Abbau der Bürokratie, Open Government Data, den Diskurs zwischen Bürgern und Behörden, aber auch die Abwicklung alltäglicher Geschäfte im Rahmen eines E-Governments. Jede neue digitale Schnittstelle und Applikation bedingt aber eine umfassende Risikoanalyse und Folgeabschätzung.
Gerne nehmen wir wie folgt Stellung:

Art. 9 Abs. 6 CSV

Anregung: Streichung Abs. 6 oder Änderung, dass die Offenlegung grundsätzlich weiterhin nach Abs. 1-4 durchgeführt wird, aber unter Berücksichtigung der Besonderheiten der BAKOM Kontrolle.

Begründung:
Art. 9 CSV sieht eine koordinierte Offenlegung von Schwachstellen nach internationalen Standards vor. Abs. 6 setzt diese Regelung aber für Funde ausser Kraft, die das BAKOM «im Rahmen seiner Aufsichtskontrollen» entdeckt.

Im erläuternden Bericht wird dies damit begründet, dass das BAKOM im Rahmen der Kontrolle dem Wirtschaftsakteur, also demjenigen, der die fragliche Anlage einführt, betreibt o.ä., die Auskunft über die Schwachstelle schon vorgängig bekannt mache. Das bedeutet, dass dieser vor dem ausländischen Fabrikanten Kenntnis erlangt. Dies widerspricht je nachdem durchaus dem Ablauf der Offenlegung, aber scheint unwesentlich anders als das Vorwissen eines beliebigen betroffenen Betreibers, der die Angaben dem BACS zur Offenlegung übermittelt.

In der vorliegenden Fassung von Art. 9 Abs. 6 bleibt gänzlich unklar, was mit den Informationen geschieht. Dem erläuternden Bericht ist zwar zu entnehmen, dass das BACS damit vielleicht doch mit Abs. 1 fortfahren könnte, aber dieser Ablauf ist dem Verordnungstext schlicht nicht zu entnehmen.

Angesichts dessen, dass es sich hier um Schwachstellen in kritischer Infrastruktur – Fernmeldeanlagen bzw. Funkanlagen – handelt, ist dieser undefinierte Umgang aus unserer Sicht ungenügend. Die Behebung der Schwachstellen sollte nach gleichem Muster erfolgen (Streichung Abs. 6) oder zumindest sinngemässe Anwendung finden (Änderung Abs. 6). Wenn das BACS, nach erläuterndem Bericht, «gegebenenfalls» dann doch «die koordinierte Offenlegung der Schwachstellen nach Abs. 1 durchführt», sollte dies in der Verordnung auch festgehalten werden.

Die Vermeidung von gewissen «Kompetenzkonflikten und Doppelspurigkeiten» zwischen dem BACS und dem BAKOM dürfen jedenfalls nicht zu weniger allgemeiner Sicherheit führen.

Schlussbemerkungen

Wir beschränken uns in dieser Stellungnahme auf unsere Kernanliegen. Bei Verzicht unsererseits auf umfassende allgemeine Anmerkungen oder auf Anmerkungen zu einzelnen Regelungen, ist damit keine Zustimmung durch die Piraten zu solchen Regelungen verbunden.

Kontaktdetails für Rückfragen finden Sie in der Begleit-E-Mail.

Piratenpartei Schweiz, Arbeitsgruppe Vernehmlassungen, 10. September 2024

KANTON solothurn

Finanzdepartement

Rathaus
Barfüssergasse 24
4509 Solothurn
Telefon 032 627 20 57
finanzdepartement@fd.so.ch
so.ch

Peter Hodel
Landammann

Eidgenössisches Departement für
Verteidigung, Bevölkerungsschutz und
Sport VBS
Frau Bundesrätin Viola Amherd
Bundeshaus Ost
3003 Bern

13. September 2024

Vernehmlassung zur Cybersicherheitsverordnung (CSV)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

An der Bundesratssitzung vom 22. Mai 2024 wurde die Vernehmlassung zur neuen Cybersecurity-verordnung (CSV) eröffnet. Die Verordnung gibt vor, wie die Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen umgesetzt werden soll, regelt die Organisation zur Umsetzung der Nationalen Cyberstrategie und definiert die Aufgaben des neuen Bundesamts für Cybersicher-heit (BACS). Die Verordnung soll auch festlegen, welche Behörden und Unternehmen von der Meldepflicht ausgenommen sind.

Mit Schreiben vom 22. Mai 2024 wurde dem Kanton Solothurn die CSV zur Vernehmlassung unterbreitet. Wir bedanken uns für die Gelegenheit zur Stellungnahme.

Die CSV ist eine Ergänzung zur Informationssicherheitsverordnung (ISV) und fokussiert sich auf das Verhältnis zwischen dem BACS und den beteiligten Adressaten.

Der Kanton Solothurn, in seiner Rolle als Behörde mit kritischen Infrastrukturen begrüsst es, dass viel Wert auf transparente Informationen mit Möglichkeit zur Mitwirkung aller Stakeholder gelegt wird, was auch durch die Schaffung des Steuerungsausschusses Nationale Cyberstrategie (StA NCS) bestätigt wird. Die Strukturen, welche auch mit Einführung des BACS geschaffen wurden, erachten wir als sinnvoll und zielführend.

Sehr geschätzt wird dabei das Computer Emergency Response Team (CERT), welches einen Mehrwert für alle bietet und so die Zusammenarbeit untereinander stark fördert.

Weiter wird die koordinierte Offenlegung von Schwachstellen als grosser Vorteil erachtet. Die Nutzung des MITRE ATT&CK Frameworks (Referenzwerk) und die Verwendung der CVE-Nummern (Common Vulnerabilities and Exposures; System zur standardisierten Identifikation und Benennung von öffentlich bekannten Sicherheitslücken und anderen Schwachstellen in Computersystemen) bringt viel Struktur und sorgt für eine effiziente und einheitliche Information über Schwachstellen.

Als wichtig wird dabei auch die Möglichkeit zur Bekanntgabe von Schwachstellen vor der eigentlichen «Veröffentlichung» angesehen. Dies ermöglicht es den Betroffenen, Massnahmen zu treffen, bevor diese ausgenutzt werden. Dies erachten wir als eine wirksame Risikominderung.

Wir begrüssen zudem die Bereitstellung eines sicheren Kommunikationssystems für den Datenaustausch mit dem BACS. Dies ermöglicht eine rasche Berichterstattung und erhöht die Transparenz. Alle Parteien verfügen somit über die gleichen Informationen und Vorgänge. Die Möglichkeit, selbst Informationen zu übermitteln und dabei entscheiden zu können, wer Empfänger dieser ist, ist in der Verordnung adäquat umgesetzt.
Die in Art. 16 CSV vorgesehenen Ausnahmen von der Meldepflicht sind für uns stimmig und nachvollziehbar.

Insgesamt sind wir der Überzeugung, dass die Cybersicherheitsverordnung und die Zusammen-arbeit aller Akteure zur Stärkung der nationalen Cybersicherheit beitragen.

Freundliche Grüsse

Peter Hodel
Landammann

Sunrise GmbH
Thurgauerstrasse 101B
CH-8152 Glattpark (Opfikon)

sunrise.ch

Regulatory Affairs
+41 76 777 10 52

regulatory@sunrise.net

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS
Schwarztorstrasse 59
CH-3003 Bern

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

Opfikon, 13. September 2024

Stellungnahme zum Entwurf der Cybersicherheitsverordnung (CSV)

Sehr geehrte Frau Bundespräsidentin

Sunrise erbringt als grösstes privates Telekommunikationsunternehmen der Schweiz führende Mobilfunk-, Internet-, TV- und Festnetzdienste für rund 3 Mio. Privat- und Geschäftskunden. Der vorgeschlagene Entwurf der Cybersicherheitsverordnung (CSV) ist für Sunrise als Betreiberin einer kritischen Infrastruktur von hoher Relevanz. Wir danken Ihnen deshalb für die Möglichkeit, zum Entwurf Stellung nehmen zu können. Sunrise unterstützt das Ziel des Informationssicherheitsgesetzes, die Widerstandsfähigkeit der Schweiz gegenüber Cyberrisiken zu erhöhen. Die Präzisierungen der Vorgaben des ISG in der vorgeschlagenen CSV erachten wir grundsätzlich als zweckmässig und angemessen.

Meldeverfahren harmonisieren und koordinieren

Bereits in unserer Stellungnahme zum Entwurf des Bundesgesetzes über die Informationssicherheit beim Bund (ISG) haben wir auf die Schwierigkeiten durch die verschiedenen Meldeverfahren bei Cyberangriffen hingewiesen. So müssen diese unter Umständen mit jeweils unterschiedlichen Inhalten und Fristen sowohl der Nationalen Alarmzentrale (Art. 96 FDV), dem EDÖB (Art. 15 DSV) wie auch dem BACS (Art. 74a nISG) gemeldet werden. Das ist aufwändig, ineffizient und birgt die Gefahr von Fehlern. Aus unserer Sicht ist darum dringend auf Lösungen für eine Harmonisierung und Koordination der verschiedenen Meldeverfahren hinzuwirken. In diesem Sinne sind die Regelungen zur Koordination zwischen dem BACS und dem BAKOM in Art. 9 Ziff. 7 und Ziff. 8 der richtige Ansatz.

Art. 18 E-CSV 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. Wir beantragen in Art. 18 E-CSV folgende Anpassungen:

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 (…).

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

Art. 19 E-CSV Inhalt der Meldung

Die Meldung gemäss Art. 19 kann auch Personendaten umfassen, wobei das Informationssicherheitsgesetz 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.

Art. 23 Inkrafttreten

Ein Inkrafttreten per 1. Januar 2025 ist zu früh. Der endgültige Wortlaut der Regelung wird erst mit der offiziellen Veröffentlichung der Verordnung feststehen, was vermutlich erst kurz vor dem 1. Januar 2025 geschehen wird. Viele Unternehmen werden daher bis dahin nicht wissen, ob und inwiefern sie von der Regelung betroffen sind. Auch das angekündigte Meldeformular könnte bis Ende 2024 noch nicht vollständig ausgearbeitet sein. Es bedarf deshalb eine Umsetzungsfrist von mindestens einem halben Jahr.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen. Bei Fragen stehen wir gerne zur Verfügung.

Freundliche Grüsse

Marcel Huber
General Counsel & Chief Corporate Affairs Officer

Matthias Forster
Senior Regulatory Affairs Manager

Vernehmlassung zur Cybersicherheitsverordnung

Sehr geehrte Damen und Herren

Die Transitgas AG bedankt sich für die Gelegenheit, zum Entwurf über die Verordnung der Cybersicherheit Stellung zu nehmen. Gerne dürfen wir Ihnen mitteilen, dass wir die Cybersicherheitsverordnung und die darin festgelegten Massnahmen zur Verbesserung der Cybersicherheit in der Schweiz begrüssen. Die Verordnung stellt einen wichtigen Schritt dar, um die Sicherheit und Resilienz kritischer Infrastrukturen zu gewährleisten.

Die Transitgas AG als Betreiberin einer wichtigen Infrastruktur untersteht den Meldepflichten. Dies ermöglicht es, schneller auf Bedrohungen zu reagieren und geeignete Gegenmassnahmen zu ergreifen. Wir begrüssen auch die Rolle des Bundesamts für Cybersicherheit als zentrale Anlaufstelle für die Meldung und Koordination von Cyberfällen. Das Kommunikationssystem für den sicheren Informationsaustausch wird dazu beitragen, die Zusammenarbeit zwischen Behörden und Organisation zu stärken. Auch die Einführung eines Frühwarnsystems zur Beurteilung der Bedrohungslage wird als wichtiger Bestandteil der Verordnung begrüsst, ebenso die Massnahmen zur Sicherstellung des Datenschutzes und der Datensicherheit.

Mit freundlichen Grüssen

Transitgas AG

Die Schweizerische Post AG
Stab CEO
Regulatory Affairs
Wankdorfallee 4
3030 Bern

Telefon +41 58 341 15 64
Fax +41 58 667 33 73
www.post.ch

Die Schweizerische Post AG, Stab CEO RA, Wankdorfallee 4, 3030 Bern

Eidg. Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Als PDF/Word an: ncsc@ncsn.admin.ch

Datum 9. September 2024
Kontaktperson
E-Mail
Direktwahl 079 810 00 39

Stellungnahme der Schweizerischen Post zur Vernehmlassung über die Verordnung über die Cybersicherheit

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, im Rahmen der Vernehmlassung über die Cybersicherheitsverordnung Stellung nehmen zu können.

a) Ausgangslage für die Schweizerische Post

IT ist seit Langem Teil des Postalltags: einerseits ermöglichen die sicheren und stabilen digitalen Systeme den reibungslosen Ablauf des physischen Kerngeschäfts. Andererseits schaffen sie die Voraussetzung dafür, dass die Post ihre Kompetenz, sensible Informationen sicher und vertrauensvoll zu transportieren, auch in der digitalen Welt umsetzen kann.

Informationssicherheit hat bei der Post höchsten Stellenwert. Die Post hat in den letzten Jahren ihre Kompetenzen und Ressourcen darum in der IT ausgebaut. Es ist unser Auftrag, die Daten, Informationssysteme und Dienstleistungen angemessen und verantwortungsvoll zu schützen. Cybervorfälle haben stark zugenommen. Die Post selbst ist ebenfalls regelmässig Ziel von Angriffsversuche. Aus unserer Sicht ist Sicherheit kein Zustand, sondern als kontinuierlicher Verbesserungsprozess zu verstehen. Die Post unternimmt alles, um ihre Informationssicherheit stetig zu verbessern. Insbesondere führt die Post seit 2019 ein Bug-Bounty-Programm, das ethischen Hackerinnen und Hackern aus aller Welt erlaubt, die Onlinedienste der Post zu prüfen. Damit finden wir heraus, wie sicher die digitalen Services der Post sind und wie wir den Schutz noch verbessern können.

Die Post und einzelne ihrer Konzerngesellschaften sind als Anbieterin von Postdiensten, insbesondere aber auch als Bank, als Anbieterin digitaler Vertrauensdienste, als Transportunternehmen im ÖV und als Herstellerin von Hard- und Software durch die neue Meldepflicht von Cybervorfällen betroffen. Sie pflegt

bereits heute eine enge Zusammenarbeit mit den entsprechenden Behörden. Dieser ist wichtig bei der wirkungsvollen Bekämpfung von Cyberrisiken.

b) Grundsätzliches zum Entwurf

Dass der Bund die Cybersicherheit in Zukunft weiter stärken will, begrüssen wir. Wir sind mit der Stossrichtung der vorliegenden Verordnung über die Cybersicherheit einverstanden. Folgende Punkte sind uns ein besonderes Anliegen:

1. **Steuerungsausschuss NCS (Art. 3 f. CSV:** Wir unterstützen es, einen Steuerungsausschuss Nationale Cyberstrategie (StA NCS) einzusetzen. Das ist aus unserer Sicht eine sinnvolle Massnahme. Wir schlagen aber vor, bei der Zusammensetzung dieses Steuerungsausschusses auch Vertreterinnen und Vertreter von kritischen Infrastrukturen zu berücksichtigen. Deren Einbindung ist unabdinglich. Die Formulierung «Vertreter der Wirtschaft» ist diesbezüglich zu wenig klar.

2. **Meldepflicht (Art. 18 CSV):** Wir regen an, den Schweregrad eines Cyberangriffs bei der Meldepflicht mitzuberücksichtigen. Dadurch könnte viel administrativer Aufwand vermieden werden. Wir möchten dadurch verhindern, dass beispielsweise kurze Systemausfälle bei einem eingeschränkten Personenkreis gemeldet werden müssen.
   Eine Abstufung bzw. eine Definition des Schweregrades wäre auch beim Abfluss von Informationen hilfreich. Wird lediglich ein unproblematisches Dokument publiziert, wiegt dies nicht so schwer, wie wenn vertrauliche sensible Daten an die Öffentlichkeit gelangen.

3. **Koordination des BACS:** Ziel muss sein, dass meldepflichtige Akteure jeweils nur eine Meldung an eine Behörde machen. Wir sehen das BACS in einer zentralen, koordinativen Rolle, was die Meldepflicht betrifft. Wir regen an, dass das BACS sämtliche meldepflichtigen Vorfälle entgegennimmt und diese dann mit weiteren relevanten Behördenstellen koordiniert. Eine einzige Meldestelle verhindert Mehraufwand und Doppelspurigkeiten.
   Alternativ können wir uns auch vorstellen, dass sich Behörden, an welche gemeldet werden muss (FINMA, EDÖB, BACS) untereinander koordinieren.

4. **Angaben zum Verursacher (Art. 19 CSV):** Im Rahmen der Meldung müssen auch Angaben zum Verursacher der Cyberattacke gemacht werden. Dies bedingt aufwändige forensische Verfahren und ist äusserst komplex. Aus unserer Sicht sollen die Unternehmen nicht Aufgaben im Bereich der Strafverfolgung übernehmen müssen - dies müsste zumindest freiwilliger Natur sein.

Wir bedanken uns für Ihre Kenntnisnahme und die Berücksichtigung unserer Anliegen.

Freundliche Grüsse

Die Schweizerische Post AG

Informatik / Technologie

Markus Herren
Stv. CISO Post Group

Stab CEO

Matthias Dietrich
Co-Leiter Stab CEO

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Ausschliesslich per E-Mail an:
ncsc@ncsc.admin.ch

13. September 2024

Stellungnahme zur Vernehmlassung des Bundesrates zum Erlass der Cybersicherheitsverordnung (CSV)

Sehr geehrte Damen und Herren

Im Mai 2024 haben Sie uns eingeladen, in oben genannter Sache Stellung zu nehmen. Diese Gelegenheit der Meinungsäusserung nehmen wir gerne wahr. economiesuisse nimmt gestützt auf den Input der betroffenen Mitglieder und aus einer übergeordneten, gesamtwirtschaftlichen Sicht wie folgt Stellung:

Zusammenfassung
economiesuisse unterstützt die Einführung einer schlanken und effizienten Meldepflicht für Betreiberinnen kritischer Infrastrukturen bei Cyberangriffen. Bereits das ISG hat diesem Anspruch nicht ausreichend Rechnung getragen. Die Ausführungsbestimmungen in der Vernehmlassungsvorlage gehen nun sogar noch über das Gesetz hinaus. Folgende Anpassungen für praxistaugliche Meldeprozesse sind unverzichtbar:

- Bessere Koordination und Harmonisierung mit anderen Vorschriften und Meldeverfahren, bspw. mit dem Datenschutzrecht oder dem Finanzmarktrecht.
- Weniger Formalismus und Detailregulierung, mehr partnerschaftliches und flexible, situationsgerechte Zusammenarbeit zwischen Bundesbehörden und Betreiberinnen kritischer Infrastrukturen. Dies gilt vor allem für die genaue Gestaltung der Meldeabläufe.
- Der Willen des Gesetzgebers ist besser zu berücksichtigen, insb. in Form von praktikablen Ausnahmeregeln von den neuen Meldepflichten. Ebenso ist auf einzelne Bestimmungen zu verzichten, denen eine explizite Rechtsgrundlage im ISG fehlt.
- Einführung einer Übergangsfrist von mindestens einem Jahr.

economiesuisse teilt die Einschätzung, dass aufgrund der rasant steigenden Zahl der Cyberangriffe auf Schweizer Unternehmen und Institutionen geeignete Schutzmassnahmen vorgekehrt werden müssen. Dies gilt im Speziellen für sog. kritische Infrastrukturen, welche aus systemischer Sicht eine erhöhte Resilienz aufweisen müssen, damit sie ihre versorgungskritische Funktion für Wirtschaft und Gesellschaft auch bei einem Cybervorfall oder -angriff erfüllen können. Im Lichte dieser Überlegungen

economiesuisse
Hegibachstrasse 47
Postfach
CH-8032 Zürich
Telefon +41 44 421 35 35

Verband der Schweizer Unternehmen
Fédération des entreprises suisses
Federazione delle imprese svizzere
Swiss Business Federation
www.economiesuisse.ch

hat das Parlament im vergangenen Herbst neue Meldepflichten für Betreiberinnen kritischer Infrastrukturen beschlossen.

Bereits im Rahmen dieser Revision des Informationssicherheitsgesetzes (ISG) haben wir folgende Kernanliegen der Gesamtwirtschaft eingebracht:

- Die Meldepflicht muss den betroffenen Unternehmen und der Volkswirtschaft letztlich mehr bringen, als sie kostet.
- Sie muss einen verhältnismässigen, subsidiären, risikobasierten Ansatz verfolgen, der administrative und finanzielle Aufwände auf ein Minimum reduziert.
- Es bedarf einer kooperativen Grundeinstellung, da sowohl die Behörden als auch die Unternehmen an einem bestmöglichen Schutz vor Cyber-Angriffen interessiert sind. Dabei müsste grundsätzlich von autoritären Massnahmen wie Bussen und Audits soweit möglich Abstand genommen werden, da sie die partnerschaftliche Basis der Zusammenarbeit in Frage stellen.

Im Kontext der Vernehmlassungsvorlage stellen wir generell Folgendes fest:

- Es fehlt nach wie vor an Koordination bzw. Harmonisierung der multiplen Meldeverfahren bei Cyberangriffen. So müssen Unternehmen (z.B. im Versicherungs- und Bankenbereich und der Luftfahrt) bei Cyberangriffen nicht selten gleich mehreren Verwaltungseinheiten Meldung machen (z.B. EDÖB, FINMA, BACS, BAZL) - und dies mit jeweils unterschiedlichen Inhalten und Fristen. Im Hinblick auf die breite Betroffenheit Schweizer Unternehmen vom EU Digital Operational Resilience Act kommen nebst der nationalen auch auf internationaler Ebene zusätzliche Anforderungen. Es ist deshalb auf Lösungen für eine Harmonisierung/Koordination der einzelnen Meldeverfahren hinzuwirken. Im Übrigen plädieren wir dafür, dass man die Meldepflichten an internationalen Standards auszurichten. Beispielsweise sollten die Fristen jenen der NIS-2-Richtlinie anpassen werden (24 Stunden für eine Frühwarnung, 72 Stunden für die Meldung eines Vorfalls). Die Meldequalität sollte gegenüber der Meldegeschwindigkeit im Vordergrund stehen.

- Bei der CSV handelt es sich um eine Ausführungsverordnung, welche nicht über die Konkretisierung des Gesetzes hinausgehen darf. Zahlreiche vorgeschlagene Regelungen gehen jedoch über den Willen des Gesetzgebers hinaus oder verfügen damit über Grundlage im Gesetz. Dies betrifft insbesondere die nationale Cyberstrategie und den Steuerungsausschuss (Art. 2-5 E-CSV). Zu beidem findet sich in der gesetzlichen Grundlage weder eine Bestimmung noch eine Delegationsklausel. Es ist generell fragwürdig, wenn solche Aspekte auf Verordnungsebene geregelt werden – auch wenn sie auf historisch gewachsenen Begebenheiten basieren (siehe auch Art. 164 Abs. 1 Bundesverfassung, wonach «Wichtiges» wie die Organisation der Bundesbehörden in einem Gesetz im formellen Sinn geregelt werden muss).

- Es ist festzuhalten, dass das "Bundesamt für Cybersicherheit" (BACS) seit dem 1. Januar 2024 das Nationale Zentrum für Cybersicherheit (NCSC) abgelöst hat. Diese Änderung hat im Schlussabstimmungstext der ISG-Revision vom 29. September 2023 noch keinen Eingang gefunden. Um Missverständnisse zu vermeiden, sollte diese Änderung im ISG baldmöglichst noch nachgezogen werden und ansonsten ist darauf zu achten, dass diese Änderung genug klar kommuniziert wird, damit dies auch für die Betroffenen der neuen Meldevorschriften verständlich ist.

- Bereits bei der Revision des ISG haben wir den unklaren Geltungsbereich als kritischer Punkt hervorgehoben. Auch im aktuellen Verordnungsentwurf bleiben Unsicherheiten, bspw.

hinsichtlich Betroffenheit von Unterlieferanten, wie etwa Cloud-Computing-Dienstleistern, Anbieterinnen von Sicherheitssoftware oder Suchmaschinen. Wir sind hier klar der Meinung, dass der Einbezug solcher Lieferanten nicht regulatorisch, sondern vertraglich zwischen den Betreiberinnen kritischer Infrastrukturen und ihren Lieferanten zu regeln ist.

- Ein Inkrafttreten per 1. Januar 2025 ist zu früh. Der endgültige Wortlaut der Regelung wird erst mit der offiziellen Veröffentlichung der Verordnung feststehen, was vermutlich erst kurz vor dem 1. Januar 2025 der Fall sein wird. Viele Unternehmen werden daher bis dahin nicht wissen, ob und inwiefern sie von der Regelung betroffen sind. Auch das angekündigte Meldeformular könnte bis Ende 2024 noch nicht vollständig ausgearbeitet sein. Es bedarf deshalb eine Umsetzungsfrist von mindestens einem Jahr.

Zu folgenden Artikeln nehmen wir ausführlicher Stellung:

Art. 4 E-CSV Zusammensetzung Steuerungsausschuss Nationale Cyberstrategie
Laut einer Medienmitteilung des BACS vom 7. Juni 2024 hat das VBS bereits den Steuerungsausschuss für die Nationale Cyberstrategie eingerichtet. Die Wirtschaft wird dort durch asut, future technologies und WiseStratEdge vertreten. Es wäre sinnvoll, zusätzlich zu diesen Vertretern auch ausdrücklich die Betreiber kritischer Infrastrukturen einzubeziehen. Obwohl es sicherlich Überschneidungen mit der Wirtschaftsvertretung gibt, sollte diese besonders betroffene Gruppe gezielt berücksichtigt werden. Zudem finden wir es fragwürdig, dass die Zusammensetzung des Steuerungsausschusses bereits vor Inkrafttreten der CSV festgelegt wurde.

Art. 7 E-CSV Technische Analyse von Cybervorfällen und Cyberbedrohungen
Betreffend die technische Analyse von Cybervorfällen und Cyberbedrohungen, plädieren wir für eine gemeinsame Präzisierung der Leistungen und der Zusammenarbeit zwischen BACS und privaten CERTs, sowie von der Meldepflicht betroffenen Unternehmen der kritischen Infrastrukturen. Um dies zu besprechen, braucht es ein entsprechendes Stakeholder-Treffen, welches wir entsprechend sehr begrüssen würden.

Art. 9 E-CSV Koordinierte Offenlegung von Schwachstellen

Antrag:
Art. 9 Abs. 1 und 2 E-CSV

[1]Das BACS sorgt nach deren Behebung für die koordinierte Offenlegung der Schwachstellen nach international anerkannten Standards.
[2]Es setzt der Herstellerin der betroffenen Hard- oder Software eine angemessene Frist ~~von 90 Tagen~~ zur Behebung der Schwachstellen.

Begründung:
Koordinierte Offenlegung nach Behebung der Schwachstellen: Die Anpassung, dass die Offenlegung der Schwachstellen erst nach deren Behebung erfolgt, basiert auf den Diskussionen im Rahmen der Revision ISG. Dort hat sich das Parlament bewusst gegen eine Offenlegungspflicht von Schwachstellen (vor ihrer Behebung) ausgesprochen. Die Offenlegung einer Schwachstelle vor ihrer Behebung bringt erhebliche Risiken für die betroffenen Systeme und deren Nutzerinnen und Nutzer mit sich. Durch die vorgeschlagene Änderung wird gewährleistet, dass mögliche Angriffspunkte erst dann

publik gemacht werden, wenn die Schwachstellen bereits geschlossen sind, was die Sicherheit und den Schutz der betroffenen Systeme erhöht.
Anpassung der Frist auf "angemessen": Die Änderung der starren 90-Tage-Frist in eine flexible, „angemessene“ Frist berücksichtigt die Komplexität und Variabilität moderner Hard- und Softwarelandschaften. Die ständige Weiterentwicklung und Diversifikation der Systeme erfordert eine flexible Handhabung der Fristen zur Schwachstellenbehebung. Ein „One-Size-Fits-All“-Ansatz, bei dem pauschal 90 Tage als Frist, könnte in einigen Fällen zu einer hastigen und möglicherweise unzureichenden Behebung führen, was die Qualität der Sicherheitsmassnahmen beeinträchtigen könnte. Ein flexibleres System erlaubt es, die Frist entsprechend der Art und Schwere der Schwachstelle sowie den spezifischen Umständen der betroffenen Herstellerin anzupassen, um so eine gründliche und qualitativ hochwertige Behebung sicherzustellen.

Art. 11 E-CSV Kommunikationssystem für den sicheren Informationsaustausch

Antrag:
Art. 11 Abs. 1 E-CSV

[1]Zugang zum Kommunikationssystem des BACS für den sicheren Informationsaustausch (Artikel 74 Abs. 2 Buchstabe a ISG) haben meldepflichtige Organisationen und Behörden ~~mit Sitz in der Schweiz~~ ,

Begründung:
Basierend auf den bisherigen Erfahrungen mit dem Informationsaustausch über den Cyber Security Hub (CSH) des BACS scheint der aktuelle Formulierungsvorschlag unnötig restriktiv zu sein. Es sollten alle im Land tätigen Betreiber kritischer Infrastrukturen (Art. 74 rev. ISG) – auch jene ohne Sitz in der Schweiz – am Informationsaustausch teilnehmen dürfen. Für globale Unternehmen ist der länderübergreifende Austausch von entscheidender Bedeutung. Auf dem Finanzplatz wird dies bereits erfolgreich umgesetzt, indem auch Zweigniederlassungen ausländischer Finanzinstitute mit FINMA-Bewilligung am CSH teilnehmen können. Dieses Prinzip sollte bei der Gestaltung von Art. 11 Abs. 1 E-CSV ebenfalls berücksichtigt werden.

Art. 13 E-CSV Registrierung

Antrag:
Art. 13 Abs. 2 E-CSV

Streichen.

Eventualiter:
Art. 13 Abs. 2 lit. b E-CSV
[2] Die Registrierung muss mindestens folgende Informationen enthalten:
a. Firma, Name oder Bezeichnung und Adresse;
b. ~~Kontaktangaben der gemeldeten Person.~~ Angaben zu einer oder mehreren Kontaktpersonen.

Begründung:
Die Festlegung der Registrierungskriterien ist zu detailliert und formalistisch für eine Verordnung. Dies vor allem, da Firma und Adresse offensichtlich sind. Somit ist Art. 13 Abs. 2 streichen. Alternativ sollte Art. 13 Abs. 2 lit. b immerhin zu «Angaben zu einer oder mehreren Kontaktpersonen» geändert werden.

Die jetzige Formulierung impliziert eine Verantwortlichkeit der gemeldeten Person, dabei soll es laut Botschaft lediglich eine Kontaktperson sein.

Art. 16 E-CSV Ausnahmen von der Meldepflicht

Antrag:
Art. 16 Abs. 2 E-CSV
[2] Unternehmen nach Artikel 74b Absatz 1 Buchstaben f, g, h, l und p ISG, ~~für die Absatz 1 nicht anwendbar ist~~, sind von der Meldepflicht ausgenommen, sofern sie ~~im betroffenen Bereich weniger als 50 Personen beschäftigen und ihr Jahresumsatz beziehungsweise ihre Jahresbilanzsumme im betroffenen Bereich 10 Millionen Franken nicht übersteigt~~ jeweils am 1. Januar eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen.

Begründung:
Der Gesetzgeber hat hier bewusst eine offene Formulierung gewählt und die Konkretisierung dieser Bestimmung dem Bundesrat übertragen, um eine praxisnahe Lösung zu erwirken. Ausnahmen aufgrund der Grösse der Unternehmen festzulegen, ist grundsätzlich ein praktikabler Ansatz. Die Definition eines kleinen Unternehmens sollte jedoch mit anderen, ähnlichen Schweizer Bestimmungen kohärent sein und nicht neue Massstäbe setzen. Eine Begründung für den gewählten Ansatz in den Erläuterungen ist nicht ersichtlich. Gemäss Bundesamt für Statistik (BfS) sind in der Schweiz mindestens in statistischer Hinsicht marktwirtschaftliche Unternehmen mit weniger als 250 Beschäftigten als kleine und mittlere Unternehmen definiert. Entsprechend hat bspw. diese Grösse auch Eingang in Art. 24 DSV gefunden, welche Unternehmen, die jeweils am 1. Januar eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, von der Verzeichnisführungspflicht gemäss DSG ausgenommen hat. Somit sollte diese Definition auch in der CSV übernommen werden.

Art. 18 E-CSV Zu meldende Cyberangriffe

Antrag:
Art. 18 E-CSV Abs. 1, Abs. 2

[1] Die Funktionsfähigkeit einer kritischen Infrastruktur gilt als durch einen Cyberangriff gefährdet, wenn:
a. Gleichzeitig mehrere Mitarbeitende oder systemrelevante Dritte von absichtlich durch den Cyberangriff verursachten Systemunterbrüchen betroffen sind; oder (…).

[2] Eine Manipulation oder ein Abfluss von Informationen liegt vor, wenn:
a. geschäftsrelevante Informationen von Unbefugten verändert oder offengelegt ~~werden~~, entwendet, zerstört, deaktiviert oder sonst wie bearbeitet werden, welche sich mittel- oder langfristig auf wesentliche Applikationen oder Systeme auswirken; oder
b. eine Verletzung der Datensicherheit nach Artikel 24 des Datenschutzgesetzes vom 25. September 2020 vorliegt, welche voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt.

Begründung:
Das Informationssicherheitsgesetz verlangt die Meldung eines erfolgreichen Cyberangriffs, wenn dieser die Funktionsfähigkeit kritischer Infrastrukturen gefährdet (Art. 74d). Wichtig ist, dass nur erfolgreiche Angriffe mit funktionalen Folgen meldepflichtig sind, um unnötigen Verwaltungsaufwand zu vermeiden. Ein reiner Phishing-Angriff ohne funktionalen Schaden sollte nicht gemeldet werden müssen.

Der Bundesrat stellt klar, dass nur gezielte und absichtliche Angriffe meldepflichtig sind, wie in Art. 5 lit. e nISG definiert. Unbeabsichtigte Ausfälle, etwa durch Fehlbedienung, fallen nicht unter die Meldepflicht. Ein Angriff ist meldepflichtig, wenn er absichtlich die Vertraulichkeit, Verfügbarkeit oder Integrität beeinträchtigt.

Der Begriff „Systemunterbruch" sollte so definiert werden, dass nur Unterbrechungen mit systemrelevanten Folgen gemeldet werden müssen, nicht jedoch solche durch Wartungsarbeiten oder den Ausfall weniger kritischer Systeme. Auch „Dritte" sollten nur dann meldepflichtig sein, wenn deren Ausfall kritische Infrastrukturen betrifft. Grundsätzlich wäre es gut, wenn die Meldevorschriften internationalen Standards entsprechen.

Schliesslich sollte die Schwelle für die Meldung von Datensicherheitsverletzungen an die Anforderungen des Datenschutzgesetzes angepasst werden. Eine Meldung ist nur nötig, wenn ein hohes Risiko für die betroffene Person besteht. Ein Angriff, der gemeldet werden muss, liegt nur vor, wenn er erhebliche Auswirkungen auf Systeme hat und die Schutzziele gefährdet.

Art. 19 E-CSV Inhalt der Meldung

Antrag:
Art. 19 Abs. 3

Streichen.

Begründung:
Art. 74e nISG spricht nur von Informationen zur Art und Ausführung des Cyberangriffs, zu seinen Auswirkungen, zu ergriffenen Massnahmen und - soweit bekannt - zum geplanten Vorgehen. Art. 19 Abs. 3 E-CSV geht darüber hinaus. Ebenso sind die relevanten Informationen im Ernstfall stark kontextabhängig, weshalb eine derart detaillierte Regelung unnötig starr ist. Entsprechend sollte Art. 19 Abs. 3 m.E. gestrichen werden. Darüber hinaus begrüssen wir explizit, dass Art. 19 Abs. 4 auch Meldungen einschliesst, die nicht über das Informationssystem erflogen, denn damit kann Art. 13 CSV klar als bedingte Registrierungspflicht gelesen werden. Eine solche besteht dann nur, wenn eine meldepflichtige Organisation sich freiwillig entscheidet, über das NCSC-Kommunikationssystem zu kommunizieren.

Art. 20 E-CSV Übermittlung der Meldung

Antrag:
Art. 20

Falls ~~die~~ eine Meldung nicht über das Kommunikationssystem des BACS erfolgt, informiert dieses das BACS die Kontaktperson nach Artikel 13 Absatz 2 Buchstabe b einer registrierten und von der Meldung betroffenen Organisation über den Eingang und den Inhalt der Meldung, indes ohne die Kontaktangaben der meldenden Organisation oder Person, es sei denn, auch die Kontaktangaben sind zum Schutz der Cybersicherheit erforderlich.

Begründung:
Wir verstehen diesen Artikel so, dass es sich dabei um eine Meldung durch eine Drittperson handelt, welche an sich nicht meldepflichtig wäre, deren Meldung aber eine (weitere) registrierte Organisation betrifft. In diesem Falle würde die nun vorgeschlagene Formulierung bedeuten, dass die meldende Person gegenüber der meldepflichtigen Organisation bekannt wird. Denn diese muss gemäss Art. 19 Abs. 4 Bst. b deren Kontaktangaben bekannt geben, womit diese zum Inhalt der Meldung werden, welche

weitergegeben wird. Dies kann ein mögliches Hindernis für Drittmeldungen darstellen. Nicht meldepflichtige Personen/Organisationen möchten ggf. anonym bleiben, das bei dieser Vorgabe nicht möglich wäre.

Gerne verweisen wir ausserdem auf die Stellungnahmen unserer Mitglieder.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse

economiesuisse

Lukas Federer
Stv. Bereichsleiter Umwelt, Energie und Infrastruktur

Leonie Ritscher
Projektleiterin Wettbewerb & Regulatorisches

Swico
Lagerstrasse 33
CH-8004 Zürich

Tel.: +41 44 446 90 90
www.swico.ch
info@swico.ch

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS
Schwarztorstrasse 59
3003 Bern

Ausschliesslich per E-Mail an:
ncsc@ncsc.admin.ch

Zürich, 13.09.2024

Vernehmlassung zur Cybersicherheitsverordnung (CSV)

Sehr geehrte Frau Bundespräsidentin Amherd
Sehr geehrte Damen und Herren

Gerne nehmen wir die Möglichkeit wahr, innerhalb der festgesetzten Frist Stellung zur Vernehmlassung zur Cybersicherheitsverordnung (CSV) zu nehmen.

Swico ist der Wirtschaftsverband der Digitalindustrie und vertritt die Interessen etablierter Unternehmen sowie Start-ups in Politik, Wirtschaft und Gesellschaft. Swico zählt über 750 Mitglieder aus der ICT- und Internetbranche. Diese Unternehmen beschäftigen 56'000 Mitarbeitende und erwirtschaften jährlich einen Umsatz von 40 Milliarden Franken.

Zusammenfassung: Grundsätzlich begrüsst Swico, dass mit der vorliegenden Ausführungsverordnung zum Bundesgesetz über die Informationssicherheit (ISG) insgesamt zielführend die Cyber-Resilienz der Schweiz gestärkt wird, sofern einige notwendige Verbesserungen erzielt werden. Wir begrüssen, dass die Rolle des Bundesamts für Cybersicherheit (BACS) gestärkt und geschärft wird. Aus den Beratungs- und Unterstützungsleistungen des neuen Bundesamtes darf aber keine Konkurrenz zur Privatwirtschaft entstehen. Dies würde Swico entschieden ablehnen. Zudem muss der Geltungsbereich bezüglich Unterlieferanten geschärft werden, Meldepflichten verhältnismässig, subsidiär und risikobasiert definiert sein sowie bestehende multiple Meldeverfahren zwingend harmonisiert werden. Nur so und verbunden mit einer breiter gefassten Ausnahme für KMUs welche mit bestehenden Regelungen (Verordnung über den Datenschutz) abgestimmt ist, lässt sich ein optimales Kosten-Nutzen-Verhältnis bezüglich Meldepflichten erzielen – im Sinne von Staat, Gesellschaft und Wirtschaft. Weiter erachten wir den sicheren und aktiven Einbezug und Anhörung der Hersteller bzw. Anbieter im Kontext der Behebung von Schwachstellen als zentral, um rasch und gleichzeitig nachhaltige Lösungen zu erzielen. In diesem Zusammenhang ist es wichtig sicherzustellen, dass bezüglich der Weitergabe und Verwendung von Informationen klare Schranken gesetzt werden und insgesamt eine Orientierung an internationalen Standards stattfindet.

1 Allgemeine Würdigung

Swico begrüsst, dass mit der Änderung des Bundesgesetzes über die Informationssicherheit (ISG) und den nun mit Augenmass zu entwickelnden und implementierenden Ausführungsbestimmungen insgesamt die Cyber-Resilienz der Schweiz gestärkt werden kann. Mit dem vorliegenden Entwurf der Cybersicherheitsverordnung werden die Rolle des BACS, als die für zuständig definierte Behörde, geschärft und dessen Möglichkeiten gezielt ausgebaut. Mittels der vorgesehenen Meldepflicht gewinnt das BACS eine verbesserte Übersicht über Cyberangriffe in der Schweiz. Dies ist die Grundlage, um Betroffene bei der Bewältigung von Cyberangriffen zu unterstützen und Betreiberinnen kritischer Infrastrukturen zweckmässig zu warnen. Voraussetzung dafür ist jedoch, dass Behörden und Wirtschaft kooperativ zusammenwirken. Zum einen bei der Erarbeitung und Weiterentwicklung des strategischen Rahmens («Nationale Cyberstrategie»). Andererseits bei der operativen Zusammenarbeit im Bereich Meldungen. Es muss sichergestellt sein, dass die Meldepflicht insgesamt einen positiven Effekt schafft und keinen Mehraufwand mit sich bringt, sodass die Cyber-Resilienz der Schweiz nachhaltig gestärkt wird und zu Gunsten von Staat, Gesellschaft und Wirtschaft ein effektiver Mehrwert geschaffen wird. Kurz: Mehr Cybersicherheit begrüssen wir. Mehr Bürokratie lehnen wir entschieden ab.

2 Wichtige Einbettung in strategischen Gesamtrahmen

Wir begrüssen, dass mit der Nationalen Cyberstrategie gemäss Art. 2 CSV ein zentraler, strategischer Rahmen, der gemeinsam mit dem Steuerungsausschuss Nationale Cyberstrategie (StA NCS) laufend weiterentwickelt wird, für die Prävention, Früherkennung sowie Reaktion auf Cyberbedrohungen definiert ist. Dieses Set-Up fördert die Akzeptanz sowie das zielgerichtete, gesamthafte und koordinierte Handeln aller Akteure.

3 Klare Rollen, Geltungsbereich und gezielte Kooperation als Erfolgsfaktor

Wir erachten klare Rollen und entsprechende Zuordnung der Verantwortlichkeiten sowie insgesamt die gezielte Kooperation zwischen Behörden und Wirtschaft - gerade auch im Bereich der Meldepflichten – als einer der zentralen Erfolgsfaktoren, um die Cybersicherheit der Schweiz nachhaltig zu stärken. Wir begrüssen, dass der «Erläuternde Bericht» dies explizit anerkennt (S. 8 - 9). Mit Blick auf diesen Erfolgsfaktor heben wir folgende Punkte hervor:

3.1 Aktiver Einbezug der Schweizer ICT- und Internetbranche zwingend (StA NCS)

Wir beurteilen die gemischte Zusammensetzung des StA NCS, insbesondere auch mit Vertreterinnen und Vertretern der Wirtschaft, und das damit verbunden Verständnis der Kooperation zwischen Behörden und Wirtschaft, als zielführend (Art. 4 & 5 CSV). Die Ernennung der vorsitzenden Person aus den Reihen der Wirtschaft, Gesellschaft und Hochschulen, um eine ausgewogene Führung des Ausschusses zu gewährleisten, sehen wir positiv (Art. 4 Abs. 3 CSV sowie S. 9 Erläuternder Bericht). Die bereits erfolgten Ernennungen nehmen wir zur Kenntnis.[1]

Es ist für uns evident, dass es eine umfassende Betrachtung der verschiedenen Aspekte der Cybersicherheit und unterschiedliche Perspektiven braucht, um eine effiziente Umsetzung der

[1] BACS, «VBS setzt den Steuerungsausschuss der Nationalen Cyberstrategie ein» abgerufen am 14.08.2024 von https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2024/sta-ncs.html

Nationalen Cyberstrategie und den bestmöglichen Schutz der Schweiz vor Cybervorfällen und -bedrohungen zu gewährleisten. Speziell die Schweizer ICT- und Internetbranche als Anbieter von digitalen (Sicherheits-) Dienstleistungen und Produkten und in Teilen selbst Betreiber von kritischen Infrastrukturen[2], ist Dreh- und Angelpunkt einer starken nationalen Cybersicherheit und muss im Rahmen des StA NCS aktiv einbezogen werden. Einerseits weil die Branche besonders betroffen ist, andererseits, weil sie mit ihrem Know-How einen aktiven Mehrwert leisten kann und will. Infolgedessen schlagen wir vor, Art. 4 Abs. 1 CSV wie folgt zu präzisieren:

Art. 4 Zusammensetzung des StA NCS [Anpassung in Rot] [1] Der StA NCS setzt sich aus Vertreterinnen und Vertretern der Departemente, der Bundeskanzlei, der Kantone, der Wirtschaft, der Gesellschaft der Hochschulen zusammen mit angemessener Vertretung von Betreiberinnen kritischer Infrastrukturen.

3.2 BACS als zentrale, koordinierende Behörde etablieren

Wir begrüssen, dass mit der vorliegenden Cybersicherheitsverordnung die Rolle des BACS als zentrale, koordinierende Stellung hinsichtlich Cybersicherheit in der Schweiz gestärkt wird (siehe insbesondere Art. 6 – 15 CSV). Zentral dabei ist auch, dass eine enge Koordination zwischen BACS und dem Bundesamt für Kommunikation (BAKOM) stattfindet, wie in Art. 9 Abs 6 & 7 CSV festgehalten – insgesamt sind jedoch multiple Meldeverfahren zu harmonisieren (siehe 4.3).

Weiter erachten wir es als positiv, dass Art. 15a Abs. 2 lit. h OV-VBS neu aufführt, dass das BACS die Schweiz zur technischen Analyse von Cyberbedrohungen und zur Bewältigung von Cybervorfällen in internationalen Gremien vertritt. Dieser Informationsaustausch stärkt die zentrale Stellung des BACS in der Schweiz und ist insofern auch wichtig, als dass Cyberbedrohungen ein globales Phänomen sind, welches globale Lösungen fordert.

3.3 Geltungsbereich klären – Einbezug von Unterlieferanten ist vertraglich zu regeln

Bereits bei der Revision des ISG haben wir den unklaren Geltungsbereich als kritischer Punkt hervorgehoben.[3] Auch im aktuellen Verordnungsentwurf bleiben Unsicherheiten, bspw. hinsichtlich Betroffenheit von Unterlieferanten, wie etwa Cloud-Computing-Dienstleistern, Anbieterinnen von Sicherheitssoftware oder Suchmaschinen. Wir sind hier klar der Meinung, dass der Einbezug solcher Lieferanten nicht regulatorisch, sondern vertraglich zwischen den Betreiberinnen kritischer Infrastrukturen und ihren Lieferanten zu regeln ist.

3.4 Keine Konkurrenzierung privatwirtschaftlicher Angebote

Im Sinne der konstruktiven Kooperation und bezugnehmend auf Art 74 Abs. 3 und Art. 74a Abs. 3 ISG sowie Art. 8 CSV begrüssen wir einerseits die Beratung und Unterstützung bei Cyberangriffen durch das BACS verbunden mit den vorgeschlagenen Priorisierungs-Kriterien. Gleichzeitig halten wir ausdrücklich fest, dass gerade mit Blick auf Angriffe mit geringer Beratungs-Priorität keine staatliche Konkurrenz zu (Beratungs-) Angeboten von Privaten

[2] Siehe Art. 74b Abs 1 lit q ff. ISG.
[3] Swico, 2022, «Stellungnahme re Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe (Vernehmlassungsantwort)», S. 2. abgerufen am 13.08.2024 von https://www.swico.ch/media/filer_public/8d/af/8dafc8da-ae27-4827-8229-cd38e2528d70/220413_stellungnahme_swico.pdf

erwachsen darf, zumal hier im Sinne von Art. 74 Abs. 3 die Beschaffung gleichwertiger Unterstützung auf dem Markt rechtzeitig möglich ist.

4 Meldepflichten müssen insgesamt Mehrwert schaffen und umsetzbar sein

Wie im Rahmen unserer allgemeinen Würdigung (siehe 1.) betont, muss das Ziel dieser Vorlage sein, einen effektiven Mehrwert für die Gesellschaft, den Staat und die Wirtschaft zu schaffen, indem die Sicherheit erhöht wird und dabei die aus Cyberangriffen resultierende Schäden und Kosten reduziert werden. Konkret müssen die vorgesehenen Meldepflichten den betroffenen Unternehmen und der Volkswirtschaft letztlich mehr Nutzen stiften als Kosten generieren. Die Meldepflichten müssen daher verhältnismässig, subsidiär und risikobasiert definiert sein. Des Weiteren sollen sie internationalen Standards entsprechen, sodass ein optimales Kosten-Nutzen-Verhältnis erzielt wird. Administrative und finanzielle Aufwände sind auf ein Minimum zu reduzieren.

4.1 Notwendige Präzisierungen und Eingrenzung bezüglich Fristen und Meldepflichten

Hinsichtlich der Meldepflichten gilt es aus unserer Sicht erstens, Rücksicht auf die Schwere eines Cyberangriffs beziehungsweise dessen Auswirkungen zu nehmen. Die vorgeschlagene Formulierung in Art. 18 Abs. 1 lit. a legt nahe, dass jegliche potenzielle Kompromittierung eines Systems dem BACS zu melden ist. Der erläuternde Bericht schafft hierbei keine Klarheit: «[d]ie Funktionsfähigkeit einer kritischen Infrastruktur kann durch einen Cyberangriff gefährdet sein, wenn die IT-Systeme, Netzwerke oder Steuerungssysteme, die für den Betrieb der Infrastruktur wesentlich sind, derart kompromittiert werden, dass es zu Systemunterbrüchen für Mitarbeitende und Dritte führt» (S. 27). Damit ist nicht abschliessend geklärt, was mit «für den Betrieb wesentlich» gemeint ist. Begrüssenswert ist dementsprechend eine Präzisierung, die klarstellt, dass es sich um Ereignisse handeln muss, die den Betrieb der Infrastruktur unmittelbar gefährden. Gleiches gilt für Art. 18 Abs. 2 lit. a, worin von «geschäftsrelevanten Informationen» die Rede ist. Es erscheint uns auch hier sinnvoll, zu präzisieren, dass es sich um kritische Informationen handeln muss, die tatsächlich in Zusammenhang mit dem unmittelbaren Betrieb der kritischen Infrastruktur stehen.

Darüber hinaus ist zweitens festzuhalten, dass «nur» Cyberangriffe der Meldepflicht unterliegen – also Cybervorfälle - die absichtlich ausgelöst wurden (Art. 5 lit. e ISG). Die vorgeschlagene Formulierung spricht jedoch lediglich von «Systemunterbrüchen», was zu Verwirrung führen kann (Art. 18 Abs. 1 lit. a). Deshalb erachten wir es als sinnvoll, eine Präzisierung vorzunehmen.

Beide Änderungsvorschläge tragen zudem dazu bei, exzessive administrative Aufwände, sowohl für die Betreiberinnen der kritischen Infrastrukturen als auch das BACS, zu vermeiden und relevante Cyberangriffe mit entsprechendem Mehrwert hinsichtlich Effizienz und Reaktionsmöglichkeiten zu priorisieren.

Art. 18 Zu meldende Cyberangriffe [Anpassung in Rot]

[1] Die Funktionsfähigkeit einer kritischen Infrastruktur gilt als gefährdet, wenn:

a. Mitarbeitende oder Dritte, welche den unmittelbaren Betrieb der kritischen Infrastruktur verantworten, von absichtlich ausgelösten 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 Abfluss von Informationen liegt vor, wenn:

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

b. eine Verletzung der Datensicherheit nach Artikel 24 des Datenschutzgesetzes vom 25. September 2020 vorliegt.

4.2 Wichtige Ausnahme für KMU

Vor allem für KMU und Start-ups kann die Meldepflicht schnell zu erheblichen administrativen Aufwänden führen. Daher erachten wir es als sinnvoll, dass meldepflichtige Organisationen nach Art. 74b ISG von der Meldepflicht ausgenommen werden, wenn sie eine bestimmte Grösse nicht überschreiten. Die vorgeschlagene Regelung, wonach Organisationen ausgenommen sind, wenn sie weniger als 50 Personen im betroffenen Bereich beschäftigen und ihr Jahresumsatz bzw. ihre Jahresbilanz im betroffenen Bereich CHF 10 Mio. nicht übersteigt (Art. 16 Abs. 2 CSV), erscheint uns jedoch umständlich und wirft Auslegungsfragen auf, insbesondere hinsichtlich der Formulierung «im betroffenen Bereich». Zudem ist anzumerken, dass diese Definition ganz grundsätzlich nicht kohärent mit anderen Schweizer Bestimmungen ist.[4]

Deshalb fordern wir, der Einfachheit und Kohärenz halber, dass Unternehmen und andere privatrechtliche Organisationen von der Meldepflicht ausgenommen werden, die am 1. Januar eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, analog zur Verordnung über den Datenschutz (DSV). Dies entspricht im Übrigen auch der gängigen Definition von KMU.[5]

[4] Siehe bspw. Datenschutzverordnung (DSV) Art. 24 «Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten»

[5] Siehe Bundesamt für Statistik (BFS) «Kleine und mittlere Unternehmen»., abgerufen am 26.08.2024 von https://www.bfs.admin.ch/bfs/de/home/statistiken/industrie-dienstleistungen/unternehmen-beschaeftigte/wirtschaftsstruktur-unternehmen/kmu.html

Art. 16 Zu meldende Cyberangriffe [Anpassung in Rot] [2] Unternehmen nach Artikel 74b Absatz 1 Buchstaben f, g, h, l und p ISG, für die Absatz 1 nicht anwendbar ist, sind von der Meldepflicht ausgenommen, sofern sie ~~im betroffenen Bereich weniger als 50 Personen beschäftigen und ihr Jahresumsatz be-ziehungsweise ihre Jahresbilanzsumme im betroffenen Bereich 10 Millionen Franken nicht übersteigt~~ jeweils am 1. Januar eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen.

4.3 Gezielte Harmonisierung multipler Meldeverfahren

Bereits in unserer Stellungnahme zur «Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe»[6] haben wir darauf hingewiesen, dass auf nationaler Ebene zahlreiche Meldepflichten im Bereich Cybersicherheit und anderen Bereichen existieren. So müssen beispielsweise Fernmeldedienstanbieterinnen entsprechende Meldungen unter Umständen mit jeweils unterschiedlichen Inhalten und Fristen sowohl der Nationalen Alarmzentrale (Art. 96 FDV), dem EDÖB (Art. 15 DSV) wie auch dem BACS (Art. 74a nISG) melden. Im Kontext der öffentlichen Beschaffung müssen Leistungserbringerinnen basierend auf den Mustervertragsklausel der BKB betreffend Cyberangriffen» (Ziff. 3) Meldungen einerseits an «den Leistungsbezüger und andererseits an das BACS (ex NCSC) Meldung erstatten.

Im Hinblick auf die breite Betroffenheit Schweizer Unternehmen vom EU Digital Operational Resilience Act kommen nebst der nationalen auch auf internationaler Ebene zusätzliche Anforderungen. Es ist deshalb auf Lösungen für eine Harmonisierung / Koordination der einzelnen Meldeverfahren hinzuwirken. Denkbar ist bspw. die Fristen jenen der NIS-2-Richtlinie anzupassen (24 Stunden für eine Frühwarnung, 72 Stunden für die Meldung eines Vorfalls). Die Meldequalität sollte gegenüber der Meldegeschwindigkeit im Vordergrund stehen.

Diese multiplen Meldeverfahren sind aufwändig, ineffizient und bergen die Gefahr von Fehlern. Aus unserer Sicht ist darum dringen auf Lösungen für eine Harmonisierung und Koordination der verschiedenen Meldeverfahren hinzuwirken.

5 Sicherer Umgang mit und Behebung von Schwachstellen

Bezüglich dem sicheren Umgang mit und der nachhaltigen Behebung von Schwachstellen heben wir folgende Aspekte hervor:

5.1 Umgang gemäss international anerkannten Standards wichtig und richtig

Wir begrüssen, dass der Umgang mit identifizierten Schwachstellen in enger Abstimmung mit den Herstellern und ausdrücklich nach internationalen Standards (ISO/IEC Norm 29147:2018-10) erfolgen soll (Art. 9 Abs 1 CSV & Erläuternder Bericht, S. 14). Dies garantiert einen sicheren und gleichzeitig effizienten Umgang mit Schwachstellen, da die entsprechenden Prozesse den Akteuren bekannt und im Sinne von Best Practices erprobt sind.

[6] Swico, 2022, «Stellungnahme re Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe (Vernehmlassungsantwort)», S. 2. abgerufen am 13.08.2024 von https://www.swico.ch/media/filer_public/8d/af/8dafc8da-ae27-4827-8229-cd38e2528d70/220413_stellungnahme_swico.pdf

5.2 Hersteller sind zwingend und jederzeit zu informieren

Eine zentrale Voraussetzung dafür, eine Schwachstelle sicher zu managen, ist es, jederzeit zwingend sicherzustellen, dass das BACS, wie vorgeschlagen, «keine Schwachstellen geheim behält oder anderen Behörden weiterleitet, ohne die Hersteller zu informieren». (Art. 9 Abs. 1 CSV & S. 14 Erläuternder Bericht). Nur wenn der Hersteller voll im Bilde ist, auch bezüglich Informationsträger betreffend Schwachstellen, kann eine sichere, nachhaltige und fristgerechte Behebung derselben umgesetzt werden.

5.3 Flexible Fristen unter Einbezug der Hersteller definieren

Wir können nachvollziehen, dass das BACS zwecks Behebung von Schwachstellen eine Frist setzt. Gleichzeitig halten wir fest, dass gerade auch die Hersteller daran interessiert und gewillt sind, Schwachstellen möglichst zeitnah und nachhaltig zu beheben, wobei der Komplexitäts-Grad einer entsprechenden Behebung ein einschränkender Faktor darstellt – entsprechende Realitäten sind zu berücksichtigen. Vor diesem Hintergrund schlagen wir vor, dass jeweils eine «angemessene» Frist (anstatt einer starren Frist) gesetzt wird und begrüssen, dass diese angemessene Frist gemäss Art. 9 Abs. 4 CSV verlängert werden kann. Wir nehmen gleichzeitig zur Kenntnis, dass gemäss Art. 9 Abs 3 CSV eine Frist Risiko-bedingt verkürzt werden kann. Eine allfällige Frist-Verkürzung soll jedoch nur nach Anhörung des betroffenen Herstellers stattfinden können, zumal genau dieser die oben beschriebenen Realitäten und limitierende Faktoren am besten kennt. Nur auf Basis effektiv machbarer, realitäts-bezogener Fristen und in enger Abstimmung zwischen Hersteller und BACS kann eine nachhaltige Schwachstellen-Behebung erzielt werden.

5.4 Vorabinformation an kritische Infrastrukturen umsichtig handhaben

Gemäss Art. 9 Abs. 5 CSV und dem Erläuternden Bericht (S. 15), kann das BACS, wenn ihm eine Schwachstelle bekannt ist, die für andere kritische Infrastrukturen eine «akute Cyberbedrohung» darstellen, die Betreiberinnen entsprechender Infrastrukturen informieren, bevor die Schwachstelle veröffentlicht oder durch die Herstellerin der Hard- oder Software behoben wurde. Entsprechende Vorabinformationen erachten wir als sinnvoll und zielführend verbunden damit, dass die oben genannten Aspekte (siehe 5.1 bis 5.3) berücksichtig werden und es sich, wie vorgeschlagen, effektiv um eine akute Bedrohung handelt.

Aufgrund unserer Ausführungen in Kapitel 5 regen wir folgende Anpassungen an:

Art. 9 Koordinierte Offenlegung [Anpassung in Rot]

[2] Es setzt der Herstellerin der betroffenen Hard- oder Software eine angemessene Frist ~~von 90 Tagen~~ zur Behebung der Schwachstellen.

[4] Es [das BACS] kann die Frist nach Anhörung der Herstellerin verkürzen, wenn eine Schwachstelle:

a. die Funktionsfähigkeit von kritischen Infrastrukturen gefährdet;
b. besonders leicht für einen Cyberangriff ausgenutzt werden kann; oder
c. weit verbreitete Systeme betrifft.

6 Effizienter und sicherer Informationsaustausch gewährleisten

Wir begrüssen, dass der vorliegende Verordnungsentwurf die Anforderungen, Prozesse und Verantwortlichkeiten im Zusammenhang mit dem vorgesehenen Informationsaustausch regelt, wobei wir folgende Punkte explizit hervorheben:

6.1 Sicherheit der Kommunikationssysteme von grösster Bedeutung

Dass das BACS gemäss Art. 11 und 12 CSV ein zentrales Kommunikationssystem für den sicheren Informationsaustausch zu Cybervorfällen und -bedrohungen betreibt und registrierte Organisationen dadurch schnell und effizient mit Informationen über Vorfälle und Bedrohungen informiert, erachten wir als sinnvoll. Gleichzeitig weisen darauf hin, dass es sich bei genau solchen Informationssystemen für Cyberkriminelle um «lohnende Ziele» handeln kann. Ein hohes Mass an Sicherheit ist deshalb zwingend. Die Verantwortung dafür muss, wie vorgeschlagen, in erster Linie beim BACS liegen (Art. 11 Abs. 2 CSV & Art. 12 Abs. 2 CSV).

6.2 Sinnvolle Abgrenzung und Freiwilligkeit für Dienstleister

Wir begrüssen, dass Dienstleister von Betreiberinnen kritischer Infrastrukturen Zugang zu den genannten Informationssystemen (siehe oben) erhalten können – dies auf freiwilliger Basis. Die entsprechende, vorgesehene Meldung durch die Betreiberinnen und anschliessende Anmeldung durch die Dienstleister selbst erachten wir als sinnvoll (Art 14 CSV).

6.3 Notwendige Präzisierung bezüglich Kontaktperson(en)

Hinsichtlich der Registrierung für die Teilnahme am Informationsaustausch durch interessierte Organisationen sehen wir Präzisierungsbedarf. Gemäss Art. 13 Abs. 2 lit. b CSV muss eine Registrierung die «Kontaktangaben der gemeldeten Person» enthalten. Im Erläuternden Bericht wird ausgeführt, dass es sich hierbei um eine «Kontaktperson» handelt (S. 19). Die Formulierung im Verordnungsentwurf impliziert eine Verantwortlichkeit der gemeldeten Person, was dem Bericht widerspricht. Gleiches gilt darüber hinaus für Art. 14 Abs. 2 CSV, wo auch von «der gemeldeten Person» die Rede ist. Um Klarheit zu schaffen, schlagen wir deshalb vor, Art. 13 Abs. 2 lit. b CSV sowie Art. 14 Abs. 2 CSV wie folgt zu präzisieren:

Art. 13 **Registrierung** [Anpassung in Rot]

[2] Die Registrierung muss mindestens folgende Informationen enthalten:

a. Firma, Name oder Bezeichnung und Adresse;

b. ~~Kontaktangaben der gemeldeten Person~~ Angaben zu einer oder mehreren Kontaktpersonen.

Art. 14 **Dienstleister** [Anpassung in Rot]

[2] Die Dienstleister müssen sich mit der Firma oder dem Namen sowie ~~Kontaktangaben der gemeldeten Person~~ Angaben zu einer oder mehreren Kontaktpersonen registrieren.

6.4 Klare Schranken bezüglich Weitergabe und Verwendung von Informationen

Mit Blick auf die (potenzielle) Sensitivität der übermittelten Informationen und notwendigen Vertrauensbeziehung betreffend (freiwillig) erfolgender Meldungen von Cybervorfällen und -bedrohungen, ist es entscheidend, dass die übermittelnde Organisation oder Behörde gemäss Art. 15 Abs. 1 CSV bestimmt, ob und an wen diese gemeldeten Informationen weitergegeben werden dürfen. Die Abstützung auf internationale Standards (TLP-Protokoll) gemäss Erläuterndem Bericht (S. 20 – 21) erachten wir als zweckmässig. In diesem Zusammenhang begrüssen wir auch die Pflicht zum Schutz der Informationen durch die Informationsempfänger als auch deren ausschliessliche Verwendung zwecks Schutz kritischer Infrastrukturen (Art 15. Abs 3 und 4), um unlautere bzw. ungerechtfertigte Wettbewerbsvorteile zu verhindern.

Wir bedanken uns für die Berücksichtigung unserer Anliegen und stehen für Rückfragen gerne zu Verfügung.

Freundliche Grüsse
Swico

Jon Fanzun
CEO

Simon Ruesch
Head Legal & Public Affairs
Mitglied der Geschäftsleitung

Swissgrid AG
Bleichemattstrasse 31
Postfach
5001 Aarau
Schweiz

T +41 58 580 21 11
info@swissgrid.ch
www.swissgrid.ch

Ihr Kontakt
Michael Rudolf
T direkt +41 58 580 35 15
michael.rudolf@swissgrid.ch

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

13. September 2024

Stellungnahme Swissgrid: Vernehmlassung Cybersicherheitsverordnung (CSV)

Sehr geehrte Damen und Herren

Besten Dank für die Möglichkeit zur Stellungnahme zur im Betreff erwähnten Vernehmlassungsvorlage.

Als nationale Netzgesellschaft sorgt Swissgrid dauernd für einen diskriminierungsfreien, zuverlässigen und leistungsfähigen Betrieb des Übertragungsnetzes als wesentliche Grundlage für die sichere Versorgung der Schweiz (Art. 20 Stromversorgungsgesetz, StromVG).

Swissgrid hatte bereits im Rahmen der Vernehmlassung des Informationssicherheitsgesetzes von 2022 die Einführung einer Meldepflicht für Cyberangriffe begrüsst. Vorliegender Entwurf der Cybersicherheitsverordnung (CSV) ist unserer Ansicht nach eine gute Grundlage zur Präzisierung und Regelung dieser Meldepflicht. An folgenden Stellen sehen wir Ergänzungs- und Präzisierungsbedarf:

Art. 2 Nationale Cyberstrategie

Für Swissgrid ist nicht ersichtlich, weshalb in Art. 2 Abs. 2 CSV die nationale Cyberstrategie «nur» in Abstimmung mit den Kantonen festgelegt wird und nicht auch in Abstimmung mit weiteren bedeutenden Interessengruppen (vgl. Art. 4 Abs. 1 CSV) **inkl. Betreibern von kritischen Infrastrukturen.**

Art. 4 Zusammensetzung des StA NCS

Änderungsantrag:

[1] Der StA NCS setzt sich aus Vertreterinnen und Vertretern der Departemente, der Bundeskanzlei, der Kantone, der Wirtschaft, **der kritischen Infrastrukturen,** der Gesellschaft und der Hochschulen zusammen.

[3] Er ernennt aus dem Kreis der Vertreterinnen und Vertreter der Wirtschaft, **der kritischen Infrastrukturen,** der Gesellschaft und der Hochschulen die vorsitzende Person.

Begründung: Swissgrid beantragt eine explizite Nennung der Betreiber von kritischen Infrastrukturen in Art. 4 Abs. 1 CSV. Die Erläuterungen weisen auf Seite 6 darauf hin, «*dass sämtliche Vorgaben zur Cybersicherheit der Bundesverwaltung, die Zuständigkeiten und Aufgaben der Fachstelle des Bundes für Informationssicherheit und die sich daraus ergebenden Schnittstellen zu den Aufgaben des BACS in der ISV [und damit nicht in der CSV] geregelt werden*». **Die Betreiber von kritischen Infrastrukturen sind somit zentral Betroffene der CSV, weshalb sie auch explizit in Art. 4 CSV aufzunehmen sind**.

Art. 15 Übermittlung und Nutzung der Informationen

Für Swissgrid bestehen bei Art. 15 CSV folgende Fragen:

- Was sind die Folgen, wenn eine TLP-Klassifizierung nicht eingehalten wird?
- Welche TLP-Protokoll Vorgabe ist zu verwenden, sollte der Informationslieferant den Empfängerkreis nicht festlegen? Aus Sicht Swissgrid ist in diesem Fall (bis zur Klärung) «TLP amber strict» anzuwenden.

Wir beantragen entsprechende Ergänzungen der Verordnung oder der Erläuterungen.

Art. 16 Ausnahmen von der Meldepflicht

Art. 16 Abs. 1 Bst. b Ziffer 1 CSV verweist auf Art. 5a Abs. 1 und Anhang 1a der Stromversorgungsverordnung (StromVV) resp. die dortigen Minimalstandards. Die dortigen Bestimmungen regeln u.a. die Pflichten von «*Dienstleistern, die dauerhaft Anlagen von Netzbetreibern fernsteuern können*». Aus Sicht Swissgrid sind von der Meldepflicht auch **Dienstleister** zu erfassen**, welche intelligente Mess- und Steuersysteme steuern**, sofern sie den entsprechenden Grenzwert nach Anhang 1a StromVV erfüllen. Wir beantragen eine entsprechende Überprüfung und ggf. Anpassung der Vernehmlassungsvorlage.

Bei der Ausarbeitung der Minimalstandards gemäss StromVV ist zudem darauf zu achten, dass dies möglichst EU-kompatibel erfolgt.

Begründung: Gemäss Art. 31e StromVV sind bis 2027 80% aller Messeinrichtungen mit einem intelligenten Messsystem auszustatten. Intelligente Messsysteme müssen gemäss Art. 8a Abs. 1 Bst. a Ziffer 3 StromVV über eine bidirektionale Kommunikation verfügen. D.h. die Messsysteme können ein Signal empfangen und darauf bspw. eine Rundsteuerung oder Wärmepumpe ansteuern. Im Rahmen des Bundesgesetzes über eine sichere Stromversorgung mit

erneuerbaren Energien (sog. «Stromgesetz») ist weiter die Einführung einer zentralen Datenplattform (Datahub) vorgesehen. Dadurch und aufgrund weiterer Bestimmungen des Stromgesetzes dürften die Pflichten der Verteilnetzbetreiber hinsichtlich Datenerfassung und Datenaustausch erheblich zunehmen. Swissgrid vermutet, dass zunehmend mehr (kleine) Verteilnetzbetreiber Aufgaben im Zusammenhang mit intelligenten Mess- und Steuersystemen an Dienstleister auslagern und somit bei diesen bündeln werden.

Art. 19 Inhalt der Meldung

Änderungsantrag:

[1] Die Meldung muss folgende Informationen zum Cyberangriff enthalten:

d. Angriffsmethode; ~~und~~

e. **sofern bekannt,** Angaben zum Verursacher**; und**

f. Angegriffene Systeme.

Begründung: Eine Zuordnung eines Angriffs an einen Verursacher dürfte – gerade im Hinblick auf die Meldefrist von 24 Stunden – in vielen Fällen nur schwer (zuverlässig) durchführbar sein. Die Informationen sind somit «sofern bekannt» zu liefern. Zudem schlagen wir vor, dass auch Informationen zu den angegriffenen Systemen in die Meldung aufzunehmen sind. Diese Information dürfte insbesondere im Falle von weitverbreiteten Applikationen von Standardanbietern relevant sein.

Art. 21 Frist zur Erfassung der Meldung

Gemäss Erläuterungen stützt sich Art. 21 CSV auf Art. 74e ISG. Gemäss diesem hat die Meldung innert 24 Stunden nach der Entdeckung des Cyberangriffs zu erfolgen. Im Sinne der Verständlichkeit regen wir an, dass dies in Art. 19 CSV ergänzt wird oder ein direkter Verweis auf Art. 74e Abs. 1 ISG aufgenommen wird.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse
Swissgrid AG

Roger Wirth
Head of Cyber Security

Michael Schmid
Head of Legal, Regulatory & Compliance

suva

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS
Schwarztorstrasse 59
3003 Bern

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

Suva

Marc Epelbaum
Direktwahl 041 419 55 00
marc.epelbaum@suva.ch
www.suva.ch

Postadresse
Suva
Generalsekretariat
Fluhmattstrasse 1
Postfach
6004 Luzern

Datum 13.09.2024

Betrifft Vernehmlassung zur Verordnung über die Cybersicherheit (Cybersicherheitsverordnung)

Sehr geehrter Frau Bundespräsidentin
Sehr geehrte Damen und Herren

Wir bedanken uns für die Gelegenheit, im Rahmen der Vernehmlassung zur Cybersicherheitsverordnung (CSV) Stellung nehmen zu können. Die Suva mit ihren Rehakliniken in Bellikon und Sion ist als Betreiberin von kritischen Infrastrukturen der Meldepflicht für Cyberangriffe und somit der Cybersicherheitsverordnung unterstellt.

Wir begrüssen die Ausführungsbestimmungen zur Gesetzesänderung aufgrund der Einführung der Meldepflicht für Cyberangriffe auf kritische Infrastrukturen. Die geplante Umsetzung der Meldepflicht stellt den gegenseitigen Informationsaustausch sicher und legt die Grundlage, um die Cybersicherheit in der Schweiz zu erhöhen.

Koordination BACS und EDÖB

Wir erachten es als nicht opportun, dass die Meldeprozesse zwischen dem Bundesamt für Cybersicherheit (BACS) und dem Eidgenössischen Datenschutzbeauftragten (EDÖB) nicht aufeinander abgestimmt sind. Aus unserer Sicht sollten meldepflichtige Akteure jeweils nur eine Meldung an eine Behörde machen müssen. Dadurch können Mehraufwand und Doppelspurigkeiten vermieden werden. Sofern eine koordinierte Meldung sich aus berechtigten Gründen nicht umsetzen lässt, muss zumindest klar hervorgehen, ob und welche zusätzliche Meldung an den EDÖB gemacht werden muss. Die aktuelle Formulierung im Entwurf der Benutzeroberfläche für das geplante Kommunikationssystem im Falle von Cyberangriffen ist hinsichtlich Meldung an den EDÖB nicht eindeutig und muss präzisiert werden.

Berücksichtigung Schweregrad bei zu meldenden Cyberangriffen

Wir empfehlen, den Schwergerad eines Cyberangriffes bei der Meldepflicht gemäss Artikel 18 mitzuberücksichtigen. Dadurch kann verhindert werden, dass beispielsweise kurze Systemausfälle bei einem eingeschränkten Personenkreis gemeldet werden müssen.

Wir regen dementsprechend an, in Artikel 18 Absatz 1 Buchstaben a von kritischen Systemunterbrüchen und in Artikel 18 Absatz 2 Buchstaben a von kritischen geschäftsrelevanten Informationen zu sprechen.

Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme und stehen Ihnen für weitere Auskünfte gerne zur Verfügung.

Freundliche Grüsse

Marc Epelbaum
Generalsekretär

scienceindustries
Wirtschaftsverband
Chemie Pharma Life Sciences

Nordstrasse 15
Postfach
8021 Zürich
Schweiz

T +41 44 368 17 11
info@scienceindustries.ch

per E-Mail an:
Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

ncsc@ncsc.admin.ch

Zürich, 13. September 2024

Stellungnahme zur Vernehmlassung der Cybersicherheitsverordnung (CSV)

Sehr geehrte Damen und Herren

Mit Ihrem Schreiben vom Mai 2024 haben Sie uns eingeladen, zum Erlass der Cybersicherheits-verordnung (CSV) Stellung zu nehmen. Wir bedanken uns für diese Möglichkeit, welche wir hiermit gerne wahrnehmen.

scienceindustries ist der Wirtschaftsverband der Schweizer Industrien Chemie, Pharma und Life Sciences. Wir vertreten die wirtschaftspolitischen Interessen von rund 250 in der Schweiz tätigen Unternehmen aus den genannten und verwandten Branchen gegenüber staatlichen Behörden, der Öffentlichkeit und internationalen Organisationen. Zu unseren Mitgliedern zählen Firmen, die von der eingangs erwähnter Verordnung direkt betroffen sein werden.

scienceindustries schliesst sich der Stellungnahme von economiesuisse vollumfänglich an.

Im Rahmen der Revision des Informationssicherheitsgesetzes (ISG) haben wir uns bereits gegen eine Meldepflicht mit Sanktionsandrohungen ausgesprochen. scienceindustries befürwortet zwar die Einführung einer einfachen und effektiven Meldepflicht für Betreiber kritischer Infrastrukturen im Falle von Cyberangriffen. Die vorgeschlagenen Vorschriften erfüllen diesen Anspruch jedoch nicht vollständig. Mit den folgenden Anpassungen können die Meldeprozesse praxisgerechter gestaltet werden:

- Bessere Abstimmung und Angleichung mit bestehenden Vorschriften und Meldeprozessen, beispielsweise im Datenschutz- oder Finanzmarktrecht.
- Weniger bürokratische Hürden und detaillierte Regulierungen, dafür mehr partnerschaftliche und flexible Zusammenarbeit zwischen Bundesbehörden und den Betreibern kritischer Infrastrukturen, insbesondere bei der Ausgestaltung der Meldeprozesse.
- Berücksichtigung des Gesetzgeberwillens, insbesondere durch praktikable Ausnahmeregelungen bei den neuen Meldepflichten und den Verzicht auf Bestimmungen, die im ISG keine klare rechtliche Grundlage haben.
- Einführung einer Übergangsfrist von mindestens einem Jahr.

Insbesondere lehnen wir Art. 16 Abs. 2 E-CSV ab. Der Gesetzgeber hat die Konkretisierung der Ausnahme von der Meldepflicht dem Bundesrat übertragen, um eine praxisnahe Lösung zu erwirken. Ausnahmen aufgrund der Grösse der Unternehmen festzulegen, ist grundsätzlich ein praktikabler Ansatz. Die Definition eines kleinen Unternehmens sollte jedoch mit anderen, ähnlichen Schweizer Bestimmungen kohärent sein und nicht neue Massstäbe setzen. Eine Begründung für den gewählten Ansatz in den Erläuterungen ist nicht ersichtlich. Gemäss Bundesamt für Statistik (BfS) sind in der Schweiz mindestens in statistischer Hinsicht marktwirtschaftliche Unternehmen mit weniger als 250 Beschäftigten als kleine und mittlere Unternehmen definiert. Die Grösse ist auch in Art. 24 DSV verankert. Demnach sind Unternehmen, die am 1. Januar weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, von der Verzeichnisführungspflicht gemäss DSG ausgenommen. Diese Definition sollte auch in der CSV übernommen werden.

Die vom Bundesrat vorgeschlagene Regelung zu Art. 16 Abs. 2 CSV ist unklar, wird zu zahlreichen Rechtsfragen in der Umsetzung führen und ist in der Schweizer Rechtspraxis nicht verankert. So sollen nur Unternehmen von der Meldepflicht ausgenommen werden, welche im betroffenen Bereich weniger als 50 Personen beschäftigen und ihr Jahresumsatz beziehungsweise ihre Jahresbilanzsumme im betroffenen Bereich 10 Millionen Franken nicht übersteigt. Es stellen sich hier zu viele Auslegungsfragen: Was heisst in diesem Kontext Unternehmen? Was heisst weniger als 50 Beschäftigte im betroffenen Bereich? Dieselbe Frage stellt sich dann für den Umsatz resp. die Jahresbilanzsumme im betroffenen Bereich, welche 10 Millionen Franken nicht übersteigen soll. Diese Bestimmung erweist sich als zu rechtsunsicher und im Ergebnis unpraktikabel. Wir lehnen diesen Vorschlag deshalb ab; vielmehr müsste die Bestimmung wie folgt lauten:

[2]Unternehmen nach Artikel 74b Absatz 1 Buchstaben f, g, h, l und p ISG, ~~für die Absatz 1 nicht anwendbar ist~~, sind von der Meldepflicht ausgenommen, sofern ~~sie im betroffenen Bereich weniger als 50 Personen beschäftigen und ihr Jahresumsatz beziehungsweise ihre Jahresbilanzsumme im betroffenen Bereich 10 Millionen Franken nicht übersteigt~~ jeweils am 1. Januar eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen.

Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme.

Freundliche Grüsse

Stephan Mumenthaler
Direktor

Jürg Granwehr
Bereichsleiter Pharma & Recht

Sicherheitsdirektion, Postfach, 6301 Zug

Per E-Mail

Eidgenössisches Departement
für Verteidigung,
Bevölkerungsschutz und Sport
VBS
Bundeshaus Ost
3003 Bern

T direkt +41 41 594 56 84
Anders.Rasmussen@zg.ch
Zug, 11.09.2024 RADE
SD SDS 7.11 / 402

Vernehmlassung zur Cybersicherheitsverordnung
Stellungnahme des Kantons Zug

Sehr geehrte Frau Bundespräsidentin
Sehr geehrte Damen und Herren

Mit Schreiben vom 22. Mai 2024 haben Sie die Kantonsregierungen eingeladen, sich bis am 13. September 2024 zur Cybersicherheitsverordnung vernehmen zu lassen. Der Regierungsrat des Kantons Zug hat die Sicherheitsdirektion mit der direkten Erledigung der Vernehmlassung beauftragt. Gerne nehmen wir wie folgt Stellung:

I. Allgemeines

Der Kanton Zug begrüsst die Einführung der Cybersicherheitsverordnung (CSV), welche einen umfassenden Rahmen zur Stärkung der Cybersicherheit in der Schweiz schafft. Die Erläuterungen zur Verordnung stellen treffend fest, dass Cyberkriminalität territoriale Grenzen überschreitet, seien dies nationale oder kantonale Grenzen. Die Notwendigkeit der engen Zusammenarbeit mit den Kantonen kann deshalb nicht genug betont werden. Heute bestehen sehr heterogene Organisationsstrukturen bei der Vorfalls- und Krisenbewältigung. Fragestellungen rechtlicher, wirtschaftlicher oder politischer Natur über die unmittelbare Krisenbewältigung hinaus sind schwierig strukturiert zu bearbeiten.

Im Einzelnen stellen wir folgende Anträge:

II. Anträge und Begründungen

1. In Art. 5 CSV sei eine Regelung bezüglich regelmässiger Konsultationen zwischen dem Steuerungsausschuss Nationale Cyberstrategie (StA NCS) und den Kantonen (bzw. kantonalen Vertretungen) aufzunehmen.

Begründung: Um die Effizienz und Effektivität der Nationalen Cyberstrategie (NCS) zu gewährleisten, ist ein regelmässiger Austausch zwischen dem StA NCS und kantonalen Vertretungen vorzusehen.

2. **In den 3. Abschnitt der CSV sei aufzunehmen, dass das Bundesamt für Cybersicherheit (BACS) langfristige Partnerschaften mit kantonalen Behörden eingeht, um nachhaltige Schulungs- und Unterstützungsprogramme zu entwickeln.**

   Begründung: Die Expertise und Ressourcen des BACS sind für die Kantone von grosser Bedeutung, insbesondere bei der Bewältigung komplexer Cybervorfälle. Nachhaltige Schulungs- und Unterstützungsprogramme ermöglichen es, das technische Know-how auf kantonaler Ebene kontinuierlich zu verbessern.

3. **Art. 9 Abs. 1 CSV sei wie folgt zu ergänzen: «Das BACS sorgt für die koordinierte Offenlegung der Schwachstellen nach international anerkannten Standards und Best Practices.»**

   Begründung: Durch die Ergänzung um Best Practices kann sichergestellt werden, dass auch anerkannte Methoden oder Vorgehensweisen, die sich in der Praxis als besonders effektiv und effizient erwiesen haben, bei der Offenlegung von Schwachstellen mitberücksichtigt werden.

4. **Art. 9 Abs. 2 CSV sei wie folgt zu ergänzen: «Es setzt der Herstellerin oder dem Betreiber der betroffenen Hardware, Software oder Dienstes eine Frist von 90 Tagen zur Behebung der Schwachstellen.»**

   Begründung: Der Anwendungsbereich der Norm sei auf Betreiber auszuweiten. Um sicherzustellen, dass von der Regelung auch Dienste erfasst werden, soll auch dieser Begriff explizit erfasst werden.

5. **In den 4. Abschnitt der CSV sei eine Bestimmung aufzunehmen, wonach eine ständige Evaluierung und Verbesserung der Systeme zu gewährleisten ist, um den sich ständig weiterentwickelnden Cyberbedrohungen gerecht zu werden.**

   Begründung: Nebst umfassenden Schulungsprogrammen für kantonale Behörden ist eine ständige Evaluierung und Verbesserung der Systeme unabdingbar, um jeweils auf dem neusten Stand zu bleiben. Nur so kann den sich stets verändernden Cyberbedrohungen stark entgegengetreten werden.

6. **Es seien ausreichende Ressourcen zur Verfügung zu stellen und kontinuierliche Schulungsmassnahmen durchzuführen, um die Umsetzung der Massnahmen zu optimieren und die Cybersicherheit in der Schweiz nachhaltig zu verbessern.**

Begründung: Nur wenn ausreichende finanzielle und personelle Ressourcen zur Verfügung gestellt werden, kann eine wirkungsvolle Verbesserung der Cybersicherheit erreicht werden.

7. **Die Verordnung sowie die dazugehörigen Erläuterungen seien hinsichtlich der nicht einheitlich verwendeten Begriffe zu überarbeiten.**

   Begründung: Es werden beispielsweise die Begriffe Betreiberin und Herstellerin verwendet, andererseits ist von Diensteistern, Betreibern von Gasleitungen oder Mitarbeitern die Rede. Im erläuternden Bericht taucht das Wort Hersteller wiederholt auf und das Wort Herstellerin ein Mal. Dies ist zu vereinheitlichen.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme und die Berücksichtigung unserer Anträge.

Freundliche Grüsse
Sicherheitsdirektion

Laura Dittli
Regierungsrätin

Versand per E-Mail an:
– ncsc@ncsc.admin.ch (als PDF und Word-Version)

Kopie per E-Mail an:
– Sicherheitsdirektion (info.sd@zg.ch)
– Finanzdirektion (info.fd@zg.ch)
– Zuger Polizei (kommandooffice.polizei@zg.ch)
– Obergericht des Kantons Zug (marc.siegwart@zg.ch)
– Datenschutzstelle des Kantons Zug (datenschutz.zug@zg.ch)

Bundesanwaltschaft
Ministère public de la Confédération
Ministero pubblico della Confederazione
Procura publica federala

CH-3003 Bern, BA

Par e-mail à
ncsc@ncsc.admin.ch

Département fédérale de la défense,
de la protection de la population et des sports DDPS
Madame la Conseillère fédérale Viola Amherd

Référence : RD.24.0066
Berne, 13 septembre 2024

Adoption de l'ordonnance sur la cybersécurité (OCyS)
Procédure de consultation du Ministère public de la Confédération (MPC)

Madame la Conseillère fédérale,
Mesdames et Messieurs,

Les autorités de poursuite pénale, en particulier le Ministère public de la Confédération (ci-après : MPC), collaborent étroitement et depuis plusieurs années avec l'Office fédéral de la cybersécurité (ci-après : OFCS, et avant lui le Centre national pour la cybersécurité, NCSC) dans le domaine de la lutte contre la cybercriminalité. L'OFCS est ainsi également un acteur majeur de ce domaine. Le projet d'ordonnance sur la cybersécurité devrait davantage tenir compte de cette collaboration indispensable entre cybersécurité et lutte contre la cybercriminalité.

De manière plus concrète :

Art. 15 du projet d'ordonnance : Transmission et utilisation des informations

Les traces laissées par les auteurs sont essentiellement de nature numérique et, partant, particulièrement volatile et éphémères. Il s'agit donc de sauvegarder le plus rapidement possible les données et informations liées à une cyberattaque. Dans les cas où les victimes s'adressent à l'OFCS et lui transmettent des informations, il est essentiel que celles-ci soient sauvegardées par l'office en vue de leur transmission à l'autorité de poursuite pénale. Il conviendrait donc de mentionner expressément cette sauvegarde dans le texte de l'art. 15, par exemple sous la forme d'un ajout à la fin du deuxième alinéa, tel que « L'OFCS sauvegarde

Ministère public de la Confédération MPC
Besna Karatas
Guisanplatz 1
3003 Berne
www.bundesanwaltschaft.ch

les informations transmises en vue de leur communication aux autorités de poursuite pénale. ».

Art. 18 du projet d'ordonnance : Cyberattaques à signaler

Du point de vue de l'autorité de poursuite pénale qu'est le MPC, il serait souhaitable que l'Office fédéral de la cybersécurité dénonce automatiquement les cas de cyberattaques pouvant constituer des infractions pénales et qui sont portés à sa connaissance, en particulier lorsque des infrastructures telles que définies à l'article 5 let. c de la Loi fédérale sur la sécurité de l'information au sein de la Confédération (RS 128 – ci-après : LSI). Toutefois, la modification de la LSI du 29 septembre 2023 (FF 2023 2296) prévoit à son nouvel art. 73d al. 3 LSI, que le directeur du NCSC « **peut** dénoncer cette possible infraction aux autorités de poursuite pénale si la gravité de cette dernière le justifie ».

Il s'agit donc d'une *Kannvorschrift* du directeur NCSC qui laisse à celui-ci l'interprétation de la gravité des faits et le choix de les porter ou non à la connaissance de l'autorité de poursuite pénale. Du point de vue du MPC, il paraît cependant essentiel qu'en cas de cyberattaque sur des infrastructures techniques susceptibles de constituer des délits ou des crimes, les autorités de poursuite pénale soient informées sans délai, dès lors que c'est la sécurité du pays qui est concernée. A ce titre, on peut souligner que, dans les cas visés par l'art. 18 al. 4 du projet d'ordonnance, qui vise les cyberattaques liées à des actes de chantage, de menaces ou de contrainte (art. 74d, let. d LSI), la dénonciation aux autorités de poursuite pénale devrait être automatique (en ajoutant une formule telle que, par exemple : « ces cas devraient être dénoncés ») ; cet alinéa pourrait ainsi renforcer la nécessité de dénoncer le cas pour le directeur du NCSC sans contredire la LSI. On ne saurait en effet rappeler, comme le souligne d'ailleurs le rapport explicatif du Conseil fédéral, les conséquences très graves de ce type d'attaques qui doivent par conséquent être poursuivies et ne sauraient rester impunies (cf. rapport explicatif pp. 27-28). Ce n'est que dans ces conditions que les infrastructures du pays seront correctement protégées.

En outre, on reproche souvent aux particuliers – entreprises et personnes privées – de ne pas dénoncer les cyberattaques dont ils sont victimes, ce qui empêche les autorités de disposer d'une vision réelle et globale de l'état de la situation en Suisse en matière de cybercriminalité. Il ne paraît dès lors pas cohérent de faire ce reproche aux personnes privées et sociétés dans notre pays, et d'accepter que l'Office qui est responsable de la cybersécurité ne dénonce pas lui-même de telles attaques.

Le MPC vous remercie d'avoir pris en compte la présente procédure de consultation.

Nous vous prions d'agréer, Madame la Conseillère fédérale, Mesdames, Messieurs, l'assurance de notre considération distinguée.

Ministère public de la Confédération MPC

Besna Karatas
Juriste Service juridique

SSK | CMP
Schweizerische Staatsanwaltschaftskonferenz SSK
Conférence suisse des Ministères publics CMP
Conferenza svizzera dei Ministeri pubblici CMP

An
Bundesamt für Cybersicherheit BACS
3003 Bern

Per E-Mail
ncsc@ncsc.admin.ch

Bern,13. September 2024

Vernehmlassung Cybersicherheitsverordnung (CVS) – Stellungnahme SSK

Sehr geehrte Damen und Herren

Mit Schreiben vom 22. Mai 2024 haben Sie unsere Konferenz eingeladen, zur erwähnten Vorlage Stellung zu nehmen. Hierfür danken wir Ihnen bestens.

Fristgerecht möchten wir uns gerne zu folgenden Punkten äussern:

- **Schnittstelle BACS zu den Strafverfolgungsbehörden**

Gemäss den Erläuterungen zur Verordnung über die Cybersicherheit vom 22. Mai 2024 zur Vorfallsbewältigung (nachfolgend Erläuterungen), soll das nationale Computer Emergency Response Team (CERT) des BACS eine zentrale Rolle spielen bei der Bewältigung von Cybervorfällen und Cyberbedrohungen in der Schweiz. Das BACS arbeite dabei eng mit den betroffenen Behörden und Organisationen und ihren allfälligen Sicherheitsdiensten zusammen. Es helfe zudem bei der Koordination zwischen den an der technischen Bewältigung beteiligten Akteuren.

Mit Bezug auf die technische Vorfallsbewältigung ist das CERT eine längst (seit Schaffung MELANI) etablierte Stelle mit sehr gutem Fachwissen und grossem Netzwerk. In den Erläuterungen zu Art. 7 CSV ist die Zusammenarbeit mit den Strafverfolgungsbehörden aber nicht explizit erwähnt. Es ist fraglich und offen, ob mit betroffenen Behörden auch die Staatsanwaltschaft und die Polizei gemeint sind.
Wichtig ist bei Vorfällen die zeitnahe Involvierung der Strafverfolgungsbehörden. Es besteht üblicherweise Gefahr im Verzug zur Sicherung der nötigen Beweise. Zudem können Sicherungsmassnahmen der Betroffenen oder des CERT die forensische Erhebung von Beweismitteln vereiteln, da die Daten durch vorgängig vorgenommene Manipulationen kompromittiert wurden, was einen faktischen oder rechtlichen Beweisverlust zur Folge haben kann.
Gerade bei Offizialdelikten ist für den Erfolg einer Strafuntersuchung zentral, dass die betroffenen Behörden zeitnah informiert werden.

Unseres Erachtens sollten die in der Praxis durchaus vorhandenen Kontakte des BACS (CERT) zu den Strafverfolgungsbehörden in der Verordnung institutionalisiert (vgl. Ausführungen auf Seite 2) **und in den Erläuterungen beschrieben werden.**

Bezüglich der Zulässigkeit von in den Erläuterungen mehrfach erwähnten Gegenmassnahmen (S. 11, 15 und 17) bestehen unterschiedliche Auffassungen und ein rechtlich enger Rahmen. Demgegenüber ist technisch sehr vieles möglich. Es ist zu definieren, was das CERT unter Präventiv- und Gegenmassnahmen versteht.

Je nach Verständnis und Umfang sind erweiterte gesetzliche Grundlagen erforderlich für Massnahmen, welche in der Regel nur den Strafverfolgungsbehörden gemäss StPO oder dem Nachrichtendienst gemäss NDG offenstehen.

Wir schlagen deshalb vor, Gegenstand, Wirkungsziele und Umfang der «Gegenmassnahmen» zu definieren und die dafür nötigen Kompetenzen des CERT zu umschreiben.

- **Weitergabe von Informationen Gemäss Art. 15 CSV**

Laut Entwurf von Artikel 15 CSV soll das BACS über die Weitergabe der Informationen frei entscheiden können. Diese Kompetenz steht im Spannungsfeld zum Informationsbedarf der Strafverfolgungsbehörden. Dass ein vertrauensbasierter Informationsaustausch mit den Informationslieferanten schützenswert ist, ist anzuerkennen. Eine effektive Strafverfolgung ist aber ohne zeitnahe Informationen nicht möglich. Im Ergebnis und angesichts der betroffenen Rechtsgüter sind öffentliche Interessen, namentlich Strafverfolgungsinteressen, höher zu gewichten als das Selbstbestimmungsrecht des BACS. Immerhin sind die Informationen bei den Strafverfolgungs-behörden durch das Amtsgeheimnis geschützt und werden nur zweckgebunden verwendet.

Wir regen deshalb an, die in Art. 15 Abs. 2 CSV vorgeschlagene Kompetenz über die Weitergabe von Informationen so weit zu beschränken, als sie die vollständige Übermittlung der Informationen an die Strafverfolgungsbehörden betrifft.

- **Meldepflicht für Betreiber kritischer Infrastrukturen gemäss Art. 18 Abs. 4 CVS / Kannvorschrift Anzeigenerstattung Direktor BACS gemäss Art. 73d Abs. 3 ISG**

Laut des erläuternden Berichts sollen das revidierte Kapitel 5 des Informationssicherheitsgesetz ISG und die Cybersicherheitsverordnung gleichzeitig per 1. Januar 2025 in Kraft treten. Mitarbeitende des BACS sind gemäss Art. 73d Abs.3 ISG von der Anzeigepflicht nach Art. 22a Abs. 1 BPG befreit und melden Hinweise auf eine mögliche Straftat ausschliesslich der Direktorin oder dem Direktor des BACS. Dieser wiederum **kann** Anzeige bei den Strafverfolgungsbehörden erstatten, **«sofern dies aufgrund der Schwere der möglichen Straftat geboten scheint.»**

Aus Sicht der Strafverfolgung ist die Anzeigenerstattung durch das BACS bei Cyberangriffen auf kritische Infrastrukturen bei möglichen Vergehen oder Verbrechen **imme**r geboten – geht es letztlich um die Sicherheit des Landes. Die Erläuterungen zur Verordnung führen denn auch aus, welche gravierende Folgen bis hin zu Sicherheitsrisiken meldepflichtige Cyberangriffe haben können und begründen die Meldepflicht im Sinne von Art. 18 Abs. 4 CSV damit, dass das BACS müsse einschätzen können, «wie stark die Bedrohung kritischer Infrastrukturen durch Cyberkriminelle ist» (S. 27 und 28).

Die Übersicht über die Cyberkriminalität in der Schweiz ist lückenhaft, die Dunkelziffer hoch. Privatpersonen und Unternehmen wird denn auch oft vorgeworfen, dass sie Cyberangriffe nicht melden, was wiederum die Arbeit der Strafverfolgungsbehörden von Bund und Kantonen im Kampf gegen die Cyberkriminalität erschwer. Dass selbst das für Cybersicherheit verantwortliche Bundesamt solche Angriffe nicht anzeigt, erachten wird als widersprüchlich.

Wir schlagen deshalb vor, Art. 18 CSV mit einem Absatz 5 zu ergänzen, wonach das BACS (zumindest) **Fälle im Sinne von Absatz 4 den zuständigen Strafverfolgungsbehörden zur Anzeige bringt.**

- **Kein Vertretungsmonopol BACS**

In Artikel 15*a* Absatz 2 Buchstabe h OV-VBS wird neu aufgeführt, dass das BACS die Schweiz zur technischen Analyse von Cyberbedrohungen und zur Bewältigung von Cybervorfällen in internationalen Gremien vertritt. Gemäss den Erläuterungen (S. 33) dient dieser Informationsaustausch dazu, relevante Erkenntnisse und Daten über aktuelle Bedrohungen zu teilen und gemeinsame Massnahmen zur Bewältigung von Cybervorfällen und Cyberbedrohungen zu koordinieren. Der nationale und internationale Austausch zwischen Fachstellen sei deshalb für den Schutz vor Cybervorfällen und Cyberbedrohungen unerlässlich. Das BACS tausche diesbezüglich aktiv Informationen mit inländischen und internationalen Stellen aus, die ähnliche Aufgaben wie das BACS wahrnehmen würden.

Weder Art. 15a Abs. 2 Bst. h OV-VBS noch die Erläuterungen umschreiben, wie weit dieses Vertretungsmonopol geht. Die Polizei nimmt im Bereich Cyberbedrohungen ähnliche Aufgaben wahr, auch die Staatsanwaltschaften bewältigen Cybervorfälle. Der nationale und internationale Austausch zwischen Strafverfolgungsbehörden ist längst etabliert.

Der Umfang, in welchem das BACS die Gremienarbeit vornimmt, ist unseres Erachtens genauer zu definieren und auf den Bereich Cybersicherheit zu beschränken. Der nationale und internationale Austausch der Strafverfolgungsbehörden präventiv zum Schutz vor Cyberbedrohungen sowie repressiv zur Bewältigung von Cybervorfällen darf durch diese Bestimmung nicht eingeschränkt werden.

Für die Berücksichtigung unserer Anliegen danken wir bestens.

Mit freundlichen Grüssen

Michel-André Fels, Präsident

Kopie

Mitglieder SSK-CMP

Envoi électronique
ncsc@gs-efd.admin.ch

swissuniversities

Comité de swissuniversities

Luciana Vaccaro
Présidente
T +41 31 335 07 40
luciana.vaccaro@
swissuniversities.ch

swissuniversities
Effingerstrasse 15, Case Postale
3001 Berne
www.swissuniversities.ch

3001 Berne, le 13 septembre 2024

Prise de position de swissuniversities concernant le projet d'ordonnance sur la cybersécurité

Madame, Monsieur,

Nous vous remercions de la possibilité qui nous est offerte de prendre position sur le projet d'ordonnance sur la cybersécurité (OCyS).

swissuniversities est favorable à l'augmentation de la transparence concernant les cyberattaques et soutient en principe le projet d'ordonnance. Nous sommes en effet convaincu·es qu'une meilleure information sur la situation de la menace, les scénarios d'attaque concrets et les expériences tirées des stratégies de défense mises en place bénéficiera à tous les acteurs et contribuera à une augmentation de la cybersécurité en Suisse.

Nous considérons cependant que le regroupement de toutes les hautes écoles sous le terme "hautes écoles" à l'art. 74, al. 1, let. a de la Loi sur la sécurité de l'information (LSI) est trop peu différencié en ce qui concerne la cybersécurité et l'obligation de déclaration. Des valeurs seuils, telles que proposées dans le Message relatif à la modification de la loi sur la sécurité de l'information du 2 décembre 2022 devraient également être introduites pour les hautes écoles (voir ci-après notre suggestion d'exception à l'obligation de signaler). En effet, ledit message prévoit que le Conseil fédéral fixe des exceptions à l'obligation de signaler au sein de certains domaines au moyen de valeurs seuils, et qu'il est donc tenu de veiller à la proportionnalité de l'obligation de signaler en exemptant les organisations qui ne sont pas essentielles pour le fonctionnement de l'économie ou pour le bien-être de la population, comme prévu à l'art. 74c.

Par ailleurs, nous relevons dans notre commentaire ci-après des différents articles de l'ordonnance plusieurs éléments, notamment concernant la représentation des hautes écoles dans les instances qui seront créées, les liens avec les services existants de Switch, le potentiel de coordination que cette organisation offre pour les hautes écoles. Divers autres aspects y sont également abordés et nous vous prions de les considérer.

swissuniversities

Finalement, nous souhaitons relever encore deux points :

- L'introduction d'une obligation de déclaration n'est pas neutre en termes de coûts pour les hautes écoles. Il conviendra de déterminer qui prendra en charge les coûts supplémentaires.
- La création d'un registre contenant des informations sur les incidents de sécurité, les dispositifs de sécurité et les points faibles des composants d'infrastructure comporte le risque que les données collectées soient rendues publiques ou accessibles à des cercles cybercriminels en cas de fuite de données. Différentes obligations de notification (par exemple, par le biais de réglementations cantonales) existent déjà et fonctionnent avec différents délais d'annonce. Nous recommandons de tenir compte de cette situation de départ dans la perspective de la nouvelle ordonnance et de prévoir une réglementation aussi uniforme que possible.

Nous vous remercions par avance de la prise en compte de notre position, nous tenons bien volontiers à disposition pour toute précision et vous prions d'agréer, Madame, Monsieur, nos salutations les meilleures.

Dr Luciana Vaccaro
Présidente de swissuniversities

Commentaire des différents articles de l'ordonnance

Art. 4 Composition du CP CSN
En tant que faîtière des hautes écoles suisses, swissuniversities se tient à disposition pour la recherche d'une représentation adéquate des hautes écoles au sein du CP CSN. À ce sujet, le rôle de Switch devra également être clarifié.

Art. 7 Analyse technique des cyberincidents et des cybermenaces
Switch gère également une CERT pour les hautes écoles. La collaboration entre la CERT de l'OFCS, celle de Switch et les organisations de cybersécurité existantes des hautes écoles doit être réglée. Les doublons doivent être évités et Switch pourrait se charger de la coordination, en particulier pour les hautes écoles qui n'ont pas d'organisation spécifique de cybersécurité.

Art. 8 Priorités pour les conseils et l'assistance en cas de Cyberattaque
Si, en cas de cyberattaque, les demandes de conseils et d'assistance dépassent les capacités de l'OFCS, Switch pourrait soulager l'OFCS pour les hautes écoles.

Art. 10 Soutien aux autorités
Il s'agit de vérifier ici si les hautes écoles ne devraient pas également pouvoir bénéficier de ce soutien.

Art. 12 Systèmes d'information permettant l'échange automatique
Les hautes écoles profiteraient grandement de l'obtention d'informations sur les menaces actuelles (Threat Intelligence) directement auprès de l'OFCS ou via Switch et de leur utilisation pour la détection.

swissuniversities

Art. 13 Enregistrement
Les hautes écoles ont un intérêt à pouvoir s'enregistrer dès que possible. Elles se tiennent également à disposition pour tout éventuel pré-enregistrement. Une éventuelle coordination par Switch doit également être examinée.

Art. 16 Exceptions à l'obligation de signaler
Des valeurs seuils ont été définies pour d'autres institutions, cela devrait donc également être le cas pour les hautes écoles. En effet, les exigences et la charge de travail pour satisfaire à l'obligation de déclaration sont proportionnellement bien plus élevées dans les petites hautes écoles et sont difficiles à maîtriser. Des ressources limitées rendent difficile la mise en place des processus nécessaires dans le domaine de la cybersécurité ou l'obtention de ressources supplémentaires pour ce thème. En outre, certaines hautes écoles n'exploitent et n'entretiennent pas leurs propres systèmes et font appel à des prestataires de services (p. ex. fournisseurs de cloud). Par ailleurs, les instances cantonales pourraient vraisemblablement se charger de transmettre les messages de la haute école à l'OFCS.

Une possibilité consisterait à introduire une exception supplémentaire à l'alinéa 1, comme suit :

Les hautes écoles au sens de l'art. 74b, al. 1, let. a, LSI : qui
1. n'exploitent pas leur propre système de communication ou
2. n'exploitent pas leur propre centre de calcul ou
3. comptent moins de 2000 étudiant·es et/ou moins de 500 collaborateurs·trices employés en EQTP (selon la statistique actuelle de l'OFS) ou
4. les hautes écoles sans système de recherche propre ou
5. qui sont soumises à une obligation cantonale de déclaration.

Art. 18 Cyberattaques à signaler
Les annonces des hautes écoles à l'OFCS devront être coordonnées avec SWITCH CERT et une concertation entre les deux entités sera nécessaire à cet effet.

Art. 20 Transmission du signalement
Il devrait être possible pour une entreprise ou plusieurs entreprises de décider conjointement de notifier les incidents par l'intermédiaire d'un organisme tiers spécialisé qui prenne également en charge la notification des incidents, par exemple un MSSP (Managed Security Service Provider), un CERT sectoriel, un ISAC (Information Sharing and Analysis Center) sectoriel et d'autres.... Nous suggérons donc de compléter l'article 20 OCyS par un alinéa supplémentaire :
[2] Une ou plusieurs autorités ou organisations soumises à l'obligation de notification peuvent décider de sous-traiter le processus de notification, individuellement ou collectivement, à une organisation tierce spécialisée.

Art. 21 Délai de saisie du signalement
Les exigences relatives au délai d'annonce de 24 heures posent des défis importants aux petites hautes écoles en ce qui concerne la maturité des processus existants ainsi que le personnel engagé ou nécessaire. Une adaptation de ces processus nécessitera vraisemblablement des moyens financiers supplémentaires, qui devront être libérés par les processus et les instances nécessaires.

RAILplus
Die Meterspurigen
La voie métrique
A scartamento metrico

Département fédéral des finances (DFF)
Bundesgasse 3
3003 Bern

Aarau, le 13 septembre 2024

Par courriel à: ncsc@gs-efd .admin.ch

Objet : Prise de position de RAILplus dans le cadre de la procédure de consultation relative à l'adoption de l'ordonnance sur la cybersécurité (OCyS)

Madame, Monsieur,

Nous vous remercions de nous donner l'opportunité de prendre position au sujet de l'ordonnance sur la cybersécurité. Cette ordonnance, qui inclut notamment l'obligation de signaler les cyberattaques, a un impact sur chacun des membres de RAILplus.

Le texte proposé répond aux attentes de RAILplus et est en conformité avec les dispositions prévues dans le projet de loi, qui fût également soumis à consultation en 2022. En conséquence, nous n'avons pas de commentaires majeurs à formuler.

Nous vous prions d'agréer, Madame, Monsieur, l'expression de nos salutations distinguées.

Joachim Greuter
Directeur RAILplus

Urs Siegenthaler
Responsable du groupe de travail informatique RAILplus en Suisse alémanique

Nicolas Murbach
Responsable du groupe de travail informatique RAILplus en Suisse romande

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

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 Unternehmensprozess 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

Erlass einer Bundesverordnung über die Cybersicherheit – Cybersicherheitsverordnung (CSV)

Stellungnahme seitens NEDIK (Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung), Zugeordnet zur KKPKS/KKJPD

Mit diesem Schreiben beziehen wir uns auf Ihre E-Mail vom 25. Juli 2024 und bedanken uns bereits im Voraus für die Möglichkeit, Stellung beziehen zu dürfen.

Aus Sicht von NEDIK, dem Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung angegliedert an die KKPKS/KKJPD, haben wir folgende Anmerkungen:

Art. 9 Abs 5 / Koordinierte Offenlegung von Schwachstellen

Es kann die Betreiberinnen kritischer Infrastrukturen bereits vor der Behebung oder Offenlegung über Schwachstellen informieren.

Wenn Informationen über Schwachstellen vorliegen, sollten diese in der Regel veröffentlicht werden, da das Wort „kann“ zu unbestimmt ist. Das BACS sollte die Betreiber grundsätzlich vor der Behebung oder Offenlegung der Schwachstelle informieren; jedoch sollte es in bestimmten Fällen die Möglichkeit haben, abzuwarten (zum Beispiel, wenn die Informationen noch nicht verbreitet werden dürfen). Darüber hinaus entscheidet das BACS gemäss Art. 15 Abs. 2 CSV über die Veröffentlichung der Informationen, die zur Weitergabe freigegeben sind.

Art. 15 / Übermittlung und Nutzung der Informationen

Abs. 1
Registrierte Unternehmen und Behörden übermitteln Informationen dem BACS und bestimmen dabei, ob und an wen dieses die Informationen weitergeben darf, soweit eine Weitergabe der In-formation nicht gesetzlich vorgesehen ist.

Die Meldung kann vom Melder selbst gesteuert werden. Es gibt verschiedene Klassifizierungen: Persönlich (red), innerhalb der Organisation (amber strict), Organisation und Partner (amber), Weitergabe erlaubt, aber nicht öffentlich (green) und öffentlich (clear). Bei möglichen Meldungen ist darauf zu achten, dass diese korrekt klassifiziert werden (interner Prozess). Die Melder müssen die Weitergabe der Informationen auf bestimmte Daten ein- oder ausgrenzen können. Obwohl dies das Handling der Meldungen für die Melder und das BACS komplizierter macht, ermöglicht es den Meldenden, individueller und angemessener über die Weitergabe zu entscheiden.

Abs. 3
Die Informationsempfänger müssen den Schutz der Informationen gewährleisten.

Sobald Strafverfolgungsbehörden, die an das Informationssystem angeschlossen sind, von einem Offizialdelikt (z.B. Erpressung, Nötigung, unbefugte Datenbeschaffung, qualifizierte Datenbeschädigung, etc.) Kenntnis erlangen, sind sie gesetzlich verpflichtet, Ermittlungen einzuleiten. Daher muss das BACS sicherstellen, dass in den veröffentlichten Informationen die betroffene Betreiberin kritischer Infrastruktur nicht identifizierbar oder ermittelbar ist. Generell sollte in der Verordnung präziser festgelegt werden, wie das BACS und die Strafverfolgungsbehörden mit strafrechtlich relevanten Informationen umgehen sollen, die sie über das Informationssystem erhalten (vgl. Art. 76 Abs. 3 Satz 2 ISG).

Art. 18 Abs. 1 lit. a / Zu meldende Cyberangriffe

1 Die Funktionsfähigkeit einer kritischen Infrastruktur gilt als gefährdet, wenn:
a. Mitarbeitende oder Dritte von Systemunterbrüchen betroffen sind;

Nach diesem Vorschlag müsste eine Meldung erfolgen, wenn auch nur ein einzelner Mitarbeiter (oder ein einzelner Arbeitsplatz) kurzzeitig von einem isolierten Systemausfall betroffen ist, wie zum Beispiel durch einen Virus auf einem nicht ans Unternehmensnetzwerk angeschlossenen Notebook. Es ist jedoch fraglich, ob eine solche Meldung verhältnismäßig wäre. Daher sollte die Verordnung präziser definieren und eingrenzen, was unter einem „Systemausfall“ zu verstehen ist.

Art. 19 / Inhalt der Meldung

Abs 1
Die Meldung muss folgende Informationen zum Cyberangriff enthalten:
a. Datum und Uhrzeit der Feststellung des Angriffs;
b. Datum und Uhrzeit des Angriffs;
c. Art des Angriffs;

Bei der Meldung fehlt die Klassifizierung für die Weitergabe der Information (vgl. Art. 15 Abs. 1). Diese Klassifizierung sollte von Anfang an eindeutig festgelegt werden, um sicherzustellen, dass die Informationen den erforderlichen Schutz erhalten.

Abs 2
Die Meldung sollte auch beinhalten, bei welcher Behörde Strafanzeige erstattet wurde, damit das BACS bei entsprechender Datenfreigabe die notwendigen Informationen mit dieser Behörde austauschen kann.

Serdar Günal Rütsche, Leiter NEDIK

SUISSEDIGITAL

per E-Mail an ncsc@ncsc.admin.ch

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Bundeshaus Ost
CH-3003 Bern

Bern, 13. September 2024

Stellungnahme zum Entwurf der Verordnung über die Cybersicherheit (CSV)

Sehr geehrte Frau Bundespräsidentin
Sehr geehrte Damen und Herren

Mit Schreiben vom 22. Mai 2024 haben Sie interessierte Kreise eingeladen, bis zum 13. September 2024 zu den geplanten Ausführungsbestimmungen zur Meldepflicht für Cyberangriffe nach dem geänderten Informationssicherheitsgesetz («**ISG**») bzw. zur geplanten Cybersicherheitsverordnung («**E-CSV**») Stellung zu nehmen.

Suissedigital ist der Dachverband der Schweizer Telekommunikationsnetzunternehmen und vertritt die Interessen von ca. 180 privatrechtlich oder öffentlich-rechtlich organisierten Unternehmen verschiedener Grösse, die lokal, regional oder landesweit Telekommunikationsinfrastrukturen (Fest- und Mobilfunknetze) betreiben und darüber verschiedene Fernmelde- inklusive Radio- und Fernsehdienste erbringen.

Wir bedanken uns für die Möglichkeit der Meinungsäusserung, die für unsere Mitglieder wichtig ist, weil Anbieterinnen von Fernmeldediensten, die beim BAKOM nach Art. 4 Abs. 1 FMG registriert sind, ab Inkraftsetzung der ISG-Änderungen bzw. der E-CSV bei Cyberangriffen auf kritische Infrastrukturen (gemäss ISG gelten Telekommunikationsnetze als kritische Infrastruktur) neu einer Meldepflicht an das Bundesamt für Cybersicherheit (BACS) unterstehen werden. Unsere Mitglieder sind von den Vorlagen direkt betroffen, welche betriebliche Anpassungen erfordern. Aus diesem Grund fordern wir eine **spätere Inkraftsetzung bzw. längere Übergangsfrist**.

Zur Inkraftsetzung der CSV (Art. 23 E-CSV)

Art. 23 E-CSV sieht vor, dass die Verordnung am 1. Januar 2025 in Kraft tritt. Eine Inkraftsetzung der neuen Meldepflicht bzw. der Cybersicherheitsverordnung auf Anfang 2025 ist für unsere Mitglieder jedoch nicht umsetzbar. Die finale Fassung der CSV wird erst nach der offiziellen Veröffentlichung feststehen, die voraussichtlich erst gegen Ende des laufenden Jahres, also kurz vor dem 1. Januar 2025 und damit in der Weihnachts- und

Neujahrszeit, erfolgen wird. Bis dahin werden die betroffenen Mitglieder nicht genau wissen, wie die neue Regelung effektiv aussieht. Es ist selbsterklärend, dass betriebliche Prozesse zur Umsetzung der Meldepflicht in den Unternehmen im Detail erst dann geplant und umgesetzt werden können, wenn klar ist, was es effektiv regulatorisch umzusetzen gibt. Die Implementierung erfordert sodann immer eine gewisse Vorlaufzeit. Wir beantragen deshalb eine Übergangsfrist für die Umsetzung der Meldepflicht. **Zwischen der Veröffentlichung des amtlichen Wortlauts der CSV und dem tatsächlichen Beginn der Meldepflicht muss mindestens ein Zeitraum von 9 Monaten liegen. Wir ersuchen Sie deshalb dringend, die E-CSV mit einer entsprechenden Übergangsbestimmung zu ergänzen.**

***

Wir danken Ihnen im Voraus, dass Sie unseren Antrag bei der weiteren Ausarbeitung der E-CSV berücksichtigen. Für Fragen stehen wir Ihnen jederzeit gerne zur Verfügung.

Freundliche Grüsse

SUISSEDIGITAL – Verband für Kommunikationsnetze

Dr. Simon Osterwalder, Rechtsanwalt
Geschäftsführer

Stefan Flück, Fürsprecher LL.M.
Leiter Rechtsdienst

MIGROS

Beilage zu VERNEHMLASSUNG VERORDNUNG ÜBER DIE CYBERSICHERHEIT (CYBERSICHERHEITSVERORDNUNG, CSV)

https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-101088.html

Artikel	Bestimmung (Verordnungsentwurf)	Bemerkung	Anpassungsvorschlag
Art. 9 Abs. 5	Es kann die Betreiberinnen kritischer Infrastrukturen bereits vor der Behebung oder Offenlegung über Schwachstellen informieren.	Das BACS soll verpflichtet werden, die Betreiberinnen kritischer Infrastruktur sofort nach Erkennen von Schwachstellen zu informieren.	Es **muss** die Betreiberinnen kritischer Infrastrukturen bereits vor der Behebung oder Offenlegung über Schwachstellen informieren.
Art. 18 Abs. 1 lit. a	Die Funktionsfähigkeit einer kritischen Infrastruktur gilt als gefährdet, wenn: a. Mitarbeitende oder Dritte von Systemunterbrüchen betroffen sind	Nicht jeder Systemunterbruch gefährdet die Funktionsfähigkeit einer kritischen Infrastruktur. Beispiel: Der Ausfall eines Übersetzungstools ist nicht kritisch für den Betrieb der kritischen Infrastruktur. Nur der Ausfall eines "geschäftskritischen" oder "geschäftsrelevanten" Systems sollte eine Meldepflicht auslösen.	Die Funktionsfähigkeit einer kritischen Infrastruktur gilt als gefährdet, wenn: a. Mitarbeitende oder Dritte von ~~**Systemunterbrüchen**~~ **Unterbrüchen eines geschäftskritischen Systems** wesentlich betroffen sind
Art. 19 Abs. 1	[…] c. Art des Angriffs; d. Angriffsmethode; und […]	"Art des Angriffs" und "Angriffsmethode" können nicht sinnvoll unterschieden werden. Der Erläuterungsbericht nennt als Beispiele für die Art des Angriffs u.a. "DDoS" und für die Angriffsmethode u.a. "Überlastungsangriffe auf Server", was im Grunde dasselbe ist. Auf die Differenzierung sollte verzichtet werden und Art des Angriffs sowie Angriffsmethode zu einem Punkt zusammengefasst werden.	[…] c. Art **und Methode** des Angriffs; **und** ~~d. **Angriffsmethode; und**~~ […]
Art. 19 Abs. 3	Sie muss folgende Informationen zu den Auswirkungen des Cyberangriffs enthalten: a. betroffene Einheiten der Organisation oder Behörde;	Art. 74e nISG spricht nur von Informationen zur Art und Ausführung des Cyberangriffs, zu seinen Auswirkungen, zu ergriffenen Massnahmen und soweit bekannt, zum geplanten Vorgehen. Art. 19 Abs. 3 E-CSV	Streichen

	b. Schweregrad der Beeinträchtigung der Verfügbarkeit, Integrität und Vertraulichkeit der eigenen Informationen und der Informationen von Dritten; und c. Auswirkung des Cyberangriffs auf die Funktionsfähigkeit der betroffenen Einheiten der Organisation oder Behörde.	geht darüber hinaus. Ebenso sind die relevanten Informationen im Ernstfall stark kontextabhängig, weshalb eine derart detaillierte Regelung unnötig starr ist.	

Migros-Genossenschafts-Bund

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Bundeshaus Ost
CH-3003 Bern

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

Ort/Datum Zürich, 11. September 2024

Betreff **Stellungnahme zur Cybersicherheitsverordnung (CSV)**

Sehr geehrte Frau Bundespräsidentin
Sehr geehrte Damen und Herren

Die Migros bedankt sich für die Gelegenheit, zur Verordnung über die Cybersicherheit (CSV) Stellung nehmen zu können.

Die Migros ist in all ihren Geschäftsfeldern auf funktionierende kritische Infrastrukturen angewiesen. Für uns ist es von zentraler Bedeutung, dass unsere Güter sowie Dienstleistungen den Menschen in der Schweiz stets zur rechten Zeit, in ausreichender Menge und optimaler Qualität sowie auf kosteneffiziente Weise zur Verfügung stehen. Deshalb setzen sich die Unternehmen der Migros-Gruppe für Lösungen zu Gunsten einer Sicherstellung der Landesversorgung, des Erhalts bzw. der Verbesserung der Lebensqualität in der Schweiz sowie der Stärkung des Standortes Schweiz ein.

Aufgrund der zentralen Bedeutung von IKT bei der Erbringung unserer Leistungen ist es uns ein wichtiges Anliegen, an der Vernehmlassung zur Cybersicherheitsverordnung teilzunehmen.

Zusammenfassung

- Die Migros unterstützt grundsätzlich die Stärkung der Cybersicherheit in der Schweiz.
- Verfahren für die Umsetzung einer Meldepflicht sollen effektiv, jedoch auch wirtschaftlich verkraftbar sein.
- Neue Vorgaben sollen nicht über die Regelungen des Informationssicherheitsgesetzes ISG hinausgehen.
- Die heute multiplen Meldeverfahren sollen harmonisiert werden.
- Ein kooperativer Ansatz, welcher die Betroffenen in konkreten Fällen zusammenführt und ein gemeinsames Lernen ermöglicht, würde begrüsst.
- Vertretende wesentlicher kritischen Infrastrukturen sollten im Steuerungsausschuss zur Nationalen Cyberstrategie Einsitz nehmen können.

Grundsätzliche Unterstützung für eine Stärkung der Cybersicherheit

Migros teilt die Einschätzung, dass aufgrund der schlechter werdenden Sicherheitslage und der erhöhten Risikolage hinsichtlich Cyberangriffe auf Schweizer Unternehmen und Institutionen in entsprechende Schutzmassnahmen investiert werden muss. Dies gilt im Speziellen für kritische Infrastrukturen.

Migros-Genossenschafts-Bund
Direktion Wirtschaftspolitik
Limmatstrasse 152
Postfach 1766
CH-8031 Zürich

Direktwahl +41 58 570 18 03
Zentrale +41 44 277 21 11
juerg.maurer@mgb.ch
www.migros.ch

Migros-Genossenschafts-Bund

Wirtschaftlichkeit der Meldeverfahren
Verfahren für die Umsetzung einer Meldepflicht sollen risikobasiert und wirtschaftlich verkraftbar sein. Die Ausführungen der Vernehmlassungsvorlage sollen in diese Richtung optimiert werden. Melde-Anforderungen unterschiedlicher Bundesstellen (BACS, FINMA, …) sollten harmonisiert werden, um den Schutz-Effekt zu erhöhen und gleichzeitig der Kosteneffizienz Rechnung zu tragen. Auch sollen neue Vorgaben nicht über die Regelungen des Informationssicherheitsgesetzes ISG hinausgehen.

Kooperativer Ansatz
Bei der Umsetzung harmonisierter Meldepflichtverfahren soll weniger auf Formalismus, sondern mehr auf die Stärkung eines partnerschaftlichen Dialogs zwischen Behörden und Vertretenden kritischer Infrastrukturen Wert gelegt werden. Mit der Etablierung von strukturierten Dialogen sollen Lösungen erarbeitet, persönliche Netzwerke gefördert und gemeinsames Stärken der Resilienz ganzer Wertschöpfungsketten ermöglicht werden. Migros ist bereit, an der Ausarbeitung entsprechender Lösungen mitzuwirken.

Im Rahmen des Dialogs sollen die Details lagegerecht für folgende Aspekte ausgearbeitet werden:

1. Anforderungen an die Servicequalität (Art. 7)
2. Technische Analyse von Cybervorfällen und Cyberbedrohungen (Art. 7)
3. Prioritäten, Dokumentation und Veröffentlichung für Wiederanläufe (Art. 8 Abs 2)
4. Wahl der internationalen Standards für die Offenlegung von Standards (Art. 9 Abs 1)
5. Definition von Fristen (Art. 9 Abs 2).

Einsitz in Steuerungsausschuss zur Nationalen Cyberstrategie (Art. 4 E-CSV)
Als Teil des kooperativen Ansatzes soll der Steuerungsausschuss zur Nationalen Cyberstrategie so besetzt werden, dass wesentliche, für die Landesversorgung mit Gütern und Dienstleistungen kritische Unternehmungen, direkt vertreten sind (nicht via Verbände). Wir gehen davon aus, dass die Besetzung des Steuerungsausschusses im Hinblick auf die Inkraftsetzung der Verordnung geregelt wird und nicht vorher.

Änderungsanträge zu Art. 9, 15, 18 und 19
Für die genannten Artikel finden Sie in der Beilage eine Liste mit konkreten Änderungsanträgen.

Wir danken für die Kenntnisnahme und für die Berücksichtigung unserer Anmerkungen bei der weiteren Bearbeitung der Vorlage.

Freundliche Grüsse

Migros-Genossenschafts-Bund

Rainer Deutschmann
Leiter Direktion Sicherheit und Verkehr
Leiter Nationaler Krisenstab Migros-Gruppe

Dr. sc. techn. ETH Lukas Ruf
Group Chief Security & Risk Officer, CISO
Head Group Architecture, Security & Risk

Beilage

Migros-Genossenschafts-Bund

Beilage zu VERNEHMLASSUNG VERORDNUNG ÜBER DIE CYBERSICHERHEIT (CYBERSICHERHEITSVERORDNUNG, CSV)

DIE SPITÄLER DER SCHWEIZ
LES HÔPITAUX DE SUISSE
GLI OSPEDALI SVIZZERI

Bundesamt für Cybersicherheit BACS
Schwarztorstrasse 59
CH-3003 Bern

Per Mail an:
ncsc@ncsc.admin.ch

Ort, Datum	Bern, 13.09.2024	Direktwahl	031 335 11 63
Ansprechpartner/in	Dorit Djelid	E-Mail	dorit.djelid@hplus.ch

Vernehmlassung: Cybersicherheitsverordnung (CSV)

Sehr geehrte Damen und Herren

Für die Möglichkeit einer Stellungnahme zur «Cybersicherheitsverordnung (CSV)» möchten wir uns herzlich bedanken. Auch wenn H+ Die Spitäler der Schweiz nicht offiziell zur Vernehmlassung eingeladen wurde, so nehmen wir im Rahmen dieses Schreibens gerne Stellung zur entsprechenden Verordnung. Denn das Gesundheitswesen gehört mit seinen Spitälern und Kliniken zu den kritischen Infrastrukturen und ist von der Verordnung betroffen.

H+ Die Spitäler der Schweiz ist der nationale Spitzenverband der öffentlichen und privaten Spitäler, Kliniken und Pflegeinstitutionen. Ihm sind 205 Spitäler, Kliniken und Pflegeinstitutionen als Aktivmitglieder an 435 Standorten sowie 138 Verbände, Behörden, Institutionen, Firmen und Einzelpersonen als Partnerschaftsmitglieder angeschlossen.

Stellungnahmen H+ zur Cybersicherheitsverordnung (CSV)
Die Regelung der Umsetzung der Meldepflicht gemäss Informationssicherheitsgesetzt (ISG Art. 74) durch eine Cybersicherheitsverordnung (CSV) wird grundsätzlich begrüsst und als sinnvoll erachtet. Der vorliegende Entwurf der CSV wird als ausgewogen und zweckmässig beurteilt.

Hinsichtlich folgender Punkte sehen wir allerdings Bedarf für Ergänzungen bzw. Spezifikationen:

- CSV Art. 4: Im Artikel 4 wird definiert, dass der Steuerungsausschusses Nationale Cyberstrategie (StA NCS) aus Vertreterinnen und Vertreter der Departemente, der Bundeskanzlei, der Kantone, der Wirtschaft, der Gesellschaft und der Hochschulen zusammensetzt wird. Nicht explizit genannt bzw. berücksichtigt sind Vertreterinnen und Vertreter von kritischen Infrastrukturen, obwohl diese gleichermassen betroffen wie gefordert sind. Die Zusammensetzung des StA NCS ist daher um diese Gruppe zu ergänzen.

- CVS Art. 9 Abs. 2: Häufig sind die Spitäler und Klinken mit Lieferanten konfrontiert, die einen niedrigen Median der Cybersicherheitsreife haben, also nicht den dem anwendbaren Stand der Technik, der anwendbaren europäischen Regulierung für medizinische Geräte bzw. Anwendungen und Gegenstände (siehe MDR) entsprechen. Damit dieser Punkt in der Verordnung den Spitälern und Kliniken wirklich nützt, sollte die

Geschäftsstelle · Lorrainestrasse 4 A · 3013 Bern
T 031 335 11 11 · geschaeftsstelle@hplus.ch
www.hplus.ch

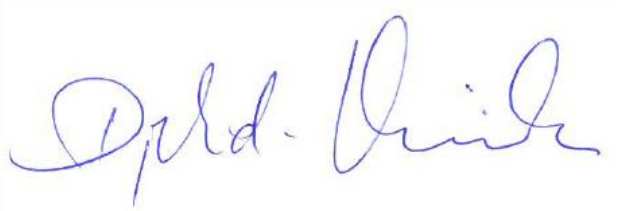
Formulierung wie folgt angepasst werden: *«Er setzt den Herstellern von Hard- oder Software, die von kritischen Infrastrukturen betrieben wird, eine Frist von 90 Tagen zur Beseitigung von Schwachstellen.»*

- CSV Art. 16: Hier werden die möglichen Ausnahmen von der Meldepflicht geregelt. Dabei wird ausgeführt, für welche Organisationen eine Ausnahme besteht. Erst aus den Erläuterungen zur CSV geht hervor, dass für Organisationen, die Leistungen zur Absicherung gegen die Folgen von Krankheit, Unfall etc. erbringen, grundsätzlich keine Ausnahme möglich ist. Somit sind Gesundheitseinrichtungen explizit von Ausnahmen ausgeschlossen. Dies darf nicht nur aus den Erläuterungen hervor gehen, sondern muss bereits aus der CSV explizit ersichtlich sein.

- CSV Art. 18: Gemäss Artikel 18 a) gilt die Funktionsfähigkeit einer kritischen Infrastruktur als gefährdet, sobald Mitarbeitende oder Dritte von Systemunterbrüchen betroffen sind. Diese Formulierung ist zu allgemein gehalten, da unklar ist, ob zum Beispiel der Ausfall eines einzelnen Laptops bereits gemeldet werden muss oder nicht. Art. 18 a) muss daher den Erläuterungen zur CSV folgend spezifiziert werden. Darin wird festgehalten, dass ein Systemunterbruch vorliegt, wenn Mitarbeitende oder Dritte für ihre Tätigkeit wichtige Arbeitsschritte nicht mehr ausführen können.

Wir danken Ihnen für die Aufnahme der Anliegen und stehen Ihnen für ergänzende Auskünfte gerne zur Verfügung.

Freundliche Grüsse



Dorit Djelid
Stv. Direktorin
Leiterin Geschäftsbereich Kommunikation

digitalswitzerland

Departement für Verteidigung, Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS
Schwarztorstrasse 59
CH-3003 Bern

Einreichung per Mail an:
ncsc@ncsc.admin.ch

Zürich, 13. September 2024

Betreff: Vernehmlassungsantwort zur Cybersicherheitsverordnung CSV

Sehr geehrte Frau Bundesrätin Amherd,
Sehr geehrter Herr Suter,

Wir danken Ihnen für die Gelegenheit, uns zur Vernehmlassung zur Cybersicherheitsverordnung (CSV) äussern zu können, welche wir hiermit für digitalswitzerland wahrnehmen.

digitalswitzerland begrüsst die Konkretisierung der im neuen ISG festgehaltenen Meldevorgänge bei Cyberangriffen auf kritische Infrastrukturen. Obschon die Vorlage äusserst klar und nachvollziehbar ist, erlauben wir uns, einige konkrete Änderungsvorschläge zu machen (jeweils in Gelb):

Art. 4. CSV Steuerungsausschuss NCS

Wir unterstützen es, einen Steuerungsausschuss Nationale Cyberstrategie (StA NCS) einzusetzen, schlagen aber vor, bei der Zusammensetzung auch Vertreterinnen und Vertreter von kritischen Infrastrukturen zu berücksichtigen. Die Formulierung «Vertreter der Wirtschaft» ist diesbezüglich zu wenig klar.

Art. 4, Abs. 1: Der StA NCS setzt sich aus Vertreterinnen und Vertretern der Departemente, der Bundeskanzlei, der Kantone, der Wirtschaft, ***insbesondere der Betreiber kritischer Infrastrukturen,*** *der Gesellschaft und der Hochschulen zusammen.*

Art. 9 Koordinierte Offenlegung von Schwachstellen

Artikel 9 Absatz 1 legt fest, dass die Offenlegung von Schwachstellen nach international anerkannten Standards zu erfolgen hat, obschon es diese noch nicht in ausreichendem Masse gibt. Um diese Lücke zu schliessen, sollen auch Best Practices[1] einbezogen werden. Der Änderungsvorschlag lautet:

Art. 9, Abs. 1: Das BACS sorgt für die koordinierte Offenlegung der Schwachstellen nach international anerkannten Standards ***und Best Practices.***

[1] CERT/CC hat bspw. eine Policy und einen Guide. Weitere Beispiele sind der OWASP Vulnerability Management Guide, oder NIST SP 800-53. FIRST hat Standards für die Koordination und Offenlegung von Schwachstellen entwickelt, siehe hier, hier und hier

In der vorgeschlagenen Formulierung der CSV ist der Bereich von "Prozessen" oder Konfigurationen von digitalen Services nicht abgedeckt. Es handelt sich bei Schwachstellen in diesem Bereich nicht (direkt) um Hard- oder Software-Probleme, sondern um falsche Konfiguration oder falsche Verwendung von Services. Jüngste Beispiele solcher Vorgänge sind:

- Eine Schwachstelle bei der Authentifizierung, die es Kriminellen ermöglichte, die für die Erstellung eines Kontos auf einer cloudbasierten Arbeitsumgebung erforderliche E-Mail-Verifizierung zu umgehen
- Ein öffentlicher Docker-Container, der einen GitHub Access-Token enthält.[2]
- Hinweise auf geheime, militärische Einrichtungen durch die Verwendung von Lokalisierungsdiensten durch Angestellte.[3]

Deswegen schlagen wir folgende Änderung vor:

Art. 9, Abs. 2: Es setzt ***dem für die betroffene Hardware, Software oder Services Verantwortlichen*** *eine Frist von 90 Tagen zur Behebung der Schwachstellen.*

Art. 11 Kommunikationssystem für den sicheren Informationsaustausch

Alle Betreiber kritischer Infrastrukturen im Land, einschliesslich solcher ohne Sitz in der Schweiz, sollten die Möglichkeit haben, am Informationsaustausch teilzunehmen (Art. 74 rev. ISG). Für globale Unternehmen ist der grenzüberschreitende Austausch von zentraler Bedeutung.

Deswegen schlagen wir folgende Änderung vor:

Art. 11 Abs. 1 1 Zugang zum Kommunikationssystem des BACS für den sicheren Informationsaustausch (Artikel 74 Abs. 2 Buchstabe a ISG) 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.***

Art. 13 Registrierung

Die aktuelle Formulierung deutet auf eine Verantwortlichkeit der gemeldeten Person hin, dabei soll es laut Botschaft lediglich um eine Kontaktperson gehen. Daher sollte die Formulierung in «Angaben zu einer oder mehreren Kontaktpersonen» angepasst werden.

Deswegen schlagen wir folgende Änderung vor:

Art. 13 Abs. 2., Bst. b: ~~*Kontaktangaben der gemeldeten Person.*~~ ***Angaben zu einer oder mehreren Kontaktpersonen.***

[2] Siehe: https://www.schneier.com/blog/archives/2024/08/leaked-github-python-token.html

[3] Siehe: https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/

Art. 18 Zu Meldende Cyberangriffe

Wir regen an, den Schweregrad eines Cyberangriffs bei der Meldepflicht mitzuberücksichtigen. Dadurch könnte viel administrativer Aufwand vermieden werden. Wir möchten dadurch verhindern, dass beispielsweise kurze Systemausfälle bei einem eingeschränkten Personenkreis gemeldet werden müssen. In bereits existierenden sektorspezifischen Compliance-Regelwerken[4] wird dem Schweregrad Rechnung getragen.

Deshalb schlagen wir folgende Änderungen vor, die zur Harmonisierung/Angleichung der Verordnung mit anderen Regelwerken beitragen:

Art. 18 Abs. 1 Bst. a: «Mitarbeitende oder Dritte, ***welche den unmittelbaren Betrieb der kritischen Infrastruktur verantworten, von durch Cyberangriffen verursachten Unterbrüchen kritischer Systeme betroffen sind und dadurch der stabile Betrieb der Infrastruktur unmittelbar gefährdet ist*** *oder…»*

*Art. 18 Abs. 2 Bst. a: «****Kritische*** *geschäftsrelevante Informationen …offengelegt* ~~***werden***~~***, entwendet, zerstört, deaktiviert oder sonst wie bearbeitet werden, welche sich mittel- oder langfristig auf wesentliche Applikationen oder Systeme auswirken;***»*

Neu eingefügt als Abs. 2 Bst. b: ***«die Integrität der Geschäftsprozesse beeinträchtigt ist, oder»***

Eine Abstufung bzw. eine Definition des Schweregrades wäre auch beim Abfluss von Informationen hilfreich. Wird lediglich ein unproblematisches Dokument publiziert, wiegt dies nicht so schwer, wie wenn vertrauliche sensible Daten an die Öffentlichkeit gelangen.

Art 19 Angaben zum Verursacher:

Im Rahmen der Meldung müssen auch Angaben zum Verursacher der Cyberattacke gemacht werden. Dies bedingt aufwändige forensische Verfahren, die äusserst komplex sind und im Aufgabenbereich der Strafverfolgung, und nicht der Unternehmen, liegen.

Deswegen schlagen wir folgende Änderung vor:

Art. 19, Abs. 1, Bst. e: Angaben zum Verursacher, ***falls diese ohne aufwändige forensische Verfahren ermittelt werden können.***

Art. 20 Übermittlung der Meldung

Der Artikel scheint eine Meldung durch eine Drittperson zu betreffen, die nicht meldepflichtig ist, jedoch eine registrierte Organisation betrifft. Die vorgeschlagene Formulierung würde dazu führen, dass die meldende Person der meldepflichtigen Organisation bekannt wird, da ihre Kontaktdaten gemäss Art. 19 Abs. 4 Bst. b weitergegeben werden. Dies könnte ein Hindernis für Drittmeldungen darstellen, da nicht

[4] Bspw. FINMA 05/2020, siehe: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20200507-finma-aufsichtsmitteilung-05-2020.pdf

meldepflichtige Personen oder Organisationen möglicherweise anonym bleiben möchten, was in diesem Fall nicht möglich wäre.

Deshalb schlagen wir folgende Änderungen vor:

Art. 20: Falls ~~die~~ ***eine*** *Meldung nicht über das Kommunikationssystem des BACS erfolgt, informiert dieses das BACS die Kontaktperson nach Artikel 13 Absatz 2 Buchstabe b* ***einer registrierten und von der Meldung betroffenen Organisation*** *über den Eingang und den Inhalt der Meldung,* ***indes ohne die Kontaktangaben der meldenden Organisation oder Person, es sei denn, auch die Kontaktangaben sind zum Schutz der Cybersicherheit erforderlich.***

Weitergehende Bemerkungen

Zudem möchten wir die Gelegenheit ergreifen, aufbauend auf der Zielsetzung des ISG und der CSV, vier weitere Diskussionspunkte zu nennen, die die Digitalwirtschaft beschäftigen:

Koordination des BACS

Ziel muss sein, dass meldepflichtige Akteure jeweils nur eine Meldung an eine Behörde machen. Das BACS spielt eine zentrale, koordinative Rolle, was die Meldepflicht betrifft. Wir regen an, dass das BACS sämtliche meldepflichtigen Vorfälle entgegennimmt und diese dann mit weiteren relevanten Behördenstellen koordiniert. Eine einzige Meldestelle verhindert Mehraufwand und Doppelspurigkeiten. Alternativ können wir uns auch vorstellen, dass sich Behörden, an welche gemeldet werden muss, (FINMA, EDÖB, BACS) untereinander koordinieren.

Meldeverhalten bei Schwachstellen

Unabhängig der gesetzlichen Meldevorschriften ist für digitalswitzerland und seine Mitglieder eine proaktive, offene Meldekultur bei Cyberschwachstellen von grosser Bedeutung. Artikel 9 zur koordinierten Offenlegung von Schwachstellen gibt die richtige Richtung vor, spezifiziert aber nur die Pflichten des BACS gegenüber Herstellern von Hard - bzw. Software und anderen Behörden. Komplementär ist es aber auch notwendig, gegenüber der Wirtschaft Anreize zu setzen, die ein proaktives Meldeverhalten fördern. Massnahmen und Instrumente zur Erhöhung von freiwilligen Meldungen sollten gemeinsam mit der Wirtschaft entwickelt, kontinuierlich getestet und weiterentwickelt werden.

Priorisierung von Meldungen

Unter Art. 8, Absatz 2 wird die Priorisierung von Meldungen bei Cyberangriffen unter Berücksichtigung öffentlicher Interessen festgehalten. Eine Liste der spezifischen Kriterien bzw. eine Abstufung der konkreten Schadensszenarien, nach denen priorisiert wird, wäre für die Digitalwirtschaft eine wichtige Hilfestellung.[5] digitalswitzerland hat schon in seiner Vernehmlassungsantwort zum neuen Militärgesetz

[5] In der laufenden Diskussion um die digitale Souveränität liefert die Swiss Data Alliance hilfreiche Ansätze für eine mögliche Bewertung eines Schadensszenarios. siehe: https://www.swissdataalliance.ch/publikationen/whitepaper-digitale-souveraenitaet

(insb. Art. 95) in Bezug auf eine sog. “ausserordentliche Lage in Friedenszeiten in Bezug auf Cyberbedrohungen” eine nachvollziehbare Kategorisierung angeregt.[6]

Vertrauen durch Zuverlässigkeit

Nicht zuletzt sehen wir in der Verordnung zum Informationssicherheitsgesetz einen wichtigen Schritt hin zur Förderung **einer vertrauenswürdigen digitalen Infrastruktur** für die Schweiz. Zuverlässige, von der Wirtschaft schnell umsetzbare Meldeabläufe bei Cyberangriffen sind dafür ein Grundpfeiler. digitalswitzerland ist überzeugt, dass diese Elemente die nächsten Jahre des Erfolges der Digitalisierung der Schweiz massgeblich prägen werden und stellt sich als Dialogpartner in diesen Fragen dem Bundesamt für Cybersicherheit jederzeit zur Verfügung.

Für Ihre Kenntnisnahme und für die wohlwollende Prüfung und Berücksichtigung unserer Anliegen, sehr geehrte Frau Bundesrätin Amherd, sehr geehrter Herr Suter, danken wir Ihnen.

Freundliche Grüsse,

Stefan Metzger
Managing Director digitalswitzerland
stefan@digitalswitzerland.com

Guillaume Gabus
Public Affairs & Management
guillaume@digitalswitzerland.com

---

*Der Austausch zwischen Wirtschaft, Wissenschaft, Behördenorganisation und Politik steht im Zentrum der Arbeit von **digitalswitzerland**. Mit Impulsen und konkreten Beiträgen sollen die Möglichkeiten der digitalen Technologien genutzt werden. Darüber hinaus müssen die damit verbundenen Risiken gemanagt und das Vertrauen der Menschen in die Technologien gefördert werden, um die Schweiz in eine führende digitale Nation zu transformieren. Mit der künstlichen Intelligenz hat ein neues Kapitel in der Digitalisierung begonnen. Besondere Prioritäten sind die Bildung, eine vertrauenswürdige digitale Infrastruktur, Cybersecurity, eSustainability, Digital Health und eGovernment. Die damit verbundenen Herausforderungen geht digitalswitzerland in enger Zusammenarbeit mit den über 170 Mitgliedern, Partnern und anderen Verbänden an.*

[6] Siehe Vernehmlassungsantwort von digitalswitzerland zur Revision des Militärgesetzes (Art. 95): https://digitalswitzerland.com/wp-content/uploads/2024/03/digitalswitzerland_-Vernehmlassung_Militargesetz_DE.pdf

Salt.

Salt Mobile SA
Rue du Caudray 4
CH-1020 Renens 1

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Viola Amherd, Bundespräsidentin
CH-3003 Bern

Eingereicht als pdf und word per email an: ncsc@ncsc.admin.ch

Renens, 13. September 2024

Stellungnahme zur Vernehmlassung der Cybersicherheitsverordnung (CSV)

Sehr geehrte Frau Bundespräsidentin, sehr geehrte Damen und Herren

Wir möchten uns für die Möglichkeit zur Stellungnahme betreffend die Vernehmlassung der Cybersicherheitsverordnung (CSV) bedanken.

Salt Mobile SA («Salt») ist eine Fernmeldedienstanbieterin und Mobilfunkkonzessionärin und betreibt als solche u.a. ein eigenes Festnetz und Mobilfunknetz. Salt ist als Betreiberin kritischer Infrastrukturen damit direkt von den vorgeschlagenen Änderungen betroffen.

Wir verweisen auf die Stellungnahme unseres Branchenverbandes asut und unterstützen diese vollends. Wir bitten Sie um wohlwollende Aufnahme.

Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse

Felix Weber
Senior Regulatory Affairs Manager

Beilage: Stellungnahme der asut

CH++

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
Bundesrätin Viola Amherd
Eingabe per Mail an: ncsc@ncsc.admin.ch

Vernehmlassungsantwort zur Cybersicherheitsverordnung (CSV)

Mit grossem Interesse haben wir die Vernehmlassung zur Cybersicherheitsverordnung zur Kenntnis genommen. Unsere Organisation CH++ widmet sich unabhängig einer nachhaltigen, wohlhabenden und handlungsfähigen Schweiz durch Wissenschaft und Technologie — und dazu gehört fraglos auch die Cybersicherheit. Gerne nehmen wir entsprechend hiermit von der Möglichkeit gebrauch, Ihnen unsere Vernehmlassungsantwort zukommen zu lassen.

CH++ begrüsst die Stossrichtung des Entwurfs und hält ihn für zweckdienlich, um die Sicherheit des Landes effektiv, kollaborativ und vertrauenswürdig zu erhöhen. Punktuell sind allerdings Schärfungen und Klärungen nötig, die wir gerne im Folgenden erläutern.

Die vorgeschlagene Cybersicherheitsverordnung stellt einen wichtigen Schritt zur Stärkung der Cybersicherheit in der Schweiz dar. Mit den von uns vorgeschlagenen Präzisierungen und Ergänzungen könnte die Wirksamkeit der Verordnung noch weiter erhöht werden. Wir danken Ihnen für die Berücksichtigung unserer Anmerkungen und stehen Ihnen für weiteren Dialog stets gerne zur Verfügung.

Marcel Salathé, Präsidium
Hannes Gassert, Präsidium
Olga Baranova, Geschäftsleitung

2. Abschnitt: Nationale Cyberstrategie und Steuerungsausschuss Art. 2 Nationale Cyberstrategie 1 Die Nationale Cyberstrategie (NCS) legt den strategischen Rahmen für die Prävention im Bereich der Cybersicherheit, die Früherkennung von Cyberbedrohungen, die Reaktionsmöglichkeiten und die Resilienz bei Vorfällen sowie die Bekämpfung der Cyberkriminalität fest. 2 Sie wird in Abstimmung mit den Kantonen festgelegt.	Wir begrüßen grundsätzlich die Festlegung einer Nationalen Cyberstrategie (NCS). Allerdings sehen wir mit Besorgnis, dass laut Artikel 2, Absatz 2 die NCS nur "in Abstimmung mit den Kantonen" festgelegt wird. Dies wirft die Frage auf, inwiefern zukünftig gewährleistet ist, dass die NCS nicht ausschließlich durch Teilnehmende aus Bund und Kantonen festgelegt wird.
Art. 4 Zusammensetzung des StA NCS 1 Der StA NCS setzt sich aus Vertreterinnen und Vertretern der Departemente, der Bundeskanzlei, der Kantone, der Wirtschaft, der Gesellschaft und der Hochschulen zusammen. 2 Der Bundesrat bestimmt alle fünf Jahre die Mitglieder des StA NCS, mit Ausnahme der Vertreterinnen und Vertreter der Kantone; diese werden von der Konferenz der Kantonsregierungen bestimmt. 3 Er ernennt aus dem Kreis der Vertreterinnen und Vertreter der Wirtschaft, der Gesellschaft und der Hochschulen die	Die breite Zusammensetzung des Steuerungsausschusses ist grundsätzlich zu begrüssen. Allerdings fehlen klare Kriterien für die Auswahl der Mitglieder, insbesondere aus Wirtschaft, Gesellschaft und Hochschulen. Wir schlagen vor, transparente Auswahlkriterien festzulegen, die sicherstellen, dass die Mitglieder über die notwendige Expertise im Bereich Cybersicherheit verfügen. Dabei sollte besonders darauf geachtet werden, dass ausgewiesene Sicherheitsexperten angemessen vertreten sind. Die aktuelle Zusammensetzung, bei der nur eine von drei Vertretern der Wirtschaft eine

vorsitzende Person.	ausgewiesene Sicherheitsexpertin ist, erscheint uns nicht ausgewogen.
Art. 7 Technische Analyse von Cybervorfällen und Cyberbedrohungen 1 Das BACS betreibt das nationale Einsatzteam für Computersicherheit (Computer Emergency Response Team [CERT]), das insbesondere die folgenden Aufgaben wahrnimmt: a. technische Vorfallbewältigung; b. Analyse technischer Fragestellungen; c. Identifikation und Beurteilung von Cyberbedrohungen. 2 Es betreibt für die Analyse der Cybervorfälle und Cyberbedrohungen eine resiliente Infrastruktur; diese muss unabhängig von der restlichen Bundesinformatik funktionieren	Der Begriff “CERT” ist eine urheberrechtlich geschützte Marke. Um allfälligen künftigen Komplikationen aus dem Weg zu gehen, bietet es sich an, den Begriff CSIRT (Computer Security Incident Response Team) zu nutzen. “Resilient” ist aus unserer Sicht ein nicht genügend präziser Begriff. Wir schlagen vor, mittels einer Formulierung wie der folgenden zusätzliche Klarheit zu schaffen: “Der Betrieb dieser Infrastruktur muss jederzeit und möglichst unabhängig von Dritten sichergestellt werden können.” Zudem stellt sich die Frage nach der technischen Infrastruktur für die Analysen. Es sollte präzisiert werden, ob und inwiefern Cloud-Dienste für die technischen Analysen verwendet werden dürfen. Falls ja, wie werden diese Cloud-Dienste ausgewählt? Handelt es sich um vom Bund betriebene oder kommerziell verfügbare Dienste? Wie werden wichtige Sicherheitsaspekte wie Abhängigkeit und Verfügbarkeitsgarantie geregelt?

Art. 9 Koordinierte Offenlegung von Schwachstellen 1 Das BACS sorgt für die koordinierte Offenlegung der Schwachstellen nach international anerkannten Standards. 2 Es setzt der Herstellerin der betroffenen Hard- oder Software eine Frist von 90 Tagen zur Behebung der Schwachstellen. 3 Es kann die Frist verkürzen, wenn eine Schwachstelle: a. die Funktionsfähigkeit von kritischen Infrastrukturen gefährdet; b. besonders leicht für einen Cyberangriff ausgenutzt werden kann; oder c. weit verbreitete Systeme betrifft. 4 Es kann die Frist verlängern, wenn sich die Behebung der Schwachstelle als besonders aufwendig erweist. 5 Es kann die Betreiberinnen kritischer Infrastrukturen bereits vor der Behebung oder Offenlegung über Schwachstellen informieren.	Wir schlagen vor, Punkt 4 strenger zu formulieren, um sicherzustellen, dass die Fristen nicht in zu vielen verlängert werden, bzw. um den Druck leicht zu erhöhen: Fristen dürfen nur “in begründeten Ausnahmefällen" verlängert werden. Wir schlagen vor, Punkt 5 zu schärfen. Es gilt hier sicherzustellen, dass möglichst nicht der Eindruck entstehen kann, das VBS behalte Informationen über Sicherheitslücken in riskanten Situationen zurück, um diese allenfalls selbst länger offensiv nutzen zu können. Entsprechend schlagen wir vor, die Kann-Formulierung abzuändern zu: “Es informiert grundsätzlich die Betreiberinnen kritischer Infrastrukturen bereits vor der Behebung oder Offenlegung über Schwachstellen.”

6 Auf die vom Bundesamt für Kommunikation (BAKOM) im Rahmen seiner Aufsichtskontrollen (Art. 36 ff. der Verordnung vom 25. November 20152 über Fernmeldeanlagen) entdeckten Schwachstellen sind die Absätze 1 bis 4 nicht anwendbar. Das BAKOM informiert in solchen Fällen das BACS. 7 Das BACS informiert das BAKOM umgehend über die in Fernmeldeanlagen nach Artikel 3 Buchstabe d des Fernmeldegesetzes vom 30. April 19973 entdeckten Schwachstellen.	
5. Abschnitt: Meldepflicht Art. 16 Ausnahmen von der Meldepflicht 1 Die folgenden Behörden und Organisationen sind unter den nachstehenden Voraussetzungen von der Meldepflicht ausgenommen: a. Stellen nach Artikel 74b Absatz 1 Buchstaben b und c ISG: sofern sie für weniger als 1000 Einwohnerinnen und Einwohner zuständig sind; massgeblich ist die ständige Wohnbevölkerung; b. Unternehmen nach Artikel 74b Absatz 1 Buchstabe d ISG, sofern sie:	Die Spitäler sollten unabhängig von ihrer Grösse als meldepflichtig qualifiziert werden, da sie eine kritische Rolle in der Gesundheitsversorgung spielen. Zudem fehlt eine Regelung zum Umgang mit Kumulations-Risiken. Wie wird vorgegangen, wenn viele kleine, nicht meldepflichtige Organisationen betroffen sind und dies in der Summe ein wesentliches Risiko ergibt? Dies ist besonders relevant, da durch die zunehmende Vernetzung auch größere Organisationen im Sinne einer Kaskadierung betroffen sein können. Wir schlagen vor, einen Mechanismus zur Erfassung und Bewertung solcher

1. als Netzbetreiber, Elektrizitätserzeuger, Elektrizitätsspeicherbetreiber oder Dienstleister im Elektrizitätsbereich gemäss Artikel 5a Absatz 1 und Anhang 1a der Stromversorgungsverordnung vom 14. März 20084 weder das Schutzniveau A noch das Schutzniveau B einhalten müssen, 2. als Betreiber von Gasleitungen nach Artikel 2 Absatz 3 der Rohrleitungssicherheitsverordnung vom 4. Juni 20215 im Durchschnitt der letzten fünf Jahre eine transportierte Energie von weniger als 400 GWh/Jahr aufweisen; c. Unternehmen nach Art. 74b Absatz 1 Buchstabe n ISG, sofern sie: 1. kein Information Security Management System nach den Artikeln 2 und 4 und dem Anhang II der Verordnung (EU) 2023/2036 oder nach Artikel 2 und dem Anhang II der Verordnung (EU) 2022/16457 einrichten müssen, 2. die Vorgaben nach Punkt 1.7 des Anhangs der Verordnung (EU) 2015/19988 in ihrem Security-Programm nach Artikel 2, 12, 13 oder 14 der Verordnung (EG) 300/20089 nicht umsetzen müssen; d. Eisenbahnunternehmen sowie Seilbahn-,	kumulativen Risiken in die Verordnung aufzunehmen.

Trolleybus-, Autobus- und Schifffahrtsunternehmen nach Artikel 74b Absatz 1 Buchstabe m ISG, sofern sie: 1. nicht mit Systemaufgaben (Art. 37 des Eisenbahngesetzes vom 20. Dezember 195710 [EBG]) beauftragt sind, 2. über eine Personenbeförderungskonzession nach Artikel 6 des Personenbeförderungsgesetzes vom 20. März 200911 (PBG) verfügen, aber keine durch Bund und Kantone gemeinsam bestellten Angebote erbringen (Art. 28–31c PBG), 3. sie über eine Infrastrukturkonzession nach Artikel 5 EBG verfügen, diese aber nicht erteilt wurde, weil ein öffentliches Interesse am Bau und Betrieb der Infrastruktur besteht (Art. 6 Abs. 1 Bst. a EBG); e. Anbieterinnen und Betreiberinnen nach Artikel 74b Absatz 1 Buchstabe t ISG: sofern sie einen Sitz in der Schweiz haben und ihre Leistungen weder teilweise noch vollumfänglich gegen Entgelt für Dritte erbringen. 2 Unternehmen nach Artikel 74b Absatz 1 Buchstaben f, g, h, l und p ISG, für die	

Absatz 1 nicht anwendbar ist, sind von der Meldepflicht ausgenommen, sofern sie im betroffenen Bereich weniger als 50 Personen beschäftigen und ihr Jahresumsatz beziehungsweise ihre Jahresbilanzsumme im betroffenen Bereich 10 Millionen Franken nicht übersteigt.	

Beat Lehman
lic.iur. Fürsprech
Acting Counsel RioTinto / Alcan Holdings Switzerland AG
Kongoweg 9 (Home Office)
5034 Suhr

Festnetz 062 842 49 52
Mobil-Tf 079 500 82 32
e-mail b.lehmann-aarau@bluewin.ch

Suhr, 13. September 2024

Elektronisch übermittelt ncsc@ncsc.admin. Ch

Frau Bundesrätin und Bundespräsidentin Viola Amherd
Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS)

z.K. Herren M. Suter Stv Direktor BACS und R. Siffert, Leiter Rechtsdienst BVACS

Ergänzende Überlegungen

zum Erlass der Cybersiehrheitsverordnug ("CSV")

Der Unterzeichnende* erlaubt sich, gestützt auf Art. 4 Abs. 1 und Art. 7 Abs. 3 Bst. c) VlG iVm Art. 1, Art. 5 und Art. 20 Abs. 3 VwVG und in Ergänzung seiner Mitwirkung in einer Arbeitsgruppe der ISSS - Information Security Society Switzerland zum Text der CSV noch folgende "Ergänzenden Überlegungen und Empfehlungen" festzuhalten, mit dem Ziel, dadurch einen kleinen Beitrag zum Ausbau und zur Weiterentwicklung der Massnahmen gegen die erkannten heutigen und die möglichen künftigen Bedrohung der Informatik-Infrastruktur unseres Landes, seiner Gesellschaft und Wirtschaft beizutragen.

---

* aufgrund von mehr als 2'000 Diensttagen im militärischen Nachrichtendienst, zuletzt als Leitender Nof einer Heereseinheit (Feld Div 5); Rechtskonsulent IBM Schweiz und Europa in Zürich und Paris; hierauf Angehöriger im Konzernstab Recht der Alusuisse Lonza Gruppe sowie der Alcan / Rio Tinto Holdings Switzerland; Mitglied der Expertenkommission des Bundes zur Schaffung des geltenden Datenschutzgesetzes von 1992 sowie der Gesetzgebung über die Führung und Aufbewahrung von Geschäftsbüchern und Buchungsbelegen in maschinell lesbarer Form (Art. 958f OR und GeBüV); langjähriger Lehrbeauftragter für Datenschutz- und Informatikrecht an ETHZ / Universität Zürich und FHNW Campus Brugg; Mitwirkung in Vorstand oder Beirat von Fachorganisationen wie SWISSMEM, VUD, SWICO, ISSS, S-I zu Fragen von Informatik und Recht; 1994 -2020 Mitglied des Verwaltungsrats / VR Präsident eines mittelständischen Chemie-Unternehmens

A Allgemeine Feststellungen und Überlegungen

1. Mit grosser Genugtuung und Dankbarkeit durfte ich feststellen, dass in der Ergänzung des ISG vom 29. September 2023 und vorliegenden Entwurf der CSV verschiedene Vorschläge und Empfehlungen meiner Stellungnahme vom 14. April 2022 zur Ergänzung des Bundesgesetzes über die Informationssicherheit beim Bund (”ISG”) durch Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen Eingang gefunden haben.

   Zur Vermeidung von Wiederholungen sei auf die erwähnte Stellungnahme 14 April 2023 verwiesen, welche ich als integrierten Teil der nachfolgenden Ausführungen verstehe.

2. Nach hier vertretener Auffassung bilden das Informationssicherheitsgesetz (”ISG”), vom 18.Dezember 2020, ergänzt durch die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen vom 29. September 2023 und die CSV wichtigen Elemente in einem umfassenden Komplex von Massnahmen der von Gesellschaft und Politik (durch Gesetzgebung), Wirtschaft (insbesondere Anbieter und Anwender von Informatiklösungen) und militärischer Verteidigung gegen die Bedrohungen der Informatik-Infrastruktur durch Cyberangriffe an die Hand genommenen Massnahmen.

3. Das bedeutet, dass ISG und CSV auf die von den übrigen Akteuren ergriffenen Massnahmen zur Abwehr von Cyberangriffen ergriffenen Massnahmen durch Koordination und Harmonierung abgestimmt werden sollten

B. Besondere Anmerkungen,Vorschläge und Empfehlungen

I. Es gibt nach hier vertretener Auffassung grundsätzlich **zwei typische Fallsituationen**, bei denen sich die Bedrohung durch einen Cyberangriff auswirken kann

   a. Sicherheitsmängel **bei einem einzelnen ITAnwender**: Beispiel **Dataleak bei Xplain** mit Offenbarung verarbeiteter Personen- und Geschäftten: In solchen Fällen kann das NCSC geeignete Massnahmen zur Beseitigung derSicherheitslückeanordnen und dereun Umsetzung kntrolleieren https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-100315.html https://www.srf.ch/news/schweiz/datenleck-bei-xplain-adressen-von-bundesraeten-im-darknet-veroeffentlicht https://www.watson.ch/digital/schweiz/534924956-hacker-leaken-fast-1-terabyte-an-daten-von-schweizer-it-firma-xplain https://www.watson.ch/digital/schweiz/633322892-nach-datendiebstahl-bei-xplain-diese-massnahmen-ergreift-der-bund-jetzt

   b. Cyberangriffe welche eine **Vielzahl von Anwendern mit der gleichen Informatik-Infrastruktur** betreffen. Beispiel: **Crowdstrike Computerpanne** entstanden in der Nacht vom 18. auf den 19.Juli 2024 bei der Installation des mit einem Programmfehler belasteten Update der ”Falcon” Software, wobei die betroffenen Rechner den Betrieb einstellten, mit Schäden im Milliardenbereich; ein **Menetekel**, welches die Abhängigkeit der IT Nutzer von Millionen gleichartiger Computersysteme demonstriert hat https://www.nzz.ch/technologie/flugverkehr-weltweit-wegen-it-problemen-eingeschraenkt-ld.1840322 https://www.nzz.ch/technologie/flugverkehr-weltweit-wegen-it-problemen-eingeschraenkt-

ld.1840322 https://www.nzz.ch/technologie/ein-einzelner-fehler-legt-flughaefen-banken-und-fernsehsender-weltweit-lahm-wie-kann-das-sein-ld.1840351 https://www.nzz.ch/meinung/crowdstrike-der-groesste-it-ausfall-der-geschichte-ist-alarmzeichen-das-wir-ernst-nehmen-sollten-ld.1840617

Ähnliche Massenphnomne traten es übrigens auch schon früher auf : derUnterzeichnende erinnert sich dnoch gut daran, wie die Alusuisse-Lonza Gruppe und benachbarte Firmen im Zürcher Seefeld sich anfangs Mai 2000 mit den Herausforderungen des "**I Love You," Virus** auseinandersetzen mussten https://en.wikipedia.org/wiki/ILOVEYOU

2. Bei den **Meldepflichten** sollten folgende Situationen Beachtung geschenkt werden

   a. **Massenauftritt von Störungen** mit einer grossen Anzahl betroffenen IT Anwendern, wie bei der vorstehend umschriebenen Datenpanne von Crowdstrike in der Nacht vom 18. Auf den 19.Juli 20024. Angesichts der "Monokultur der in der Praxis verwendeten Informatik-Infrastruktur können weitere derartigen Massenausfällen eintreten-In solchen Fällen besteht das Risiko, dass das Online-Meldesystem des NCSC zusammenbricht, vergleichbar einer DDoS Attacke.

   b. Meldepflicht bei **Auftragsbearbeitung**: Wer ist in Outsourcing-Situationen zur Meldung verpflichtet: Die verantwortliche Auftraggeberin oder der Auftragsbearbeiter, v.s. dann, wenn sich der von einem Cyberangriff betroffene Auftragsbearbeiter im Ausland befindet.

   c. Meldepflicht bei **verbundenen Unternehmen**, z.B. Konzern mit Dutzenden von Konzerngesellschaften (im In-und Ausland!) oder ein Unternehmen mit selbständigen / unselbständigen Verkaufsstellen, die von einem Cyberangriff betroffen sein können. In solchen Fällen wäre denkbar, dass verbundene Unternehmen durch interne Weisungen die Meldepflicht von Cyberangriffen koordinieren und regeln können.

   d Anzustreben wäre auch der **Harmonisierung** der in Bezug auf Frist, Inhalt und Sanktion **unterschiedlichen Meldepflichten** nach Art. 74a ff ISG mit der Strafdrohung nach Art. 74 g/h ISG mit Art. 24 DSG und Art 29 Abs. 2 FINMAG.

   e. Bei **grenzüberschreitenden Cyberangriffen** wäre ferner die Meldepflichten den anwendbaren mit ausländischen Rechtsvorschriften zu koordinieren.

   f. Analog zur Kompetenz des NCSC nach Art. 74a ISG wäre es für die Praxis nützlich, wenn das NCSC die Kompetenz erhielte zu typischen wie vorstehend erwähnten **Fallgruppen Merkblätter oder Richtlinien** zur Erfüllung der Meldepflicht herauszugeben.

3. Die Bedrohung der Informatik-Infrastruktur ist **dynamisch**: Die Verordnung sollte dem Bundesrat bzw. dem BACS / NCSC die Kompetenz einräumen, zeitgerecht Massnahmen zur Abwehr von Cberangriffen bei geänderten Bedrohungslage anzuordnen:

   a. Aufgrund der "Zeitenwende" vom 24. Februar 2024 Störung der IT Infrastruktur durch einen offen oder verdeckt handelnden ausländischen Staat oder dessen Agenten wie sog. "Trollfabriken" https://de.wikipedia.org/wiki/Troll-Armee in der Anfangsphase des Angriffs von Russland auf

die Ukrtaine im Jahr 2022 https://de.wikipedia.org/wiki/Cyberkrieg_im_Bezug_zum_Russland-Ukraine-Krieg Es ist nicht auszuschliessen, dass solche Cyber-Angriffe verdeckter Herkunft weiterhin auf westeuropäische Staaten gerichtet werden, einschliesslich die offiziell als ”unfreundliches Land” deklarierte Schweiz.

b. Cyberangriffe können als Bestandteil hybriden Kriegführung unter Nutzung des Potentials der ”sozialen Netzwerke auch in der Form **gezielter Desinformation** ausgeführt werden; diese Form der Bedrohung sollte in die Weiterentwicklung des Abwehrdispositivs aufgenommen werden.

c. Nicht nur die ”Klassische Datenverarbeitung” kann Ziel von Cyberangriffen werden: Vielmehr werden sich Cyber-Attacken vermehrt auch gegen die **Betriebstechnologie** (OT) und **SCADA** Systeme richten, die in der bisherigen Fassung des ergänzten ISG und der CSV noch nicht ausdrücklich behandelt werden.

d. Die **künstliche Intelligenz** wird für die Entwicklung der Mittel und Verfahren vonCyber-Attacken und deren Abwehr eine Schlüsselrolle spielen KI ist ein Beispieldass das erweiterte ISG und die CSV für die Bewältigung der Zukunft der Bedrohung und dieG ewährleistung derSicherheit der Informatik-Infrastruktur unseres Landes, seiner Wirtschaft und gesedlslchaft offen sein muss.

4. Die Bedrohung durch Cyberangriffe ist **an keine Landesgrenzen** gebunden: Demgemäss sollte durch die Gesetzgebung ausdrücklich die Möglichkeit des BACS und des Nationalen Zentrums für Cybersicherheit NCSC **zur internationalen Zusammenarbeit der ”Cyber Defence**” im Rahmen von OECD, EU / ENISA, NATO hervorgehoben werden.

5. Die Abwehr von Cyber-Attacken ist eine Aufgabe, **welche alle Kräfte** unseres Landes herausfordert; das erweiterte ISG und die CSV solle die Grundlage für eine **umfassende ”Public -Private Partner-ship**” der staatlichen Behörden aller Stufen, der Wirtschaft (Anbieter und Anwender der Informationstechnologie) und Wissenschaft (Hochschulen, Fachhochschulen, aber auch die wichtigen Forschungseinrichtungen der grossen IT Unternehmen unserem Land.

Abschliessend möchte sieh der Unterzeichnende für die Unvollständigkeit und Fehlerhaftigkeit dieser aus spontanem Antrieb unter Zeitdruck aufgrund einer nun über50 jährigen Tätigkeit als Rechtsanwalt im faszinierenden Gebiet der Informatik entstandenen Ausführungen bei den Empfängern dieses Dokument entschuldigen und um Nachsicht bitten.

Beat Lehmann

Von: FAMH <info@famh.ch>
Gesendet: Freitag, 13. September 2024 11:20
An: _NCSC-National Cyber Security Centre
Betreff: WG: FAMH | Stellungnahme Vernehmlassung | Verordnung über die Cybersicherheit

Sehr geehrte Frau Bundesrätin Amherd
Sehr geehrte Damen und Herren

Als Verband der medizinischen Laboratorien der Schweiz (FAMH) begrüssen wir die ausgearbeitete **Verordnung über die Cybersicherheit.**
Gemäss dem rahmengebenden **Informationssicherheitsgesetz** sind medizinische Laboratorien mit einer Bewilligung nach Art. 16 Abs. 1 des Epidemiengesetzes vom 28. September 2012 meldepflichtig.
Mit dieser Definition (die mikrobiologische Labore betrifft) sind nicht alle medizinischen Laboratorien in der Schweiz erfasst, die ähnlich schützenswerte Informationen wie jene nach EPG halten. Die FAMH wird daher Ihren Mitgliedern empfehlen, entsprechende Meldungen auch dann zu machen, wenn Sie nicht unter diese Definition fallen.

Mit freundlichen Grüssen
Thomas Zurkinden

Generalsekretariat FAMH
Secrétariat général FAMH
Segretariato generale FAMH

Altenbergstrasse 29, Postfach 686
CH-3000 Bern 8

Tel +41 (0) 31 313 88 30
info@famh.ch, www.famh.ch

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Commission fédérale de la Consommation (CFC)

CH-3003 Berne, CFC

E-Mail
ncsc@ncsc.admin.ch

Référence : ACF / voj
Votre référence :
Notre référence : teb
Berne, le 1er juillet 2024

Prise de position de la CFC sur le projet d'ordonnance sur la cybersécurité (OCyS)

Mesdames, Messieurs

La CFC se détermine comme suit sur la consultation relative au projet d'ordonnance sur la cybersécurité (OCyS).

- Art. 5a : la période de cinq ans entre deux contrôles de la Cyberstratégie nationale par le Comité de pilotage apparaît longue eu égard à l'évolution rapide des technologies et des menaces en matière de sécurité. Un délai de deux ans au maximum pourrait être plus indiqué.

- Art. 7 al. 1 : la question se pose de savoir comment sera composée l'équipe nationale d'intervention (Computer Emergency Response Team ou CERT), il pourrait être utile de compléter dans ce sens le rapport explicatif, voire le texte de l'ordonnance.

- Art. 7.1 let. a : "Incidents techniques" : le terme semble mal choisi. Un incendie dans un data center est un incident technique, mais il n'est pas nécessairement lié à la cybersécurité. Pour être plus précis, il pourrait être indiqué un incident relevant de la cybersécurité.

- Art. 7 al. 1 let. b : la même remarque que pour la lettre a vaut ici pour "questions techniques".

- Art. 8 al. 1 : la question se pose de savoir s'il faut prévoir de demander l'aide de prestataires privés en cas de crise majeure. Le cas échéant, il pourrait être indiqué de définir les critères permettant de les identifier et les sélectionner à l'avance.

Commission fédérale de la consommation
Jean-Marc Vögele
Secrétariat
Palais fédérale est, CH-3003 Berne
Tel.: +41 58 462 20 46, Fax: +41 58 462 43 70
jean-marc.voegele@bfk.admin.ch
www.konsum.admin.ch

- Art. 9 : une contradiction potentielle apparaît dans la formulation proposée, entre “raccourcir le délai si la vulnérabilité peut être facilement exploitée” et “prolonger le délai lorsque l’élimination de la vulnérabilité s’avère particulièrement complexe”. Que fait-on quand on a une vulnérabilité critique complexe à corriger ? Il pourrait être utile de mentionner la possibilité de mettre en place des mesures d’atténuation le temps de corriger la vulnérabilité.

- Art. 9 al. 5 : la question se pose de savoir s’il ne faudrait pas qu’ « il informe » au lieu de pouvoir informer” ?

- Art. 16 al. 2 : la formulation proposée vise à dispenser les « petites » structures de l’obligation de signaler. Mais ce critère est-il adéquat ? Qu’en est-il si ces petites structures sont d’importance systémique malgré qu’elles comptent “moins de 50 personnes” et que leur bilan “ne dépasse pas 10 millions de francs”. D’autres critères pertinents pourraient être considérés par ex. la taille de la clientèle touchée ? Cette question semble particulièrement pertinente dans une optique de protection des consommateurs.

- Art. 18 al. 2 : une fuite d’informations peut être avérée avant que les informations soient « publiées par des personnes non autorisées », par ex. grâce à une journalisation de l’accès aux données qui permettrait de détecter une intrusion et un téléchargement de données par des personnes non autorisées. Cet élément pourrait être ajouté à la définition.

- Art. 18 al. 4 : la formulation est peu claire et mériterait d’être améliorée.

La question de la détection des cybermenaces est peu traitée dans l’ordonnance, soulevant plusieurs interrogations. Il pourrait être adéquat de définir un cadre minimum en matière de management de la sécurité de l’information à mettre en place dans les organisations concernées par l’ordonnance, par analogie avec ce que prévoient les art. 5 ss de l’Ordonnance sur la sécurité de l’information (OSI). On renvoie également à l’art. 7 al. 1 let. c : comment s’y prend-elle ?

Pour la Commission fédérale de la Consommation

Prof. Dr. Anne-Christine Fornage
Présidente

Prof. Melinda Lohmann
Vice-présidente

Der Regierungsrat des Kantons Thurgau

Thurgau

Staatskanzlei, Regierungskanzlei, 8510 Frauenfeld

Eidgenössisches Departement für
Verteidigung, Bevölkerungsschutz und
Sport (VBS)
Frau Viola Amherd
Bundesrätin
3003 Bern

Frauenfeld, 20. August 2024
Nr. [RRB-Nr.]

Cybersicherheitsverordnung (CSV)

Vernehmlassung

Sehr geehrte Frau Bundesrätin

Wir danken Ihnen für die Möglichkeit der Stellungnahme zur Verordnung über die Cybersicherheit (Cybersicherheitsverordnung, CSV) und teilen Ihnen mit, dass wir mit der Vorlage einverstanden sind.

Mit freundlichen Grüssen

Der Präsident des Regierungsrates

Der Staatsschreiber

Regierungsgebäude, 8510 Frauenfeld
T +41 58 345 53 10
www.tg.ch

Fédération des Entreprises Romandes
FER Genève - FPE Bulle - UPCF Fribourg
FER Arcju - FER Neuchâtel - FER Valais

Département fédéral de la défense, de la protection de la population et des sports (DDPS)
3003 Berne

ncsc@ncsc.admin.ch

Madame Viola Amherd,
Présidente de la Confédération

Genève, le 20 août 2024
NR/3359 – FER No 29-2024

Ordonnance sur la cybersécurité (OCyS)

Madame la Présidente de la Confédération,

Nous vous remercions de nous avoir consultés et vous prions de trouver ci-après notre prise de position.

L'Office fédéral de la cybersécurité (OFCS) a la responsabilité de la sécurité et de la protection des données. Il peut ainsi gérer les intérêts des différents secteurs de manière appropriée.

Le système de communication prévu doit permettre de réagir rapidement aux menaces et de prendre des contre-mesures. Il contribue également à une meilleure compréhension de la nature et de l'ampleur des cyberincidents et des cybermenaces.

L'Office fédéral de la cybersécurité (OFCS) participe à des forums internationaux pour partager des connaissances et bénéficier du savoir d'autres pays.

De ce fait, la structure du projet permet un ajustement continu aux nouvelles évolutions en matière de cybersécurité et favorise une participation équilibrée des différents groupes d'intérêt à la mise en œuvre de la Stratégie nationale pour la protection de la Suisse contre les cyber-risques (CSN). Cela contribue à l'amélioration protection de la Suisse contre les cyberincidents et les cybermenaces.

Points à considérer :

- Complexité : Il pourrait y avoir des défis à harmoniser les procédures de l'OFCOM et de l'OFCS. Par exemple, l'OFCOM doit informer l'OFCS des vulnérabilités, qui procède ensuite, le cas échéant, à la divulgation coordonnée des vulnérabilités.

- Évaluation subjective : L'évaluation des conséquences des cyberattaques peut varier d'une organisation à l'autre.

- Mesures de cyberdéfense : Ces mesures ne sont pas régies par l'ordonnance sur la cybersécurité. Elles se rapportent aux mesures militaires et de renseignement et incluent notamment les mesures actives prévues à l'art. 37 de la loi fédérale du 25 septembre 2015 sur le renseignement afin de perturber et de ralentir les cyberattaques. Elles concernent aussi les mesures de l'armée visant à garantir sa disponibilité opérationnelle dans toutes les situations, et à mettre à disposition des capacités destinées à appuyer subsidiairement les autorités civiles.

Par ailleurs, nous préconisons de maintenir et développer une collaboration étroite avec le secteur privé afin de tirer parti des forces complémentaires des deux secteurs et permettre ainsi de renforcer la capacité à prévenir, détecter et répondre aux cybermenaces.

Ainsi, compte tenu de l'importance croissante des risques cyber, la FER soutien cette démarche qui vise à améliorer la sécurité des infrastructures critiques en Suisse.

En vous remerciant de l'intérêt que vous porterez à ces lignes, nous vous prions de recevoir, Madame la Présidente de la Confédération, l'expression de notre haute considération.

Olivier Sandoz
Secrétaire général adjoint

Emmanuel Meurant
Directeur Contrôle et Sécurité
FER Genève

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

BASEL LANDSCHAFT
REGIERUNGSRAT

Regierungsrat, Rathausstrasse 2, 4410 Liestal

Eidgenössisches Departement für
Verteidigung, Bevölkerungsschutz und Sport
VBS, Bern

ncsc@ncsc.admin.ch

Liestal, 13. August 2024

Vernehmlassung betreffend Erlass der Cybersicherheitsverordnung (CSV)

Sehr geehrte Frau Bundespräsidentin

Wir bedanken uns für die Möglichkeit, zur Verordnung über die Cybersicherheit (Cybersicherheitsverordnung, CSV) Stellung beziehen zu dürfen. Wir begrüssen grundsätzlich den Erlass der Cybersicherheitsverordnung.

Zu den einzelnen Bestimmungen haben wir folgende Bemerkungen:

Zur Verordnung über die Cybersicherheit (Cybersicherheitsverordnung, CSV):

Art. 4
Es wäre wünschenswert, die personelle Zusammensetzung des Steuerungsausschusses Nationale Cyberstrategie StA NCS zu präzisieren – z.B. aus wie vielen Vertretern des Bundes, der Kantone usw. sich der Steuerungsausschuss Nationale Cyberstrategie StA NCS zusammensetzt.

Art. 18 Abs. 1 Buchstabe a
«Systemunterbrüche» sollten hier präzisiert werden.
Begründung: Wenn zum Beispiel bei einer Anwendung einer künstlichen Intelligenz (KI) das Buchhaltungssystem einen Unterbruch erleidet, hat dies kaum Auswirkungen auf die Kernkompetenz des Systems.

Zu den Erläuterungen zur Verordnung über die Cybersicherheit (Cybersicherheitsverordnung, CSV):

zu Art. 1 Buchstabe a
Die Rolle des Sicherheitsverbunds Schweiz SVS sollte hier ebenfalls geregelt werden.

zu Art. 2 letzter Abschnitt
Wir beantragen, den Abschnitt wie folgt zu ergänzen:
«Die Nationale Cyberstrategie NCS legt den Rahmen für diese verschiedenen Aspekte fest und koordiniert die Anstrengungen auf nationaler **und kantonaler** Ebene gemäss *Absatz 2* in enger Abstimmung mit den Kantonen. Mit einer umfassenden Strategie soll sichergestellt werden, dass die Schweiz gesamthaft besser gegen Cybervorfälle und Cyberbedrohungen geschützt ist und effektiv auf diese reagieren kann.»

zu Art. 4 Abs. 1
Wir möchten anregen, Vertreter der Gemeinden und der kritischen Infrastrukturen in den Mitgliederkreis des Steuerungsausschusses Nationale Cyberstrategie NCS zu integrieren.

Allgemeine Bemerkungen

Im Rahmen der Vernehmlassung der Änderung des Bundesgesetzes über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) vom 18. Dezember 2020 stellte die Konferenz der Kantonalen Polizeikommandantinnen und -kommandanten der Schweiz KKPKS mit Vernehmlassungsantwort vom 15. Februar 2022 folgende Anträge:

- Art. 73c Abs. 2 sei zu streichen, um die Weiterleitung der Meldungen von Offizialdelikten durch das Bundesamt für Cybersicherheit NCSC an die Strafverfolgungsbehörden sicherzustellen.
- Die in Art. 76 Abs. 1 vorgesehene Unterstützung des NDB durch das Bundesamt für Cybersicherheit NCSC mit Auswertungen zu Anzahl, Art und Ausmass von Cyberangriffen sowie technischen Analysen von Cyberrisiken sei auf die Strafverfolgungsbehörden zu erweitern.
- Die maximale Aufbewahrungsfrist der Daten in Art. 79 habe sich an der Verfolgungsverjährung (Art. 97 und 109 StGB) zu orientieren.
- Es sei eine gesetzliche Regelung einzufügen, die vorsieht, wie seitens der Strafverfolgungsbehörden umzugehen ist, wenn sich Geschädigte eines meldungspflichtigen Vorfalls an die Polizei, nicht jedoch an das Bundesamt für Cybersicherheit NCSC wenden.

Leider fanden diese aus Sicht der Strafverfolgungsbehörden wünschenswerten Anträge keinen Eingang im geänderten Informationssicherheitsgesetz, welches nach Gutheissung im Parlament am 29. September 2023 und unbenutzter Referendumsfrist am 18. Januar 2024 in Kraft trat.

Daher wird erneut der Antrag gestellt, dass die Strafverfolgungsbehörden bei Cyberangriffen auf kritische Infrastrukturen, ob diese nun im Sinne von Art. 16 CSV von der Meldepflicht entbunden sind oder nicht, in jedem Fall miteinbezogen werden.

Hochachtungsvoll

Isaac Reber Elisabeth Heer Dietrich

Regierungspräsident	Landschreiberin

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Bundesrätin Viola Amherd
Bundeshaus Ost, 3003 Bern

Eingabe per Mail an: ncsc@ncsc.admin.ch

Bern, 07. August 2024

Stellungnahme zur Cybersicherheitsverordnung des Bundes

Sehr geehrte Frau Bundesrätin Amherd,
Sehr geehrter Herr Stv. Direktor BACS Suter,
Sehr geehrte Damen und Herren,

Die Vernehmlassung zur Cybersicherheitsverordnung des Bundes verfolgen wir mit grossem Interesse. Um die Vorreiterrolle der Schweiz betreffend Wissenschaft und Wirtschaft weiter zu stärken, arbeitet der Thinktank Pour Demain an gesellschaftlichen Themen, welche ein grosses Nutzen- und Schadenspotential aufweisen. Die Verknüpfung von Cybersicherheit und kritischen Infrastrukturen ist ein solches Thema.

Deshalb nehmen wir hiermit gerne die Möglichkeit wahr, Ihnen unsere Vernehmlassungsantwort zukommen zu lassen. Für einen weiteren Dialog stehen wir gerne zur Verfügung und bedanken uns für Ihr Interesse.

Patrick Stadler, Geschäftsführer & Mitgründer, Pour Demain
David Marti, Programmleiter KI & Mitgründer, Pour Demain

Allgemeine Würdigung

Pour Demain begrüsst die Cybersicherheitsverordnung, die unter anderem die Aufgaben des BACS regelt, den Informationsaustausch des BACS mit Behörden und Organisationen zum Schutz vor Cybervorfällen und Cyberbedrohungen sowie die Meldepflicht für Cyberangriffe.

Die Verordnung überzeugt in weiten Teilen, insbesondere in folgenden Punkten:

- Erläuterungen zur nationalen Cyberstrategie, inklusive eines Steuerungsausschusses mit breiter Stakeholder-Vertretung und einem vom BACS gestellten Sekretariat.
- Aufgaben des BACS mit technischer Analyse von Cybervorfällen und Cyberbedrohungen.
- Weiterleitung von Informationen zur frühzeitigen Erkennung von Sicherheitsbedrohungen.
- Klare Meldefristen bei Cyberangriffen.
- Internationale Zusammenarbeit.
- Unterstützung der Betreiber:innen kritischer Infrastrukturen.

3. Abschnitt, Artikel 7

1a technische Vorfallbewältigung

Gemäss der Nationalen Cyberstrategie ist ein Cybervorfall definiert als Ereignis, das bei der Nutzung von Informatik- und Kommunikationsmitteln (IKT) die Vertraulichkeit, Verfügbarkeit oder Integrität von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt. Solche Ereignisse können insbesondere auch ohne Fremdeinwirkung ein Sicherheitsrisiko darstellen, wenn eine fehlerhafte Anwendung eine Störung oder ein Datenleck verursacht. Um dies klarzustellen, sollte §1a ergänzt werden auf “technische Vorfallbewältigung, inklusive Ereignisse ohne Fremdeinwirkung”.

Neuer Paragraph 1d: Monitoring von Vorfällen im Zusammenhang mit künstlicher Intelligenz
Das BACS soll zuständig sein für das Monitoring von Vorfällen im Zusammenhang mit künstlicher Intelligenz (KI) im Sinne von Cyberbedrohungen und Cybervorfällen. Diese Aufgabe dient der Gewinnung von Erkenntnissen über potenzielle Fehlentwicklungen und Risiken im Bereich der KI. Zu diesem Zweck führt das BACS eine zentrale Datenbank, in der KI-Vorfälle erfasst, analysiert und ausgewertet werden. Die gewonnenen Informationen tragen dazu bei, Präventionsmassnahmen zu entwickeln und die Sicherheit von KI-Systemen zu verbessern.

Generelle Bemerkung

In unserer Vernehmlassungseingabe vom Mai 2022 zur Revision des Informationssicherheitsgesetzes haben wir bereits festgehalten, dass eine Meldepflicht für kritische Infrastrukturen auf Cybervorfälle auszuweiten sei, da Cyberangriffe nur einen Teil der sicherheitsrelevanten Ereignisse darstellen. Das BACS hätte eine geeignete Ausgangslage, um diese Ausweitung umzusetzen. Dies ist insbesondere relevant, da mit zunehmender Ausbreitung von nicht-erklärbaren KI-Systemen eine entsprechende Zunahme von Cybervorfällen ohne Fremdeinwirkung zu antizipieren ist.

GENÈVE
AÉROPORT

DIRECTION GENERALE

DG/gpo

Par courrier électronique
Département fédéral de la défense,
de la protection de la population et
des sports
Madame Viola Amherd
Conseillère fédérale
3003 Berne
ncsc@ncsc.admin.ch

Genève, le 5 août 2024

Procédure de consultation relative à l'ordonnance sur la cybersécurité (OCyS)

Madame la Conseillère fédérale,

Nous nous référons à l'affaire visée en marge, et vous remercions de l'invitation à prendre position.

De façon générale, le projet d'ordonnance n'appelle pas de commentaires particuliers de notre part.

Tout au plus, il implique, en tant qu'exploitant d'une infrastructure critique, de mettre à jours nos processus en vue de l'échange automatique d'informations, et d'identifier les fournisseurs de prestations qui pourraient vouloir participer audit échange. Nous le ferons en concertation avec les services de la Confédération en tant que de besoin.

Tout en vous remerciant de l'attention que vous porterez à la présente, nous vous prions de croire, Madame la Conseillère fédérale, à l'assurance de notre parfaite considération.

André Schneider
Directeur général

Gaël Poget
Délégué aux affaires extérieures

Copie (électronique) :
- Interne : ccb, cwi, ctt, aam, dsh, mgt, gru
- Mme Emanuela Dose Sarfatis, Secrétaire générale adjointe, Département des finances, République et canton de Genève
- M. David Karrer, Directeur, Relations publiques, Flughafen Zürich AG
- AEROSUISSE, Secrétariat général

Conseil d'Etat
Staatsrat

CP 670, 1951 Sion

CANTON DU VALAIS
KANTON WALLIS

P.P. CH-1951 Sion A-PRIORITY Poste CH SA

Madame
Viola Amherd
Présidente de la Confédération
Cheffe du Département fédéral de la défense, de la protection de la population et des sports (DDPS)
Palais fédéral
3003 Berne

Notre réf. SSCM
Votre réf. /

Date

Ordonnance sur la cybersécurité (OCyS)
Procédure de consultation

Madame la Présidente de la Confédération,

Le Conseil d'Etat du canton du Valais a pris connaissance avec attention du projet d'ordonnance sur la cybersécurité et vous en remercie.

Le canton du Valais salue la volonté de renforcer et développer l'état de préparation national face aux risques et menaces cyber au moyen d'une nouvelle ordonnance.

Dans l'ensemble, le Conseil d'Etat valaisan soutient ce projet d'ordonnance soumis à consultation.

Néanmoins, il désire apporter ici quelques remarques ou compléments aux articles suivants :

Article 4, alinéa 1 - Composition du CP CSN
Les exploitants d'infrastructures critiques endossant des responsabilités toujours plus importantes dans le maintien des biens et des services nécessaires à la population, nous proposons que ces derniers soient également intégrés dans la composition du comité de pilotage de la Cyberstratégie nationale.

Article 7, alinéa 2 - Analyse technique des cyberincidents et des cybermenaces
La nécessité de disposer d'une infrastructure résiliente ne fait aucun doute. Cependant, la mise en place et l'exploitation d'une infrastructure spécifique est couteuse tant du point de vue financier qu'humain. Les ressources du NCSC étant, à l'heure actuelle, restreintes, les collaborateurs qui s'occuperont de cette infrastructure spécifique risquent de manquer pour assurer la tâche principale dévolue à l'OFCS qui est la Cybersécurité. Dans ce sens, nous préconisons une mutualisation des infrastructures, ou du moins des ressources, avec d'autres organisations fédérales existantes.

Article 14 - Fournisseurs de prestations
Afin de gagner en précision, il s'agirait ici de préciser s'il s'agit de tous les fournisseurs de prestations informatiques ou seulement ceux en lien avec la cybersécurité, tel qu'il est indiqué dans le rapport explicatif accompagnant le projet d'ordonnance.

Article 15, alinéa 4 - Transmission et utilisation des informations
Cette disposition nous paraît trop restrictive. En effet, un fournisseur de prestations, informé d'une vulnérabilité, devrait pouvoir exploiter cette information afin de mieux protéger ses autres clients, ceci dans un objectif d'amélioration globale de la cybersécurité à l'échelon national.

Article 16 - Exception à l'obligation de signaler
Il y a lieu d'inverser les lettres c et d afin de respecter l'ordre établi dans la loi sur la sécurité de l'information (LSI).

Article 19 - Contenu du signalement
Nous attirons votre attention sur le fait que certaines entreprises vont devoir annoncer une cyberattaque à plusieurs entités de la Confédération (l'OFCS, le PFPDT, voir également à la FINMA ou à l'OFEN). Il semblerait plus efficient que les annonces de cyberattaques soient centralisées uniquement auprès de l'OFCS.

Remarques conclusives
Dans un objectif de clarification et de simplification, il serait intéressant de déplacer dans l'OCyS les tâches de l'OFCS mentionnées à l'article 15a de l'ordonnance d'organisation du DDPS (Org-DDPS).

Le Conseil d'Etat préconise également de généraliser l'acronyme français OFCS, ou sa version anglaise NCSC, dans toutes les bases légales existantes (LSI, OSI et OCyS).

En vous remerciant de nous avoir consultés, nous vous adressons, Madame la Présidente de la Confédération, nos respectueuses salutations.

Au nom du Conseil d'Etat

Le président	La chancelière
Franz Ruppen	**Monique Albrecht**

Copie à - ncsc@ncsc.admin.ch

Die Regierung
des Kantons Graubünden

La Regenza
dal chantun Grischun

Il Governo
del Cantone dei Grigioni

Sitzung vom	Mitgeteilt den	Protokoll Nr.
27. August 2024	28. August 2024	680/2024

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Frau Bundespräsidentin Viola Amherd

Per E-Mail (PDF und Word) an: ncsc@ncsc.admin.ch

Erlass der Cybersicherheitsverordnung (CSV)

Vernehmlassung

Sehr geehrte Frau Bundespräsidentin,
Sehr geehrte Damen und Herren

Die Regierung des Kantons Graubündens dankt Ihnen für die Gelegenheit zur Stellungnahme zur Verordnung über die Cybersicherheit (CSV).

Die im Entwurf vorgeschlagene Regelung der Aufgaben des neuen Bundesamts für Cybersicherheit (BACS) und die gleichzeitige Umsetzung der Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen begrüssen wir.

Folgende Punkte sollten aus unserer Sicht nochmals überdacht resp. präzisiert werden:

Art. 15 Abs. 1

In Anbetracht der Tatsache, dass bestimmte Informationen regelmässig schnell geteilt werden sollen und können, andere aber insbesondere aus taktischen Gründen

erst später, sollte bei der Übermittlung auch bestimmt werden können, *welche* Informationen weitergegeben werden dürfen, statt nur ob die Weitergabe erfolgen darf.

Änderungsantrag:

*Registrierte Unternehmen und Behörden übermitteln Informationen dem BACS und bestimmen dabei, **~~ob und~~** an wen dieses **welche ~~die~~** Informationen weitergegeben darf, soweit eine Weitergabe der Informationen nicht gesetzlich vorgesehen ist.*

Art. 16 Abs. 1 lit. a

Wir begrüssen grundsätzlich die Entlastung kleiner, öffentlicher Institutionen. Wir sehen jedoch durch den konvergierenden Markt von IT-Dienstleistern auch ein erhöhtes Risiko der kaskadierenden Ausbreitung eines Datenvorfalls (bspw. Sicherheitslücke bei einem für mehrere Kleingemeinden / Kraftwerkbetreiber zuständigen, regionalen IT-Dienstleister). Dies sollte bei der Grössendefinition berücksichtigt werden.

Art. 18 Abs. 3

In Anlehnung an die Erläuterungen beantragen wir, dass die Bestimmung den Startzeitpunkt genauer definiert und wesentliche Anzeichen eines Cyberangriffs, welcher der Vorbereitung weiterer Angriffe dient, ausdrücklich nennt.

Änderungsantrag:

*Ein Cyberangriff gilt als über einen längeren Zeitraum unentdeckt, wenn der **~~Vorfall~~** **Initialkontakt** mehr als 90 Tage zurückliegt **oder Anzeichen dafür bestehen, dass er zur Vorbereitung weiterer Cyberangriffe ausgeführt wurde. Solche Anzeichen liegen insbesondere vor, wenn der Cyberangriff mit fortgeschrittenen Techniken und Werkzeugen, zielgerichtet, schrittweise oder mit verschleierten Aktivitäten erfolgt**.*

Besten Dank für die Berücksichtigung unserer Anliegen.

Freundliche Grüsse

Namens der Regierung

Der Präsident:	Der Kanzleidirektor:
Dr. Jon Domenic Parolini	Daniel Spadin

Kopie:

- Departement für Justiz, Sicherheit und Gesundheit
- Amt für Informatik