Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Bundesamt für Cybersicherheit BACS

Bern, 27. November 2024

Entwurf der Verordnung über die Cybersicherheit (Cybersicherheitsverordnung, CSV)

Vernehmlassung vom 22. Mai 2024 bis zum 13. September 2024

Bericht über die Ergebnisse der Vernehmlassung

Inhaltsverzeichnis

1 Ausgangslage

Am 22. Mai 2024 hat der Bundesrat den Entwurf der Cybersicherheitsverordnung (CSV) sowie den erläuternden Bericht verabschiedet und das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) beauftragt, ein Vernehmlassungsverfahren durchzuführen. Die Vernehmlassung dauerte vom 22. Mai 2024 bis zum 13. September 2024. Die Liste aller Vernehmlassungsteilnehmenden mit den nachfolgend verwendeten Abkürzungen findet sich im Anhang.

Es sind 69 Stellungnahmen eingegangen:

69	**Total eingegangene Stellungnahmen**
23	Kantonsregierungen
3	Kantonale Konferenzen und Eidgenössische Kommissionen
4	Parteien
2	Gesamtschweizerische Dachverbände der Gemeinden und Städte
19	Gesamtschweizerische Verbände
12	Betroffene Unternehmen
7	Weitere interessierte Kreise

Die Stellungnahmen sind auf der Publikationsplattform des Bundesrechts «Fedlex» aufgeschaltet.[1]

2 Gegenstand des Vernehmlassungsentwurfs

Der Bundesrat erteilte dem Eidgenössischen Finanzdepartement (EFD) am 11. Dezember 2020 den Auftrag, die Rechtsgrundlagen für die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen zu erstellen. Sodann verabschiedete der Bundesrat am 2. Dezember 2022 den Entwurf über diese Rechtsgrundlagen und die Botschaft zur Änderung des Bundesgesetzes über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) vom 18. Dezember 2020[2] zuhanden des Parlaments. In der Folge hiess das Parlament die Änderungen des ISG am 29. September 2023 gut;[3] die Referendumsfrist verstrich am 18. Januar 2024 ungenutzt.

Der Verordnungsentwurf enthält einerseits die Ausführungsbestimmungen zum 5. Kapitel des revidierten ISG über die Meldepflicht für Cyberangriffe auf kritische Infrastrukturen. Andererseits werden auch organisationale Aspekte im Zusammenhang mit der Cybersicherheit geregelt. Die Verordnung soll zusammen mit dem revidierten 5. Kapitel des ISG am 1. April 2025 in Kraft treten.

Das ISG ist – ohne das oben erwähnte revidierte 5. Kapitel über die Aufgaben des neu geschaffenen Bundesamtes für Cybersicherheit (BACS) und die Meldepflicht für Cyberangriffe auf kritische Infrastrukturen – bereits am 1. Januar 2024 in Kraft getreten. Auf diesen Zeitpunkt hin wurde zudem die Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV) vom 27. Mai 2020[4] ausser Kraft gesetzt.[5] Die darin enthaltenen Bestimmungen wurden teilweise in das revidierte ISG überführt, insbesondere die Begriffsdefinitionen. Jene Bestimmungen, welche in der CyRV die Informatiksicherheit des Bundes regelten, wurden in die Verordnung über die Informationssicherheit in der Bundesverwaltung (Informationssicherheitsverordnung, ISV)[6] übernommen. Die in der CyRV definierten Aufgaben des Nationalen Zentrums für Cybersicherheit (NCSC) – insbesondere dessen Aufgaben gegenüber der Wirtschaft und der Bevölkerung – werden nicht in der ISV geregelt, da sie mit der Revision des ISG eine neue gesetzliche

1 www.fedlex.admin.ch > Vernehmlassungen > Abgeschlossene Vernehmlassungen > 2024 > VBS
2 SR **128**
3 BBl **2023** 2296
4 SR **120.73**
5 AS **2023** 735 (Anhang 2 Ziff. I).
6 SR **128.1**

Grundlage erhalten haben. Zudem wurde am 1. Januar 2024 das NCSC als BACS in das VBS überführt. Aus diesem Grund finden sich organisationale Bestimmungen zum BACS in Art. 15*a* Abs. 1 und 2 Bst. a–g OV-VBS[7].

Die Aufgaben des BACS werden im Verordnungsentwurf – zusammen mit der Meldepflicht für Cyberangriffe auf kritische Infrastrukturen – präzisiert und konkreter umschrieben. Sie regelt daher das Verhältnis zwischen dem BACS und Betroffenen ausserhalb der Bundesverwaltung, während die ISV die Aufgaben und Zuständigkeiten für die Informationssicherheit innerhalb der Bundesverwaltung definiert.

3 Ergebnisse der Vernehmlassung

3.1 Gesamtbeurteilung der Vorlage

Die CSV erhält überwiegend eine positive Resonanz. Eine grosse Mehrheit der Stellungnahmen bewertet die Initiative zur Stärkung der Cybersicherheit in der Schweiz grundsätzlich positiv. Viele Akteure begrüssen die Bemühungen, die Sicherheit in diesem Bereich zu verbessern.

Trotz der allgemeinen Zustimmung gibt es jedoch zahlreiche konstruktive Kritikpunkte und Verbesserungsvorschläge. Diese beziehen sich oft auf spezifische Aspekte der Verordnung und zielen darauf ab, deren Praktikabilität und Effektivität zu steigern.

Hauptanliegen sind dabei die Harmonisierung und Koordination verschiedener Meldeverfahren, Präzisierungen bestimmter Begriffe und Prozesse sowie eine Anpassung der Meldepflichten, um übermässigen administrativen Aufwand zu vermeiden. Auch die stärkere Berücksichtigung der Zusammenarbeit mit Strafverfolgungsbehörden sowie Flexibilität bei Fristen und Ausnahmeregelungen sind wichtige Punkte.

Zudem äussern verschiedene Sektoren, wie der Finanzsektor, das Gesundheitswesen und die Telekommunikation, ihre branchenspezifischen Anliegen, die ihre jeweiligen Bedürfnisse und Herausforderungen widerspiegeln.

Aus föderaler Perspektive betonen die Kantone die Notwendigkeit der Zusammenarbeit zwischen Bund und Kantonen sowie die Berücksichtigung kantonaler Strukturen.

Wirtschaftliche Aspekte spielen ebenfalls eine Rolle. Wirtschaftsverbände und Unternehmen unterstützen die Verordnung zwar grundsätzlich, mahnen jedoch zur Verhältnismässigkeit und fordern wirtschaftlich tragbare Lösungen.

Insgesamt besteht ein breiter Konsens über die Notwendigkeit des Erlasses der CSV, begleitet von dem Wunsch nach praxisnahen Anpassungen und Präzisierungen bei der Umsetzung.

3.2 Gruppierte Stellungnahmen zur CSV nach Einschätzung und Stossrichtung

3.2.1 Übersicht der positiven Vernehmlassungsantworten zur CSV ohne wesentliche Änderungsvorschläge

Die CSV hat in der Vernehmlassung bei einigen Vernehmlassungsteilnehmenden uneingeschränkte Zustimmung gefunden:

- Mehrere *Kantone* äusserten sich besonders positiv (*BS, OW, SZ, SG, NW* und *TI*).

7 SR **172.214.1**

- Im Bereich der *Infrastrukturbetreiber* zeigte sich *Transitgas AG* sehr positiv und sah die Verordnung als wichtigen Schritt zur Gewährleistung der Sicherheit kritischer Infrastrukturen. Auch *RAILplus* erklärte, dass der Text den Erwartungen entspricht und hatte keine wesentlichen Kommentare. *FAMH* begrüsst die CSV. Der Verband weist darauf hin, dass nicht alle medizinischen Laboratorien von der Meldepflicht bei Cyberangriffen erfasst sind und empfiehlt seinen Mitgliedern, freiwillig Meldungen zu machen, auch wenn sie nicht unter die gesetzliche Definition fallen.

3.2.2 Positive Bewertung mit Verbesserungsvorschlägen oder Anmerkungen

Die CSV hat überwiegend positive Resonanz erfahren, wobei viele Vernehmlassungsteilnehmenden ihre grundsätzliche Zustimmung mit Verbesserungsvorschlägen oder Anmerkungen verbanden:

- Auf *kantonaler Ebene* zeigte sich eine breite Unterstützung. Kantone wie *AG, BE, FR, GE, GL, GR, LU, SH, SO, UR, VD, VS, ZG* und *ZH* begrüssten die Verordnung, brachten aber gleichzeitig verschiedene Anliegen vor. Diese reichten beispielsweise von Verbesserungsvorschlägen bei Ausnahmen von der Meldepflicht (*AG*) bis hin zu Forderungen nach Präzisierungen und stärkerer Berücksichtigung der Lieferkette (*ZH*).

- *Bundesbehörden* wie *BA* und *BFK* unterstützten die Verordnung grundsätzlich, forderten aber eine stärkere Berücksichtigung der Strafverfolgung bzw. eine Begrenzung des Aufwands für initiale Meldungen.

- *Politische Parteien* wie *Die Mitte, FDP* und *SP* befürworteten die Verordnung, wiesen aber auf unterschiedliche Aspekte hin, die es zu beachten gilt. Während *Die Mitte* die Notwendigkeit starker nationaler Strukturen betonte, warnte *FDP* vor übermässiger administrativer Belastung.

- *Verbände und Interessengruppen* zeigten ebenfalls breite Unterstützung mit diversen Anmerkungen. Organisationen wie *asut, VSE, CH++, digitalswitzerland, economiesuisse, ISSS, PourDemain, sgv, Swiss Banking, Swiss FS-CSC, SwissICT, Swico, SUISSEDIGITAL, scienceindustries, SVV, SGV, H+, NEDIK, SSK, CH++, suisseuniversities, NFP 77 ETHZ UNIL und eAHV/IV* gehören dazu, machten aber gleichzeitig auf Verbesserungspotenziale aufmerksam. Häufig genannt wurden die Notwendigkeit der Harmonisierung mit bestehenden Regelwerken, die Forderung nach praxisgerechteren Anpassungen und der Wunsch nach flexibleren Fristen.

- *Unternehmen und Infrastrukturbetreiber* wie *Flughafen ZH, FER, Primeo, Migros, SBB, CH Post AG, Sunrise, SUVA, Salt, Swissgrid* und *Switch* begrüssten die Verordnung ebenfalls, brachten aber zum Teil spezifische Anliegen ihrer Branchen vor. Diese reichten von der Forderung nach Präzisierungen der Meldepflicht bis hin zur Kritik an der Komplexität der Verordnung und unabgestimmten Meldeprozessen.

Insgesamt zeigt sich, dass die CSV auf breite Zustimmung stösst, gleichzeitig aber in vielen Bereichen Verbesserungspotenzial gesehen wird. Die häufigsten Anmerkungen betreffen zusammengefasst die Notwendigkeit von Präzisierungen, die Harmonisierung mit bestehenden Regelwerken, die Berücksichtigung branchenspezifischer Bedürfnisse und die Gewährleistung einer praxisnahen und wirtschaftlich vertretbaren Umsetzung.

3.2.3 Neutrale oder gemischte Bewertung

Im Rahmen der Vernehmlassung zur CSV gab es einige Vernehmlassungsteilnehmende, die neutrale oder gemischte Bewertungen abgaben. Diese Rückmeldungen zeichnen sich durch zurückhaltende oder fokussierte Stellungnahmen aus:

- *Flughafen GE* nahm eine neutrale Position ein und enthielt sich einer inhaltlichen Bewertung der Verordnung. *Flughafen GE* beschränkte sich darauf, lediglich geplante Prozessanpassungen zu erwähnen, ohne dabei spezifische Kommentare zur Verordnung selbst abzugeben.

- *KKJPD* entschied sich für eine neutrale Position, indem sie komplett auf eine inhaltliche Stellungnahme verzichtete. Stattdessen überliess sie es den einzelnen Kantonen, sich zur Vorlage zu äussern.

- *Piratenpartei Schweiz* äussert sich nicht wertend zur CSV, sondern konzentriert sich in ihrer Stellungnahme auf ein spezifisches Kernanliegen bezüglich der koordinierten Offenlegung von Schwachstellen.

- *ASIP* nahm eine sehr fokussierte Haltung ein und äusserte sich ausschliesslich in Bezug auf eine Ausnahme von der Meldepflicht für die von ihrer vertretenen Branche.

3.3 Anträge und Bemerkungen zum Vorentwurf

3.3.1 Vorbemerkung

Im Folgenden werden die Bemerkungen, Änderungsvorschläge und Kritikpunkte zu den einzelnen Bestimmungen des Entwurfs der CSV aufgeführt. Es werden jeweils lediglich die in einer Stellungnahme vorgebrachten Hauptargumente erwähnt. Besonders ausführliche Stellungnahmen werden nur insoweit wiedergegeben, als sie konkrete materielle Änderungen fordern. Weitere Einzelheiten können den im Internet publizierten Stellungnahmen entnommen werden.

Stillschweigende Zustimmung bzw. der Verzicht auf eine Rückmeldung zu einem Artikel wird nicht erwähnt. Dies soll die Leserschaft aber nicht darüber hinwegtäuschen, dass trotz zahlreicher kritischer Stimmen zu einzelnen Bestimmungen eine Mehrzahl der Vernehmlassungsteilnehmenden mit weiten Teilen der vorgeschlagenen Verordnungsbestimmungen grundsätzlich einverstanden ist. Zur Verordnungssystematik als solche sind keine Stellungnahmen eingegangen.

3.3.2 Anträge und Bemerkungen zu den einzelnen Bestimmungen

3.3.2.1 Artikel 1 (Gegenstand)

Art. 1

Diese Verordnung regelt:

a. die Nationale Cyberstrategie und deren Steuerungsausschuss;

b. die Aufgaben des Bundesamtes für Cybersicherheit (BACS);

c. den Informationsaustausch des BACS mit Behörden und Organisationen zum Schutz vor Cybervorfällen und Cyberbedrohungen;

d. die Meldepflicht für Cyberangriffe.

Zum vorliegenden Artikel sind 3 Stellungnahmen eingegangen, die sich im Wesentlichen auf die Präzisierung des Geltungsbereichs und die Abgrenzung zu anderen Regelwerken fokussieren:

- *FER* weist auf eine fehlende Regelung der Cyberverteidigung hin.

- *BL* fordert eine Berücksichtigung des Sicherheitsverbunds Schweiz (SVS).

- *BE* verlangt eine klare Abgrenzung der CSV-spezifischen BACS-Aufgaben von den generellen Aufgaben in der ISV.

3.3.2.2 Artikel 2 (Nationale Cyberstrategie)

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.

Zum vorgeschlagenen Geltungsbereich sind 13 Reaktionen eingegangen.

❖ **Erweiterung des Stakeholder-Einbezugs**

- *asut, Salt* und *Switch* fordern den Einbezug von Wirtschaft, Wissenschaft und Zivilgesellschaft bei der Erarbeitung der NCS. Dementsprechend soll Art. 2 Abs. 2 wie folgt geändert werden: «Sie wird in Abstimmung mit den Kantonen und unter Einbezug der Wirtschaft, der Wissenschaft und von Vertretern der Zivilgesellschaft festgelegt.»

- *ZG* und *Swissgrid* kritisieren den fehlenden Einbezug weiterer Interessengruppen, insbesondere der Betreiber kritischer Infrastrukturen, bei der Erarbeitung des NCS.

- *sgv/usam* beantragt die Einbeziehung von Gemeindevertretungen bei der Erarbeitung der NCS.

- *SSV* kritisiert den fehlenden Einbezug grösserer Städte/Gemeinden bei der Erarbeitung der NCS.

❖ **Rolle und Einbezug spezifischer Behörden/Organisationen**

- *BL* fordert die Ergänzung des erläuternden Berichts, damit dort festgehalten wird, dass die Anstrengungen mit der NCS in enger Abstimmung mit den Kantonen erfolgen soll.

- *UR* betont Wichtigkeit des Sicherheitsverbunds Schweiz (SVS und dieser sollte daher weiterhin massgeblich an der zukünftigen NCS-Gestaltung mitarbeiten.

- *ZH* fordert, dass beim Aspekt der «Bekämpfung der Cyberkriminalität» der Beizug von Staatsanwaltschaft und Polizei als fachkompetente Behörden sichergestellt werden muss.

- *CH Post AG* schlägt vor, bei der Zusammensetzung auch Vertreterinnen und Vertreter von kritischen Infrastrukturen zu berücksichtigen und diese einzubinden. Die Formulierung «Vertreter der Wirtschaft» ist diesbezüglich zu wenig klar.

❖ **Inhaltliche Ergänzungen und Kritik**

- *ISSS* kritisiert die fehlende Berücksichtigung der internationalen Zusammenarbeit im Verordnungstext, da diese gemäss der NCS eine massgebliche Rolle haben soll.

- *SBB* beantragen die Aufnahme der «Identifikation von Bedrohungen» («Identity») in die Aufzählung von Art. 2 Abs. 1, damit alle fünf Funktionen des NIST Cybersecurity Framworks abgedeckt werden.

- *SVV* zweifelt an der ausreichenden Grundlage im ISG für den Erlass der Art. 2 ff. E-CSV.

❖ **Positive Bewertungen**

- *ZH* begrüsst die koordinierte Definition einer NCS.

- *Swico* begrüsst den zentralen strategischen Rahmen für Prävention, Früherkennung und Reaktion auf Cyberbedrohungen**.**

3.3.2.3 Artikel 3 (Einsetzung und Organisation des Steuerungsausschuss)

Art. 3 Einsetzung und Organisation des StA NCS
[1] Der Bundesrat setzt einen Steuerungsausschuss Nationale Cyberstrategie (StA NCS) ein.
[2] Der StA NCS verfügt über ein Sekretariat; das BACS betreibt das Sekretariat.

2 Vernehmlassungsteilnehmende haben sich unterstützend zur Einsetzung und Organisation des StA NCS geäussert.

❖ **Unterstützung für den StA NCS**

- *ISSS* und *CH Post AG* unterstützen die Einsetzung des StA NCS.

3.3.2.4 Artikel 4 (Zusammensetzung des StA NCS)

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 vorsitzende Person.

Die 27 Vernehmlassungsteilnehmende haben sich zur Zusammensetzung des StA NCS geäussert.

❖ **Art. 4 Abs. 1**

- *CH++* begrüsst die breite Zusammensetzung des StA NCS, fordert aber klare Auswahlkriterien für Mitglieder und eine angemessene Vertretung von Sicherheitsexperten.

- *Swiss Banking* und *Swiss FS-CSC* schlagen vor, die Worte «der Gesellschaft» im Verordnungswortlaut zu streichen.

- *economiesuisse* und *scienceindustries* kritisieren die vorzeitige Festlegung der Zusammensetzung und fordern zusammen mit *digitalswitzerland, Flughafen ZH, H+, ISSS, VS, Primeo, Swiss Banking, Swiss FS-CSC, VSE, CH Post AG, SVV und Swissgrid* den Einbezug von Vertretern kritischer Infrastrukturen in den StA NCS und eine entsprechende Anpassung im Verordnungstext.

- *Flughafen ZH* begrüsst den Einbezug der Wirtschaft und bietet sich als Vertretung an.

- *BL* wünscht eine Präzisierung zu der personellen Zusammensetzung und Integration von Vertretern der Gemeinden und kritischen Infrastrukturen in den StA NCS.

- *FR* schlägt eine obligatorische Vertretung des Energiesektors im StA NCS vor.

- *GE* schlägt vor, in zu Art. 4 Abs. 1 «société» durch «civile» zu ergänzen, um die Absicht besser widerzuspiegeln, die Interessen der Bürgerinnen und Bürger zu vertreten.

- *VD* und *SGV* empfehlen die Aufnahme von Gemeindevertretern in den StA NCS.

- *Migros* schlägt vor, dass der StA NCS so besetzt werden soll, dass wesentliche, für die Landesversorgung mit Gütern und Dienstleistungen kritische Unternehmungen direkt und nicht über Verbände vertreten sind.

- *SBB* kritisieren die unzureichenden Angaben zu Grösse und Zusammensetzung des StA NCS. Sie fordern eine Präzisierung der generischen Begriffe wie «Wirtschaft», um sicherzustellen, dass betroffene Branchen adäquat vertreten sind.

- *sgv/usam* fordert eine direkte Vertretung im StA NCS.

- *SSV* kritisiert eine fehlende Vertretung der Städte/Gemeinden im StA NCS.

- *Swico* beurteilt die gemischte Zusammensetzung des StA NCS als zielführend und schlägt die explizite Einbeziehung der ICT- und Internetbranche vor.

- *swissuniversities* bietet ihre Unterstützung bei der Suche nach einer angemessenen Vertretung der Hochschulen im StA NCS an und weist darauf hin, dass die Rolle von *Switch* in diesem Zusammenhang geklärt werden muss.

- *Die Mitte* begrüsst die breite Zusammensetzung des StA NCS.

❖ **Artikel 4 Absatz 2**

- *Swiss Banking* und *Swiss FS-CSC* schlagen eine Ergänzung von Art. 4 Abs. 2 bezüglich angemessener Erfahrungen oder Kenntnisse im Cyberbereich vor: «Bei der Bestimmung der Mitglieder des StA NCS ist auf angemessene Erfahrungen oder Kenntnisse im Cyberbereich zu achten.»

❖ **Artikel 4 Absatz 3**

- *GE* schlägt vor, in Art. 4 Abs. 1 und 3 «société» durch «civile» zu ergänzen, um die Absicht besser widerzuspiegeln, die Interessen der Bürgerinnen und Bürger zu vertreten.

- *Swissgrid* beantragt die explizite Nennung der Betreiber kritischer Infrastrukturen als mögliche vorsitzende Person.

3.3.2.5 Artikel 5 (Aufgaben des StA NCS)

Art. 5 Aufgaben des StA NCS

Der StA NCS hat folgende Aufgaben:

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

b. Er erarbeitet in Absprache mit den in der NCS aufgeführten Akteuren Vorschläge für die Prioritäten und Zeitpläne für die Umsetzung der Massnahmen der NCS.

c. Er beurteilt laufend die Umsetzung der Massnahmen und informiert den Bundesrat und die Kantone über Verzögerungen.

d. Er unterbreitet dem Bundesrat bei Bedarf Vorschläge für ergänzende Massnahmen.

e. Er erstattet dem Bundesrat, den Kantonen und der Öffentlichkeit jährlich Bericht über die Umsetzung der NCS.

10 Teilnehmende haben sich zu den Aufgaben des StA NCS geäussert. Im Allgemeinen hat Absatz 1 Buchstabe a betreffend dem Überprüfungsintervall der NCS am meisten Reaktionen hervorgerufen.

❖ **Allgemeine Vorschläge und Ergänzungen**

- Sowohl *SH* als auch *NFP 77 ETHZ UNIL* verlangen eine *Erweiterung der Kompetenzen des StA NCS*. So regt *SH* an, eine Notbestimmung in Art. 5 aufzunehmen, damit der StA NCS nicht nur Empfehlungen und Pläne machen kann, sondern bei Dringlichkeit die Befugnis erhält, umgehend geeignete Massnahmen zu treffen. *NFP 77 ETHZ UNIL e*mpfiehlt eine Erweiterung der Kompetenzen betreffend die Verantwortung für NCS-Kohärenz und -Umsetzung.

- Von einigen Teilnehmenden wird eine *Verbesserung der Koordination* verlangt Daher schlägt *ZG* regelmässige Konsultationen zwischen dem StA NCS und den Kantonen vor. *NFP 77 ETHZ UNIL* fordert in diesem Zusammenhang eine bessere Koordination zwischen NCS-Akteuren und Abstimmung mit anderen nationalen Strategien.

- Auch *organisatorische Aspekte* werden vom *NFP 77 ETHZ UNIL* gefordert, da es im Zusammenhang mit Art. 5 eine Klärung des BACS-Organigramms und -Status sowie mögliche Spezifizierung von Kompetenzen anderer Stellen verlangt.

❖ **Artikel 5 Buchstabe a (Überprüfungsintervall der NCS)**

- Der bestehende *Überprüfungsintervall* wurde von zahlreichen Vernehmlassungsteilnehmenden als zu lang kritisiert. *ISSS* und *Die Mitte* finden den 5-Jahres-Intervall als zu lang, machen aber keine Angabe, auf wie viele Jahre das Intervall zu kürzen sei. *SBB* verlangen eine jährliche Überprüfung mit ausführlicher Prüfung alle zwei Jahre. *UR* verlangt, dass eine Überprüfung mindestens alle drei Jahre stattfindet und schliesslich verlangt *Flughafen ZH, dass* eine Überprüfung mindestens alle vier Jahre stattfindet.

- Es wurden in den Stellungsnahmen auch Vorschläge zur *Art der Überprüfung* gemacht. So fordert *ISSS* zusätzliche risikobasierte und anlassbezogene Kurskorrekturen. *GE* schlägt vor, in Art. 5 Bst. a «contrôle» durch «audite» zu ersetzen, um eine detailliertere und präzisere Überprüfung anzudeuten.

3.3.2.6 Artikel 6 (Halterabfragen)

Art. 6 Halterabfragen Das BACS kann zur Warnung von Behörden, Organisationen und Personen bei unmittelbaren Cyberbedrohungen oder laufenden Cyberangriffen bei der Registerbetreiberin von Domain-Namen, die in die Kompetenz des Bundes fallen oder die diesen Domain-Namen untergeordnet sind, die Kontaktangaben der Halter von Domain-Namen abfragen.

3 Teilnehmende haben sich zustimmend zu diesem Artikel geäussert und verlangen lediglich textliche Änderungen:

- *GE* schlägt eine Umformulierung vor, um die Absicht und den Zweck der Anforderung von Kontakdaten der Domainname-Inhaber klarer zu formulieren: «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.»

- *SH* begrüsst die in Art. 6 festgeschriebene Befugnis des BACS, Domainhalter abfragen zu dürfen. Es wird jedoch vorgeschlagen, diese Befugnis auf die Sperrung krimineller Domains zu erweitern, statt nur Warnungen auszusprechen.

- ISSS merkt an, dass dem BACS die Kompetenz fehlt, im Nachgang zu Angriffen Halterabfragen zu machen sowie historische Halterinformationen zu beziehen.

3.3.2.7 Artikel 7 (Technische Analyse von Cybervorfällen und Cyberbedrohungen)

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.

16 Vernehmlassungsteilnehmende haben sich zu dieser Verordnungsbestimmung geäussert. Die meisten Anträge betreffen Textänderungen oder Klärungen.

❖ **Artikel 7 Absatz 1: Technische Analyse und CERT**

- Zur *Definition und Aufgaben des CERT* merkt *CH++* an, dass man anstelle von «CERT» den Begriff «CSIRT» verwenden soll, da «CERT» markenrechtlich geschützt sei. Das *BFK* regt an, die Zusammensetzung des CERT im Begleitbericht zu präzisieren und schlägt vor in Art. 7 Abs. 1 Bst. a und b «Technische Vorfälle» durch «Vorfall im Bereich der Cybersicherheit» zu ersetzen. *ISSS* kritisiert die fehlende Regelung, wem das CERT zur Verfügung steht, und merkt an, dass Buchstaben a und b einen technischen Fokus haben, der Buchstabe c aber nicht. *ISSS* verlangt, den Artikel zu überdenken und die Vorgabe zu ergänzen sowie die erarbeiteten Analysen im Regelfall zu publizieren. Schliesslich schlägt *Pour Demain* vor, den Art. 7 Abs. 1 Bst. a auf «technische Vorfallbewältigung, inklusive Ereignisse ohne Fremdeinwirkung» zu erweitern und einen neuen Art. 7 Abs. 1 Bst. d zu schaffen und darin das Monitoring von Vorfällen im Zusammenhang mit künstlicher Intelligenz vorzusehen und so die Auflistung zu erweitern.

- Mit Blick auf die *Zusammenarbeit und Koordination* plädieren *economiesuisse* und *scienceindustries* für eine gemeinsame Präzisierung der Leistungen und Zusammenarbeit zwischen BACS, privaten

CERTs und kritischen Infrastrukturen. *Swiss Banking* und *Swiss FS-CSC* erscheint es wichtig, dass eine technische Vorfallbewältigung auch auf Anfrage von anderen Behörden und Organisationen unterstützt wird und dementsprechend wird vorgeschlagen, Art. 7 Abs. 1 Bst. a durch den Nebensatz: «dies bei Bedarf auch auf Anfrage von anderen Behörden und Organisationen.» zu ergänzen. *SSK* stellt fest, dass die Zusammenarbeit mit Strafverfolgungsbehörden nicht explizit erwähnt wird, und schlägt vor, Kontakte zu Strafverfolgungsbehörden in der Verordnung zu institutionalisieren. *Switch* verlangt, den Austausch des CERT mit nationalen und internationalen Kompetenzzentren in der Verordnung zu verankern. *Swissuniversities* empfiehlt, die Zusammenarbeit zwischen CERT des BACS, Switch-CERT und Hochschul-Cybersicherheitsorganisationen in der Verordnung zu regeln. Schliesslich plädiert *VSE* für eine gemeinsame Präzisierung der Leistungen und Zusammenarbeit zwischen BACS, privaten CERTs und kritischen Infrastrukturen.

- Betreffend die *Ressourcen und Infrastruktur* empfiehlt *VS* eine gemeinsame Nutzung von Infrastrukturen oder Ressourcen mit anderen Bundesorganisationen.

❖ **Artikel 7 Absatz 2: Infrastruktur**

- *CH++* merkt mit Blick auf Art. 7 Abs. 2 an, dass «resilient» ein nicht genügend präziser Begriff ist. Die Organisation schlägt vor, mittels einer Formulierung wie «Der Betrieb dieser Infrastruktur muss jederzeit und möglichst unabhängig von Dritten sichergestellt werden können» zusätzliche Klarheit zu schaffen. Zudem wirft *CH++* die Frage nach der technischen Infrastruktur für die Analysen auf und empfiehlt eine Präzisierung bezüglich der Verwendung von Cloud-Diensten.

- *Flughafen ZH* begrüsst die Unabhängigkeit der Infrastruktur des BACS von der restlichen Bundesinformatik und schlägt ein hohes Schutzniveau vor.

❖ **Weitere Anmerkungen**

- *eAHV/IV* fordert eine verständlichere Beschreibung der Soforthilfe durch das BACS im erläuternden Bericht.

- *GE* schlägt vor, in der französischen Fassung im Art. 7 Abs. 1 «qui» durch «laquelle» zu ersetzen, um Mehrdeutigkeiten zu vermeiden.

- *SSK* empfiehlt auch, Gegenstand, Wirkungsziele und Umfang der «Gegenmassnahmen» zu definieren und die dafür nötigen Kompetenzen des CERT zu umschreiben.

3.3.2.8 Artikel 8 (Priorisierung der Beratung und Unterstützung bei Cyberangriffen)

Art. 8 Priorisierung der Beratung und Unterstützung bei Cyberangriffen [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.

12 Vernehmlassungsteilnehmende haben sich zu dieser Verordnungsbestimmung geäussert.

❖ **Allgemeine Anmerkungen zu Artikel 8**

- Mit Blick auf die in dieser Bestimmung geregelte *Zusammenarbeit und Zuständigkeiten* stellt *BFK* die Frage, ob im Falle einer schweren Krise vorgesehen werden sollte, die Hilfe von privaten Dienstleistern in Anspruch zu nehmen. Gegebenenfalls könnte festgelegt werden, welche Kriterien im Voraus

zur Identifizierung und Auswahl dieser Dienstleister herangezogen werden sollen. *ZH* empfiehlt die Formalisierung der Zusammenarbeit mit Staatsanwaltschaft und Polizei sowie Einbezug kantonaler Behörden. In diesem Zusammenhang empfiehlt *Switch* die Konkretisierung der BACS-Subsidiarität und Festschreibung der Eigenverantwortung privater Betreiber. Schliesslich schlägt *swissuniversities* vor, dass *Switch* das BACS bei Cyberangriffen auf Hochschulen entlasten könnte.

- Betreffend *Kompetenzen und Massnahmen* dieser Bestimmung schlägt *ISSS* vor, eine externe Verstärkung des CERT bei Cyberangriffen zu ermöglichen und *ZH* empfiehlt es, Gegenstand, Wirkungszielen und Umfang der «Gegenmassnahmen» sowie die Umschreibung der CERT-Kompetenzen im Verordnungstext zu definieren.

- Zur Rolle des BACS erwähnt *eAHV/IV*, dass Artikel 8 in Bezug auf die Priorisierung zur Geltung kommt, wenn es um die Sammlung weiterer Informationen bei einem Sicherheitsvorfall geht. *SBB* regen die Klärung des Verhältnisses zwischen Meldung und Unterstützungsanforderung an. *Swico* begrüsst die Beratung und Unterstützung durch das BACS, warnt aber vor staatlicher Konkurrenz zu privaten Angeboten bei Angriffen mit geringer Priorität.

❖ **Artikel 8 Absatz 1: Priorisierung und Kriterien**

- Zur *Festlegung von Priorisierungskriterien* fordert *digitalswitzerland* eine Liste spezifischer Kriterien und Abstufung konkreter Schadensszenarien für die Priorisierung. *GE* schlägt vor, die Kriterien für das Prioritätenmanagement zu ergänzen. Seitens von *UR* wird empfohlen, meldepflichtige Unternehmen und Organisationen nach Funktionen zu priorisieren. Und *SBB* beantragen, eine klare Priorisierung bei Kapazitätsengpässen zu machen. Schliesslich fordert *VSE* eine transparente Festlegung der Priorisierungskriterien, orientiert an der Liste kritischer Infrastrukturen des Bundesamts für Bevölkerungsschutz (BABS).

- Betreffend die *Kommunikation der Prioritäten* schlägt *GE* vor, einen neuen Absatz 3 zu schaffen, welcher was folgt vorsieht: «Il communique alors aux parties concernées les priorités définies».

❖ **Artikel 8 Absatz 2: Berücksichtigung öffentlicher Interessen**

- *digitalswitzerland* hält zu Art. 8 Abs. 2 fest, dass eine Liste der spezifischen Kriterien bzw. eine Abstufung der konkreten Schadensszenarien, nach denen priorisiert wird, für die Digitalwirtschaft eine wichtige Hilfestellung wäre.

3.3.2.9 Artikel 9 (Koordinierte Offenlegung von Schwachstellen)

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.
[6] Auf die vom Bundesamt für Kommunikation (BAKOM) im Rahmen seiner Aufsichtskontrollen (Art. 36 ff. der Verordnung vom 25. November 2015 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 1997 entdeckten Schwachstellen.

Dieser Artikel hat viele Reaktionen hervorgerufen. 25 Vernehmlassungsteilnehmende haben sich zur koordinierten Offenlegung von Schwachstellen geäussert.

❖ **Allgemeine Anmerkungen zu Artikel 9**

- Mit Blick auf die *Definition und den Umgang mit Schwachstellen* weist *SH* allgemein darauf hin, dass man den Herstellern ausreichende Behebungszeit geben muss, bevor Schwachstellen öffentlich gemacht werden. *Swiss Banking*, *Swiss FS-CSC* und *SBB* fordern eine Definition des Begriffs «Schwachstelle». Zudem fordert *SBB* Klärungen bezüglich Fristen zur Behebung von Schwachstellen, der Kommunikation zwischen BACS und das Bundesamt für Verkehr (BAV) der Abgrenzung der Meldepflicht zwischen Herstellern und Betreibern, der Verknüpfung von Hersteller und Betreiber.

- Betreffend die *Rolle und Aufgaben des BACS* erachtet *Die Mitte* diese als angemessen und notwendig.

- *NFP 77 ETHZ UNIL* empfiehlt, in der Verordnung die Konsequenzen bei einer Nichtbehebung zu konkretisieren.

- *SwissICT* äussert *Bedenken* hinsichtlich zusätzlicher Belastung für Hersteller und Vertraulichkeitsrisiken.

❖ **Artikel 9 Absatz 1: Grundsatz der koordinierten Offenlegung**

- *SP* begrüsst die Regelung ausdrücklich und sieht darin eine klare Verbesserung im Vergleich zum Status Quo.

- *asut, Salt, digitalswitzerland* und *ZG* schlagen vor, im Verordnungswortlaut die «Best Practices» neben den internationalen Standards zu berücksichtigen. *asut, Salt und digitalswitzerland* schlagen folgenden Wortlaut von Art. 9 Abs. 1 vor: «[1] Das BACS sorgt für die koordinierte Offenlegung der Schwachstellen nach deren Behebung nach international anerkannten Standards und Best Practices». *ZG* fordert überdies den Anwendungsbereich auf Betreiber und Dienste auszuweiten.

- *BE* schlägt vor, den Absatz wie folgt zu formulieren: «[1] Das BACS sorgt für die koordinierte Offenlegung von Schwachstellen.»

- *economiesuisse* und *scienceindustries* schlagen mit Blick auf den Zeitpunkt der Offenlegung vor, dass eine Offenlegung erst nach der Behebung der Schwachstellen erfolgen soll.

❖ **Artikel 9 Absatz 2: Frist zur Behebung von Schwachstellen**

- Seitens *digitalswitzerland, asut, Salt, economiesuisse, sicienceindustries* und *Swico* wird eine *Flexibilisierung der Frist* gefordert. So fordern *economiesuisse, scienceindustries* und *Swico* im Verordnungswortlaut den Passus «angemessene Frist» anstelle einer starren 90-Tage-Frist zu verwenden; *asut und Salt* plädieren aber dafür, dass man präzisiert, dass die angemessene Frist mindestens 90 Tage dauern soll.

- Betreffend die *Spezifizierung der Adressaten* schlägt *H+* eine Präzisierung auf Hersteller von Hard- oder Software kritischer Infrastrukturen vor und *SwissICT* fordert eine Ergänzung der Betreiber als potenziell Behebungspflichtige.

❖ **Artikel 9 Absatz 3: Information bei akuter Cyberbedrohung**

- *BE* empfiehlt, Art. 9 Abs. 3 zur besseren Verständlichkeit wie folgt zu formulieren: «[3] Ist dem BACS eine Schwachstelle bekannt, die für einzelne kritische Infrastrukturen eine akute Cyberbedrohung darstellt, informiert es umgehend deren Betreiberinnen, noch bevor die Schwachstelle veröffentlicht oder behoben wurde».

❖ **Artikel 9 Absatz 4: Verkürzung oder Verlängerung der Frist**

- *CH++* schlägt vor, Art. 9 Abs. 4 strenger zu formulieren, um sicherzustellen, dass die Fristen nicht in zu vielen Fällen verlängert werden.

- *Swico* macht den Vorschlag zur Anhörung der Herstellerin vor Fristverkürzung und verlangt, Art. 9 Abs. 4 wie folgt zu formulieren: «Es [das BACS] kann die Frist nach Anhörung der Herstellerin verkürzen, wenn eine Schwachstelle: …».

- *BFK* merkt an, dass ein möglicher Widerspruch zwischen «die Frist verkürzen, wenn die Schwachstelle leicht ausgenutzt werden kann» und «die Frist verlängern, wenn die Beseitigung der Schwachstelle besonders komplex ist» besteht.

❖ **Artikel 9 Absatz 5: Information der Betreiber kritischer Infrastrukturen**

- *CH++* regt an, die Formulierung zu schärfen, um den Eindruck zu vermeiden, das VBS könnte Informationen über Sicherheitslücken in riskanten Situationen zurückhalten, um diese möglicherweise selbst länger offensiv nutzen zu können. *CH++* schlägt vor, in Art. 9 Abs. 5 die Kann-Formulierung abzuändern: «Es informiert grundsätzlich die Betreiberinnen kritischer Infrastrukturen bereits vor der Behebung oder Offenlegung über Schwachstellen.»

- Sowohl *Migros* (sofortige Information) als auch *Flughafen ZH* (zwingende Information innerhalb von 72 Stunden) verlangen nach einer schnelleren Information.

- *NEDIK* empfiehlt, dass das BACS die Betreiber grundsätzlich vor der Behebung oder Offenlegung der Schwachstelle informieren sollte, mit der Möglichkeit in bestimmten Fällen abzuwarten.

- *BFK* stellt die Frage, was man macht, wenn eine kritische, komplex zu behebende Schwachstelle vorliegt, und schlägt vor, dass man die Möglichkeit erwähnt, vorübergehende Abschwächungsmassnahmen einzurichten, bis die Schwachstelle behoben ist.

❖ **Artikel 9 Absatz 6 und 7: Koordination mit BAKOM**

- *Sunrise* begrüsst die Regelungen zur Koordination zwischen dem BACS und dem BAKOM als richtigen Ansatz zur Harmonisierung und Koordination der verschiedenen Meldeverfahren.

- *FER* weist daraufhin, dass eine Harmonisierung des Verfahrens des BAKOM und des BACS herausfordernd sein könnte (z.B. das BAKOM muss das BACS über Schwachstellen informieren, damit dieses dann allenfalls eine koordinierte Offenlegung der Schwachstellen vornehmen kann).

- *Piratenpartei Schweiz* schlägt vor, Abs. 6 zu streichen oder so zu ändern, dass die Offenlegung grundsätzlich weiterhin nach Abs. 1-4 durchgeführt wird, aber unter Berücksichtigung der Besonderheiten der BAKOM-Kontrolle. Die Partei kritisiert, dass der undefinierte Umgang mit Informationen über Schwachstellen in kritischen Infrastrukturen ungenügend ist und fordert eine klarere Regelung in der Verordnung.

3.3.2.10 Artikel 10 (Unterstützung von Behörden)

Art. 10 Unterstützung von Behörden Das BACS unterstützt die Behörden von Bund und Kantonen bei der Entwicklung, Umsetzung und Prüfung von Standards und Regulierungen im Bereich der Cybersicherheit.

Lediglich zwei Vernehmlassungsteilnehmende haben sich zu dieser Bestimmung geäussert, ohne diese abzulehnen:

- *UR* stellt die Frage, wie die Gemeinden in den Gesamtprozess eingebunden werden.

- *swissuniversities* regt an, zu prüfen, ob Hochschulen nicht ebenfalls von dieser Unterstützung profitieren sollten.

3.3.2.11 Artikel 11 (Kommunikationssystem für den sicheren Informationsaustausch)

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. [2] Das BACS ist für die Sicherheit des Kommunikationssystems und die Rechtmässigkeit der Bearbeitung der Daten verantwortlich.

Insgesamt 13 Teilnehmende haben sich zur Bestimmung und zu den folgenden drei Themenbereichen geäussert.

❖ **Zugang zum Kommunikationssystem**

- *NFP 77 ETHZ UNIL* merkt an, dass unklar ist, ob alle Behörden und Organisationen mit Sitz in der Schweiz Zugang zum Kommunikationssystem des BACS haben oder ob nur kritische Infrastrukturen betroffen sind. Es empfiehlt eine Präzisierung in der Verordnung.

- *Swiss Banking*, S*wiss FS-CSC*, *digitalswitzerland*, *economiesuisse* und *scienceindustries* schlagen vor, den Zugang auf alle meldepflichtigen Organisationen und Behörden auszuweiten, unabhängig von einem schweizerischen Sitz. Sie argumentieren, dass dies für die Stärkung der Cyberresilienz auf dem Wirtschaftsstandort Schweiz notwendig sei und den grenzüberschreitenden Austausch für globale Unternehmen erleichtert.

❖ **Funktionalität und Umsetzung des Kommunikationssystems**

- *Swico* begrüsst das zentrale Kommunikationssystem für den sicheren Informationsaustausch, weist aber auf die Notwendigkeit eines hohen Sicherheitsstandards hin.

- *BE* fordert eine Verdeutlichung der Abgrenzung der Systeme nach Art. 11 und Art. 12 und argumentiert, dass weder aus den Normen noch aus dem erläuternden Bericht die Abgrenzung beider Systeme, die unterschiedlichen Nutzungsvorgaben und Zwecke klar verständlich hervorgehen.

- *SGV* betont die Wichtigkeit einer einfachen und unbürokratischen Registrierung für die Teilnahme am Informationsaustausch sowie eines unkomplizierten Zugangs in der Praxis. Der Verband ersucht das BACS, in der praktischen Umsetzung der Verordnung für eine leichte Zugänglichkeit zu sorgen.

- *SBB* bemängeln fehlende Klarheit bezüglich der Verantwortlichkeiten für die Überwachung neuer Bedrohungen auf der Kommunikationsplattform des BACS sowie der Zugriffrechte. Sie fordert eine Klärung dieser Punkte.

❖ **Vorschläge zur Erweiterung und Präzisierung**

- *BE* empfiehlt, eine Registrierungspflicht für meldepflichtige Organisationen und Behörden sowie Betreiberinnen kritischer Infrastrukturen auf dem Kommunikationssystem für den sicheren Informationsaustausch bzw. den Informationssystemen für den automatischen Austausch einzuführen.

- *SVV* betont die Wichtigkeit einer regelmässigen detaillierten (anonymisierten) Berichterstattung durch das BACS über die eingegangenen Meldungen. Dies wird als entscheidend für die Versicherungsbranche erachtet, um zur Erhöhung der Cyber-Resilienz der Schweizer Wirtschaft beizutragen und gleichzeitig die Versicherungsdurchdringung zu erhöhen.

- *eAHV/IV* sieht im Rahmen der Umsetzung der Meldepflicht die Möglichkeit, dass das BACS eine Drehscheibenfunktion im Sinne des Once-Only-Prinzips übernehmen sollte.

- *Switch* empfiehlt, die Subsidiarität des BACS in bestimmten Fällen zu konkretisieren und einen zusätzlichen Absatz einzufügen, der den Grundsatz der Eigenverantwortung von privaten Betreiberinnen für Cybersicherheit festschreibt.

3.3.2.12 Artikel 12 (Informationssysteme für den automatischen Austausch)

Art. 12 Informationssysteme für den automatischen Austausch
[1] Das BACS stellt den Betreiberinnen kritischer Infrastrukturen Informationssysteme für den automatischen Austausch von technischen Informationen zu Cyberbedrohungen und Cybervorfällen zur Verfügung.
[2] Das BACS ist für die Sicherheit der Informationssysteme und die Rechtmässigkeit der Bearbeitung der Daten verantwortlich.

5 Vernehmlassungsteilnehmende haben sich zu dieser Bestimmung geäussert. Die Anträge zum Verordnungstext betreffen die Klarheit und Präzision, Sicherheitsstandards und Datenschutz sowie den Zugang und die Nutzung des Informationssystems.

❖ **Klarheit und Präzision des Verordnungstextes**

- *GL* weist auf eine Inkonsistenz in der Terminologie zwischen dem Verordnungstext und den Erläuterungen hin. Während im Verordnungstext nur von «technischen Informationen» die Rede ist, werden laut erläuterndem Bericht auch Personendaten bearbeitet.

- *SH* merkt an, dass unklar bleibt, wie der Informationsaustausch zwischen allen Beteiligten erfolgen soll. Er fordert präzisere Regelungen bezüglich der Art und Weise des Austauschs der Meldungen sowie der Benachrichtigungen.

❖ **Sicherheitsstandards und Datenschutz**

- *Flughafen ZH* schlägt vor, dass das BACS nach höchsten Sicherheitsstandards streben sollte. Sie empfiehlt, dies explizit im Verordnungstext zu verankern.

- *SBB* fordern Klarheit darüber, wie Informationen in Cloudumgebungen gehandhabt werden dürfen. Insbesondere fragen *SBB* nach den Bedingungen, unter denen Informationen in Cloud Environments ausserhalb der Schweiz gespeichert werden dürfen.

❖ **Zugang und Nutzung des Informationssystems**

- *swissuniversities* betont, dass Hochschulen stark von direkten Informationen über aktuelle Bedrohungen (Threat Intelligence) vom BACS oder über *Switch* profitieren würden. Sie unterstreicht damit die Bedeutung des Informationsaustauschs für den Hochschulsektor.

3.3.2.13 Artikel 13 (Registrierung)

Art. 13 Registrierung

[1] Die Organisationen und Behörden müssen sich für die Nutzung des Kommunikationssystems registrieren. Sie müssen Änderungen von Angaben unverzüglich melden.

[2] Die Registrierung muss mindestens folgende Informationen enthalten:

a. Firma, Name oder Bezeichnung und Adresse;

b. Kontaktangaben der gemeldeten Person.

8 Vernehmlassungsteilnehmende haben sich zu diesem Artikel geäussert; keiner hat den Artikel in der vorliegenden Form abgelehnt.

❖ **Artikel 13 Absatz 1: Begrifflichkeit und Prozess der Registrierung**

- *GE* empfiehlt, in der französischen Fassung von Art. 13 Abs. 1 den Begriff «enregistrement» durch «enrôlement» zu ersetzen, um Mehrdeutigkeiten zu vermeiden. Diese Änderung zielt darauf ab, den Registrierungsprozess präziser zu beschreiben.

- *Flughafen ZH* fordert eine verpflichtende Registrierung für kritische Infrastrukturen innerhalb von 90 Tagen nach Inkrafttreten des Gesetzes. Sie betont jedoch, dass die Teilnahme am Informationsaustausch freiwillig bleiben soll.

- *swissuniversities* erklärt, dass Hochschulen ein Interesse daran haben, sich so früh wie möglich zu registrieren und sich für eine eventuelle Vorregistrierung zur Verfügung zu stellen. Es wird auch vorgeschlagen, eine mögliche Koordination durch *Switch* zu prüfen.

❖ **Artikel 13 Absatz 2: Registrierungsinformationen und Kontaktangaben**

- *GE* schlägt vor, in der französischen Fassung in Art. 13 einen neuen Buchstaben c in Absatz 2 hinzuzufügen, der die Kontaktdaten der für die Cybersicherheit zuständigen Einheit innerhalb der Organisation oder Behörde spezifiziert.

- *SH* schlägt vor, dass bei kritischen Meldungen Benachrichtigungen nicht nur an eine einzelne Person erfolgen sollte. Er empfiehlt, die Registrierung mehrerer Personen zu ermöglichen, um die Kontinuität der Informationskette sicherzustellen. *Flughafen ZH, digitalswitzerland* und *Swico* äussern sich auch dergestalt, da sie vorschlagen, in Art. 13 Abs. 2 Bst. b anstelle der «Kontaktangaben der gemeldeten Person» den Passus «Angaben zu einer oder mehreren Kontaktpersonen» zu verwenden.

- *economiesuisse* und *scienceindustries* fordern die Streichung von Art. 13 Abs. 2 oder zumindest eine Anpassung von Art. 13 Abs. 2 Bst. b, da sie die geforderten Angaben als zu detailliert und formalistisch ansehen.

3.3.2.14 Artikel 14 (Dienstleister)

Art. 14 Dienstleister
[1] Die Betreiberinnen kritischer Infrastrukturen können dem BACS Dienstleister melden, die am Informationsaustausch teilnehmen wollen.
[2] Die Dienstleister müssen sich mit der Firma oder dem Namen sowie Kontaktangaben der gemeldeten Person registrieren.

6 Vernehmlassungsteilnehmende haben sich zu diesem Artikel geäussert. Die Stellungnahmen zeigen eine grundsätzliche Akzeptanz des Artikels, verbunden mit dem Wunsch nach Präzisierungen und Empfehlungen für Ergänzungen.

❖ **Artikel 14 Absatz 1: Definition und Umfang der Dienstleister**

- *FR* empfiehlt, in der französischen Fassung den Begriff «fournisseurs de prestations de cybersécurité» (Anbieter von Cybersicherheitsdienstleistungen) zu verwenden, um Verwechslungen zu vermeiden. Dieser Vorschlag zielt darauf ab, den Umfang der betroffenen Dienstleister klarer zu definieren.

- *GE* schlägt vor, im Verordnungstext zu präzisieren, dass das BACS die Aufnahme der Dienstleister prüft. Dieser Vorschlag berücksichtigt die Sensibilität der auszutauschenden Daten und zielt darauf ab, die Sicherheit des Informationsaustauschs zu erhöhen.

- *VS* fordert eine Präzisierung, ob sich der Artikel auf alle IT-Dienstleister oder nur auf jene im Zusammenhang mit Cybersicherheit bezieht.

- *Swiss Banking* und *Swiss FS-CSC* schlagen vor, den Artikel dahingehend zu präzisieren, dass Betreiberinnen kritischer Infrastrukturen dem BACS Dienstleister melden können, die für sie Dienstleistungen im Rahmen ihrer Geschäftstätigkeit erbringen und deshalb am Informationsaustausch teilnehmen wollen. Sie schlagen vor, den Art. 14 Abs. 1 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.» und begründen dies mit der bestehenden Praxis, wonach solche Dienstleister bereits zur Teilnahme am Informationsaustausch zugelassen sind, wenn sie die Anforderungen des BACS erfüllen.

- *Swico* begrüsst, dass Dienstleister von Betreiberinnen kritischer Infrastrukturen auf freiwilliger Basis Zugang zu den genannten Informationssystemen erhalten können. Der Verband erachtet die vorgesehene Meldung durch die Betreiberinnen und anschliessende Anmeldung des Dienstleisters als sinnvoll.

❖ **Artikel 14 Absatz 2: Registrierung der Dienstleister**

- *Swico* schlägt vor, in Artikel 14 Absatz 2 die Formulierung «Kontaktangaben der gemeldeten Person» durch «Angaben zu einer oder mehreren Kontaktpersonen» zu ersetzen: «[2] Die Dienstleister müssen sich mit der Firma oder dem Namen sowie ~~Kontaktangaben der gemeldeten Person~~ Angaben zu einer oder mehreren Kontaktpersonen registrieren.» Der Verband argumentiert, dass die aktuelle Formulierung eine Verantwortlichkeit der gemeldeten Person implizieren könnte, was vermieden werden sollte.

3.3.2.15 Artikel 15 (Übermittlung und Nutzung der Informationen)

Art. 15 Übermittlung und Nutzung der Informationen
[1] Registrierte Unternehmen und Behörden übermitteln Informationen dem BACS und bestimmen dabei, ob und an wen dieses die Informationen weitergegeben darf, soweit eine Weitergabe der Informationen nicht gesetzlich vorgesehen ist.
[2] Das BACS entscheidet über die Veröffentlichung der zur Weitergabe freigegebenen Informationen auf dem Kommunikationssystem sowie den Informationssystemen für den automatischen Austausch.
[3] Die Informationsempfänger müssen den Schutz der Informationen gewährleisten.
[4] Die Dienstleister von Betreiberinnen kritischer Infrastrukturen dürfen Informationen, die sie erhalten, ausschliesslich zum Schutz kritischer Infrastrukturen nutzen.

Insgesamt 12 Vernehmlassungsteilnehmende haben sich mit der Übermittlung und Nutzung der Informationen auseinandergesetzt. Niemand hat den Artikel 15 abgelehnt. Die Stellungnahmen enthalten überwiegend Vorschläge zur Präzisierung, Erweiterung oder Anpassung des Artikels.

❖ **Allgemeine Anmerkungen zu Artikel 15**

- *SH* erwartet, dass nicht nur eine Filterung, sondern auch eine Kategorisierung der Meldungen durch ein spezialisiertes Supportteam erfolgt. Es wird vorgeschlagen, eine zentrale Bundesbehörde mit explizitem Fachwissen einzurichten, die auf nationaler Ebene beratend tätig ist.

- *Swissgrid* stellt Fragen zu den Folgen bei Nichteinhaltung der TLP-Klassifizierung und zur Vorgehensweise, wenn der Informationslieferant den Empfängerkreis nicht festlegt. Sie beantragt entsprechende Ergänzungen der Verordnung oder der Erläuterungen.

- *NFP 77 ETHZ UNIL* schlägt vor, die Bestimmung dahingehend zu präzisieren, dass Unternehmen und Behörden bei der Übermittlung von Informationen angeben müssen, ob und an welche Empfängerkategorien gemäss dem TLP-Protokoll diese weitergeleitet werden können. Sie weisen auf einen möglichen Konflikt zwischen Art. 15 Abs. 1 und Abs. 2 hin und empfehlen eine Klarstellung in der Verordnung. Zudem sollte festgelegt werden, dass das BACS Informationen nur veröffentlichen darf, wenn dies für den Schutz kritischer Infrastrukturen oder der Schweiz vor Cyberbedrohungen erforderlich ist.

❖ **Artikel 15 Absatz 1: Übermittlung von Informationen**

- *Flughafen ZH* schlägt vor, dass registrierte Unternehmen und Behörden bestimmen können, welche Informationen und an wen diese weitergegeben werden dürfen.

- *GR* empfiehlt, dass bei der Übermittlung bestimmt werden kann, welche Informationen weitergegeben werden dürfen, da manche Informationen schnell geteilt werden sollen, andere aber aus taktischen Gründen erst später.

- *NEDIK* weist darauf hin, dass die Meldung vom Melder selbst gesteuert werden kann und verschiedene Klassifizierungen möglich sind. Sie betonen die Wichtigkeit einer korrekten Klassifizierung und dass Melder die Weitergabe der Informationen auf bestimmte Daten ein- oder ausgrenzen können sollten.

- *Swico* betont die Wichtigkeit, dass die übermittelnde Organisation oder Behörde bestimmt, ob und an wen gemeldete Informationen weitergegeben werden dürfen, unter Berücksichtigung der Sensitivität der Informationen und der notwendigen Vertrauensbeziehung.

❖ **Artikel 15 Absatz 2: Veröffentlichung und Weitergabe von Informationen**

- *BA* schlägt vor, die Speicherung von Informationen durch das BACS explizit zu erwähnen, um eine spätere Übermittlung an die Strafverfolgungsbehörden zu ermöglichen.

- *Swiss Banking* und *Swiss FS-CSC* fordern eine Konkretisierung der Modalitäten der Übermittlung von Meldungen an das BACS. Sie schlagen vor, dass bei Sammelmeldungen an verschiedene Behörden jede Behörde nur den für sie bestimmten Teil lesen kann. Eine Ergänzung von Art. 15 E-CSV durch zwei Absätze wird vorgeschlagen, um dies zu gewährleisten. Der erste Absatz soll wie folgt lauten: «^{1bis} 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.» und der zweite vorgeschlagene neue Absatz soll folgenden Wortlaut haben: «^{1ter} Für jene Meldungsinhalte, die auf diesem Weg mit dem BACS geteilt werden, entscheidet das BACS über die Veröffentlichung ... [weiter nach Art. 15 Abs. 2]».

- *SSK* regt an, die Kompetenz des BACS über die Weitergabe von Informationen so weit zu beschränken, dass eine vollständige Übermittlung der Informationen an die Strafverfolgungsbehörden gewährleistet ist.

- *ZH* empfiehlt, dass das BACS verpflichtet wird, Meldungen über Cyberangriffe zur strafrechtlichen Beurteilung an die zuständigen Strafverfolgungsbehörden weiterzuleiten. Es wird vorgeschlagen, in der Verordnung genauer festzulegen, wie mit strafrechtlich relevanten Informationen umzugehen ist.

❖ **Artikel 15 Absatz 3 und 4: Schutz und Verwendung der Informationen**

- *VS* findet Artikel 15 Abs. 4 zu restriktiv und schlägt vor, dass Dienstleister Informationen über Schwachstellen nutzen dürfen, um andere Kunden besser zu schützen.

- *NEDIK* weist darauf hin, dass Strafverfolgungsbehörden bei Kenntnis von Offizialdelikten gesetzlich verpflichtet sind, Ermittlungen einzuleiten. Sie fordern, dass das BACS sicherstellt, dass in veröffentlichten Informationen die betroffene Betreiberin von kritischer Infrastruktur nicht identifizierbar ist.

- *Swico* begrüsst die Pflicht zum Schutz der Informationen durch die Informationsempfänger und deren ausschliessliche Verwendung zum Schutz kritischer Infrastrukturen, um unlautere Wettbewerbsvorteile zu verhindern.

3.3.2.16 Artikel 16 (Ausnahmen von der 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 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 2008 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) 2023/203 oder nach Artikel 2 und dem Anhang II der Verordnung (EU) 2022/1645 einrichten müssen,

   2. die Vorgaben nach Punkt 1.7 des Anhangs der Verordnung (EU) 2015/1998 in ihrem Security-Programm nach Artikel 2, 12, 13 oder 14 der Verordnung (EG) 300/2008 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 1957 [EBG]) beauftragt sind,

   2. über eine Personenbeförderungskonzession nach Artikel 6 des Personenbeförderungsgesetzes vom 20. März 2009 (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.

Insgesamt 24 Vernehmlassungsteilnehmende haben sich zu dieser Bestimmung geäussert und keiner hat diese abgelehnt. Es gibt jedoch kritische Stimmen und Vorschläge für Änderungen oder Ergänzungen.

❖ **Artikel 16 Absatz 1: Allgemeine Ausnahmen von der Meldepflicht**

- *AG, SZ, VD* und *SwissICT* kritisieren die *Ausnahme für Gemeinden* mit weniger als 1'000 Einwohnern, da diese aufgrund geringerer Ressourcen anfälliger für Cyberangriffe sein könnten, diese mit dem Kantonsnetz verbunden sind und Cyberangriffe negative Auswirkungen auf die kantonale Infrastruktur haben könnten, diese oft am verwundbarsten sind und ihre Ausnahme ein falsches Signal senden würde, und kleinere Institutionen wichtig für die Früherkennung von Cyberangriffen sind.

Demgegenüber begrüsst *SGV* die Ausnahme für Gemeinden mit weniger als 1'000 Einwohnern, betont aber die Wichtigkeit freiwilliger Meldungen und technischer Unterstützung für alle Gemeinden.

- Betreffend die *Ausnahmen für Hochschulen und andere Institutionen* schlägt *Switch* vor, Hochschulen und Registrare in bestimmten Fällen von der Meldepflicht auszunehmen, da eine vollständige Meldepflicht für diese Kategorien unverhältnismässig sei. *swissuniversities* empfiehlt die Einführung von Schwellenwerten für Hochschulen, basierend auf verschiedenen Kriterien wie Grösse, Infrastruktur und Forschungssysteme.

- *Swiss Banking* und *Swiss FS-CSC* schlagen vor, Cyberangriffe mit nur geringfügigen Auswirkungen auf die Geschäftstätigkeit von Finanzinstituten von der Meldepflicht auszunehmen. 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.»

- *SBB* beantragen, die vorgesehenen Ausnahmen für kleinere Bahnen, Betreiber von Gasleitungen und Elektrizitätswerke zu überdenken, da auch diese von sicherheitsrelevanten Angriffen betroffen sein können.

- *CH++* und *H+* argumentieren, dass Spitäler unabhängig von ihrer Grösse meldepflichtig sein sollten.

- *ASIP* beantragt eine Erweiterung der Befreiung von der Meldepflicht für sämtliche registrierten und nicht registrierten Vorsorgeeinrichtungen (mit und ohne reglementarische Leistungen) bis zu einer Grösse von 30'000 Versicherten. *ASIP* argumentiert, dass die Verantwortlichkeit für Cybersicherheit beim obersten Organ der Vorsorgeeinrichtung liegen und nicht unnötig durch gesetzliche Bestimmungen eingeschränkt werden sollte.

- *Swissgrid* beantragt, auch Dienstleister zu erfassen, welche intelligente Mess- und Steuersysteme steuern, sofern sie bestimmte Grenzwerte erfüllen.

❖ **Artikel 16 Absatz 2: Ausnahmen für kleine Strukturen**

- *BFK* hinterfragt die Angemessenheit des Begriffs «kleine Strukturen» für die Befreiung von der Meldepflicht und regt an, andere Kriterien wie die Grösse der betroffenen Kundschaft zu berücksichtigen.

- *economiesuisse, scienceindustries und Swico* schlagen vor, Unternehmen und andere privatrechtliche Organisationen von der Meldepflicht auszunehmen, die weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen. Es wird folgender Verordnungswortlaut zu Art. 16 Abs. 2 vorgeschlagen: «[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~~ jeweils am 1. Januar eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen.»

- *SwissICT* empfiehlt, die Ausnahmen basierend auf Mitarbeiterzahl und Umsatz eines Unternehmens zu streichen, da diese den Sinn und Zweck der Meldepflicht gefährden könnten.

❖ **Sonstige Vorschläge und Anmerkungen**

- *SSV* fragt, ob eine Ergänzung der «Allgemeinen Geschäftsbedingungen für IKT-Leistungen» vorgesehen ist und merkt an, dass der erläuternde Bericht zu diesem Artikel schwer verständlich formuliert sei.

- *BE* schlägt eine Präzisierung des Einleitungssatzes vor, um zwischen Betreiberinnen kritischer Infrastrukturen sowie Behörden und Organisationen zu unterscheiden: «Die folgenden Behörden, Organisationen und Betreiberinnen von kritischen Infrastrukturen sind unter den nachstehenden Voraussetzungen von der Meldepflicht ausgenommen: ...»

- *GE* merkt an, dass in Art. 16 Abs. 1 Bst. b nicht klar ist, ob die beiden Bedingungen kumulativ oder alternativ sind.

- *GR* empfiehlt, bei der Definition der Grösse von Institutionen das Risiko der kaskadierenden Ausbreitung eines Datenvorfalls zu berücksichtigen.

- *SO* findet die vorgesehenen Ausnahmen von der Meldepflicht stimmig und nachvollziehbar.

- *VS* schlägt vor, die Reihenfolge der Buchstaben c und d in Art. 16 Abs. 1 umzukehren, um der Reihenfolge im ISG zu entsprechen.

- *Swiss Banking* und *Swiss FS-CSC* schlagen 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.

- *CH++* bemängelt das Fehlen einer Regelung zum Umgang mit Kumulations-Risiken.

3.3.2.17 Artikel 17 (Dokumentationspflicht bei Gesuchen um Auskunft über die Unterstellung unter die Meldepflicht)

> Art. 17 Dokumentationspflicht bei Gesuchen um Auskunft über die Unterstellung unter die Meldepflicht
>
> Die interessierten Behörden und Organisationen müssen dem BACS alle Unterlagen zur Verfügung stellen, die dieses benötigt, um Auskunft über die Unterstellung unter die Meldepflicht zu erteilen.

1 Teilnehmender hat sich zu dieser Bestimmung geäussert. Dieser hat den Wortlaut von Artikel 17 als unpräzis kritisiert.

- *NFP 77 ETHZ UNIL* kritisiert die unklare Formulierung des Titels der Bestimmung, zumindest in der französischen Version. Es wird vorgeschlagen, alternative Formulierungen wie «Obligation de mettre à disposition des informations», «Obligation de collaborer» oder «Obligation d'information» zu verwenden.

3.3.2.18 Artikel 18 (Zu meldende Cyberangriffe)

> Art. 18 Zu meldende Cyberangriffe
>
> [1] Die Funktionsfähigkeit einer kritischen Infrastruktur gilt als gefährdet, wenn:
>
> a. Mitarbeitende oder Dritte von Systemunterbrüchen betroffen sind; 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 von Unbefugten verändert oder offengelegt werden; oder

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

[3] Ein Cyberangriff gilt als über einen längeren Zeitraum unentdeckt, wenn der Vorfall mehr als 90 Tage zurückliegt.

[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 ehemaliger Verantwortlicher oder Mitarbeitender, oder gegen für die meldepflichtige Behörde oder Organisation tätige Personen richten.

33 Vernehmlassungsteilnehmende haben sich zu den zu meldenden Cyberangriffen vernommen. Keiner hat den Artikel 18 abgelehnt, sondern die Stellungnahmen enthalten überwiegend Vorschläge zur Präzisierung, Erweiterung oder Anpassung des Artikels.

❖ **Artikel 18 Absatz 1: Definition meldepflichtiger Cyberangriffe**

- Von zahlreichen Vernehmlassungsteilnehmenden wurden *Präzisierungen zur Meldepflicht* verlangt:

  - *asut* und *Salt* schlagen vor, die Meldepflicht auf Vorfälle zu beschränken, die direkte Auswirkungen auf den Betrieb der kritischen Infrastruktur haben.

  - *Flughafen ZH* fordert, dass nur erfolgreiche Cyberangriffe mit funktionalen Konsequenzen der Meldepflicht unterliegen sollten.

  - *economiesuisse* und *scienceindustries* betonen, dass nur erfolgreiche Angriffe mit funktionalen Folgen meldepflichtig sein sollten.

  - *BL* merkt zu Art. 18 Abs. 1 Bst. a an, dass «Systemunterbrüche» präzisiert werden sollen, da wenn beispielsweise das Buchhaltungssystem einen Unterbruch bei der Anwendung einer KI erleidet, dies kaum Auswirkungen auf die Kernkompetenz des Systems haben soll.

  - *H+* argumentiert, dass die Formulierung zu allgemein gehalten sei und spezifiziert werden sollte.

  - *GR* beantragt eine genauere Definition des Startzeitpunkts eines Cyberangriffs und die ausdrückliche Nennung wesentlicher Anzeichen eines vorbereitenden Angriffs.

  - *SGV* fordert Präzisierungen bezüglich der Definition von meldepflichtigen Cyberangriffen.

  - *SBB* kritisieren die zu generischen und umfassenden Formulierungen und beantragen eine Präzisierung und Eingrenzung.

  - *SVV* argumentiert, dass nur absichtlich ausgelöste Systemunterbrüche meldepflichtig sein sollten.

  - *Swico* schlägt Präzisierungen vor, um klarzustellen, dass es sich um Ereignisse handeln muss, die den Betrieb der Infrastruktur unmittelbar gefährden.

  - *SwissICT* kritisiert die Definition der Funktionsfähigkeitsgefährdung als zu ausufernd und schlägt eine Gewichtung vor.

- *Migros* argumentiert, dass nicht jeder Systemunterbruch die Funktionsfähigkeit einer kritischen Infrastruktur gefährdet, und schlägt vor, nur Unterbrüche eines «geschäftskritischen Systems» als meldepflichtig zu betrachten.

- Einige Vernehmlassungsteilnehmende verlangen eine *Berücksichtigung des Schweregrades*. So regen *digitalswitzerland*, *SUVA* und CH Post AG an, den Schweregrad eines Cyberangriffs bei der Meldepflicht zu berücksichtigen, um administrativen Aufwand zu vermeiden.

- Es wird von Vernehmlassungsteilnehmenden auch eine *Spezifizierung von Begriffen* verlangt:

  - *NEDIK* argumentiert, dass die Verordnung präziser definieren und eingrenzen sollte, was unter einem «Systemausfall» zu verstehen ist.

  - *GE* schlägt vor, im erläuternden Bericht zu präzisieren, was unter einem «part importante» zu verstehen ist.

  - *GL* empfiehlt, im erläuternden Bericht deutlicher darauf hinzuweisen, dass Systemunterbrüche nur im Zusammenhang mit einem Cyberangriff dem BACS zu melden sind.

❖ **Artikel 18 Absatz 2: Manipulation oder Abfluss von Informationen**

- *BFK* weist darauf hin, dass ein Informationsleck festgestellt werden kann, bevor die Informationen von unbefugten Personen veröffentlicht werden.

- *NFP 77 ETHZ UNIL* kritisiert, dass der Verweis auf das DSG nicht ideal ist, da das DSG auch Meldepflichten bei nicht vorsätzlichen Verletzungen der Datensicherheit vorsieht.

- *SVV* argumentiert zu Art. 18 Abs. 1 Bst. a, dass nur absichtlich ausgelöste Systemunterbrüche meldepflichtig sein sollten, in Art. 18 Abs. 2 ergänzt werden soll, dass eine Manipulation oder ein Abfluss von Informationen vorliegt, wenn geschäftsrelevante Informationen von Unbefugten verändert, offengelegt, und hierbei «entwendet, zerstört, deaktiviert oder sonst wie bearbeitet werden, welche sich mittel- oder langfristig auf wesentliche Applikationen oder Systeme auswirken». Und Art. 18 Abs. 2 Bst. c durch die Einfügung eines letzten Teilsatzes «welche voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt» ergänzt werden soll.

- *Swiss Banking* und *Swiss FS-CSC* schlagen vor, die Formulierungen zu präzisieren, um den Fokus konsequent auf Cyberangriffe zu beschränken und weitere Aspekte wie den Datenschutz wegzulassen.

❖ **Artikel 18 Absatz 3: 90-Tage-Frist**

- *ZH* regt an, dass eine grundsätzliche Regelung wünschenswert wäre, die sich darüber ausspricht, welche Logdaten wie lange aufbewahrt werden dürfen.

❖ **Artikel 18 Absatz 4: Meldepflicht bei Erpressung, Drohung oder Nötigung**

- *BE* schlägt vor, die Meldepflicht bei Erpressung, Drohung oder Nötigung entweder direkt auf die ehemaligen Verantwortlichen oder Mitarbeitenden der Meldepflichtigen auszudehnen oder auf diese Personengruppe ganz zu verzichten.

- *SBB* beantragen, die Reichweite von Art. 18 Abs. 4 einzugrenzen, sodass nur strafrechtlich relevante und glaubwürdige Cyberangriffe gemeldet werden müssen.

❖ **Weitere Anmerkungen zu Artikel 18**

- *BA* plädiert dafür, dass das BACS Cyberangriffe, die möglicherweise Straftaten darstellen, automatisch den Strafverfolgungsbehörden meldet.

- *ISSS* kritisiert, dass die verschiedenen Absätze keine Begriffe wie «insbesondere» oder ähnliche Formulierungen enthalten, die eine nicht abschliessende Aufzählung andeuten würden.

- *Die Mitte* hält fest, dass der Adressatenkreis eine ausreichende Grösse haben muss, damit die Meldepflicht ihre volle Wirkung entfalten kann.

- *SH* kritisiert, dass Art. 18 zu kurz formuliert sei und die Meldepflicht selbst nicht explizit erwähnt werde.

- *UR* argumentiert, dass einwohnermässig kleinere Gemeinden, die in einen der zwei Rechenzentrumsverbunde eingebunden sind, nicht von einer Meldepflicht enthoben werden sollten.

- *SSK* schlägt vor, einen neuen Absatz 5 hinzuzufügen, der das BACS verpflichtet, zumindest Fälle im Sinne von Absatz 4 den zuständigen Strafverfolgungsbehörden zur Anzeige zu bringen.

- *swissuniversities* weist darauf hin, dass die Meldungen der Hochschulen an das BACS mit SWITCH-CERT koordiniert werden müssen.

3.3.2.19 Artikel 19 (Inhalt der Meldung)

Art. 19 Inhalt der Meldung

[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;
d. Angriffsmethode; und
e. Angaben zum Verursacher.

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

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

a. betroffene Einheiten der Organisation oder Behörde;
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.

[4] Erfolgt die Meldung nicht über das Kommunikationssystem des BACS, so muss sie zusätzlich folgende Informationen zur meldepflichtigen Behörde oder Organisation enthalten:

a. Firma, Name oder Bezeichnung und Adresse; und
b. Kontaktangaben der meldenden Person.

30 Vernehmlassungsteilnehmende haben sich zum Inhalt der Meldung geäussert und niemand hat diese Bestimmung vollständig abgelehnt.

❖ **Artikel 19 Absatz 1: Inhalt der Meldung**

- Von zahlreichen Vernehmlassungsteilnehmern wurden Präzisierungen zum *Umfang und Art der zu meldenden Informationen* im Verordnungstext verlangt:

    - *BE* und *NFP 77 ETHZ UNIL* schlagen vor, «Angaben zum Verursacher» durch «Angaben zum Angreifer» zu ersetzen.

    - *GE* empfiehlt, in Art. 19 Abs. 1 Bst. e «lorsqu'elles sont disponibles» am Ende des Absatzes hinzuzufügen.

    - *ZH* empfiehlt zur Berücksichtigung von Angriffen auf die Lieferkette und zur angemessenen Beurteilung der nationalen Bedrohungslage durch das BACS, den Inhalt der Meldung um «involvierte Dienstleister oder andere Dritte» zu ergänzen.

    - *Migros* schlägt vor, die Punkte «Art des Angriffs» und «Angriffsmethode» zusammenzufassen.

    - *VSE* schlägt vor, «angegriffene Systeme» in die Liste der zu meldenden Informationen aufzunehmen.

    - *FDP* kritisiert den detaillierten Informationskatalog als zu umfangreich und schwer verständlich.

    - *Swiss Banking* und *Swiss FS-CSC* empfehlen, den Artikel zu ergänzen, um die Anforderungen an den Inhalt der Meldung zu flexibilisieren und auf das Wissen abzustellen, welches vernünftigerweise vorhanden sein kann.

    - *CH Post AG* und *digitalswitzerland* sehen die Angaben zum Verursacher der Cyberattacke als problematisch an und schlagen vor, diese nur zu verlangen, falls sie ohne aufwändige forensische Verfahren ermittelt werden können.

    - *NEDIK* weist darauf hin, dass bei der Meldung die Klassifizierung für die Weitergabe der Information fehlt und empfiehlt, diese von Anfang an eindeutig festzulegen.

    - *Primeo* schlägt vor, als zusätzlichen Punkt der Meldepflicht aufzuführen, welcher OT-Bereich von einem Angriff betroffen ist.

    - *Swissgrid* schlägt vor, die Angaben zum Verursacher nur «sofern bekannt» zu verlangen und zusätzlich Informationen zu den angegriffenen Systemen in die Meldung aufzunehmen.

- Zu den Aspekten des *Datenschutzes und der Personendaten* merken *asut, Salt, Switch* sowie *Sunrise* an, dass die Meldung auch Personendaten umfassen kann und empfehlen, die Abläufe so zu gestalten, dass Personendaten nur bei gesicherten Vorfällen weitergegeben werden müssen.

❖ **Artikel 19 Absatz 2: Zusätzliche Informationen**

- *GE* schlägt eine neue Formulierung vor, um das Verständnis zu erleichtern: «…des informations sur l'éventualité ou la réalité d'un chantage, ainsi que d'une dénonciation pénale».

- *NEDIK* hält fest, dass die Meldung auch beinhalten sollte, bei welcher Behörde Strafanzeige erstattet wurde.

- *SwissICT* empfiehlt, Art. 19 Abs. 2 CSV ersatzlos zu streichen bzw. diese Informationen im Meldeformular fakultativ abzufragen.

❖ **Artikel 19 Absatz 3: Auswirkungen des Cyberangriffs**

- *SSV* fragt nach dem Unterschied zwischen «hoch» und «schwerwiegend» im erläuternden Bericht und schlägt alternative Formulierungen vor.

- *Flughafen ZH* schlägt vor, dass die Meldung die Funktion der betroffenen Einheiten enthalten soll.

- *Swiss Banking* und *Swiss FS-CSC* schlagen vor, den Schweregrad des Angriffs pauschal mit leicht, mittel oder schwer zu qualifizieren.

- *economiesuisse* und *scienceindustries* fordern die Streichung von Art. 19 Abs. 3, da dieser über die gesetzlichen Vorgaben hinausgehe und zu starr sei.

- *VSE* hält zu Art. 19 Abs. 3 fest, dass sich dieser auf «betroffene Einheiten der Organisation oder Behörde» bezieht und daher «angegriffene Systeme» ebenfalls in der Meldung gemäss Art. 19 Abs. 1 enthalten sein sollen.

- *Migros* empfiehlt ebenfalls, diesen Absatz zu streichen, da die relevanten Informationen im Ernstfall stark kontextabhängig sind.

❖ **Artikel 19 Absatz 4: Meldeweg**

- *Flughafen ZH* schlägt vor, dass die Meldung für meldepflichtige Organisationen ausschliesslich über das Kommunikationssystem des BACS zu erfolgen hat und dass nicht meldepflichtige Unternehmen ebenfalls einen Cyberangriff an das BACS melden können.

- *GE* empfiehlt, einen neuen Buchstaben c in Absatz 4 hinzuzufügen, der die Kontaktdaten der für die Cybersicherheit zuständigen Einheit innerhalb der Organisation oder Behörde angibt

❖ **Allgemeine Anmerkungen zu Artikel 19**

- *LU* empfiehlt die Einführung von Meldungskategorien basierend auf den Auswirkungen des Ereignisses: Minor-Vorfall (keine Meldung oder optional), Medium-Vorfall (zwingende Meldung innerhalb einer Woche) und Major-Vorfall (zwingende Meldung innerhalb von 24 Stunden). Dies soll sicherstellen, dass dem BACS nur relevante Vorfälle gemeldet werden.

- *VS* schlägt vor, die Meldungen von Cyberangriffen beim BACS zu zentralisieren, um Mehrfachmeldungen an verschiedene Bundesstellen zu vermeiden.

- *FER* merkt an, dass die Bewertung der Folgen von Cyberangriffen subjektiv sein und von Organisation zu Organisation unterschiedlich ausfallen kann.

- *ISSS* schlägt vor, zwischen dem Inhalt der Erstmeldung und je nach Klassifizierung des Vorfalls zwischen weiteren Inhalten zu unterscheiden.

- *SBB* erachten die geforderten Informationen als teilweise unpraktikabel und unrealistisch und beantragen, den Artikel so anzupassen, dass eine Meldung auch ohne Vorhandensein aller Angaben gemacht werden kann.

- *SVV* empfiehlt eine Harmonisierung der Eintrittsschwelle für ISG-Meldungen mit DSG-Meldungen.

- *lughafen ZH* fordert, dass das BACS Informationen nicht ohne Zustimmung der meldepflichtigen Behörde oder Organisation an Strafverfolgungsbehörden und weitere Behörden weitergeben darf.

- *Switch* schlägt vor, die Bestimmung in mehrfacher Hinsicht zu konkretisieren, insbesondere durch die Festlegung einer zeitlichen Grenze und einer Grenze der Anzahl betroffener Personen.

3.3.2.20 Artikel 20 (Übermittlung der Meldung)

Art. 20 Übermittlung der Meldung
Falls die Meldung nicht über das Kommunikationssystem des BACS erfolgt, informiert dieses die Kontaktperson nach Artikel 13 Absatz 2 Buchstabe b über den Ein-gang und den Inhalt der Meldung.

5 Vernehmlassungsteilnehmende haben sich zur Übermittlung der Meldung geäussert. Keiner der Vernehmlassungsteilnehmenden hat den Artikel 20 abgelehnt. Die Stellungnahmen enthalten Vorschläge zur Ergänzung und Präzisierung des Artikels.

❖ **Meldung über Drittorganisationen**

- *Switch* schlägt vor, dass sich ein Unternehmen oder mehrere Unternehmen gemeinsam entscheiden können, Meldungen über eine spezialisierte Drittorganisation zu melden, welche auch die Incident Response unterstützt.

- *swissuniversities* empfiehlt, den Artikel 20 CSV um einen zusätzlichen Absatz zu ergänzen, der es einem oder mehreren Unternehmen ermöglicht, gemeinsam zu entscheiden, Vorfälle über eine spezialisierte Drittorganisation zu melden. Sie schlagen eine konkrete Formulierung für diesen Zusatz vor: «[2] Eine oder mehrere meldepflichtige Behörden oder Organisationen können beschliessen, den Meldeprozess einzeln oder gemeinsam an eine spezialisierte Drittorganisation auszulagern.»

❖ **Anonymität bei Meldungen**

- *economiesuisse, scienceindustries* und *digitalswitzerland* schlagen eine Anpassung der Formulierung vor, um die Anonymität von Drittmeldungen zu gewährleisten. Sie empfehlen ebenfalls eine Formulierung, die die Weitergabe von Kontaktangaben nur in Fällen erlaubt, in denen dies zum Schutz der Cybersicherheit erforderlich ist: «Falls ~~die~~ eine Meldung nicht über das Kommunikationssystem des BACS erfolgt, informiert dieses 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.»

3.3.2.21 Artikel 21 (Frist zur Erfassung der Meldung)

Art. 21 Frist zur Erfassung der Meldung
[1] Sind innerhalb der Meldefrist von 24 Stunden nicht alle erforderlichen Informationen bekannt, so gewährt das BACS der betreffenden Behörde oder Organisation eine Frist von 14 Tagen zur Ergänzung der Meldung.
[2] Liegen bis zum Ablauf der Frist nicht alle erforderlichen Informationen vor, so fordert das BACS die betreffende Behörde oder Organisation auf, diese umgehend zu ergänzen oder zu bestätigen, dass die Informationen nicht vorhanden sind.

10 Vernehmlassungsteilnehmende haben sich zur Frist und Erfassung der Meldung geäussert. Keiner der Vernehmlassungsteilnehmenden hat den Artikel 21 abgelehnt. Die Stellungnahmen enthalten Vorschläge zur Ergänzung und Präzisierung des Artikels.

❖ **24-Stunden-Frist für die Erstmeldung**

- *NFP 77 ETHZ UNIL* empfiehlt, die Formulierung «innerhalb von 24 Stunden nach der Entdeckung des Cyberangriffs» zu präzisieren, um das Verständnis für die meldepflichtigen Behörden und Organisationen zu erleichtern.

- *Switch* erachtet die Frist von 24 Stunden vor allem für kleinere Organisationen als einen unverhältnismässigen Aufwand. Es wird vorgeschlagen, dass sich die 24-Stunden-Frist auf Arbeitswochen und Bürozeiten bezieht.

- *Swissgrid* regt an, in der Verordnung zu präzisieren, dass die Meldung innerhalb von 24 Stunden nach der Entdeckung des Cyberangriffs zu erfolgen hat, oder einen direkten Verweis auf Art. 74*e* Abs. 1 ISG aufzunehmen.

- *swissuniversities* weist darauf hin, dass die Anforderungen an die 24-Stunden-Meldefrist für kleine Hochschulen grosse Herausforderungen in Bezug auf die Reife der bestehenden Prozesse sowie das eingesetzte oder erforderliche Personal darstellen.

❖ **14-Tage-Frist für Nachmeldungen**

- *LU* regt an, zu präzisieren, ob bei der erwähnten 14-tägigen Frist zur Ergänzung der Meldung Arbeitstage oder Wochentage gemeint sind.

- *SwissICT* empfiehlt, die 14-tägige Frist für Nachmeldungen zu verkürzen. Zudem wird angeregt, zu ergänzen, was das BACS mit den Informationen tut.

❖ **Anpassung der Fristen an internationale Standards**

- *economiesuisse* und *scienceindustries* plädieren dafür, dass man die Meldepflichten an internationalen Standards ausrichtet und dementsprechend die Fristen jenen der EU-NIS-2-Richtlinie anpasst (24 Stunden für eine Frühwarnung, 72 Stunden für die Meldung eines Vorfalls).

❖ **Rolle des BACS und Unterstützung bei der Informationssammlung**

- *eAHV/IV* schlägt vor, dass in Art. 21 CSV zur Geltung kommen sollte, dass die Sammlung von weiteren Informationen, die gegebenenfalls nicht unmittelbar erhoben werden können, im Austausch und mit der Unterstützung des BACS erfolgt.

❖ **Sanktionen bei Nichteinhaltung**

- *UR* stellt die Frage, welche Sanktionen vorgesehen sind, wenn eine betroffene Behörde die erforderlichen Informationen nicht liefert und der Meldepflicht ans BACS nicht nachkommt.

3.3.2.22 Artikel 22

Art. 22 Änderung anderer Erlasse Die Änderung anderer Erlasse wird im Anhang geregelt.

Es hat sich niemand zu Art. 22 geäussert.

3.3.2.23 Artikel 23

Art. 23 Diese Verordnung tritt am 1. Januar 2025 in Kraft.

10 Vernehmlassungsteilnehmende haben sich zum Inkrafttreten geäussert. Keiner der Vernehmlassungsteilnehmenden hat den Artikel 23 abgelehnt. Die Stellungnahmen verlangen ein späteres Inkrafttreten der Meldepflichterfordernis.

❖ **Forderung nach einer Übergangsfrist von mindestens 6 Monaten**

- *asut, Salt* und *Sunrise* schlagen eine Einführungsfrist von mindestens sechs Monaten vor, um den Unternehmen ausreichend Zeit für die Anpassung ihrer Prozesse und technischen Systeme zu geben.

❖ **Forderung nach einer Übergangsfrist von mindestens 9 Monaten**

- *SUISSEDIGITAL* fordert eine Übergangsfrist von mindestens 9 Monaten zwischen der Veröffentlichung des amtlichen Wortlauts der CSV und dem tatsächlichen Beginn der Meldepflicht.

❖ **Forderung nach einer Übergangsfrist von mindestens 12 Monaten**

- *FDP, Swiss Banking und Swiss FS-CSC* fordern eine Übergangsfrist von mindestens einem Jahr, vorzugsweise zwei Jahren, zwischen dem Vorliegen des finalen Wortlauts der Verordnung und ihrem Inkrafttreten.

- *SVV, CH Post AG, economiesuisse* und *scienceindustries* argumentieren, dass ein Inkrafttreten per 1. Januar 2025 zu früh sei, und fordern eine Umsetzungsfrist von mindestens einem Jahr nach der offiziellen Veröffentlichung der Verordnung.

3.3.2.24 Organisationsverordnung vom 7. März 2003 für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (OV-VBS)

Art. 15*a* Abs. 2 Einleitungssatz sowie Bst. f und h [2] Es nimmt insbesondere folgende Funktionen wahr: f. Es betreibt das nationale Einsatzteam für Computersicherheit (Computer Emergency Response Team [CERT]). h. Es vertritt die Schweiz zur technischen Analyse von Cyberbedrohungen und zur Bewältigung von Cybervorfällen in internationalen Gremien.

3 Vernehmlassungsteilnehmende haben sich zu den Änderungen der OV-VBS geäussert. Keiner der Vernehmlassungsteilnehmenden hat diese abgelehnt. Die Stellungnahmen enthalten Vorschläge zur Präzisierung und Anpassung des Artikels.

❖ **Umfang und Beschränkung der internationalen Mitwirkung des BACS**

- *ZH* regt an, den Umfang, in dem das BACS in den internationalen Gremien mitwirkt, genauer zu umschreiben und auf den Bereich Cybersicherheit zu beschränken. Es wird betont, dass der nationale und internationale Austausch der Strafverfolgungsbehörden zum präventiven Schutz vor Cyberbedrohungen und zur repressiven Bewältigung von Cybervorfällen nicht eingeschränkt werden darf.

- *SSK* fordert in Art. 15*a* Abs. 2 Bst. h OV-VBS eine genauere Definition des Umfangs, in dem das BACS die Gremienarbeit vornimmt, und eine Beschränkung auf den Bereich Cybersicherheit. Sie betont ebenfalls, dass der nationale und internationale Austausch der Strafverfolgungsbehörden präventiv zum Schutz vor Cyberbedrohungen sowie repressiv zur Bewältigung von Cybervorfällen durch diese Bestimmung nicht eingeschränkt werden darf.

❖ **Verschiebung und Vereinheitlichung der Aufgabenauflistung**

- *VS* regt an, die Aufgabenauflistung in Art. 15*a* OV-VBS in die CSV zu verschieben und das französische Akronym BACS bzw. seine englische Version NCSC in allen bestehenden Rechtsgrundlagen (ISG, ISV und CSV) zu verallgemeinern.

3.3.2.25 Verordnung über den Datenschutz vom 31. August 2022 (DSV)

Art. 41 Abs. 1 *Aufgehoben*

Es hat sich niemand zur Aufhebung von Art. 41 Abs. 1 DSV geäussert.

3.3.2.26 Weitere Bemerkungen

9 Vernehmlassungsteilnehmende haben in ihren Vernehmlassungen, ohne direkten Bezug auf den Verordnungstext zu machen, weitere Bemerkungen angeführt:

❖ **Zentrale Koordination durch das BACS**

- *Flughafen ZH* schlägt einen neuen Artikel vor, der vorsieht, dass eine Meldung an das BACS automatisch alle anderen Meldepflichten im Falle eines Cyberangriffs aufhebt. Das BACS soll als zentrale Koordinationsstelle fungieren und die Anfragen der Behörden koordinieren.

- *CH Post AG* regt an, dass das BACS sämtliche meldepflichtigen Vorfälle entgegennimmt und diese dann mit weiteren relevanten Behördenstellen koordiniert. Alternativ schlägt sie vor, dass sich die Behörden, an welche gemeldet werden muss, untereinander koordinieren.

- *digitalswitzerland* regt an, dass das BACS eine zentrale, koordinative Rolle bei der Meldepflicht einnehmen sollte, um Mehraufwand und Doppelspurigkeiten zu vermeiden.

- *economiesuisse* und *scienceindustries* bemängeln das Fehlen an Koordination bzw. Harmonisierung der multiplen Meldeverfahren bei Cyberangriffen und fordert Lösungen für eine Harmonisierung/Koordination der einzelnen Meldeverfahren.

- *Migros* betont die Wichtigkeit eines kooperativen Ansatzes bei der Umsetzung harmonisierter Meldepflichtverfahren und schlägt vor, weniger auf Formalismus und mehr auf die Stärkung eines partnerschaftlichen Dialogs zwischen Behörden und Vertretenden kritischer Infrastrukturen zu setzen.

- *Swico* begrüsst die Stärkung der Rolle des BACS als zentrale, koordinierende Stelle, vertritt aber auch die Ansicht, dass multiple Meldeverfahren zu harmonisieren sind.

❖ **Weitere Themen**

- *LU* verlangt eine klarere Definition des Begriffs «grosses Schadenspotenzial» im Zusammenhang mit der Bekämpfung der Cyberkriminalität als Element der Nationalen Cyberstrategie.

- *digitalswitzerland* schlägt vor, Anreize für ein proaktives Meldeverhalten bei Cyberschwachstellen zu setzen und eine Liste spezifischer Kriterien für die Priorisierung von Meldungen zu erstellen.

- Da *Beat Lehmann* keine spezifischen Kommentare zu einzelnen Artikeln und Absätzen der Verordnung gemacht hat, werden seine Vorschläge und Empfehlungen nachfolgend thematisch wiedergegeben:

    - *Meldepflichten*: Er empfiehlt, verschiedene Situationen zu beachten, wie Massenauftritt von Störungen, Meldepflicht bei Auftragsbearbeitung und bei verbundenen Unternehmen. Des Weiteren schlägt er eine Harmonisierung der unterschiedlichen Meldepflichten nach verschiedenen Gesetzen vor und empfiehlt die Koordination von Meldepflichten bei grenzüberschreitenden Cyberangriffen. Weiter schlägt er vor, dass das BACS die Kompetenz erhält, Merkblätter oder Richtlinien zu typischen Fallgruppen herauszugeben.

    - *Dynamische Bedrohungen*: Er weist auf mögliche Störungen der IT-Infrastruktur durch ausländische Staaten oder deren Agenten hin. Hierbei betont er die Gefahr von Cyberangriffen als Teil hybrider Kriegführung und gezielter Desinformation und hebt hervor, dass nicht nur die klassische Datenverarbeitung, sondern auch Betriebstechnologie (OT) und SCADA-Systeme Ziele von Cyberangriffen werden können. Er betont die Schlüsselrolle der künstlichen Intelligenz für die Entwicklung von Mitteln und Verfahren von Cyber-Attacken und deren Abwehr.

    - *Internationale Zusammenarbeit*: Er empfiehlt, die Möglichkeit zur internationalen Zusammenarbeit des BACS mit OECD, EU / ENISA, NATO hervorzuheben.

    - *Public-Private Partnership*: Er schlägt vor, dass das erweiterte ISG und die CSV die Grundlage für eine umfassende «Public-Private Partnership» der staatlichen Behörden aller Stufen, der Wirtschaft und Wissenschaft bilden sollten.

4 Anhang

4.1 Kantone

AG	Staatskanzlei des Kantons AG	Regierungsgebäude 5001 Aarau
AI	Ratskanzlei des Kantons AI	Marktgasse 2 9050 Appenzell
BE	Staatskanzlei des Kantons Bern	Postgasse 68 3000 Bern 8
BL	Landeskanzlei des Kantons Basel-Landschaft	Regierungsgebäude Rathausstrasse 2 4410 Liestal
BS	Staatskanzlei des Kantons Basel-Stadt	Marktplatz 9 4001 Basel
FR	Staatskanzlei des Kantons Freiburg	Rue des Chanoines 17 1701 Fribourg
GE	Chancellerie d'Etat du Canton de Genève	Rue de l'Hôtel-de-Ville 2 Case postale 3964 1211 Genève 3
GL	Staatskanzlei des Kantons GL	Rathaus 8750 Glarus
GR	Standeskanzlei des Kantons GR	Reichsgasse 35 7001 Chur
LU	Staatskanzlei des Kantons LU	Bahnhofstrasse 15 6002 Luzern
NW	Staatskanzlei des Kantons NW	Dorfplatz 2 Postfach 1246 6371 Stans
OW	Staatskanzlei des Kantons OW	Rathaus 6061 Sarnen
SG	Staatskanzlei des Kantons SG	Regierungsgebäude 9001 SG
SH	Staatskanzlei des Kantons SH	Beckenstube 7 8200 Schaffhausen
SO	Staatskanzlei des Kantons SO	Rathaus Barfüssergasse 24 4509 Solothurn
SZ	Staatskanzlei des Kantons SZ	Regierungsgebäude Bahnhofstrasse 9 Postfach 1260 6431 Schwyz
TG	Staatskanzlei des Kantons Thurgau	Regierungsgebäude Zürcherstrasse 188 8510 Frauenfeld
TI	Cancelleria dello Stato del Cantone Ticino	Piazza Governo 6 6501 Bellinzona
UR	Standeskanzlei des Kantons Uri	Rathausplatz 1 6460 Altdorf
VD	Chancellerie d'Etat du Canton de Vaud	Place du Château 4 1014 Lausanne

VS	Chancellerie d'Etat du Canton du Valais	Planta 3 1950 Sion
ZG	Staatskanzlei des Kantons Zug	Seestrasse 2 Regierungsgebäude am Postplatz 6300 Zug
ZH	Staatskanzlei des Kantons ZH	Neumühlequai 10 Postfach 8090 Zürich

4.2 Kantonale Konferenzen und Eidgenössische Kommissionen

BFK	Eidgenössisches Büro für Konsumentenfragen	Eidgenössisches Büro für Konsumentenfragen (BFK) Bundeshaus Ost 3003 Bern
KKJPD	KKJPD Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD)	Haus der Kantone Speichergasse 6 Postfach 3001 Bern
SSK	Schweizerische Staatsanwälte-Konferenz	Haus der Kantone Speichergasse 6 Postfach 3001 Bern

4.3 In der Bundesversammlung vertretene politische Parteien

Die Mitte		Generalsekretariat Hirschengraben 9 Postfach 3001 Bern
FDP	FDP. Die Liberalen	Generalsekretariat Neuengasse 20 Postfach 3001 Bern
SP	Sozialdemokratische Partei der Schweiz SP	Zentralsekretariat Theaterplatz 4 Postfach 3001 Bern

4.4 Gesamtschweizerische Dachverbände der Gemeinden, Städte und Berggebiete

SGV	SGV	Holzikofenweg 8 Postfach 3001 Bern
SSV	SVV (SSV)	Monbijoustrasse 8 Postfach 3001 Bern

4.5 Gesamtschweizerische Dachverbände der Wirtschaft

econo-mie-suisse	Verband der Schweizer Unternehmen	Hegibachstrasse 47 Postfach 8032 Zürich
SGB	Schweizerischer Gewerkschaftsbund	Monbijoustrasse 61 3007 Bern
sgv/usam	Schweizerischer Gewerbeverband	Schwarztorstrasse 26 Postfach 3001 Bern
Swiss Banking	Schweizerische Bankiervereinigung	Aeschenplatz 7 Postfach 4182 4002 Basel

4.6 Weitere interessierte Kreise

ASIP	Schweizerischer Pensionskassenverband	Kreuzstrasse 26 8008 Zurich
asut	Schweizerischer Verband der Telekommunikation	Hirschengraben 8 3011 Bern
BA	BA BA	Guisanplatz 1 3003 Bern
Beat Lehmann		Acting Counsel RioTinto / Alcan Holdings Switzerland AG Kongoweg 9 (Home Office) 5034 Suhr
digital-switzer-land	digitalswitzerland	Waisenhausplatz 14 3011 Bern
eAHV/IV		p.a. mundi consulting ag Marktgasse 55 Postfach 3001 Bern
FAMH	Verband der medizinischen Laboratorien der Schweiz (FAMH)	Altenbergstrasse 29 Postfach 686 3000 Bern 8
FER	Fédération des Entreprises Romandes (FER)	98 rue de Saint-Jean 1211 Genève 11
Flughafen GE		Aéroport international de Genève CP100 CH 1215 Genève
Flughafen ZH		Flughafen Zurich AG 8058 Zürich Flughafen
H+	H+ Die Spitäler der Schweiz	Geschäftsstelle Lorainestrasse 4A 3013 Bern
ISSS	Information Security Society Switzerland	Kochergasse 6 3011 Bern
Migros	Migros	Migros Direktion Wirtschaftspolitik

		Limmatstrasse 152 Postfach 1766 8031 Zürich
NEDIK	NEDIK (Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung), zugeordnet zur KKPKS/KKJPD	c/o Generalsekretariat KKJPD Haus der Kantone Speichergasse 6 Postfach 3001 Bern
NFP 77 ETHZ UNIL	Gemeinsame Stellungnahme	
Piraten-partei Schweiz	Piratenpartei Schweiz	Piratenpartei Bern 3000 Bern
Post CH AG	Post CH AG	Wankdorfallee 4 Postfach 3030 Bern
Pour Demain	Pour Demain	Marktgasse 46 3011 Bern
Primeo		Weidenstrasse 27 4142 Münchenstein
RAILplus AG	RAILplus AG	Bahnhofstrasse 85 5001 Aarau
Salt		Salt Mobile SA Rue du Caudray 4 1020 Renens 1
SBB		SBB AG Public Affairs and Regulation Hilfikerstrasse 1 3000 Bern 65
science-industries	Wirtschaftsverband Chemie Pharma Life Sciences	Nordstrasse 15 Postfach 8021 Zürich
Suissedi-gital	Verband für Kommunikationsnetze	Bollwerk 15 3011 Bern
Sunrise		Sunrise GmbH Thurgauerstrasse 101B 8152 Glattpark (Opfikon)
SUVA		Fluhmattstrasse 1 Case postale 4358 6004 Luzern
SVV	Schweizerische Versicherungsverband	Conrad-Ferdinand-Meyer-Strasse 14 Case postale 8022 Zürich
Swico	Swico	Lagerstrasse 33 8004 Zürich
Swiss FS-CSC	Swiss Financial Sector Cyber Security Centre (Swiss FS-CSC)	Aeschenplatz 7 Postfach 4182 4002 Basel
Swissgrid		Bleichemattstrasse 31 Postfach 5001 Aarau

Swiss-ICT	SwissICT	Vulkanstr. 120 8048 Zürich
swiss-universi-ties	Dachorganisation der Schweizer Hochschulen	swissuniversities Effingerstrasse 15 Case Postale 3001 Bern
Switch		Werdstrasse 2 Postfach 8021 Zürich
Transit-gas	Transitgas AG	Franklinstrasse 27 8050 Zürich
CH++	Verein CH++	Sattelgasse 4 4051 Basel
VSE	Verband Schweizerischer Elektrizitätsunternehmen	Hintere Bahnhofstrasse 10 5000 Aarau