



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS

Bern, 1. April 2025

Verordnung über die Cybersicherheit

Cybersicherheitsverordnung (CSV) Erläuterungen

Übersicht

Mit der Einführung einer Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen stärkt die Schweiz ihre Cybersicherheitsstrategie. Die Verordnung über die Cybersicherheit (CSV) präzisiert die Umsetzung der jüngsten Gesetzesänderung und schafft klare Regeln für den Informationsaustausch und die Prävention. Ziel ist es, das Bundesamt für Cybersicherheit (BACS) in die Lage zu versetzen, rascher und gezielter auf Bedrohungen zu reagieren, frühzeitig zu warnen und den Schutz kritischer Infrastrukturen zu gewährleisten.

Ausgangslage

Mit der Änderung des Informationssicherheitsgesetzes (ISG, SR 128) vom 29. September 2023 (BBl 2023 2296) hat das Parlament die Einführung einer Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen beschlossen. Die Meldepflicht soll es dem BACS ermöglichen, eine verbesserte Übersicht über Cyberangriffe in der Schweiz zu gewinnen, Betroffene bei der Bewältigung von Cyberangriffen zu unterstützen und Betreiberinnen kritischer Infrastrukturen frühzeitig zu warnen.

Die CSV enthält die für den Vollzug dieser Gesetzesänderung erforderlichen Ausführungsbestimmungen und regelt insbesondere die Ausnahmen von der Meldepflicht. Der Bundesrat hat am 22. Mai 2024 die Vernehmlassung zur CSV eröffnet. Diese dauerte bis am 13. September 2024.

Inhalt der Vorlage

Die Verordnung über die Cybersicherheit enthält neben den Ausführungsbestimmungen zur Meldepflicht auch eine Bestimmung über die Nationale Cyberstrategie (NCS), und Bestimmungen über die Aufgaben des BACS und den Informationsaustausch des BACS mit Behörden und Organisationen.

Inhaltsverzeichnis

1	Ausgangslage	5
2	Rechtsvergleich, insbesondere mit dem europäischen Recht	6
3	Grundzüge der Vorlage	6
4	Erläuterungen zu einzelnen Artikeln	7
4.1	Art. 1.....	7
4.2	Art. 2 - Nationale Cyberstrategie.....	8
4.3	Art. 3 - Halterabfragen	10
4.4	Art. 4 - Technische Analyse von Cybervorfällen und Cyberbedrohungen	11
4.5	Art. 5 - Priorisierung der Beratung und Unterstützung bei Cyberangriffen	12
4.6	Art. 6 - Offenlegung von Schwachstellen.....	13
4.7	Art. 7 - Unterstützung von Behörden	16
4.8	Art. 8 - Kommunikationssystem für den sicheren Informationsaustausch und Informationssysteme für den automatischen Austausch	16
4.9	Art. 9 - Registrierung	18
4.10	Art. 10 - Dienstleister	19
4.11	Art. 11 - Übermittlung und Nutzung der Informationen	20
4.12	Art. 12 - Ausnahmen von der Meldepflicht.....	22
4.13	Art. 13 - Einreichung von Unterlagen zur Abklärung der Meldepflicht	28
4.14	Art. 14 - Zu meldende Cyberangriffe.....	28
4.15	Art. 15 - Inhalt der Meldung	31
4.16	Art. 16 - Frist zur Erfassung der Meldung	34
4.17	Art. 17 - Übermittlung der Meldung.....	34
4.18	Art. 19 - Inkrafttreten	35
4.19	Änderung anderer Erlasse	35
4.19.1	Art. 15a Abs. 2 Bst. f Organisationsverordnung vom 7. März 2003 für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (OV-VBS)	35
4.19.2	Art. 15a Abs. 2 Bst. h Organisationsverordnung vom 7. März 2003 für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (OV-VBS)	35
4.19.3	Art. 41 Abs. 1 Verordnung über den Datenschutz vom 31. August 2022 (DSV)	36
5	Auswirkungen	36
5.1	Auswirkungen auf den Bund	36
5.2	Auswirkungen auf Kantone und Gemeinden sowie auf urbane Zentren, Agglomerationen und Berggebiete	37
5.3	Auswirkungen auf die Volkswirtschaft.....	37

5.4	Auswirkungen auf die Gesellschaft.....	37
5.5	Auswirkungen auf die Umwelt.....	37
6	Rechtliche Aspekte.....	37
6.1	Verfassungsmässigkeit	37
6.2	Vereinbarkeit mit internationalen Verpflichtungen der Schweiz.....	38
6.3	Erlassform	38
6.4	Einhaltung der Grundsätze des Subventionsgesetzes	38
6.5	Delegation von Rechtsetzungsbefugnissen	38
6.6	Datenschutz	39

1 Ausgangslage

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 2020¹ zuhanden des Parlaments. In der Folge hiess das Parlament die Änderungen des ISG am 29. September 2023 gut²; die Referendumsfrist verstrich am 18. Januar 2024 unbenutzt.

Die vorliegende Verordnung 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.

Das Informationssicherheitsgesetz 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 wurde zudem die Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV) vom 27. Mai 2020³ ausser Kraft gesetzt.⁴ Die darin enthaltenen Bestimmungen wurden teilweise in das revidierte ISG überführt (insbesondere Begriffsdefinitionen). Jene Bestimmungen, welche in der CyRV die Informatiksicherheit des Bundes regelten, wurden in die Verordnung über die Informationssicherheit in der Bundesverwaltung (Informationssicherheitsverordnung, ISV)⁵ 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 Grundlage erhalten hat. Zudem wurde am 1. Januar 2024 das NCSC in das BACS umgewandelt und im Eidgenössischen Department für Verteidigung, Bevölkerungsschutz und Sport (VBS) überführt. Aus diesem Grund finden sich daher organisationale Bestimmungen zum BACS in Artikel 15a Absatz 1 und Absatz 2 Buchstabe a–g OV-VBS⁶.

Die Aufgaben des BACS werden in der vorliegenden Verordnung – zusammen mit der Meldepflicht für Cyberangriffe auf kritische Infrastrukturen – präzisiert und konkreter umschrieben. Die künftige Verordnung über die Cybersicherheit (Cybersicherheitsverordnung, CSV) regelt somit in Ergänzung zur ISV die Aufgaben des BACS und die Meldepflicht für Cyberangriffe auf kritische Infrastrukturen. Sie regelt daher schwerge-

¹ [SR 128](#)

² [BBI 2023 2296](#)

³ [SR 120.73](#)

⁴ [AS 2023 735](#) (Anhang 2 Ziff. I).

⁵ [SR 128.1](#)

⁶ [SR 172.214.1](#)

wichtig das Verhältnis zwischen dem BACS und Adressaten ausserhalb der Bundesverwaltung, während die ISV die Aufgaben und Zuständigkeiten für die Informationssicherheit innerhalb der Bundesverwaltung definiert.

2 Rechtsvergleich, insbesondere mit dem europäischen Recht

Die Einführung einer Meldepflicht für Cyberangriffe in der Schweiz schliesst eine bestehende Lücke im nationalen Dispositiv der Cybersicherheit. Die Massnahme steht im Einklang mit internationalen Standards und trägt zur Harmonisierung mit den EU-Regelungen bei. Seit 2018 gilt in allen EU-Mitgliedstaaten eine Meldepflicht für Cybervorfälle gemäss der 2016 verabschiedeten NIS-Richtlinie (Richtlinie (EU) 2016/1148), die darauf abzielt, ein hohes Niveau der Netzwerk- und Informationssicherheit zu gewährleisten. Diese Cybersicherheitsrichtlinie wurde 2022 durch die NIS-2-Richtlinie (Richtlinie (EU) 2022/2555) ersetzt, welche die Meldepflicht ausbaut. Mit der Umsetzung der Meldepflichten in der CSV, demonstriert die Schweiz die Kohärenz ihrer Nationalen Cyberstrategie (NCS) mit der Cybersicherheitspolitik der EU.

3 Grundzüge der Vorlage

Die Verordnung über die Cybersicherheit enthält neben den Ausführungsbestimmungen zur Meldepflicht auch Bestimmungen über die NCS, die Aufgaben des BACS und den Informationsaustausch des BACS mit Behörden und Organisationen.

Nachfolgend findet sich eine kurze Erläuterung der Bestimmungen der Verordnung über die Cybersicherheit:

- Abschnitt 1 - Gegenstand (Art. 1): Der einleitende Artikel definiert den Regelungsbereich der Verordnung, wobei der Fokus auf der NCS, den Aufgaben des BACS, dem Informationsaustausch und der Meldepflicht liegt.
- Abschnitt 2 - Nationale Cyberstrategie (Art. 2): Diese Bestimmung etabliert den strategischen Rahmen für die Cybersicherheit in der Schweiz. Die NCS wird partizipativ mit Vertretungen aus verschiedenen Bereichen erarbeitet.
- Abschnitt 3 - Aufgaben des BACS (Art. 3-7): Das BACS erhält weitreichende Kompetenzen für die operative Cybersicherheit. Dies umfasst Halterabfragen bei Domain-Namen, den Betrieb eines nationalen Einsatzteams für Computersicherheit und die koordinierte Offenlegung von Schwachstellen. Bei Ressourcenengpässen kann das BACS seine Unterstützungsleistungen nach Art. 74 Abs. 3 ISG priorisieren.
- Abschnitt 4 - Informationsaustausch (Art. 8-11): Die Verordnung konkretisiert die Grundlagen für einen sicheren Informationsaustausch zwischen dem BACS und relevanten Behörden und Organisationen. Es werden sichere Kommunikationssysteme bereitgestellt und klare Registrierungspflichten definiert. Auch Cybersicherheit-Dienstleister der kritischen Infrastrukturen können am Informationsaustausch teilnehmen.

Diese Verordnung regelt in den Artikeln 8–11 den Informationsaustausch zwischen dem BACS und den Behörden und Organisationen zum Schutz vor Cybervorfällen und Cyberbedrohungen über aktuelle Vorfälle, Bedrohungen und Angriffe im Bereich der Cybersicherheit. Es werden hierbei die Vorgaben, die Zuständigkeiten und Verantwortlichkeiten sowohl für das Kommunikationssystem für den sicheren Informationsaustausch als auch für das Informationssystem für den automatischen Austausch festgelegt, um sicherzustellen, dass relevante Informationen schnell und effektiv an die richtigen Stellen weitergeleitet werden können.

Bst. d: Meldepflicht bei Cyberangriffen

In der Vernehmlassung zur Ergänzungsrevision des ISG wurde wiederholt gefordert, dass die Bestimmungen zur Meldepflicht bei Cyberangriffen auf kritische Infrastrukturen auf Verordnungsstufe konkretisiert werden sollen. Diesem Anliegen, das bereits in der Botschaft zur Änderung des Informationssicherheitsgesetzes⁹ mehrfach erwähnt wurde, soll mit den Artikeln 12–17 in der vorliegenden Verordnung Rechnung getragen werden. So werden insbesondere die Details der Meldepflicht geregelt, d.h. welche Behörden und Organisationen von der Meldepflicht ausgenommen sind, welche Cyberangriffe gemeldet werden müssen, was der Inhalt und der Umfang der Meldungen und der Ablauf des Meldeprozesses ist.

Erwähnenswert mit Blick auf die in diesem Artikel enthaltene Aufzählung des Regelungsgegenstandes ist, dass sämtliche Vorgaben zur Cybersicherheit der Bundesverwaltung, die Zuständigkeiten und Aufgaben der Fachstelle des Bundes für Informationssicherheit und die sich daraus ergebenden Schnittstellen zu den Aufgaben des BACS in der ISV geregelt werden.

Ebenfalls nicht von der Cybersicherheitsverordnung werden die Massnahmen der Cyberverteidigung geregelt. Letztere betreffen die militärischen und nachrichtendienstlichen Massnahmen und umfassen insbesondere die in Artikel 37 des Nachrichtendienstgesetzes¹⁰ vorgesehenen aktiven Massnahmen zur Störung und Verlangsamung von Cyberangriffen. Sie betreffen auch die Massnahmen der Armee zur Gewährleistung ihrer Einsatzbereitschaft in allen Lagen und zur Bereitstellung von Fähigkeiten zur subsidiären Unterstützung der zivilen Behörden. Diese Massnahmen sind im Nachrichtendienstgesetz und im Militärgesetz¹¹ sowie in den dazugehörigen Verordnungen geregelt.

4.2 Art. 2 - Nationale Cyberstrategie

Die Bestimmungen zur nationalen Cyberstrategie waren bis Ende 2023 in Artikel 5 der aufgehobenen CyRV geregelt. Der vorliegende Artikel knüpft an die damalige Regelung an und verpflichtet den Bundesrat, die Ziele und Massnahmen im Bereich des Schutzes vor Cyberrisiken in der Nationalen Cyberstrategie (NCS) festzulegen. Innerhalb der Bundesverwaltung ist gemäss Artikel 15a Absatz 2 Buchstabe g OV-VBS das

⁹ [BBI 2023 84](#).

¹⁰ [SR 121](#)

¹¹ [SR 510.10](#)

BACS zuständig, die NCS für den Bundesrat zu erarbeiten und deren Umsetzung zu koordinieren.

Die NCS bildet gemäss *Absatz 1* den strategischen Rahmen für die Prävention im Bereich der Cybersicherheit, der Früherkennung von Cyberbedrohungen, die Reaktionsmöglichkeiten und der Resilienz bei Vorfällen zum Schutz des Landes vor Cybervorfällen und Cyberbedrohungen. Dies bedeutet, dass die NCS einen umfassenden Ansatz zur Bewältigung von Cybervorfällen und Cyberbedrohungen verfolgt, der verschiedene Aspekte der Cybersicherheit umfasst:

- *Prävention im Bereich der Cybersicherheit*: Die Prävention bezieht sich auf Massnahmen, die ergriffen werden, um potenzielle Schwachstellen und Angriffsmethoden zu identifizieren und zu minimieren. Dies kann durch die Implementierung von Sicherheitsrichtlinien, Schulungen für Mitarbeiter, Sicherheitsaudits und den Einsatz von Sicherheitstechnologien geschehen.
- *Früherkennung von Cyberbedrohungen*: Die Früherkennung von Cyberbedrohungen beinhaltet die Fähigkeit, Anzeichen von Cybervorfällen und Cyberbedrohungen frühzeitig zu erkennen. Dies beinhaltet die Kontrolle von Netzwerken und Systemen auf verdächtige Aktivitäten und die Implementierung von Technologien zur Erkennung von Vorfällen und Bedrohungen.
- *Reaktionsmöglichkeiten bei Vorfällen*: Reaktionsmöglichkeiten bei Vorfällen bezieht sich auf die Fähigkeit, angemessen auf Cybervorfälle sowie Cyberbedrohungen zu reagieren, sobald diese erkannt werden. Dies kann die Aktivierung des nationalen Einsatzteams für Computersicherheit, die Einleitung von Gegenmassnahmen und die Zusammenarbeit mit anderen Behörden oder Organisationen zur Bewältigung des Vorfalls oder der Bedrohung umfassen.
- *Resilienz bei Vorfällen*: Resilienz bezieht sich mitunter auf die Geschwindigkeit, mit der sich ein System nach einem Cyberangriff wiederherstellen kann. Dies umfasst beispielsweise die Implementierung von Backup-Systemen, Notfallplänen und anderen Massnahmen zur Minimierung der Auswirkungen eines Angriffs.
- *Bekämpfung der Cyberkriminalität*: Die über das Internet verfügbare digitale Infrastruktur eröffnet potenziellen Straftätern und Straftäterinnen neuartige Möglichkeiten mit grossem Schadenspotenzial für Gesellschaft und Wirtschaft. Cyberkriminalität überschreitet territoriale Grenzen, und dies in einem hochdynamischen Prozess mit kurzen Innovationszyklen. Je stärker die digitale Vernetzung ist, desto grösser wird die Gefahr, dass Cybervorfälle zwar in der virtuellen Welt beginnen, aber ihre schädigende Wirkung in der realen Welt entfalten. Vor dem Hintergrund dieser Entwicklung ist es wichtig, gesamtschweizerisch und in Zusammenarbeit mit internationalen Partnern die Interoperabilität und Reaktionsfähigkeit weiter zu verbessern sowie die fachlichen, technischen und personellen Kompetenzen wirksam aufeinander abzustimmen, ohne dabei die Befugnisse zwischen den verschiedenen Behörden und Staatsebenen zu verschieben.

- *Internationale Zusammenarbeit:* Angesichts der grenzüberschreitenden Natur von Cyberbedrohungen ist es unerlässlich, dass Staaten, internationale Organisationen und private Akteure eng zusammenarbeiten. Im Rahmen der NCS fördert die Schweiz den Austausch von Informationen über Cyberrisiken und Bedrohungen, die gemeinsame Entwicklung von Standards und Best Practices sowie die gegenseitige Unterstützung bei Cybervorfallbewältigung und Prävention. Damit trägt die Schweiz zur Stärkung der globalen Cybersicherheit bei, während sie gleichzeitig ihre eigene Resilienz verbessert und ihre Interessen in der digitalen Welt schützt.

Die NCS legt den Rahmen für diese verschiedenen Aspekte fest und koordiniert die Anstrengungen auf nationaler Ebene gemäss Absatz 2. Mit einer umfassenden Strategie soll sichergestellt werden, dass die Schweiz als Ganzes besser gegen Cybervorfälle und Cyberbedrohungen geschützt ist und effektiv auf diese reagieren kann. Die erarbeitete NCS wird sodann dem Bundesrat vorgelegt und von diesem verabschiedet.

4.3 Art. 3 - Halterabfragen

Diese Bestimmung stützt sich auf Artikel 73a Absatz 1 und 2 Buchstabe a sowie Artikel 74 Absatz 1 und 2 Buchstabe a ISG.

Die Aufgabe des BACS betreffend die Warnung der Öffentlichkeit wurde bis Ende 2023 in Artikel 12 Absatz 1 Buchstabe h der aufgehobenen CyRV geregelt und ist seit dem 1. Januar 2024 in Artikel 15a Absatz 2 Buchstabe d und e OV-VBS aufgeführt.

Seit 2010 wird MELANI (Melde- und Analysestelle Informationssicherung), welche im Jahr 2020 vom NCSC und schliesslich seit Anfang dieses Jahres durch das BACS abgelöst wurde, vom Bundesamt für Kommunikation (BAKOM) als «eine zur Bekämpfung der Cyberkriminalität vom BAKOM anerkannte Stelle» gemäss Artikel 15 Absatz 3 VID¹² betrachtet.¹³ Da das BACS aber keine strafrechtlichen Kompetenzen oder Aufgaben hat, ist es nur indirekt mit der Cyberkriminalität befasst. Um die Zuständigkeit des BACS für die Abfrage von Kontaktangaben der Halter von Domain-Namen bei der Registerbetreiberin klarzustellen, wird diese Befugnis ausdrücklich in *Artikel 3* erwähnt (vgl. diesbezüglich Artikel 28e Buchstabe b FMG und Artikel 7 ff. VID).¹⁴ Die Möglichkeit, Kontaktangaben von Haltern von Domain-Namen abzufragen, ermöglicht es dem BACS, beispielsweise im Falle von akuten Cyberbedrohungen oder Cyberangriffen schnell und gezielt potenziell betroffene Parteien zu warnen und sie gegebenenfalls bei der Umsetzung von Gegenmassnahmen zu unterstützen. Diese Befugnis ist ein wichtiges Instrument zur Bekämpfung von Cyberbedrohungen sowie -angriffen und zur Stärkung der Cybersicherheit in der Schweiz.

¹² [SR 784.104.2](#)

¹³ Siehe hierzu die [Webseite des BAKOM «Bekämpfung der Internetkriminalität»](#).

¹⁴ Das BAKOM hat der Stiftung SWITCH die Zuteilung bzw. Verwaltung der .ch-Domain-Namen übertragen (vgl. [Art. 28a Abs. 1 Fernmeldegesetz vom 30. April 1997 \[FMG; SR 784.10\]](#) und [Art. 8 Abs. 2 i.V.m. Art. 33 VID vom 5. November 2014](#)), die SWITCH in einer RDDS-Datenbank (WHOIS) verwaltet. Das BACS hat eine Vereinbarung mit SWITCH abgeschlossen, die die Bekanntgabe der Domainhalter in der RDDS-Datenbank (WHOIS) im Abrufverfahren über den RDAP-Zugang regelt.

4.4 Art. 4 - Technische Analyse von Cybervorfällen und Cyberbedrohungen

Diese Bestimmung stützt sich auf Artikel 73a Absatz 1 und Absatz 2 Buchstabe a und e sowie Artikel 74 Absatz 3 i.V.m. Artikel 74a Absatz 3 ISG.

Die Aufgaben des nationalen Einsatzteams für Computersicherheit waren bis Ende 2023 in Artikel 12 Absatz 1 Buchstabe c der aufgehobenen CyRV geregelt. Dieses wird ab 1. Januar 2024 in Artikel 15a Absatz 2 Buchstabe f OV-VBS aufgeführt.

Absatz 1: Nationales Einsatzteam für Computersicherheit

Das BACS betreibt ein nationales Einsatzteam für Computersicherheit, das eine zentrale Rolle bei der Bewältigung von Cybervorfällen und Cyberbedrohungen in der Schweiz spielt. Dieses Einsatzteam ist spezialisiert auf die technische Vorfallbewältigung, die Analyse von technischen Fragestellungen sowie Identifikation und der Einschätzung von Cyberbedrohungen aus technischer Sicht.

Das nationale Einsatzteam für Computersicherheit des BACS unterstützt bei der technischen Bewältigung von Cybervorfällen (Bst. a), indem es betroffene Organisationen mit seinem spezialisierten Fachwissen berät und begleitet. Die Unterstützung durch das BACS erfolgt im Sinne einer Soforthilfe im Notfall. Bei den nach der Vorfallbewältigung nötigen Arbeiten zur Wiederherstellung der Daten und Wiederaufbau der Systeme unterstützt das BACS nur beratend.

Die Unterstützung des BACS bei der technischen Bewältigung von Vorfällen besteht in der technischen Analyse des Angriffs (Bst. b). Diese hat zum Ziel, möglichst rasch zu verstehen, welche Angriffsmethoden die Angreifer nutzen, welche Methoden und Taktiken sie anwenden und welche Ziele sie verfolgen. Diese Erkenntnisse ermöglichen es, geeignete Gegenmassnahmen zu bestimmen und umzusetzen. Das BACS arbeitet dabei eng mit den betroffenen Behörden und Organisationen und ihren allfälligen Sicherheitsdiensten zusammen. Es hilft zudem bei der Koordination zwischen den an der technischen Bewältigung beteiligten Akteuren. Bei Bedarf kann es auch direkt vor Ort bei der betroffenen Behörde oder Organisation Unterstützung leisten.

Das nationale Einsatzteam für Computersicherheit unterstützt Behörden und Organisationen auch präventiv. Es analysiert laufend neue technische Bedrohungen und Angriffsmethoden und identifiziert geeignete Gegenmassnahmen (Bst. c). Die technischen Einschätzungen der Bedrohungslage erfordern eine Kombination aus automatisierten Tools zur Analyse von Cybervorfällen und Cyberbedrohungen, dem Informationsaustausch mit nationalen und internationalen Fachstellen sowie menschlicher Expertise zur Interpretation der Ergebnisse. Die kontinuierliche Wahrnehmung dieser Einschätzungen ermöglicht es, proaktiv auf Gefahren zu reagieren, Sicherheitslücken zu schliessen und ihre Verteidigungsstrategien anzupassen, um sich gegen aktuelle und zukünftige Cybervorfälle und Cyberbedrohungen zu schützen.

Absatz 2: Resiliente Infrastruktur

Das BACS betreibt eine resiliente Infrastruktur, die unabhängig von der restlichen Informatik des Bundes funktionieren muss. Dies bedeutet, dass das BACS ein Leistungserbringer für diese spezifische Infrastruktur des nationalen Einsatzteams für Computersicherheit ist und daher über spezielle technische Ressourcen und Systeme verfügt, um Cybervorfälle und Cyberbedrohungen zu analysieren.

Die Notwendigkeit einer unabhängigen Infrastruktur ergibt sich aus der Sensibilität und Dringlichkeit von Cybervorfällen und Cyberbedrohungen. Da das BACS die nationale Anlaufstelle für Cybersicherheit ist, muss es auch bei einer Beeinträchtigung der Bundesinformatik in der Lage sein, zuverlässig Cybervorfälle und Cyberbedrohungen zu analysieren. Es versteht sich daher von selbst, dass der Grad der Widerstandsfähigkeit, den die Infrastruktur aufweisen muss, besonders hoch ist.

Diese unabhängige und resiliente Infrastruktur ermöglicht es dem BACS, seine Aufgaben effektiv zu erfüllen und sicherzustellen, dass die Schweiz auf Cybervorfälle und Cyberbedrohungen angemessen reagieren kann.

4.5 Art. 5 - Priorisierung der Beratung und Unterstützung bei Cyberangriffen

Diese Bestimmung stützt sich auf Artikel 74 Absatz 3 und Artikel 74a Absatz 3 ISG.

Allgemeines:

Artikel 74 Absatz 3 ISG sieht vor, dass das BACS die Betreiberinnen von kritischen Infrastrukturen bei der Bewältigung von Cybervorfällen und Cyberbedrohungen sowie bei der Behebung von Schwachstellen beraten und unterstützen kann. Dies unter der Voraussetzung, dass die Funktionsfähigkeit der betroffenen kritischen Infrastruktur gefährdet und, sofern es sich um private Betreiberinnen handelt, die Beschaffung gleichwertiger Unterstützung auf dem Markt nicht rechtzeitig möglich ist. Die Betroffenen entscheiden dabei selbst, ob sie die Unterstützung des BACS in Anspruch nehmen wollen.

Die Beratung und Unterstützung erfolgen hauptsächlich durch technische Analysen und Auskünfte zu technischen und organisatorischen Massnahmen. Durch die technischen Analysen soll die Ursache des Vorfalls identifiziert, das Ausmass der Kompromittierung verstanden und die potenziellen Schwachstellen bei den Informatikmitteln sowie dem Sicherheitssystem erkannt werden. Dies kann beispielsweise die Untersuchung von Systemprotokollen, Malware-Analysen sowie Auswertungen der Netzwerküberwachung umfassen. Neben den technischen Analysen bietet das BACS auch die Beratung zu organisatorischen Massnahmen an, um den Vorfall besser zu bewältigen. Da das BACS bei vielen Vorfällen involviert ist, kann es beispielsweise Hinweise geben, wie der Vorfall kommuniziert werden kann oder welche Notfallorganisation notwendig ist.

Absatz 1: Priorisierung der Beratungs- und Unterstützungsleistungen

Absatz 1 befasst sich mit der Situation, in der das BACS mit einer höheren Anzahl von Anfragen für Beratung und Unterstützung im Falle eines Cyberangriffs konfrontiert wird,

als es mit seinen vorhandenen Personal- und technischen Ressourcen und Kapazitäten bewältigen kann. In solch einem Szenario behält sich das BACS das Recht vor, Entscheidungen darüber zu treffen, welche Anfragen zuerst bearbeitet werden und wie umfangreich die Unterstützung ausfallen wird. In anderen weniger dringenden Fällen werden die Beratung sowie Unterstützung entsprechend zeitlich verzögert geleistet. Neben dem Zeitpunkt kann auch der Grad der zur Verfügung gestellten Hilfe variieren. Einige Fälle können eine vollständige Untersuchung und umfassende Unterstützung erfordern, während andere vielleicht nur eine grundlegende Beratung erhalten. Diese Bestimmung ermöglicht es dem BACS, in Zeiten hoher Auslastung strategische Entscheidungen darüber zu treffen, wie seine Ressourcen am besten eingesetzt werden können, um die grösstmögliche Hilfe zu leisten.

Absatz 2: Priorisierung unter Berücksichtigung öffentlicher Interessen

Das BACS unterstützt im Falle einer Vielzahl von zeitgleichen Cybervorfällen und Cyberbedrohungen vorrangig die meldepflichtigen Organisationen und Behörden, bei denen das Ereignis die grössten Auswirkungen auf die Sicherheit, die öffentliche Ordnung, das Wohlergehen der Bevölkerung oder das Funktionieren der Wirtschaft hat. Das bedeutet, dass das BACS seine Ressourcen und Unterstützung gezielt dort einsetzt, wo die Auswirkungen eines Ereignisses besonders gravierend sind. Dies kann beispielsweise bedeuten, dass kritische Infrastrukturen, Behördeneinrichtungen oder andere wichtige Organisationen priorisiert werden, um sicherzustellen, dass sie angemessen geschützt sind und im Falle eines Angriffs schnell Unterstützung erhalten. Die vom BACS vorgenommene Priorisierung berücksichtigt die Kritikalität der betroffenen Behörden oder Organisationen, insbesondere auf der Grundlage der vom BABS anerkannten kritischen Sektoren und Teilsektoren. Durch diese Priorisierung kann das BACS sicherstellen, dass diejenigen Einrichtungen und Organisationen, die für das Funktionieren von Gesellschaft und Wirtschaft am wichtigsten sind, im Falle von Cybervorfällen und Cyberbedrohungen angemessen geschützt werden. Dies trägt dazu bei, die Resilienz und Stabilität des Landes im Falle eines grossflächigen Ereignisses, das viele Ziele in der Schweiz betrifft, zu gewährleisten.

4.6 Art. 6 - Offenlegung von Schwachstellen

Diese Bestimmung stützt sich auf Artikel 73a Absatz 2 Buchstabe c sowie auf Artikel 73b Absatz 3 i.V.m. Artikel 73c Absatz 2 ISG.

Die Aufgaben des BACS im Zusammenhang mit der Schwachstellenkoordination waren in der CyRV nicht explizit geregelt, sondern durch die allgemeinen Aufgaben des BACS abgedeckt, welche seit dem 1. Januar 2024 neu in Artikel 15a Absatz 2 Buchstabe b OV-VBS aufgeführt sind. Zudem ist seit dem 1. Januar 2024 eine Rechtsgrundlage für die Schwachstellensuche in der Informatikinfrastruktur der Bundesverwaltung und der Armee in Artikel 43 Absatz 1 Buchstabe c ISV enthalten. Diese Bestimmung sieht vor, dass das BACS mitunter die Bundeskanzlei, die Generalsekretariate, Departemente und die Bundesämter über aktuelle Bedrohungen und Schwachstellen sowie über Risiken, die sie betreffen, informiert und bei Bedarf Massnahmen zur Risikominderung empfiehlt.

Die Wichtigkeit eines aktiven Schwachstellenmanagements und die Rolle des BACS bei der Suche und der koordinierten Offenlegung von Schwachstellen wird ausführlicher im Bericht des Bundesrats «Die Förderung des ethischen Hackings in der Schweiz»¹⁵ beschrieben.

Absatz 1: Koordiniert Offenlegung von Schwachstellen

Die koordinierte Offenlegung von Schwachstellen in Hard- und Software ist ein wichtiger Bestandteil der globalen Cybersicherheitsbemühungen, da sie es ermöglicht, potenzielle Sicherheitslücken in IT-Systemen zu analysieren, zu bewerten und zu beheben, bevor sie von Angreifern ausgenutzt werden können. Der Prozess der koordinierten Offenlegung zielt darauf ab, eine möglichst hohe Transparenz über Schwachstellen zu ermöglichen, ohne Sicherheitsrisiken zu erzeugen. Kernelement des Prozesses ist, dass nach dem Finden einer Schwachstelle zunächst die Hersteller informiert werden. Mit diesen vereinbaren die Hacker eine Sperrfrist, innerhalb derer sie keine Informationen zur Schwachstelle öffentlich verbreiten. Dies gibt den Herstellern genügend Zeit, die Schwachstelle zu beheben, bevor sie öffentlich gemacht wird. Dieser Prozess ist international etabliert und wird beispielsweise auch in der EU durch die NIS-2-Richtlinie (Art. 12 und 13) vorgeschrieben.¹⁶

Die Regeln für die koordinierte Offenlegung von Schwachstellen sind in der ISO/IEC Norm 29147:2018-10 festgelegt.¹⁷ Das BACS ist verpflichtet, gemeldete Schwachstellen gemäss den in dieser Norm festgelegten Regeln offenzulegen. Dies bedeutet, dass das BACS keine Schwachstellen geheim behält oder anderen Behörden weiterleitet, ohne die Hersteller zu informieren. Das BACS ist vielmehr verpflichtet, über den Prozess der koordinierten Offenlegung Massnahmen umzusetzen, die dazu führen, dass die Schwachstelle nicht mehr ausgenutzt werden kann.

Durch die Zusammenarbeit mit ausländischen und internationalen Fachstellen kann das BACS sicherstellen, dass Schwachstellen auf internationaler Ebene erkannt und behoben werden. Das BACS wurde im September 2021 von der US-Organisation MITRE als Fachstelle für Schwachstellen anerkannt und autorisiert, Schwachstellen gemäss dem Standard «Common Vulnerabilities and Exposure (CVE)» zur Kennzeichnung und Identifizierung eine CVE-Nummer zuzuweisen, damit bekannte Schwachstellen eine eindeutige Bezeichnung erhalten. Dies ermöglicht Sicherheitsexperten, Herstellern, Anwendern und Behörden, sich in einheitlicher Weise auf diese Schwachstelle zu beziehen. Durch die Verwendung von CVE-Nummern können Sicherheitslücken effektiver kommuniziert, dokumentiert und behoben werden. Die Verwendung eines stan-

¹⁵ Vgl. hierzu: [Bericht des Bundesrates vom 29. November 2023, Die Förderung des ethischen Hackings in der Schweiz, Bericht des Bundesrates in Erfüllung des Postulats 20.4594, Bellaiche, vom 17. Dezember 2020](#), Ziff. 4.2.4., S. 13 f.

¹⁶ NIS-2- Richtlinie. [Richtlinie \(EU\) 2022/2555 des europäischen Parlaments und des Rates vom 14. Dezember 2022 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung \(EU\) Nr. 910/2014 und der Richtlinie \(EU\) 2018/1972 sowie zur Aufhebung der Richtlinie \(EU\) 2016/1148 \(NIS-2-Richtlinie\)](#).

¹⁷ [ISO/IEC 29147:2018-10](#) (Ausgabedatum 2018-10), S. 14.

dardisierten Namensschemas erleichtert auch die Zusammenarbeit zwischen den verschiedenen Akteuren im Bereich der Cybersicherheit und trägt dazu bei, die Transparenz und Effektivität bei der Behandlung von Sicherheitslücken zu verbessern.

Absätze 2–4: Frist für Behebung der Schwachstelle

Das BACS verlangt von den Herstellern der von Schwachstellen betroffenen Hard- oder Software, eine Schwachstelle grundsätzlich innerhalb einer Frist von 90 Tagen zu beheben. Dies ist eine gängige Praxis in der Cybersicherheitsbranche.¹⁸ Die Frist lässt den Herstellern genügend Zeit für die Analyse der Schwachstellen und für die Entwicklung und Umsetzung von Gegenmassnahmen, stellt andererseits aber auch sicher, dass die Schwachstellen nicht übermässig lange bestehen bleiben.

Abhängig von der Kritikalität und der Komplexität einer Schwachstelle kann die entsprechende Frist verkürzt werden. Es ist aber auch möglich, die angesetzte Frist im Bedarfsfall zu verlängern (z. B. infolge eines hohen Aufwands für Gegenmassnahmen oder eines erhöhten Koordinationsbedarfs). Das BACS trägt dabei der Komplexität der Verwundbarkeit Rechnung.

Absatz 5: Bekanntgabe der Schwachstelle vor Behebung oder Veröffentlichung

Wenn dem BACS eine Schwachstelle bekannt ist, die für andere kritische Infrastrukturen eine akute Cyberbedrohung darstellt, informiert das BACS die Betreiberinnen, bevor die Schwachstelle veröffentlicht oder durch die Herstellerin der Hard- oder Software behoben wurde. Dieser Schritt ist wichtig, um die Betreiberinnen kritischer Infrastrukturen frühzeitig über potenzielle Sicherheitsrisiken zu informieren und ihnen die Möglichkeit zu geben, angemessene Massnahmen zum Schutz ihrer Systeme zu ergreifen. Durch den Austausch von Informationen über Schwachstellen können Betreiber kritischer Infrastrukturen proaktiv Massnahmen zur Risikominderung ergreifen, bevor die Schwachstellen öffentlich bekannt sind. Dies kann dazu beitragen, potenzielle Angriffe auf kritische Infrastrukturen zu verhindern oder abzuschwächen.

Absatz 6: Ausnahmeregelung für das BAKOM

Das BACS stellt gemäss *Absatz 6* sicher, dass das Bundesamt für Kommunikation (BAKOM) unverzüglich über entdeckte Schwachstellen in Fernmeldeanlagen nach Artikel 3 Buchstabe d des Fernmeldegesetzes vom 30. April 1997¹⁹ informiert wird. Durch die proaktive Weitergabe von Informationen trägt das BACS dazu bei, potenzielle Risiken frühzeitig zu minimieren und hilft mit, die Sicherheit sowie die Integrität der Fernmeldeinfrastruktur zu gewährleisten.

Absatz 7: Information des BAKOM

¹⁸ Vgl. [Leitlinie des deutschen Bundesamtes für Sicherheit in der Informationstechnik zum Coordinated Vulnerability Disclosure \(CVD\)-Prozess](#), Ziff. 3.3., S.10.

¹⁹ [SR 784.10](#)

Die Regelung der Absätze 1–4 findet gemäss *Absatz 7* keine Anwendung auf Schwachstellen, die das BAKOM im Rahmen seiner Aufsichtskontrollen gemäss den Artikeln 36–40 der Verordnung über Fernmeldeanlagen vom 25. November 2015²⁰ feststellt und dem BACS meldet. Das BACS wird seitens des BAKOM über diese Befunde informiert, um gegebenenfalls weitere technische Massnahmen zu koordinieren und die Cybersicherheit auf nationaler Ebene zu stärken.

4.7 Art. 7 - Unterstützung von Behörden

Diese Bestimmung stützt sich auf Artikel 73a Absatz 2 Buchstabe c ISG.

Das BACS unterstützt als Kompetenzzentrum des Bundes für Cybersicherheit die zuständigen Behörden des Bundes und der Kantone bei der Entwicklung, Umsetzung und Prüfung von Standards und Regulierungen in Bezug auf die Cybersicherheit namentlich wie folgt:

- *Fachliche Expertise*: Es verfügt über spezialisierte Fachkräfte, welche die Behörden bei der Umsetzung der oben genannten Standards und Regulierungen zur Cybersicherheit beraten und unterstützen können.
- *Bereitstellung von technischer Unterstützung*: Es unterstützt die Behörden bei der Entwicklung und Umsetzung von Cybersicherheitsstandards und -regulierungen.
- *Koordination und Zusammenarbeit*: Es übernimmt die Koordination für die Erleichterung der Zusammenarbeit zwischen den verschiedenen Behörden und stellt sicher, dass die entwickelten Standards und Regulierungen in Bezug auf die Cybersicherheit kohärent und effektiv sind.
- *Informationsaustausch*: Es dient als Basis für den Austausch über die bewährten Praktiken und Informationen im Bereich Cybersicherheit zwischen den Behörden.

4.8 Art. 8 - Kommunikationssystem für den sicheren Informationsaustausch und Informationssysteme für den automatischen Austausch

Diese Bestimmung stützt sich auf Artikel 73a Absatz 1 und 2 Buchstabe e ISG sowie Artikel 74 Absatz 1 und 2 Buchstabe a und b ISG.

Die Aufgabe des BACS betreffend sicheren Informationsaustausch wurde bis Ende 2023 in Artikel 12 Absatz 1 Buchstabe b und i der aufgehobenen CyRV geregelt. Die OV-VBS enthält diesbezüglich keine spezifische Regelung

Absatz 1: *Kommunikationssystem für den sicheren Informationsaustausch*

²⁰ [SR 784.101.2](#)

Angreifer verwenden oftmals die gleichen Methoden und Mittel, um bei möglichst vielen Opfern erfolgreiche Attacken durchzuführen. Wenn Opfer von Cybervorfällen und Cyberbedrohungen, die zu kritischen Infrastrukturen sowie zu anderen Organisationen und Behörden gehören, dem BACS die daraus gewonnenen Erkenntnisse rasch mitteilen, kann die Zahl der Cybervorfälle und Cyberbedrohungen deutlich reduziert werden. Aus diesem Grund betreibt das BACS ein Kommunikationssystem für den sicheren Informationsaustausch zu Cybervorfällen und Cyberbedrohungen. Über dieses Kommunikationssystem kann das BACS den registrierten Behörden und Organisationen mit Sitz in der Schweiz rasch und effizient Informationen über Vorfälle und Bedrohungen mitteilen. Dies ermöglicht es, den registrierten Organisationen und Behörden, schneller auf Bedrohungen zu reagieren und Gegenmassnahmen zu ergreifen. Des Weiteren trägt dieses Kommunikationssystem auch dazu bei, ein besseres Verständnis der Art und des Ausmasses von Cybervorfällen und Cyberbedrohungen zu entwickeln.

Absatz 2: Informationssysteme für den automatischen Austausch

Die Zurverfügungstellung von Systemen seitens des BACS für den automatischen Austausch von technischen Informationen ist ein sehr wichtiges Mittel zum Schutz der kritischen Infrastrukturen vor Cybervorfällen sowie -bedrohungen und ermöglicht es den Betreiberinnen von kritischen Infrastrukturen, durch den Austausch von Informationen, die von ihren IT-Systemen gelesen werden können, stets über den aktuellsten Wissensstand zu verfügen. Das BACS nutzt diese geschützten Informationssysteme dazu, die kritischen Infrastrukturen frühzeitig über technische Indikatoren und Angriffsmuster zu informieren, die der Öffentlichkeit noch nicht bekannt sind und vom BACS aus Sicherheitsgründen auch nicht veröffentlicht werden können. Technische Indikatoren zu Cybervorfällen oder -bedrohungen sind spezifische Anzeichen oder Hinweise auf potenzielle oder tatsächliche Bedrohungen im Bereich der Informationstechnologie und Cybersicherheit. Diese Indikatoren können verschiedene Formen annehmen, wie beispielsweise Malware-Signaturen, bei denen es sich um eindeutige Merkmale von schädlicher Software handelt, die darauf hinweisen, dass ein System infiziert ist oder einer Infektion ausgesetzt war. Auch Anomalien im Netzwerkverkehr gehören dazu. Hierbei handelt es sich beispielsweise um ungewöhnliche Muster im Datenverkehr, die auf eine mögliche Cyberbedrohung hindeuten können, wie ungewöhnlich hohe Datenübertragungsraten oder verdächtige Verbindungen zu bekannten schädlichen IP-Adressen. Ebenfalls können andere digitale Forensik-Indikatoren über diese Informationssysteme mit den Betreiberinnen kritischer Infrastrukturen automatisch ausgetauscht werden. Dies können verschiedene Arten von digitalen Spuren sein, die auf einen Cybervorfall oder eine Cyberbedrohung hindeuten, wie z.B. ungewöhnliche Dateiänderungen, verdächtige Logins oder unbefugte Zugriffsversuche. Betreiberinnen kritischer Infrastrukturen werden bei der Registrierung beim BACS entsprechend als solche erfasst, so dass die vorerwähnten technischen Informationen gezielt nur im Kreis der kritischen Infrastrukturen verteilt werden können. Alle erfassten Betreiberinnen kritischer Infrastrukturen werden einem oder mehreren Sektoren zugeteilt, damit auch ein sektorspezifischer Austausch erfolgen kann.

Absatz 3: Verantwortung des BACS für die Sicherheit und den Datenschutz

Das BACS trägt sowohl für das Kommunikationssystem für den sicheren Informationsaustausch als auch für die Informationssysteme für den automatischen Austausch die Verantwortung für die Sicherheit und den Datenschutz.

4.9 Art. 9 - Registrierung

Diese Bestimmung stützt sich auf Artikel 73a Absatz 1 und 2 Buchstabe e sowie Artikel 74 Absatz 1 und 2 Buchstabe a ISG.

Absatz 1: Registrierung für die Teilnahme am Informationsaustausch

Interessierte Organisationen und Behörden müssen sich für die Teilnahme am Informationsaustausch registrieren und jeweils allfällige Änderungen der registrierten Angaben unverzüglich dem BACS melden.

Absatz 2: Zu registrierende Angaben

Die Registrierung muss mindestens folgende Angaben enthalten:

- *Firma, Name oder Bezeichnung und Adresse der Behörde oder Organisation (Bst. a)*: Damit die Behörden und Organisationen ordentlich identifiziert werden können, müssen sie anlässlich der Registrierung ihre Firma, ihren Namen oder ihre Bezeichnung und ihre Adresse mit folgenden Angaben angeben: Strasse, Hausnummer, Postleitzahl und Ortsname.
- *Kontaktperson (Bst. b)*: Die Registrierung der Behörden oder Organisationen muss mindestens den Vornamen und den Familiennamen einer Kontaktperson enthalten. Des Weiteren ist die Telefonnummer sowie die E-Mail-Adresse und die Funktion der gemeldeten Person für das BACS anzugeben. Es können mehrere Kontaktpersonen registriert werden.

Einhergehend mit der Registrierung werden die Behörde oder Organisation über die Vorgaben für die Teilnahme am Informationsaustausch gemäss Artikel 11 dieser Verordnung informiert, und ein Abschluss der Registrierung ist nur möglich, wenn die Kenntnisnahme der Vorgaben aktiv bestätigt wird.

Selbst für meldepflichtige Behörden und Organisationen ist die Registrierung für die Teilnahme am Informationsaustausch nicht zwingend. Eine frühzeitige Registrierung bedeutet für die Meldepflichtigen aber ein Zeitersparnis im Falle eines meldepflichtigen Cyberangriffs.

4.10 Art. 10 - Dienstleister

Diese Bestimmung stützt sich auf Artikel 73a Absatz 1 und 2 Buchstabe e sowie Artikel 74 Absatz 1 und 2 Buchstabe a ISG.

Absatz 1: Anmeldung

Um die Sicherheit und Integrität der kritischen Infrastrukturen in der Schweiz zu gewährleisten, haben die Betreiberinnen kritischer Infrastrukturen gemäss *Absatz 1* die Möglichkeit, ihre Dienstleister für die Cybersicherheit beim BACS zu melden, damit diese am Informationsaustausch teilnehmen können.

Absatz 2: Zu registrierende Angaben

Allfällig gemeldete Dienstleister von Betreiberinnen von kritischen Infrastrukturen müssen sich gemäss *Absatz 2* unter Angabe ihrer Firma oder dem Namen sowie Kontaktangaben der gemeldeten Person registrieren (siehe hierzu sinngemäss die Ausführungen oben bei Artikel 9 Absatz 2). Dabei handelt es sich logischerweise um die Personen, die im Namen des Leistungserbringers für Cybersicherheit registriert sind.

4.11 Art. 11 - Übermittlung und Nutzung der Informationen

Diese Bestimmung stützt sich auf Artikel 73a Absatz 1 und 2 Buchstabe e sowie Artikel 74 Absatz 1 und 2 Buchstabe a ISG.

Der Informationsaustausch erfolgt freiwillig und basiert auf dem Vertrauen, dass die gelieferten Informationen zweckdienlich verwendet werden. Es ist deshalb entscheidend, dass die Informationslieferanten unter Berücksichtigung der gesetzlichen Vorgaben bestimmen können, wie mit der von ihnen geteilten Information umgegangen wird, und dass alle Teilnehmenden die Vorgaben für den Informationsaustausch kennen und einhalten.

Absatz 1: Weitergabe der geteilten Informationen nur gemäss den Bestimmungen der Informationslieferanten

Die Regelung, dass geteilte Informationen nur – soweit eine Weitergabe der Informationen nicht gesetzlich vorgesehen ist – gemäss den Bestimmungen der Informationslieferanten im Kommunikationssystem für den sicheren Informationsaustausch weitergegeben werden dürfen, ist wichtig, um sicherzustellen, dass die Informationen nicht unbefugt verbreitet oder missbraucht werden. Informationen über Cybervorfälle und -bedrohungen müssen vertraulich geteilt werden. Sie zeigen, welche Erkenntnisse über einen Vorfall vorliegen und welche Schutzmassnahmen identifiziert wurden. Angreifer könnten solche Informationen für ihre Zwecke nutzen. Zudem enthalten solche Informationen auch Angaben, die für die betroffene Behörde oder Organisation selbst sensibel sind, z.B. weil sie ihre Reputation gefährden können. Es ist darum wichtig, dass die Informationslieferanten grundsätzlich den Empfängerkreis selbst bestimmen können. In der Cybersicherheit hat sich zu diesem Zweck die Klassifizierung nach dem «Traffic Light Protocol» (TLP-Protokoll) durchgesetzt. Dieser vom «Forum of Incident Response and Security Teams (FIRST)» proklamierte Standard²¹ unterscheidet folgende Vorgaben für die Weiterverbreitung von Informationen:

- TLP «clear» - keine Restriktion für die Verbreitung der Information.
- TLP «green» - die Empfänger dürfen Informationen weitergeben, jedoch nicht auf öffentlichen Quellen publizieren.

²¹ Siehe hierzu Forum of Incident Response and Security Teams: Traffic Light Protocol (TLP), auf der Webseite [Traffic Light Protocol \(TLP\) \(first.org\)](https://www.first.org/traffic-light-protocol).

- TLP «amber» - die Empfänger dürfen Informationen innerhalb ihrer Organisation²² und mit ihren Partnern teilen, sofern dies nötig ist.
- TLP «amber strict» - die Empfänger dürfen Informationen ausschliesslich innerhalb ihrer Organisation teilen.
- TLP «red» - die Information geht nur an das Individuum und darf nicht weitergegeben werden.

Die auf der Plattform des BACS geteilten Informationen sind gemäss dem TLP-Protokoll kategorisiert. So wird angezeigt, wie die Information weiterverbreitet werden darf. Diese Vorgaben sind für alle Empfänger verbindlich, ausser die Weitergabe der Informationen ist gesetzlich vorgesehen.

Absatz 2: Entscheidung des BACS über die Veröffentlichung von Informationen

Das BACS hat die Autorität zu bestimmen, ob und wann Informationen über Cyberbedrohungen und -angriffe öffentlich gemacht werden sollen und ist damit verantwortlich für die Entscheidung, welche dieser Informationen an wen weitergegeben werden dürfen. Es handelt sich hierbei um Informationen, die intern geprüft und bearbeitet werden. Zum Zwecke des Schutzes vor Cyberbedrohungen wird dann geprüft, welche Informationen nützlich und relevant für die Öffentlichkeit oder bestimmte Zielgruppen sind und wie deren Verbreitung am besten über das vorhandene Kommunikationssystem bzw. den Informationssystemen erfolgen kann. Diese Überlegungen gelten nicht für die Weitergabe von Informationen an Strafverfolgungsbehörden, die nur unter den Bedingungen von Artikel 73d Absatz 3 ISG erfolgt.

Absatz 3: Gewährleistung des Schutzes der Informationen

Den Informationsempfängern kommt die Verantwortung zu, Massnahmen zu ergreifen, um die Sicherheit und Vertraulichkeit der erhaltenen Informationen zu gewährleisten. Der Schutz dieser Informationen ist besonders wichtig, da sie sensibel sein können und ihre Offenlegung oder Kompromittierung negative Folgen haben könnten. Zum Beispiel könnte dies weitere Cyberangriffe begünstigen oder bereits bestehende Sicherheitsprobleme verschärfen.

Absatz 4: Vorgaben für allfällige Dienstleister von Betreiberinnen kritischer Infrastrukturen

Dienstleister, die für kritische Infrastrukturen tätig sind, und die angemeldet und registriert wurden, dürfen die Informationen, die sie erhalten, ausschliesslich für die spezifischen Tätigkeiten verwenden, die sie im Auftrag der kritischen Infrastruktur ausführen.

²² Das TLP spezifiziert nicht, was unter «ihre Organisation» zu verstehen ist. Insbesondere bei Grossunternehmen oder bei Verwaltungen kann das zu Unklarheiten führen. In der Bundesverwaltung wird das Protokoll so umgesetzt, dass unter «Organisation» eine Verwaltungseinheit, als z. B. ein Bundesamt gemeint ist.

Dies dient dazu, die Vertraulichkeit und den angemessenen Umgang mit sensiblen Informationen zu gewährleisten und das Risiko eines Missbrauchs oder eines unbefugten Zugriffs zu minimieren.

4.12 Art. 12 - Ausnahmen von der Meldepflicht

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

Allgemeines:

Sind Behörden oder Organisationen in mehreren Bereichen nach Artikel 74b ISG meldepflichtig, so führt die Ausnahme in einem Bereich nicht dazu, dass sie von der Meldepflicht ausgenommen werden, sofern sie in einem oder mehreren anderen Bereichen noch meldepflichtig sind.

Es gilt auch zu beachten, dass es meldepflichtige Behörden und Organisationen gibt, für die keine Ausnahmen von der Meldepflicht gemäss den nachfolgend erläuterten Absätzen 1 und 2 bestehen. Zu diesen gehören namentlich:

- Bundes-, Kantons- und Gemeindebehörden sowie interkantonale, kantonale und interkommunale Organisationen, mit Ausnahme der Gruppe Verteidigung, wenn die Armee einen Unterstützungsdienst oder einen Aktivdienst im Sinne der Artikel 67 und 76 des Militärgesetzes vom 3. Februar 1995 leistet (Art. 74b Abs. 1 Bst. b ISG);
- Unternehmen, die dem Bankengesetz vom 8. November 1934, dem Versicherungsaufsichtsgesetz vom 17. Dezember 2004 oder dem Finanzmarktinfrastrukturgesetz vom 19. Juni 2015 unterstehen (Art. 74b Abs. 1 Bst. e ISG);
- Gesundheitseinrichtungen, die auf der kantonalen Spitalliste gemäss Artikel 39 Absatz 1 Buchstabe e des Bundesgesetzes vom 18. März 1994 über die Krankenversicherung aufgeführt sind (Art. 74b Abs. 1 Bst. f ISG);
- Organisationen, die Leistungen zur Absicherung gegen die Folgen von Krankheit, Unfall, Arbeits- und Erwerbsunfähigkeit, Alter, Invalidität und Hilflosigkeit erbringen (Art. 74b Abs. 1 Bst. i ISG);
- die Schweizerische Radio- und Fernsehgesellschaft (Art. 74b Abs. 1 Bst. j ISG); und
- Nachrichtenagenturen von nationaler Bedeutung (Art. 74b Abs. 1 Bst. k ISG).

Absatz 1: Spezifische Schwellenwerte

Es wurde darauf verzichtet, bereits auf Gesetzesstufe bereichsspezifische Ausnahmen zu definieren, damit der Bundesrat die Möglichkeit hat, auf Verordnungsstufe die festgelegten Schwellenwerte aufgrund von neuen Entwicklungen zeitnah anzupassen. Die Schwellenwerte wurden soweit möglich gemäss den spezifischen Herausforderungen des jeweiligen Bereichs definiert.

Bst. a: Hochschule nach Artikel 74b Absatz 1 Buchstabe a ISG

Unter „Hochschulen im Sinne von Artikel 74b Absatz 1 Buchstabe a ISG“ versteht man Hochschulen i.S.v. Artikel 2 Absatz 2 des Bundesgesetzes über die Förderung der Hochschulen und die Koordination im schweizerischen Hochschulbereich (Hochschulförderungs- und -koordinationsgesetz, HFKG)²³, die weniger als 2'000 Studierende haben. Diese sind von der Meldepflicht ausgenommen. Hochschulen sind meldepflichtig, wenn durch mögliche Angriffe auf sie ein Risiko für den Wirtschaftsstandort Schweiz, für die Wissensvermittlung, die Forschung oder die Beratung bei Grossereignissen oder gesellschaftlichen und ökologischen Entwicklungen entstehen kann.

Bst. b: Unternehmen nach Artikel 74b Absatz 1 Buchstabe d ISG

Die hier für den Elektrizitätsbereich festgelegten Schwellenwerte orientieren sich an der Stromversorgungsverordnung vom 14. März 2008 (StromVV)²⁴, mit der die Empfehlungen des Minimalstandards zur Verbesserung der IKT-Resilienz²⁵ für gewisse Akteure der Elektrizitätsbranche für verbindlich erklärt werden sollen.²⁶ Darin wird vorgesehen, dass die Akteure bei der Umsetzung des Minimalstandards ein gewisses Niveau für den Schutz ihrer Anlagen vor Cyberbedrohungen erreichen müssen (Schutzniveau A, B oder C). Die Höhe des Schutzniveaus ist abhängig von der Grösse respektive dem Einfluss des Akteurs auf die Versorgungssicherheit und wird durch entsprechende Schwellenwerte bestimmt. Entsprechend sollen nur die Elektrizitätsunternehmen der beiden höchsten Schutzniveaus A und B der Meldepflicht unterstellt werden. Kleinere Akteure, welche die weniger hohen Anforderungen des Schutzniveaus C erfüllen müssen, werden von der Meldepflicht ausgenommen. Die Elektrizitätserzeuger und Elektrizitätsspeicherbetreiber sind wie die Netzbetreiber Akteure des Stromversorgungsrechts²⁷. Sofern ein Unternehmen sowohl Anlagen zur Erzeugung als auch zur Speicherung von Elektrizität betreibt und diese Anlagen über dasselbe System fern-

²³ [SR 414.20](#)

²⁴ [SR 734.71](#)

²⁵ [Bundesamt für wirtschaftliche Landesversorgung, «Minimalstandard zur Verbesserung der IKT-Resilienz», Bern 2018.](#)

²⁶ Das Eidgenössische Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK) hat am 21. September 2023 die Vernehmlassung zu Teilrevisionen von verschiedenen Verordnungen im Energiebereich eröffnet. So ist vorgesehen, dass durch die [Revision der Stromversorgungsverordnung \(StromVV\)](#) der Schutz vor Cyberbedrohungen in der Stromversorgung gestärkt werden soll. Dazu wird der IKT-Minimalstandard für die wichtigsten Stromversorger – Netzbetreiber, Produzenten, und Speicherbetreiber – für verbindlich erklärt. Sie werden dazu einem bestimmten Schutzniveau (Schutzprofil) mit abgestuften Anforderungen zugeordnet, das sie erreichen müssen.

²⁷ Zu den Elektrizitätserzeugern vgl. [Art. 5 Abs. 2 des Stromversorgungsgesetzes vom 23. März 2007 \(SR 734.7\)](#). Zu den Elektrizitätsspeicherbetreibern vgl. z.B. [Art. 17a Abs. 1 StromVG](#) oder [Art. 8a Abs. 1 Bst. a Ziff. 3 StromVV](#).

steuerbar sind, werden die Leistungen entsprechend zusammengerechnet. Dienstleister der Netzbetreiber, Elektrizitätserzeuger und Speicherbetreiber sind ebenfalls von der Ausnahmeregelung erfasst. Nicht zu den Dienstleistern gehören Herstellerinnen von Hard- oder Software gemäss Artikel 74b Absatz 1 Buchstabe u ISG, für die es keine Ausnahmeregelung gibt.

Der in *Artikel 12 Absatz 1 Bst. b Ziffer 2 dieser Verordnung* für Betreiber von Gasleitungen definierte Schwellenwert von 400 GWh/Jahr wurde in Zusammenarbeit mit dem Verband der Schweizerischen Gasindustrie (VSG) festgelegt. Massgebend ist die gesamte über ihr Netz geleitete Energie (zu den Endverbrauchern oder zu anderen Netzen). Die Ausnahmeregelung betrifft nur Betreiber von Gasleitungen, deren Geschäftstätigkeit im Gasabsatz an Endverbraucher besteht (nicht von der Ausnahmebestimmung erfasst wäre daher bspw. die Transitgas AG).

Mit Artikel 74b Absatz 1 Buchstabe d ISG werden neben den Elektrizitäts- und den Gasversorgungsunternehmen auch andere Energieunternehmen der Meldepflicht unterstellt, beispielsweise Betreiber von Rohrleitungen zur Beförderung von Erdöl, Fernheizwerke, Raffinerien oder Unternehmen in den Bereichen der Holzenergie und Kohle. Diese Unternehmen sind grundsätzlich meldepflichtig, ausser sie liegen unterhalb der in Artikel 12 Absatz 2 dieser Verordnung definierten Schwellenwerte. Unternehmen, die sowohl in der Elektrizitäts- oder Gasversorgung als auch in einem anderen Energiebereich (Erdöl, Fernwärme, etc.) tätig sind, können sich nur dann auf eine Ausnahmeregelung berufen, wenn sich der Cyberangriff bzw. dessen Auswirkungen auf diesen Energiebereich beschränkt.

Bereits nach Artikel 74b Absatz 1 Buchstabe d ISG sind die Bewilligungsinhaber gemäss Kernenergiegesetz vom 21. März 2003²⁸ von der Meldepflicht ausgenommen. Dementsprechend erübrigt sich eine Regelung auf Verordnungsebene.

Bst. c: Eisenbahnunternehmen nach Artikel 74b Absatz 1 Buchstabe m ISG

Die Meldepflicht beschränkt sich auf die vom BAV beaufsichtigten Transportunternehmen mit Systemaufgaben im öffentlichen Interesse, deren sicherer und zuverlässiger Betrieb für das Wohlergehen der Bevölkerung und das Funktionieren der Wirtschaft unerlässlich ist. Dementsprechend werden die übrigen Unternehmen von der Meldepflicht ausgenommen.

Bst. d: Unternehmen nach Artikel 74b Absatz 1 Buchstabe n ISG

Unternehmen, die nach Artikel 74b Absatz 1 Buchstabe n ISG definiert sind und keine spezifischen Sicherheitsmanagement- oder -programmvorgaben gemäss den genannten EU-Verordnungen erfüllen müssen, sind von der Pflicht ausgenommen, Cyberangriffe auf ihre Informatiksysteme an das BACS zu melden. Dies gilt für Unternehmen, die:

²⁸ [SR 732.1](#)

- nicht verpflichtet sind, nach den Artikeln 2 und 4 und Anhang II der Durchführungsverordnung (EU) 2023/203²⁹ oder nach Artikel 2 und Anhang der Delegierten Verordnung (EU) 2022/1645³⁰ ein Information Security Management System (ISMS) einrichten zu müssen. Diese sind auch von der Meldepflicht bei Cyberangriffen gegenüber dem BACS ausgenommen. Ein ISMS ist ein systematischer Ansatz zur Verwaltung sensibler Unternehmensinformationen, damit sie sicher bleiben. Es umfasst Personen, Prozesse und IT-Systeme durch Anwendung eines Risikomanagementprozesses. Die genannten Verordnungen der EU legen Standards und Anforderungen für die Einrichtung eines solchen Systems fest. Wenn ein Unternehmen nicht verpflichtet ist.
- welche nicht die Vorgaben nach Nummer 1.7 des Anhangs der Durchführungsverordnung (EU) 2015/1998³¹ umsetzen müssen: Diese Verordnung betrifft Sicherheitsvorschriften für die Zivilluftfahrt. Nummer 1.7 des Anhangs könnte spezifische Sicherheitsmassnahmen oder -standards enthalten, die in einem «Security Programme» umgesetzt werden müssen. Wenn das betreffende Unternehmen nicht verpflichtet ist, diese Vorgaben in seinem Sicherheitsprogramm umzusetzen – was wiederum auf Grundlage von Artikel 2, 12, 13 oder 14 der Verordnung (EG) Nr. 300/2008³² erfolgt – dann ist es ebenfalls von der Meldepflicht bei Cyberangriffen befreit.

²⁹ Durchführungsverordnung (EU) 2023/203 der Kommission vom 27. Oktober 2022 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 2018/1139 des Europäischen Parlaments und des Rates hinsichtlich der Anforderungen an das Management von Informationssicherheitsrisiken mit potenziellen Auswirkungen auf die Flugsicherheit für Organisationen, die unter die Verordnungen (EU) Nr. 1321/2014, (EU) Nr. 965/2012, (EU) Nr. 1178/2011, (EU) 2015/340 der Kommission, die Durchführungsverordnungen (EU) 2017/373 und (EU) 2021/664 der Kommission fallen, sowie für zuständige Behörden, die unter die Verordnungen (EU) Nr. 748/2012, (EU) Nr. 1321/2014, (EU) Nr. 965/2012, (EU) Nr. 1178/2011, (EU) 2015/340 und (EU) Nr. 139/2014 der Kommission und die Durchführungsverordnungen (EU) 2017/373 und (EU) 2021/664 der Kommission fallen, sowie zur Änderung der Verordnungen (EU) Nr. 1178/2011, (EU) Nr. 748/2012, (EU) Nr. 965/2012, (EU) Nr. 139/2014, (EU) Nr. 1321/2014, (EU) 2015/340 der Kommission und der Durchführungsverordnungen (EU) 2017/373 und (EU) 2021/664 der Kommission, in der für die Schweiz verbindlichen Fassung gemäss Ziffer 3 des Anhangs zum Abkommen vom 21. Juni 1999 zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über den Luftverkehr ([SR 0.748.127.192.68](#)).

³⁰ Delegierte Verordnung (EU) 2022/1645 der Kommission vom 14. Juli 2022 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates im Hinblick auf die Anforderungen an das Management von Informationssicherheitsrisiken mit potenziellen Auswirkungen auf die Flugsicherheit für Organisationen, die unter die Verordnungen (EU) Nr. 748/2012 und (EU) Nr. 139/2014 der Kommission fallen, und zur Änderung der Verordnungen (EU) Nr. 748/2012 und (EU) Nr. 139/2014 der Kommission, in der für die Schweiz verbindlichen Fassung gemäss Ziffer 3 des Anhangs zum Abkommen vom 21. Juni 1999 zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über den Luftverkehr ([SR 0.748.127.192.68](#)).

³¹ Durchführungsverordnung (EU) 2015/1998 der Kommission vom 5. November 2015 zur Festlegung detaillierter Massnahmen für die Durchführung der gemeinsamen Grundstandards für die Luftsicherheit, in der für die Schweiz verbindlichen Fassung gemäss Ziffer 4 des Anhangs zum Abkommen vom 21. Juni 1999 zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über den Luftverkehr ([SR 0.748.127.192.68](#)).

³² Verordnung (EG) Nr. 300/2008 des europäischen Parlaments und des Rates vom 11. März 2008 über gemeinsame Vorschriften für die Sicherheit in der Zivilluftfahrt und zur Aufhebung der Verordnung (EG) Nr. 2320/2002, in der für die Schweiz verbindlichen Fassung gemäss Ziffer 4 des An-

Bst. e: Anbieterinnen und Betreiberinnen nach Artikel 74b Absatz 1 Buchstabe t ISG

Anbieterinnen und Betreiberinnen von Cloudcomputing und Suchmaschinen sowie Rechenzentren sind nur dann meldepflichtig, wenn sie ihre Leistungen teilweise oder vollumfänglich für Dritte und gegen Entgelt erbringen. Durch das neu eingeführte Kriterium der gewerblichen Leistungserbringung fallen auch Rechenzentren nicht unter die Meldepflicht, die ihre Leistung ausschliesslich für den Eigenbedarf erbringen.

Ebenso unterliegen alle digitalen Sicherheitsdienste und alle digitalen Vertrauensdienste, die Dritten angeboten werden, unabhängig von ihrem Umsatz oder ihrer Klientel, der Meldepflicht für Cyberangriffe (ohne einen mittleren Schwellenwert). Dagegen unterliegen Dienste, die eine Person ausschliesslich für sich selbst entwickelt und nutzt, nicht der Meldepflicht.

Absatz 2: Sektorenübergreifende Schwellenwerte

Für die Meldepflicht von Unternehmen wurde als generelle Ausnahme auf den Schwellenwert der Unternehmensklasse «kleine Unternehmen» gemäss der Empfehlung der EU-Kommission abgestellt.³³ Demnach sind meldepflichtige Behörden und Organisationen nach Artikel 74b ISG von der Meldepflicht ausgenommen, wenn sie weniger als 50 Personen beschäftigen und ihr Jahresumsatz bzw. ihre Jahresbilanz CHF 10 Mio. nicht übersteigt. Es wurde darauf verzichtet, eine Umrechnung von Euro in Schweizerfranken vorzunehmen, da die europäische Regelung auch für wirtschaftlich schwächere EU-Ländern gilt, in denen der Jahresumsatz bzw. die Jahresbilanz von EUR 10 Mio. schwieriger zu erreichen sein dürfte.

Die Ausnahme nach *Absatz 2* gilt nur für meldepflichtige Unternehmen, für die keine spezifischen Schwellenwerte nach Absatz 1 definiert wurden. Hierzu gehören:

- medizinische Laboratorien mit einer Bewilligung nach Artikel 16 Absatz 1 des Epidemiengesetzes vom 28. September 2012³⁴ (Art. 74b Abs. 1 Bst. g ISG);
- Unternehmen, die für die Herstellung, das Inverkehrbringen und die Einfuhr von Arzneimitteln eine Bewilligung nach dem Heilmittelgesetz vom 15. Dezember 2000³⁵ haben (Art. 74b Abs. 1 Bst. h ISG);
- Anbieterinnen von Postdiensten, die gemäss Artikel 4 Absatz 1 des Postgesetzes vom 17. Dezember 2010³⁶ bei der Postkommission registriert sind (Art. 74b Abs. 1 Bst. l ISG); und

hangs zum Abkommen vom 21. Juni 1999 zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über den Luftverkehr ([SR 0.748.127.192.68](#)).

³³ [EU-Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen \(2003/361/EG\)](#).

³⁴ [SR 818.101](#)

³⁵ [SR 812.21](#)

³⁶ [SR 783.0](#)

- Unternehmen, welche die Bevölkerung mit unentbehrlichen Gütern des täglichen Bedarfs versorgen und deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen führen würde (Art. 74b Abs. 1 Bst. p ISG).

Es gilt an dieser Stelle hervorzuheben, dass die in Absatz 2 aufgeführte Ausnahme nicht für Bundes-, Kantons- und Gemeindebehörden (Art. 74b Abs. 1 Bst. b ISG) und Hochschulen (Art. 74b Abs. 1 Bst. a ISG) gilt.

4.13 Art. 13 - Einreichung von Unterlagen zur Abklärung der Meldepflicht

Diese Bestimmung stützt sich auf Artikel 74a Absatz 2 ISG.

Da die Meldepflicht gemäss der Aufzählung in Artikel 74b Absatz 1 ISG sehr viele verschiedene Bereiche erfasst und es zahlreiche Behörden und Organisationen gibt, die gemäss Artikel 74c ISG und Artikel 12 dieser Verordnung von der Meldepflicht ausgenommen sind, ist zu erwarten, dass trotz dieser ausführlichen Regelungen bei gewissen Behörden und Organisationen Unklarheiten darüber bestehen, ob sie der Meldepflicht unterstellt sind oder nicht. Interessierte Behörden und Organisationen können daher beim BACS vorstellig werden und darum nachsuchen, dass es Auskunft über das Bestehen einer Meldepflicht nach Artikel 74b ISG oder einer Ausnahme von der Meldepflicht nach Artikel 74c ISG erteilt.

Damit das BACS diese Auskunftsgesuche behandeln kann, sieht der vorliegende *Artikel 13* vor, dass Behörden und Organisationen dem BACS alle erforderlichen Unterlagen zur Verfügung stellen müssen, damit das Amt darüber Auskunft geben kann, ob diese Einrichtungen einer gesetzlichen Meldepflicht unterliegen. Diese Anforderung stellt sicher, dass das BACS seine Aufgaben im Bereich der Cybersicherheit effektiv wahrnehmen kann. Da die Auskunft des BACS quasi eine Momentaufnahme darstellt, die auf den zum Zeitpunkt ihrer Erstellung vorliegenden Sachverhalten basiert, liegt es in der Verantwortung der betroffenen Behörde oder Organisation, bei einer wesentlichen Änderung der relevanten Tatsachen oder Umstände unverzüglich ihrer Meldepflicht nachzukommen oder bei Unsicherheit beim BACS ein Auskunftsgesuch zu stellen.

4.14 Art. 14 - Zu meldende Cyberangriffe

Diese Bestimmung stützt sich auf Artikel 74d ISG.

Allgemeines

Die Umschreibung der zu meldenden Cyberangriffe ist in Artikel 74d Buchstabe a–d ISG festgehalten. Cyberangriffe sind grundsätzlich dann meldepflichtig, wenn sie zum Zweck der Frühwarnung und Beurteilung der Bedrohungslage für das BACS besonders relevant sind. Die Kriterien zur Bestimmung der meldepflichtigen Angriffe wurden so gewählt, dass sie für die Behörden und Organisationen möglichst direkt erkennbar sind. Sie werden in diesem Artikel auf Verordnungsstufe weiter präzisiert.

Absatz 1: Gefährdung der Funktionsfähigkeit der kritischen Infrastruktur (Art. 74d Bst. a ISG)

Die Funktionsfähigkeit einer kritischen Infrastruktur kann durch einen Cyberangriff gefährdet sein, wenn die IT-Systeme, Netzwerke oder Steuerungssysteme, die für den Betrieb der Infrastruktur wesentlich sind, dergestalt kompromittiert werden, dass es zu Systemunterbrüchen für Mitarbeitende und Dritte führt (*Art. 14 Abs. 1 Bst. a dieser Verordnung*) oder die betroffene Organisation oder Behörde ihre Tätigkeiten nur noch mit Hilfe von Notfallplänen aufrechterhalten kann (*Art. 14 Abs. 1 Bst. b dieser Verordnung*). Ein Systemunterbruch liegt dann vor, wenn Mitarbeitende oder Dritte für ihre Tätigkeit wichtige Arbeitsschritte nicht mehr ausführen können, weil die dazu nötigen Informatikmittel nicht mehr verfügbar sind. Sobald ein Angriff zu einem Systemunterbruch führt, wird dieser bereits als erfolgreich angesehen. Er ist darüber hinaus auch dann problematisch, wenn er nur kurzzeitig ein oder mehrere Systeme unterbricht. Als Notfallpläne gelten alle technischen oder organisatorischen Massnahmen, die ergriffen werden müssen, wenn die üblicherweise verwendeten Informatikmittel kurzfristig und ungeplant nicht mehr verfügbar sind.

Absatz 2: Manipulation oder Abfluss von Informationen (Art. 74d Bst. b ISG)

Von einem meldepflichtigen Cyberangriff infolge Manipulation oder einem Abfluss von Informationen geht man namentlich aus, wenn die Angreifer in der Lage sind, unbefugten Zugriff auf sensible Daten der betroffenen Organisationen und Behörden zu erlangen und diese zu verändern, zu verschlüsseln, zu stehlen, zu löschen, Unbefugten offenzulegen oder zugänglich zu machen. So können durch einen Cyberangriff Daten durch Unbefugte dergestalt manipuliert werden, dass diese gemäss *Artikel 14 Absatz 2 Buchstabe a dieser Verordnung* geschäftsrelevante Informationen in Systeme einspeisen, welche aufgrund ihrer Veränderung oder Offenlegung zu Fehlern in Geschäftsprozessen, zu falschen Entscheidungen oder sogar zu Sicherheitsrisiken führen. Möglich ist aber auch gemäss *Art. 14 Absatz 2 Buchstabe b dieser Verordnung*, dass durch den böswilligen Angriff verursachte Manipulation oder Abfluss von Informationen die Datensicherheit von Personendaten (vgl. Art. 24 DSGVO) verletzt wurde.

Absatz 3: Über einen längeren Zeitraum unentdeckter Cyberangriff (Art. 74d Bst. c ISG)

Meldepflichtig sind auch Cyberangriffe, die über einen längeren Zeitraum unentdeckt bleiben und Anzeichen aufweisen, dass diese zur Vorbereitung weiterer Angriffe ausgeführt wurden. In *Artikel 14 Absatz 3 dieser Verordnung* wird festgehalten, dass man dann von einem längeren Zeitraum i.S.v. *Artikel 74d Buchstabe c ISG* ausgeht, wenn nach der Entdeckung festgestellt wird, dass der Cyberangriff bereits vor mehr als 90 Tagen erfolgt ist (z. B. durch die Auswertung von Logdaten). Solche Cyberangriffe stellen eine ernsthafte Bedrohung für kritische Infrastrukturen dar. Sie werden häufig auch als «Advanced Persistent Threats» (APTs) bezeichnet. Sie sind in der Regel hochentwickelt, zielgerichtet und schwer zu erkennen. Aus diesem Grund sind sie als Warnung für andere Betreiberinnen und Betreiber kritischer Infrastrukturen von besonderer Relevanz. Bei dieser Art von Angriffen kann Spionage (z. B. Behörden- oder Industriespionage) nicht ausgeschlossen werden. Die Angriffe sind oft sehr komplex und werden von erfahrenen Angreifern durchgeführt, die fortgeschrittene Techniken und Werkzeuge einsetzen, um sich im System zu verstecken und ihre Aktivitäten zu verschleiern. In der Regel wird auf ausgewählte Organisationen, Branchen oder Behörden abgezielt. Es ist auch denkbar, dass die Angreifer schrittweise vorgehen, um Zugriffsberechtigungen zu erweitern und weitere Schwachstellen auszunutzen. Wenn Anzeichen dafür bestehen, dass ein Cyberangriff zur Vorbereitung für weitere Angriffe ausgeführt wurde, ist es wahrscheinlich, dass die Angreifer bereits Zugang zu kritischen Systemen oder Daten haben und diese für zukünftige Attacken nutzen können.

Absatz 4: Mit Erpressung, Drohung oder Nötigung verbundener Cyberangriff (Art. 74d Bst. d ISG)

Dieser Absatz stellt klar, dass ein Cyberangriff, der zu einer strafrechtlichen Verfolgung führen könnte, immer dann gemeldet werden muss, wenn sich die strafbaren Handlungen gegen die meldepflichtige Behörde oder Organisation oder gegen deren Verantwortliche, Mitarbeiter oder Personen, die für die meldepflichtige Behörde oder Organisation arbeiten, richten. Viele Cyberkriminelle versuchen, über die Androhung oder Durchführung von Angriffen die Betreiberinnen kritischer Infrastrukturen, deren Kundinnen und Kunden oder einzelne Mitarbeitende zu erpressen (z. B. über die Verschlüsselung mittels Ransomware, der Androhung von Angriffen auf die Verfügbarkeit mittels Distributed-Denial-of-Service-Attacken [DDoS-Attacken] oder der Androhung der Veröffentlichung von sensiblen Informationen wie Personendaten oder Unternehmensgeheimnisse). Cyberangriffe mit strafrechtlich relevanten Begleitumständen sind meldepflichtig, wenn die Erpressung, Drohung oder Nötigung einen Bezug zur meldepflichtigen Organisation oder Behörde hat und sich auf deren Geschäfts- oder Verwaltungstätigkeit negativ auswirken kann. Es geht nicht darum, alle Verhaltensweisen zu melden, die strafrechtlich verfolgt werden können, wie z.B. die Meldung einer Erpressungs-E-Mail an Mitarbeiter. Vielmehr geht es hier um die Meldung von Cyberangriffen mit schwerwiegenden Auswirkungen, die mit finanziellen Verlusten, Rufschädigung oder rechtlichen Konsequenzen verbunden sind. Die Meldung solcher Angriffe ist wichtig, damit das BACS einschätzen kann, wie stark die Bedrohung kritischer Infrastrukturen durch Cyberkriminelle ist.

4.15 Art. 15 - Inhalt der Meldung

Diese Bestimmung stützt sich auf Artikel 74e Absatz 2 ISG.

Allgemeines:

Beim Verfassen dieser Ausführungsbestimmung hat man sich in weiten Teilen an der Terminologie und dem Inhalt des per 1. September 2020 eingeführten Formulars der FINMA betreffend die «Meldepflicht von Cyber-Attacken» orientiert.³⁷ Da das BACS im Gegensatz zur FINMA keine Aufsichtsfunktion hat, wurden gewisse Angaben nicht übernommen, da sie für die Zwecke der Meldepflicht an das BACS nicht massgeblich sind. So sind zum Beispiel bei der Meldung an das BACS weder Angaben zu den kritischen Funktionen oder den Kommunikationsmassnahmen zu machen, da diese Informationen keinen Mehrwert für die Einschätzung des Cyberangriffs bzw. der Warnung allfälliger weiterer Betroffener bieten würden. Im Übrigen wurden für die Analyse von Cyberangriffen auch wichtige Hinweise aus dem Formular für IT-Sicherheitsvorfälle des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) übernommen.³⁸ Das Meldeformular für Datensicherheitsverletzungen,³⁹ deren Meldungen an den EDÖB erfolgen, wurde für die Meldepflicht bei Cyberangriffen ebenfalls als Orientierungshilfe verwendet.

Artikel 74e Absatz 2 ISG nennt den Inhalt der Meldung, d.h. die wesentlichen Informationen, die zur Erfüllung der Meldepflicht notwendig sind. Nebst den Angaben im vorerwähnten Artikel muss die Meldung noch weitere Informationen enthalten, welche in *Artikel 15* als Ausführungsbestimmung festgehalten und vom BACS in einem Formular auf seinem Kommunikationssystem übernommen werden. In diesem Formular wird zudem detailliert umschrieben, was unter den jeweils zu meldenden Informationen zu verstehen ist.

Im Übrigen wird an dieser Stelle nochmals darauf hingewiesen, dass zur Erfüllung der Meldepflicht gegenüber dem BACS keine Angaben gemacht werden müssen, die allfällige Berufs- oder Geschäftsgeheimnisse betreffen und diese verletzen oder einer strafrechtlichen Selbstbelastung gleichkommen (vgl. Art. 74e Abs. 4 ISG). Die gemachten Angaben dienen lediglich der Erkennung und Bewertung von Angriffen durch das BACS sowie der Warnung potenzieller Opfer und der Empfehlung entsprechender Massnahmen.

Absatz 1: Informationen zur Art und Ausführung des Cyberangriffs

³⁷ Vgl. [FINMA-Aufsichtsmittteilung 05/2020 vom 7. Mai 2020](#), welche sich auf [Art. 29 Abs. 2 des Bundesgesetzes über die Eidgenössische Finanzmarktaufsicht \(Finanzmarktaufsichtsgesetz, FINMAG; SR 956.1\)](#) stützt und durch die FINMA im Rundschreiben 2023/1 präzisiert wurde ([FINMA-RS 2023/1](#), Rz. 68).

³⁸ Vgl. das [Meldeformular für IT-sicherheitsrelevante Ereignisse auf dem Melde- und Informationsportal des deutschen Bundesamtes für Sicherheit in der Informationstechnik](#).

³⁹ Vgl. den [Online-Dienst zur Meldung von Datensicherheitsverletzungen \(Art. 24 DSGVO\)](#).

Die Meldung gemäss *Absatz 1* umfasst nebst den Angaben nach Artikel 74e Absatz 2 ISG folgende Informationen über die Art und Ausführung des Cyberangriffs:

- *Datum und Uhrzeit der Feststellung des Angriffs (Bst. a)*: In der Meldung ist der Zeitpunkt der Entdeckung des Cyberangriffs mit Angabe des Datums sowie Uhrzeit aufzuführen.
- *Datum und Uhrzeit des Angriffs (Bst. b)*: In der Meldung sind auch das Datum und die Uhrzeit des Angriffs anzugeben. Falls dieser nicht bekannt ist, kann auch der vermutete Zeitpunkt des Cyberangriffs angegeben werden.
- *Angaben zum Angreifer (Bst. c)*: Die Identifizierung der Verursacher eines Cyberangriffs kann eine komplexe und herausfordernde Aufgabe sein, da Angreifer oft versuchen, ihre Spuren zu verschleiern und anonym zu bleiben. Dennoch gibt es verschiedene Arten von Informationen, die zur Identifizierung der Verursacher eines Cyberangriffs beitragen können, wie beispielsweise IP-Adressen, DNS-Records, URL von verdächtigen Seiten, hash-Werte von Malware, Virensignaturen, Anomalien im Netzwerkverkehr oder verdächtiges Verhalten von Software. Sind solche Informationen vorhanden, sind diese der Meldung anzufügen.

Absatz 2: Angaben über das Vorliegen einer Erpressung, Drohung oder Nötigung im Zusammenhang mit dem Cyberangriff und ob eine Strafanzeige erstattet wurde

Je nach Verlauf des Angriffs, kann damit auch eine Erpressung, Drohung oder Nötigung vorliegen. Die Offenlegung von Erpressungsversuchen oder Drohungen im Zusammenhang mit einem Cyberangriff kann dazu beitragen, andere potenzielle Opfer zu warnen und Massnahmen zur Prävention ähnlicher Vorfälle zu ergreifen. Da eine Erpressung, Drohung oder Nötigung im Zusammenhang mit einem Cyberangriff strafrechtliche Konsequenzen haben kann, kommt es vor, dass meldepflichtige Behörden und Organisationen Strafanzeige erstatten. Falls dem so ist, so muss dies dem BACS mitgeteilt werden. Die Angabe, ob eine Strafanzeige erstattet wurde, hilft dem BACS dabei, angemessen auf den Vorfall zu reagieren.

Absatz 3: Informationen zu den Auswirkungen des Cyberangriffs

Die gemäss *Absatz 3 Buchstaben a–c* zu machenden Angaben helfen dem BACS bei einer Erstbeurteilung der Auswirkungen des Cyberangriffs und in welcher Hinsicht Informatikmittel bzw. Daten durch den Cyberangriff beeinträchtigt sind.

- *Schweregrad der Beeinträchtigung der Verfügbarkeit, Integrität und Vertraulichkeit der Informationen (Bst. a)*: Die meldepflichtige Behörde und Organisation hat abzuschätzen, welche Schutzziele (Verfügbarkeit, Integrität und Vertraulichkeit) durch den Cyberangriff auf die Informatikmittel wie stark betroffen sind. Je nach Einschätzung der Auswirkungen des Cyberangriffs wird die Beeinträchtigung der Schutzziele entsprechend einem Schweregrad mit den Prädikaten «gering, mittel, hoch oder schwerwiegend» analog dem Meldeformular

der FINMA zugeordnet. Gestützt auf diese Erstbeurteilung der Auswirkungen und die Zuordnung der Schweregrade kann unter Umständen eruiert werden, ob sich bei den Auswirkungen ein Trend abzeichnet. Diese Information ist insbesondere dann wertvoll, wenn es Anzeichen für eine Verschlimmerung gibt. Des Weiteren hilft diese Einteilung auch bei der Entscheidungsfindung im Falle einer beantragten Hilfeleistung des BACS für die konkrete Vorgehensweise bei der Vorfallbewältigung.

- *Auswirkung des Cyberangriffs auf die Funktionsfähigkeit der Organisation oder Behörde (Bst. b):* Die Angaben zur Wirkung des Cyberangriffs auf die Funktionsfähigkeit der Organisation oder Behörde müssen darüber informieren, wie beispielsweise der Zugang zu Systemen und Daten, die Verfügbarkeit von Diensten für Kunden oder Bürgerinnen, interne Abläufe sowie Prozesse, die Verfügbarkeit von Strom- und Wasserversorgungssystemen, Gesundheitsdiensten oder andere kritische Infrastrukturen betroffen sind. Die meldepflichtige Organisation oder Behörde kann sich auch zu Angaben über den Zeitrahmen und Dauer der Auswirkungen des Cyberangriffs äussern und kundtun, wie lange die Auswirkungen des Cyberangriffs voraussichtlich anhalten werden.

Absatz 4: Informationen zur meldepflichtigen Behörde oder Organisation

Sofern die meldepflichtige Behörde oder Organisation nicht bereits für die Teilnahme am Informationsaustausch registriert und zum Zeitpunkt der Meldungserstattung keine Registrierung möglich ist (z. B. infolge Ausfalls der Informatikmittel) oder seitens der meldepflichtigen Behörde oder Organisation nicht gemacht werden will, muss die Meldung des Cyberangriffs gemäss *Absatz 4* zusätzlich folgende Informationen zur meldepflichtigen Behörde oder Organisation enthalten:

- *Firma, Name oder Bezeichnung und Adresse der meldepflichtigen Behörde oder Organisation (Bst. a):* Zur ordentlichen Identifikation der meldepflichtigen Behörden und Organisationen müssen diese ihre Firma, ihren Namen oder ihre Bezeichnung sowie ihre Adresse mit folgenden Angaben: Strasse, Hausnummer, Postleitzahl und Ortsnamen angeben.
- *Kontaktangaben der meldenden Person (Bst. b):* Die Meldung hat mindestens einen Vornamen sowie den Familiennamen der gemeldeten Person zu enthalten. Des Weiteren sind die Telefonnummer sowie die E-Mail-Adresse der meldenden Person anzugeben, da diese die Kontaktperson für das BACS ist. Organisationen oder Behörden können mehrere Kontaktpersonen anmelden.

Wenn eine meldepflichtige Behörde oder Organisation pflichtgemäss einen Cyberangriff dem BACS meldet, kann sie das BACS um Unterstützung bitten, woraufhin ein Austausch zwischen dem BACS und der Behörde oder Organisation entsteht. Weitere Informationen können dann vom Meldenden mit Zustimmung der Behörde oder Organisation weitergeleitet werden.

4.16 Art. 16 - Frist zur Erfassung der Meldung

Diese Bestimmung stützt sich auf Artikel 74e Absatz 1 und 3 ISG.

Allgemeines:

Die meldepflichtigen Behörden und Organisationen müssen Cyberangriffe unverzüglich nach Bekanntwerden melden, denn es gilt der Grundsatz: «Schnelligkeit vor Vollständigkeit», da das BACS auf eine unverzügliche Meldung von meldepflichtigen Cyberangriffen angewiesen ist, um jeweils seinem gesetzlichen Auftrag der Frühwarnung gerecht zu werden.

Absatz 1: Ergänzung oder Änderung der Meldung

Da es insbesondere für die Frühwarnung und die Prävention entscheidend ist, dass Cyberangriffe unmittelbar nach ihrer Entdeckung von den meldepflichtigen Behörden und Organisationen gemeldet werden, schreibt Artikel 74e Absatz 1 ISG eine Meldefrist von 24 Stunden vor. Der Fristenlauf beginnt nach der Entdeckung des Cyberangriffs, unabhängig vom Tag oder der Uhrzeit der Entdeckung. Denn Angriffe können jederzeit stattfinden, Cyberkriminelle kennen oft die günstigsten Zeiten, um Behörden und Organisationen anzugreifen.

Innerhalb der Frist müssen die bis zu diesem Zeitpunkt bekannten Informationen gemeldet werden. Bei Cyberangriffen ist sehr oft während längerer Zeit unklar, wie gravierend der Angriff ist und was genau passiert ist. Falls die vom BACS gemäss Artikel 15 dieser Verordnung verlangten Angaben zum Zeitpunkt der Meldung nur unvollständig vorliegen, können die Betroffenen die Meldung mit den fehlenden Angaben aufgrund neuer Erkenntnisse sowie ausreichendem Kenntnisstand ergänzen oder bestätigen, dass diese Informationen nicht vorhanden sind. Diese Nachmeldung muss dem BACS innerhalb einer Frist von 14 Tagen ab dem Zeitpunkt der Meldung des Cyberangriffs übermittelt werden. Beide Fristen sind nicht verlängerbar, da es sich um gesetzliche Fristen handelt (vgl. Art. 22 Abs. 1 VwVG).

Absatz 2: Aufforderung des BACS

Wenn die meldepflichtige Behörde oder Organisation nicht fristgerecht innerhalb der vorgeschriebenen 14 Tage die verlangten Informationen über den Cyberangriff meldet, so hat das BACS eine Aufforderung an die meldepflichtige Behörde oder Organisation zu erlassen. In dieser Aufforderung verlangt das BACS von der meldepflichtigen Behörde oder Organisation, die Meldung umgehend zu ergänzen oder zu bestätigen, dass diese Informationen nicht vorhanden sind.

4.17 Art. 17 - Übermittlung der Meldung

Diese Bestimmung stützt sich auf Artikel 74f ISG.

Das BACS bestätigt gemäss *Artikel 17* den Eingang der Meldung eines Cyberangriffs gegenüber der meldepflichtigen Behörde und Organisation umgehend, falls diese nicht

über das Kommunikationssystem des BACS erfolgt. Erfolgt die Meldung beispielsweise mittels E-Mail, informiert das BACS gestützt auf *Artikel 17 Absatz 1* allfällige gemäss Artikel 9 Absatz 2 Buchstabe b dieser Verordnung vorgängig registrierte Kontaktpersonen der meldepflichtigen Behörden und Organisationen. Mit dieser Rückmeldung soll sichergestellt werden, dass die meldepflichtige Behörde oder Organisation dem BACS mitteilen können, dass es sich um eine Falschmeldung handelt (z. B. «Scherzmeldung» durch Drittpersonen).

In der Praxis ist es möglich, dass meldepflichtige Behörden und Organisationen eine dritte Organisation mit der Übermittlung der Meldung eines Cyberangriffs beauftragen. Dies kann auch bei einzelnen Einrichtungen der Fall sein, welche die Meldung einem Anbieter von Cybersicherheitsdiensten anvertrauen. Es kann sich auch um Organisationen handeln, die gemeinsam über einen solchen Leistungserbringer oder eine andere spezialisierte Drittstelle gehen, wie eine Organisation, die z.B. Organisationen eines bestimmten Sektors vertritt. *Artikel 17 Absatz 2* sieht vor, dass dies möglich ist. Wichtig hierbei ist, dass die Meldungen dem BACS weitergeleitet werden und dass das BACS sich vom Wahrheitsgehalt einer Meldung überzeugen und mit der Person, die die Meldung veranlasst hat, Kontakt aufnehmen kann, um seine verschiedenen gesetzlichen Aufgaben im Zusammenhang mit der Meldung des Cyberangriffs zu erfüllen.

4.18 Art. 19 - Inkrafttreten

Die Verordnung tritt gleichzeitig mit dem revidierten ISG am 1. April 2025 in Kraft.

4.19 Änderung anderer Erlasse

4.19.1 Art. 15a Abs. 2 Bst. f Organisationsverordnung vom 7. März 2003 für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (OV-VBS)

Da in Artikel 4 dieser Verordnung die Aufgaben des nationalen Einsatzteams für Computersicherheit des BACS näher umschrieben werden, wird der bisherige Artikel 15a Absatz 2 Buchstabe f OV-VBS entsprechend gekürzt, damit keine Doppelspurigkeit besteht.

4.19.2 Art. 15a Abs. 2 Bst. h Organisationsverordnung vom 7. März 2003 für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (OV-VBS)

In Artikel 15a Absatz 2 Buchstabe h OV-VBS wird neu aufgeführt, dass das BACS die Schweiz zur technischen Analyse von Cyberbedrohungen und zur Bewältigung von Cyberfällen in internationalen Gremien vertritt. Diese Nennung ist wichtig, da Cyberfälle und Cyberbedrohungen internationale Phänomene sind. Angreifer benutzen die gleichen Technologien und Methoden in vielen Ländern gleichzeitig. Der nationale und internationale Austausch zwischen Fachstellen ist deshalb für den Schutz vor Cyberfällen und Cyberbedrohungen unerlässlich. Das BACS tauscht diesbezügliche aktiv Informationen mit inländischen und internationalen Stellen aus, die ähnliche Aufgaben wie das BACS wahrnehmen. Dieser Informationsaustausch dient dazu, relevante Erkenntnisse und Daten über aktuelle Bedrohungen zu teilen und gemeinsame Massnahmen zur Bewältigung von Cyberfällen und Cyberbedrohungen zu koordinieren. Damit hat das BACS mit seinem nationalen Einsatzteam für Computersicherheit

im Verhältnis zu den EU-Staaten den Stellenrang eines nationalen «Computer Security Incident Response Teams (CSIRT)», wie es die NIS-2-Richtlinie der EU für alle EU-Mitgliedstaaten vorschreibt.⁴⁰

Darüber hinaus vertritt das BACS die Schweiz in internationalen Gremien zur Cybersicherheit. Das BACS trägt mit seinen technischen und fachlichen Kompetenzen zur internationalen Zusammenarbeit bei. Die Schweiz hat ein Interesse daran, in die Zusammenarbeit auf internationaler Ebene eingebunden zu werden. Aus diesem Grund arbeitet das BACS insbesondere in internationale Gremien bei der technischen Analyse von Cybervorfällen und Cyberbedrohungen sowie mit der technischen Vorfallbewältigung mit. Das bedeutet, dass das BACS an internationalen Foren und Arbeitsgruppen teilnimmt, um sein Fachwissen und seine Erfahrung im Bereich der Cybersicherheit einzubringen und von den Erkenntnissen anderer Länder zu profitieren. Durch den Austausch von Informationen und die Teilnahme an internationalen Fachgremien trägt das BACS dazu bei, dass die Schweiz auf dem neuesten Stand der Entwicklungen im Bereich der Cybersicherheit bleibt und von Best Practices aus anderen Ländern profitiert. Dies stärkt die Fähigkeit des BACS, angemessen auf Cybervorfälle und Cyberbedrohungen zu reagieren und zur globalen Sicherheit beizutragen. All diese Aufgaben erfordern einen Informationsaustausch mit inländischen, ausländischen sowie internationalen Stellen, dessen gesetzliche Grundlagen in Artikel 73d Absatz 1 und Artikeln 76, 76a und 77 ISG zu finden sind.

4.19.3 Art. 41 Abs. 1 Verordnung über den Datenschutz vom 31. August 2022 (DSV)

Da das Parlament am 29. September 2023 eine Änderung des ISG verabschiedet hat, mit welcher eine Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen auf den 1. Januar 2025 eingeführt wird, muss Artikel 41 Absatz 1 der Verordnung über den Datenschutz vom 31. August 2022 aufgehoben werden.

5 Auswirkungen

Die CSV fördert Sicherheit und Transparenz, ohne Kantonen oder Gemeinden zusätzliche Kosten aufzubürden. Sie verbessert volkswirtschaftliche Effizienz, stärkt gesellschaftliches Vertrauen und führt indirekt zu nachhaltigerem Ressourceneinsatz.

5.1 Auswirkungen auf den Bund

Mit der Änderung des ISG und der Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen wird das BACS zu einer Unterstützung von Meldenden verpflichtet. In der Botschaft zur Änderung des Informationssicherheitsgesetzes für die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen (BBI 2023 84) wird darauf hingewiesen, dass mit der Einführung der Meldepflicht mit einem finanziellen und personellen Mehraufwand für das BACS zu rechnen ist.

⁴⁰ [Richtlinie \(EU\) 2022/2555 des europäischen Parlaments und des Rates vom 14. Dezember 2022 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung \(EU\) Nr. 910/2014 und der Richtlinie \(EU\) 2018/1972 sowie zur Aufhebung der Richtlinie \(EU\) 2016/1148 \(NIS-2-Richtlinie\).](#)

5.2 Auswirkungen auf Kantone und Gemeinden sowie auf urbane Zentren, Agglomerationen und Berggebiete

Kantone und Gemeinden sind von der Vorlage direkt betroffen, da sie als kritische Infrastrukturen meldepflichtig sind. Zudem stehen viele meldepflichtige Unternehmen in ihrer Trägerschaft. Die Kosten für die zentrale Meldestelle trägt jedoch der Bund und die Umsetzung der Meldepflicht führt bei den Betroffenen nicht zu relevanten Zusatzkosten. Der Erfassungsaufwand bei Cyberangriffen ist gering, wodurch die finanzielle Belastung minimal bleibt. Die Prinzipien der Subsidiarität und der fiskalischen Äquivalenz bleiben somit gewahrt.

5.3 Auswirkungen auf die Volkswirtschaft

Die in der CSV geregelte Meldepflicht weist volkswirtschaftlich keine signifikanten Auswirkungen auf, trägt aber dazu bei, bestehende Prozesse effizienter zu gestalten, ohne den Aufbau neuer Strukturen zu erfordern.

5.4 Auswirkungen auf die Gesellschaft

Gesellschaftlich wird mit der CSV eine frühzeitige Warnung vor Bedrohungen ermöglicht, wodurch Cyberangriffe und die daraus resultierenden Schäden verhindert werden können. Für Unternehmen entsteht durch klare Meldepflichten zudem ein höheres Mass an Transparenz, welches das Vertrauen zwischen Wirtschaftspartnern und Kunden stärkt.

5.5 Auswirkungen auf die Umwelt

Umweltseitig sind direkte Effekte zwar begrenzt, doch die Reduktion von Angriffen und die damit verbundene Effizienzsteigerungen können zu einem nachhaltigeren Ressourceneinsatz in der Informationstechnologie beitragen.

6 Rechtliche Aspekte

6.1 Verfassungsmässigkeit

Eine ausdrückliche Rechtsgrundlage für die Einführung einer Meldepflicht für Cyberangriffe ist der Bundesverfassung nicht zu entnehmen. Für die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen kann sich der Bund auf seine inhärente Bundeskompetenz zum Schutz der inneren und äusseren Sicherheit der Eidgenossenschaft abstützen.

Die kritischen Infrastrukturen haben eine hohe Sicherheitsrelevanz für Gesellschaft, Wirtschaft und Staat. Die potenziell schwerwiegenden und landesweiten Auswirkungen von Cyberangriffen auf kritische Infrastrukturen gefährden die Wohlfahrt des Landes und stellen eine Bedrohung für die innere und äussere Sicherheit dar. Die Einführung einer Meldepflicht dient mithin zur Wahrung der wirtschaftlichen, gesellschaftlichen und

staatlichen Stabilität. Sie bildet die Grundlage dafür, dass die Ereignisbewältigung koordiniert und rasch eingeleitet werden kann. Die Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen hat ferner zum Ziel, anhand der Meldungen eine Analyse der Bedrohungslage zwecks Frühwarnung und Gefahrenabwehr zu erstellen. Aus dem Zweck der Meldepflicht ergibt sich, dass sie in ihrem Umfang auf Cyberangriffe auf kritische Infrastrukturen beschränkt werden soll. Das Melderecht bei Cybervorfällen und Schwachstellen, das allen Personen offensteht, steht ergänzend zur weiteren Informationsgewinnung im Dienst des Schutzes der kritischen Infrastrukturen.

Entsprechend ist die inhärente Bundeskompetenz zur Wahrung der inneren und äusseren Sicherheit – mithin Zuständigkeiten, die dem Bund nicht explizit zugeteilt werden, ihm aber aufgrund seiner Staatlichkeit zukommen – eine geeignete Verfassungsgrundlage, um gestützt darauf Gesetzesbestimmungen für eine Meldepflicht für Cyberangriffe und ein Melderecht bei Cybervorfällen und Schwachstellen einzuführen.

Als Platzhalter für diese inhärente Bundeskompetenz wird aufgrund formell-gesetzestechnischer Konvention⁴¹ Artikel 173 Absatz 2 BV zitiert. Das Informationssicherheitsgesetz erwähnt in seinem Ingress – neben den Artikeln 54 Absatz 1, 60 Absatz 1, 101, 102 Absatz 1 und 173 Absatz 1 Buchstaben a und b – auch Artikel 173 Absatz 2 als massgebende Kompetenzgrundlage. Es besteht somit kein Bedarf für die Ergänzung von Verfassungsbestimmungen im Ingress des ISG.

6.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz

Der Erlass der Ausführungsbestimmungen in der CSV zur Meldepflicht für Cyberangriffe tangiert keine bestehenden internationalen Verpflichtungen der Schweiz. Sie ist vergleichbar mit den Regulierungen, die viele andere Staaten, insbesondere die EU-Mitgliedstaaten, in den letzten Jahren eingeführt haben.

6.3 Erlassform

Mit der CSV wird eine eigenständige Verordnung geschaffen, die sich auf die Artikel 74c und 84 Absatz 1 des Informationssicherheitsgesetzes abstützt, und damit der Ausführungserlass der Änderung des Informationssicherheitsgesetzes (Einfügung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen) ist.

6.4 Einhaltung der Grundsätze des Subventionsgesetzes

Mit der CSV werden keine Subventionsbestimmungen geschaffen

6.5 Delegation von Rechtsetzungsbefugnissen

Mit der CSV wird keine Delegation von Rechtsetzungsbefugnissen vorgesehen.

⁴¹ Rz. 25 der Gesetzestechischen Richtlinien des Bundes, online abrufbar www.bk.admin.ch > Dokumentation > Rechtsetzungsbegleitung > Gesetzestechische Richtlinien GTR.

6.6 Datenschutz

Die CSV hat die datenschutzrechtlichen Vorgaben des ISG unverändert übernommen, wie sie vom Parlament im Zusammenhang mit der Unterstützung für kritische Infrastrukturen verabschiedet wurden.