Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

22.xxx

Botschaft zur Änderung des Informationssicherheitsgesetzes (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen)

vom …

Sehr geehrte Frau Nationalratspräsidentin
Sehr geehrter Herr Ständeratspräsident
Sehr geehrte Damen und Herren

Mit dieser Botschaft unterbreiten wir Ihnen, mit dem Antrag auf Zustimmung, den Entwurf einer Änderung des Informationssicherheitsgesetzes zur Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen.

Wir versichern Sie, sehr geehrte Frau Nationalratspräsidentin, sehr geehrter Herr Ständeratspräsident, sehr geehrte Damen und Herren, unserer vorzüglichen Hochachtung.

…

Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Ignazio Cassis
Der Bundeskanzler: Walter Thurnherr

Übersicht

Ausgangslage

In den letzten Jahren haben Cybervorfälle bei Privaten, in Unternehmen und auch bei Behörden stark zugenommen, mit teilweise gravierenden Auswirkungen.

Der Bundesrat erteilte dem Eidgenössischen Finanzdepartement am 11. Dezember 2020 den Auftrag, Rechtsgrundlagen für die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen zu erstellen.

Dank der Meldepflicht können Cyberangriffe frühzeitig entdeckt, ihre Angriffsmuster analysiert und andere Betreiberinnen kritischer Infrastrukturen rechtzeitig gewarnt werden. Die Meldepflicht kann dadurch einen wesentlichen Beitrag zur Erhöhung der Cybersicherheit in der Schweiz leisten. Am 12. Januar 2022 eröffnete der Bundesrat die Vernehmlassung für den Vorentwurf. Die Ergebnisse der Vernehmlassung sind in den vorliegenden Entwurf eingeflossen.

Inhalt der Vorlage

Der Entwurf definiert nicht nur die Meldepflicht für Cyberangriffe auf kritische Infrastrukturen, er regelt zugleich auch die Aufgaben des 2019 geschaffenen Nationalen Zentrums für Cybersicherheit (NCSC) auf Gesetzesstufe. Insbesondere verankert der Entwurf die Funktion des NCSC als zentrale Meldestelle für Cybervorfälle, die auch freiwillige Meldungen zu Cybervorfällen und Schwachstellen in Informatikmitteln entgegennimmt.

Die Meldepflicht wird für Cyberangriffe eingeführt, welche von Unbefugten mit Absicht gegen kritische Infrastrukturen durchgeführt wurden. Meldepflichtig sind dabei nur Cyberangriffe, die schwerwiegende Auswirkungen haben, indem sie beispielsweise eine Gefährdung für die Funktionsfähigkeit der kritischen Infrastrukturen darstellen.

Inhaltsverzeichnis

Botschaft

1 Ausgangslage

Die Einführung einer Meldepflicht wird in Zusammenhang mit Cyberangriffen immer wieder diskutiert. Das Thema hat nochmals an Bedeutung gewonnen, weil die EU mit der Verabschiedung der Richtlinie (EU) 2016/1148[1] (NIS-Richtlinie) eine Meldepflicht für Cyberangriffe eingeführt hat. In mehreren Schritten hat der Bundesrat geprüft, ob eine Einführung einer Meldepflicht auch für die Schweiz nötig und umsetzbar ist, und hat auf der Grundlage der Ergebnisse dieser Prüfungen beschlossen, eine Vorlage auszuarbeiten.

1.1 Handlungsbedarf und Ziele

In seinem Bericht vom 13. Dezember 2019 zum Postulat «Meldepflicht von schwerwiegenden Sicherheitsvorfällen bei kritischen Infrastrukturen» stellte der Bundesrat fest, dass es in der Schweiz keine Meldepflicht für Cybervorfälle bei kritischen Infrastrukturen gibt.[2] Er erteilte deshalb dem Nationalen Zentrum für Cybersicherheit (NCSC) den Auftrag, die Einführung einer Pflicht zur Meldung von Cybervorfällen zu prüfen.

Dieser Prüfauftrag war breit abgestützt, etwa durch die Strategien zum Schutz kritischer Infrastrukturen (SKI-Strategie 2018–2022, Massnahme 8) und zum Schutz der Schweiz vor Cyberrisiken (NCS 2018–2022, Massnahme 9) sowie durch den Expertenbericht zur Zukunft der Datenbearbeitung und Datensicherheit[3]. In den parlamentarischen Debatten zur Totalrevision des Bevölkerungs- und Zivilschutzgesetzes (BZG, Debatte des Nationalrats vom 14.6.2019) und zum Erlass des Informationssicherheitsgesetzes (ISG, Debatte des Nationalrats vom 04.06.2020) wurde die Frage der Meldepflicht ebenfalls aufgegriffen. Nach einer vertieften Abklärung möglicher rechtlicher Grundlagen und insbesondere zur bundesstaatlichen Zuständigkeit[4] erteilte der Bundesrat dem Eidgenössischen Finanzdepartement (EFD) am 11. Dezember 2020 den Auftrag, bis Ende 2021 eine Vernehmlassungsvorlage für die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen auszuarbeiten.

In dieser Vorlage war zu klären, wer welche Art von Angriffen wann wem melden muss. Bei der Klärung dieser Fragen wurde deutlich, dass das 2019 geschaffene

1 Richtlinie (EU) 2016/1148 des europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. L 194 vom 19.7.2016, S. 1.

2 Varianten für Meldepflichten von kritischen Infrastrukturen bei schwerwiegenden Sicherheitsvorfällen, Bericht des Bundesrates vom 13. Dezember 2019 in Erfüllung des Postulates 17.3475 Graf-Litscher vom 15.06.17.

3 Bericht der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit vom 17. August 2018 (Empfehlung 28). Die Expertengruppe wurde vom EFD in Umsetzung der Motion Rechsteiner (13.3841) «Expertenkommission zur Zukunft der Datenbearbeitung und Datensicherheit» am 27. August 2015 mit Befristung auf drei Jahre eingesetzt.

4 Bericht «Meldepflicht für schwerwiegende Sicherheitsvorfälle bei kritischen Infrastrukturen, Rechtliche Grundlagen» vom 25. November 2020, Beilage 01 zum BRA vom 11.12.2020.

NCSC – welches in der Vorlage als zentrale Meldestelle für Cyberangriffe vorgesehen ist – nicht über die nötigen gesetzlichen Grundlagen verfügt, um seine Aufgaben als Kompetenzzentrum des Bundes für Cybersicherheit gemäss den Forderungen des Parlaments[5] wahrzunehmen. Mit der Vorlage zur Einführung der Meldepflicht sollen deshalb auch die Aufgaben und Kompetenzen des NCSC auf Gesetzesstufe geregelt werden.

1.2 Geprüfte Alternativen und gewählte Lösung

Die Einführung einer Meldepflicht ist ein direkt wirksames Instrument, um sicherzustellen, dass Informationen zu Cyberangriffen an eine zentrale Fachstelle übermittelt werden. Sie ist aber nicht alternativlos. Geprüft wurde, inwiefern der Ausbau des freiwilligen Informationsaustausches zu ähnlich wirksamen Ergebnissen führen könnte und ob es möglich ist, statt eine neue Meldepflicht einzuführen, bereits bestehende Meldepflichten so auszubauen, dass sie auch Cyberangriffe umfassen.

Da davon ausgegangen werden muss, dass beide Alternativen keine zufriedenstellende Lösung darstellen, wird die Einführung einer Meldepflicht vorgesehen. Diese soll mit Hilfe von Anreizen und Sanktionen durchgesetzt werden.

1.2.1 Ausbau des freiwilligen Informationsaustausches als Alternative

In der Schweiz ist der Informationsaustausch zwischen kritischen Infrastrukturen und dem Bund gut etabliert. Kritische Infrastrukturen tauschen sich seit 2004 mit der damaligen Melde- und Analysestelle für Informationssicherheit (MELANI) und heute mit dem NCSC aus. Dieses Modell stösst jedoch zunehmend an Grenzen. Damit der gegenseitige Austausch funktioniert, braucht es ein Vertrauensverhältnis zwischen allen Beteiligten. Ein solches lässt sich aufbauen, wenn die Anzahl der Beteiligten überschaubar ist und die Möglichkeit besteht, sich regelmässig direkt auszutauschen. In der heutigen Lage, bei der Cyberangriffe zu einer Bedrohung für eine Vielzahl von Unternehmen in den kritischen Sektoren geworden sind, kann nicht mehr gewährleistet werden, dass zu allen relevanten Akteurinnen eine ausreichende Vertrauensbasis hergestellt werden kann. In der Konsequenz hat sich der Informationsaustausch über die letzten Jahre auf einen Kreis von Unternehmen und Organisationen beschränkt, mit denen die etablierte Zusammenarbeit weiterhin gut funktioniert. Aufgrund der grossen Anzahl von kritischen Infrastrukturen, die Cyberbedrohungen ausgesetzt sind, ist eine Ausweitung dieses Modells aber nicht mehr realistisch.

Der durch die Freiwilligkeit der Meldungen bedingte Fokus auf wenige meldende Unternehmen kann zu einem unvollständigen oder gar verzerrten Lagebild führen. Es kann nicht festgestellt werden, welche Cyberbedrohung in der Schweiz welche Breitenwirkung entfacht. Zusätzlich führt der freiwillige Austausch auch zu falschen Anreizen. Unternehmen, welche sich nicht am Austausch beteiligen, erhalten dank der Meldung anderer Firmen trotzdem Warnungen und technische Hinweise, da das NCSC Betreiberinnen von kritischen Infrastrukturen solche wichtigen Hinweise nicht vorenthalten kann. Es besteht dadurch die Gefahr, dass es für Unternehmen einfacher

5 17.3508 Mo. Eder «Schaffung eines Cybersecurity-Kompetenzzentrums auf Stufe Bund»

ist, sich darauf zu verlassen, wichtige Informationen ohnehin zu erhalten, statt sich aktiv am Informationsaustausch zu beteiligen.

Insgesamt ist also die Einführung einer Meldepflicht der Weiterführung des freiwilligen Informationsaustausches vorzuziehen, weil sie eine vollständigere Lageübersicht zulässt und sicherstellt, dass niemand sich der Pflicht zur gegenseitigen Frühwarnung entziehen kann. Dennoch soll die über den Informationsaustausch entwickelte Kultur der Zusammenarbeit und des gegenseitigen Vertrauens weitergeführt werden. Entscheidend dabei ist, dass den Unternehmen und Organisationen über die Einführung der Meldepflicht auch ein Mehrwert entsteht.

1.2.2 Ausbau bestehender Meldepflichten und Informationsaustausch unter den Behörden als Alternative

Als Alternative zur Einführung einer neuen Meldepflicht wurde geprüft, ob es möglich ist, die Meldepflicht für Cyberangriffe in bereits bestehenden Meldepflichten zu verankern und darauf zu verzichten, eine neue sektorübergreifende Meldepflicht einzuführen. Diese Variante wurde verworfen, da die Regelungen zu Sicherheitsvorfällen in den verschiedenen Sektoren uneinheitlich sind und häufig gar keine solchen bestehen. Der Aufwand, die bestehenden Meldepflichten zu ergänzen und aufeinander abzustimmen und zusätzlich den Informationsaustausch zwischen den betroffenen Behörden zu regeln, wäre grösser gewesen als die Einführung einer neuen Meldepflicht und hätte zu ineffizienten Prozessen geführt.

Ferner gilt, dass die neue Meldepflicht für Cyberangriffe die bestehenden Meldepflichten nicht ersetzt, sondern nur ergänzt. Es wurde darauf geachtet, dass die gesetzlichen Grundlagen eine gleichzeitige Erfüllung verschiedener Meldepflichten erlauben. Der Aufwand für die Erfüllung mehrerer Meldepflichten soll so möglichst geringgehalten werden. Dies gilt vor allem, aber nicht nur für das Verhältnis zur datenschutzrechtlichen Meldepflicht nach Artikel 24 des revidierten Datenschutzgesetzes vom 25. September 2020[6] (nDSG), da es in der Praxis häufig der Fall ist, dass Cyberangriffe zu Datenverlusten führen. Die gewählte Lösung sieht vor, dass es den Meldenden offensteht, die Meldung des Cyberangriffs oder Teile davon gleichzeitig mit der Übermittlung an das NCSC anderen Meldestellen weiterzuleiten, um damit anderweitige Meldepflichten zu erfüllen. Damit soll verhindert werden, dass Betroffene den gleichen Vorfall an verschiedene Meldestellen über unterschiedliche Verfahren melden müssen.

Wenn Unternehmen und Organisationen dem NCSC freiwillig oder in Erfüllung der Meldepflicht Cyberangriffe melden, müssen sie Klarheit darüber haben, was mit ihrer Meldung geschieht und wer darüber in Kenntnis gesetzt wird. Auch in dieser Hinsicht sollen die Grundsätze aus dem bisherigen Informationsaustausch mit MELANI beibehalten werden: Eine Weiterleitung von Meldungen oder Teilen davon erfolgt nur mit Einverständnis der Betroffenen oder anonymisiert (vgl. Art. 73d Abs. 1).

6 SR **235.1**, AS **2022** 491

Die Weitergabe von Informationen, die Rückschlüsse auf die Meldenden oder Betroffenen erlauben, soll dem NCSC jedoch in zwei Fällen auch ohne deren Einverständnis erlaubt sein. Erstens ist eine Weiterleitung an die Strafverfolgungsbehörden möglich, wenn die Meldung Informationen über eine schwere Straftat enthält. Dies gilt somit nur für Ausnahmefälle, denn die Mitarbeitenden des NCSC sind grundsätzlich von der Anzeigepflicht gemäss Artikel 22a des Bundespersonalgesetzes vom 24. März 2000[7] (BPG) ausgenommen. Die Leiterin oder der Leiter des NCSC kann aber Informationen an Strafverfolgungsbehörden weiterleiten, wenn sie oder er zum Schluss kommt, dass dies auf Grund der Schwere der Straftat nötig ist (vgl. Art. 73d Abs. 3).

Der zweite Fall einer zulässigen Weiterleitung betrifft Informationen, welche für den Nachrichtendienst des Bundes (NDB) für seine Aufgabenerfüllung, nämlich der frühzeitigen Erkennung und Verhinderung von Bedrohungen der inneren oder äusseren Sicherheit, der Beurteilung der Bedrohungslage oder der nachrichtendienstliche Frühwarnung zum Schutz von kritischen Infrastrukturen nach Artikel 6 Absätze 1 Buchstabe a, 2 und 5 des Nachrichtendienstgesetzes vom 25. September 2015[8] (NDG) relevant sind. Dadurch ist sichergestellt, dass der NDB als zuständige Behörde für die Frühwarnung von kritischen Infrastrukturen und für die Einschätzung der Bedrohungslage wichtige, sicherheitsrelevante Informationen erhält (Art. 73d Abs. 2).

1.2.3 Durchsetzung der Meldepflicht mittels Anreizen und Sanktionen

Direkt verbunden mit der Einführung der Meldepflicht ist die Frage, über welche Instrumente sie durchgesetzt werden soll. Die Bereitschaft, der Meldepflicht nachzukommen, kann durch drei Faktoren beeinflusst werden.

Erstens muss es so einfach wie möglich sein, die Meldung zu verfassen. Dies wird sichergestellt, indem das NCSC ein elektronisches Meldeformular zur Verfügung stellt, über welches die Meldung rasch erfasst und einfach übermittelt werden kann.

Zweitens braucht es positive Anreize für die Meldung. Diese bestehen in erster Linie in der durch das NCSC angebotenen technischen Einschätzung und der subsidiären Unterstützung bei der Bewältigung des Angriffs. Diese sollen im Sinne einer ersten Hilfe erfolgen und nur so weit gehen, dass sie nicht in Konkurrenz stehen zu Dienstleistungen, die am Markt erhältlich sind. Für Betroffene kann es aber sehr wertvoll sein, wenn eine Bundesstelle mit Überblick über die Gesamtbedrohungslage ihnen bei der ersten Einschätzung hilft und sie bei der Umsetzung von Sofortmassnahmen unterstützt. Meldepflichtige Behörden und Organisationen (im Folgenden: die Meldepflichtigen) erhalten mit der Erfüllung der Meldepflicht Anspruch auf diese Unterstützung.

Der dritte Faktor zur Durchsetzung der Meldepflicht besteht in negativen Anreizen in Form einer Busse. Wenn es trotz Nachfrage und Rücksprache mit der kritischen Infrastruktur zu einer Verletzung der Meldepflicht kommt, braucht es Möglichkeiten zur Sanktionierung dieses Verhaltens.

7 SR **172.220.1**
8 SR **121**

Alternativ zur Busse wäre es möglich gewesen, säumige Melder öffentlich zu benennen. Diese Alternative wurde aber verworfen, da dies für die vertrauensbasierte Zusammenarbeit der Meldepflichtigen mit dem NCSC nicht förderlich wäre. Eine andere Möglichkeit bestünde darin, dass das NCSC säumigen Meldepflichtigen die Unterstützung bei der Vorfallbewältigung versagt. Diese Alternative ist wiederum aus sicherheitspolitischen Gründen nicht umsetzbar, da dabei unter Umständen gravierende Auswirkungen auf Wirtschaft und Gesellschaft in Kauf genommen werden müssten.

Damit verbleibt als Sanktionsinstrument nur die Möglichkeit, dass das NCSC als Ultima Ratio eine Verfügung mit Bussandrohung erlässt. Die Obergrenze der Busse liegt bei 100 000 Franken, wobei sie bis zu 20 000 Franken direkt dem Geschäftsbetrieb auferlegt werden kann, welcher die kritische Infrastruktur betreibt. Aufgrund der langbewährten Zusammenarbeit mit den kritischen Infrastrukturen geht der Bundesrat davon aus, dass diese Bestimmung weitgehend symbolischen Charakter hat und in erster Linie dazu dient, der Meldepflicht die nötige Beachtung zu verschaffen.

1.3 Verhältnis zur Legislaturplanung und zur Finanzplanung sowie zu Strategien des Bundesrates

Die Vorlage wurde in der Botschaft vom 29. Januar 2020[9] zur Legislaturplanung 2019–2023 und im Bundesbeschluss vom 21. September 2020[10] über die Legislaturplanung 2019–2023 angekündigt. In der Botschaft zur Legislaturplanung 2019–2023 wurde insbesondere auf die Notwendigkeit hingewiesen, Cybervorfälle bei kritischen Infrastrukturen rasch erkennen und bewältigen zu können und die IKT-Resilienz zu erhöhen. In Artikel 19 des Bundesbeschlusses über die Legislaturplanung 2019–2023 steht als Ziel 18: «Der Bund tritt Cyberrisiken entgegen und unterstützt und ergreift Massnahmen, um die Bürgerinnen und Bürger sowie die kritischen Infrastrukturen zu schützen». In der Botschaft sowie im Bundesbeschluss zur Legislaturplanung wird auf die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018–2022 vom 18. April 2018 und den dazugehörigen Umsetzungsplan verwiesen.

Im Voranschlag 2022[11] mit integriertem Aufgaben- und Finanzplan 2023–2025 wird die Verbesserung der Cybersicherheit im Bund und in der Schweiz als strategischer Schwerpunkt definiert und die Meldepflicht als Geschäft aufgeführt. Es wird festgehalten, dass das NCSC einen Mehrwert zum Schutz vor Cyberrisiken in der Schweiz leistet.

2 Vernehmlassungsverfahren

2.1 Vernehmlassungsentwurf

Am 12. Januar 2022 hat der Bundesrat den Vorentwurf sowie den erläuternden Bericht zur Kenntnis genommen und das EFD beauftragt, ein Vernehmlassungsverfahren

9 BBl **2020** 1777, hier 1866
10 BBl **2020** 8385, hier 8392
11 Band 2B – Voranschlag 2022 mit IAFP 2023–2025 der Verwaltungseinheiten Teil II (EFD, WBF, UVEK), S. 11 ff., abrufbar unter: www.efv.admin.ch > Finanzberichte > Voranschlag mit integriertem Aufgaben- und Finanzplan

durchzuführen. Das VE-ISG ändert Kapitel 5 des ISG, welches bereits Bestimmungen zur Cybersicherheit von kritischen Infrastrukturen enthält. Zusätzlich zu den Änderungen im ISG sieht der Vorentwurf auch Änderungen des nDSG[12], des Stromversorgungsgesetztes vom 23. März 2007[13] (StromVG) und des Bundesgesetztes vom 21. Juni 2019[14] über das öffentliche Beschaffungswesen (BöB) vor.

In den allgemeinen Bestimmungen (1. Abschnitt) werden die Aufgaben des Bundes beim Schutz vor Cyberbedrohungen auf Gesetzesstufe definiert. Mit der Schaffung des NCSC im Rahmen der Beschlüsse zur Organisation des Bundes im Bereich Cyberrisiken vom 30. Januar 2019[15] ist die Notwendigkeit entstanden, spezifische gesetzliche Grundlagen für die Aufgaben des NCSC zu schaffen.

Artikel 73*a* definiert die grundsätzlichen Aufgaben des NCSC. Diese werden durch Artikel 74 ergänzt, welcher festlegt, welche Art der Unterstützung das NCSC für Betreiberinnen kritischer Infrastrukturen leistet. Mit Bezug zur Einführung der Meldepflicht ist wichtig, dass in Artikel 73*b* die Aufgabe des NCSC als Meldestelle für Cybervorfälle und Schwachstellen umschrieben wird und die Artikel 73*c* und 73*d* vorgeben, wann und wem das NCSC welche Informationen aus den Meldungen weiterleiten darf.

Der Entwurf legt fest, dass das NCSC grundsätzlich keine Informationen zu Cybervorfällen veröffentlichen oder weiterleiten darf, welche Personendaten oder Daten juristischer Personen enthalten, sofern dafür keine Einwilligung vorliegt. Möglich bleibt die Übermittlung von statistischen Auswertungen und Erkenntnissen aus den eingegangenen Meldungen an andere Behörden oder die Öffentlichkeit. Artikel 73*d* definiert aber auch Ausnahmen von diesem Grundsatz. Erstens leitet das NCSC Informationen aus Meldungen an den Nachrichtendienst des Bundes weiter, welche dieser für seinen gesetzlichen Auftrag zur Beurteilung der Bedrohungslage und zur Frühwarnung von Betreiberinnen kritischer Infrastrukturen benötigt. Zweitens können Informationen, die im Zusammenhang mit der Meldung eines Cybervorfalls oder dessen Analyse Hinweise auf eine mögliche Straftat geben, nach Ermessen der Leiterin oder des Leiters des NCSC an die Strafverfolgungsbehörden weitergeleitet werden, wenn es angesichts der Schwere der Straftat angezeigt scheint. Dies gilt nur für Ausnahmefälle. Deshalb sind die Mitarbeitenden des NCSC von der Anzeigepflicht nach Artikel 22*a* BPG ausgenommen, wenn sie im Zusammenhang mit der Meldung eines Cybervorfalls oder dessen Analyse Hinweise auf eine mögliche Straftat erhalten.

Die Meldepflicht für Cyberangriffe auf kritische Infrastrukturen wird im zweiten Abschnitt eingeführt. In Artikel 74*a* wird festgehalten, dass kritische Infrastrukturen Cyberangriffe auf ihre Informatikmittel dem NCSC zu melden haben. Artikel 74*b* definiert dann den Adressatenkreis der Meldepflicht, indem er konkret die Bereiche aufzählt, für welche die Meldepflicht eingeführt wird. Schliesslich wird der Bundesrat in Artikel 74*c* verpflichtet, den Adressatenkreis der Meldepflichtigen für gewisse Be-

12 SR **235.1**, AS **2022** 491
13 SR **734.7**
14 SR **172.056.1**
15 Vgl. Medienmitteilung vom 31.01.2019 «Bundesrat gibt Startschuss für Kompetenzzentrum Cyber-Sicherheit»

reiche einzuschränken, um unbedeutende Organisationen von der Meldepflicht auszunehmen. In Artikel 74*d* wird festgehalten, welche Cyberangriffe zu melden sind und Artikel 74*e* und 74*f* bestimmen, welche Fristen und Angaben von den Meldenden beachtet werden müssen und wie die Meldungen übermittelt werden. Artikel 74*g* und 74*h* legen schliesslich das Vorgehen und die Folgen fest, wenn Unternehmen ihren Pflichten in Bezug auf die Meldung von Cyberangriffen nicht nachkommen.

Schliesslich sieht die Vorlage auch Änderungen von drei anderen Erlassen vor. Das nDSG wird so angepasst, dass es dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) ermöglicht wird, auf das Fachwissen des NCSC bei der Beurteilung von Meldungen nach dem nDSG zurückzugreifen. Das StromVG wird angepasst, damit eine gesetzliche Grundlage besteht, um Netzbetreiber, Erzeuger und Speicherbetreiber zu Massnahmen für einen angemessenen Schutz ihrer Anlagen gegen Cyberbedrohungen verpflichten zu können. Im BöB wird eine Bestimmung eingefügt, die es erlaubt, Herstellerinnen von Hard- oder Software, die eine entdeckte Schwachstelle nicht fristgerecht beheben, im Rahmen des öffentlichen Beschaffungsrechts für dieses Fehlverhalten zur Verantwortung zu ziehen.

2.2 Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens

Die Vernehmlassung dauerte vom 12. Januar 2022 bis zum 14. April 2022. Insgesamt gingen 99 Stellungnahmen ein (25 Kantone, 4 kantonale Konferenzen, 7 Parteien, 5 Dachverbände, 39 interessierte Organisationen, 19 Unternehmen)). Die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen wurde in der Vernehmlassung überwiegend befürwortet. 89 von 99 Teilnehmenden der Vernehmlassung, darunter alle Kantone, begrüssen die Stossrichtung der Vorlage, wobei verschiedene Vorbehalte gemacht werden. 7 Teilnehmende lehnen die unterbreitete Vorlage ausdrücklich ab, darunter eine Partei, ein Dachverband der Schweizer Wirtschaft, 2 interessierte Organisationen, 2 Unternehmen und eine Einzelperson.

Die Vorbehalte der befürwortenden Teilnehmenden konzentrierten sich hauptsächlich auf folgende Punkte:

- *Aufwand für die Betroffenen:* Der Aufwand für die Erfüllung der neuen Meldepflicht muss für die Betroffenen so gering wie möglich gehalten werden. Die Meldung muss einfach erfasst werden können und es muss möglich sein, ähnlich gelagerte Meldepflichten über einen Prozess («One-Stop-Shop») erfüllen zu können.
- *Sanktionierung bei Widerhandlung:* 24 Teilnehmende lehnen die Möglichkeit einer Sanktionierung grundsätzlich ab. Sie sind der Ansicht, dass die Meldepflicht nicht über Bussen, sondern über Anreize durchgesetzt werden muss. Bestrafungen würden dem Ziel eines möglichst guten Informationsaustausches zwischen Bund und Privaten zuwiderlaufen.
- *Zu breite Definition von Cyberangriffen:* Das VE-ISG schliesst in die Definition von Cyberangriffen auch Angriffsversuche ein (Art. 5) und grenzt nicht klar ein, welche Cyberangriffe meldepflichtig sind (Art. 74*d*). 23 Teilnehmende wün-

schen diesbezüglich eine klarere und engere Eingrenzung. Allgemein wird gewünscht, dass die Begriffe (Cyberangriff, Cybervorfälle, Cyberbedrohung, Cyberrisiken) klarer definiert und stringenter verwendet werden.

– *Breiter Geltungsbereich der Meldepflicht:* Die Auflistung der betroffenen Bereiche in Artikel 74*b* ist nicht überall genügend klar eingegrenzt, was zu Rechtsunsicherheit über die Geltung der Meldepflicht führen kann. 39 Teilnehmende fordern Änderungen bei diesem Artikel, die meisten Änderungswünsche betreffen eine klarere Eingrenzung der Bereiche im Gesetz oder auf Verordnungsstufe.

– *Weiterleitung von Informationen:* Die Möglichkeit einer Weitergabe von Informationen aus Meldungen an die Strafvollzugsbehörden oder an den NDB wird von 6 Teilnehmenden kritisch beurteilt. Sie fordern, dass eine solche Weiterleitung nur anonymisiert erfolgen darf. Der Kanton Bern und die Kantonale Konferenz der Polizeikommandanten fordern hingegen, dass das NCSC alle Meldungen den Strafvollzugsbehörden weiterleiten muss.

– *Öffentlichkeitsgesetz:* 6 Teilnehmende wünschen, dass die Tätigkeiten des NCSC bzw. die Meldungen explizit vom Öffentlichkeitsgesetz vom 17. Dezember 2004[16] (BGÖ) ausgenommen werden.

Neben den Vorbehalten werden in der Vernehmlassung auch Ergänzungswünsche zur Vorlage angebracht:

– *Minimalstandards und Weisungskompetenzen des NCSC:* Die Prävention von Cybervorfällen soll nicht nur durch eine Meldepflicht, sondern auch durch die Einführung von Minimalstandards für die Cybersicherheit von kritischen Infrastrukturen gefördert werden. 9 Teilnehmende fordern zudem, dass das NCSC gegenüber Betreiberinnen kritischer Infrastrukturen Weisungen zur Cybersicherheit erteilen kann.

– *Straffreiheit für ethische Hacker:* Ethischen Hackern, welche gezielt nach Schwachstellen suchen und dann Betroffene warnen, leisten einen wertvollen Beitrag zur Cybersicherheit. Teilnehmende verlangen, dass die Meldung von Schwachstellen gefördert wird und ethische Hacker von einer Strafe für ihre Aktivitäten befreit werden.

– *Säumige Hersteller:* CH++ schlägt ein konsequenteres Vorgehen vor, wenn Herstellerinnen trotz Aufforderung durch das NCSC Schwachstellen in Soft- oder Hardware nicht beheben. Konkret soll dieser Umstand dann für bestehende Verträge oder bei laufenden Beschaffungsverfahren berücksichtigt werden können.

16 SR **152.3**

2.3 Würdigung der Ergebnisse des Vernehmlassungsverfahrens

Grosse Akzeptanz der Meldepflicht

Die Einführung einer Meldepflicht sowie die Verankerung des NCSC als nationale Meldestelle und die damit einhergehende Klärung der Aufgaben des Bundes bei der Analyse dieser Meldungen und bei der subsidiären Unterstützung der Betreiberinnen kritischer Infrastrukturen wird begrüsst. Die Vorlage wird als wichtiger Schritt für die Verbesserung der Cybersicherheit der Schweiz erachtet, weil sie explizit die Zuständigkeit des Bundes bei Cybervorfällen regelt. Viele Vernehmlassungsteilnehmende weisen aber darauf hin, dass die Vorlage hinsichtlich der Begriffsverwendung präzisiert werden muss. Insbesondere der häufig verwendete, aber nicht definierte Begriff «Cyberrisiko» wurde als unklar bezeichnet. Die Begriffsdefinitionen wurden deshalb angepasst und der Begriff «Cyberrisiko» durch «Cyberbedrohung» ersetzt.

Rolle des NCSC

Häufig wird auch eine weitergehende Rolle des NCSC gefordert. So soll das NCSC Weisungsbefugnisse gegenüber Betreiberinnen kritischer Infrastrukturen erhalten, welche beispielsweise beinhalten könnten, Minimalstandards für die Sicherheit zu verlangen oder die Schliessung von Schwachstellen direkt anzuordnen. Diesen Anliegen wurde nicht entsprochen. Die Vorlage hat zum Ziel, die Frühwarnung von und den Informationsaustausch mit kritischen Infrastrukturen zu fördern. Wenn dem NCSC eine Aufsichts- und Regulierungsfunktion übertragen wird, ist zu bezweifeln, dass Unternehmen nach wie vor bereit sind, Informationen auch auf freiwilliger Basis mit dem NCSC zu teilen.

Aufwand und Nutzen für die Meldepflichtigen

Obwohl die Mehrzahl der Vernehmlassungsteilnehmenden eine Meldepflicht begrüsst, wurden auch mehrere Vorbehalte geäussert. Wichtig ist sowohl den Kantonen als auch der Wirtschaft, dass die Meldepflicht so ausgestaltet wird, dass sie möglichst wenig Aufwand generiert und das Meldeverfahren so gestaltet wird, dass weitere Meldepflichten gleichzeitig erfüllt werden können. Die Vorlage schafft die rechtlichen Voraussetzungen für solche Lösungen.

Es wird auch gewünscht, dass für die Meldenden einen Mehrwert aus der Meldepflicht entsteht und dadurch die Wirtschaft insgesamt gestärkt wird. Die Vorlage wird deshalb mit einer Bestimmung ergänzt, welche explizit den Anspruch derjenigen Betreiberinnen, die ihrer Meldepflicht nachkommen, auf die Unterstützung durch das NCSC festhält.

Geltungsbereich der Meldepflicht

Beim persönlichen Geltungsbereich der Meldepflicht gemäss Art. 74*b* wurde angemerkt, dass der Kreis der Betroffenen sehr breit ist und auf Verordnungsstufe präzisiert werden muss. Damit allfällige Unklarheiten über die Unterstellung unter die Meldepflicht frühzeitig geklärt werden können, dürfen Interessierte Auskunft über die Unterstellung verlangen. Das NCSC kann bei Bedarf die Unterstellung auch verfügungsweise feststellen (vgl. Art. 74*a* Abs. 3 E-ISG). Ferner wurden die Kriterien für

die Ausnahmen von der Unterstellung unter die Meldepflicht geschärft (Art. 74*c* E-ISG).

Die Meldepflicht solle zudem auf jene Unternehmensteile beschränkt bleiben, welche Aufgaben nach Artikel 74b ausführen. Dies sei besonders für Konzerne relevant, welche in sehr unterschiedlichen Bereichen tätig seien. Zudem soll die Meldepflicht auch gelten, wenn Unternehmen ihre Informatikmittel im Ausland betreiben, sofern sich ein Cyberangriff in der Schweiz auswirkt. Diesen Anliegen wurde mit zwei neuen Absätzen Rechnung getragen (vgl. Art. 74b Abs. 2 und 3 E-ISG).

Beim sachlichen Geltungsbereich der Meldepflicht haben die Vernehmlassungsteilnehmenden weitere Präzisierungen gewünscht. Die Bestimmung, welche Cyberangriffe meldepflichtig sind (Art. 74d), wurde deshalb überarbeitet. Dabei wurden Kriterien, die nicht verständlich oder schwer umsetzbar sind, wegelassen. Auch die in Artikel 74a VE-ISG enthaltene Bestimmung, dass Cyberangriffe «so rasch als möglich» zu melden sind, wurde konkretisiert und durch eine klar messbare Meldefrist von 24 Stunden ersetzt (vgl. Art. 74e E-ISG).

Vertraulichkeit von Meldungen

Ein weiteres wichtiges Anliegen der Vernehmlassungsteilnehmenden war, dass die Meldungen vertraulich behandelt werden. Es wird insbesondere gewünscht, dass Meldungen an das NCSC vom BGÖ ausgenommen werden. Anderenfalls bestehe die Gefahr, dass sensible Informationen von Betreiberinnen kritischer Infrastrukturen, die dem NCSC einen Cybervorfall melden würden, öffentlich gemacht werden müssten. Diesem Anliegen wird durch eine Ausnahme vom Zugangsrecht gemäss BGÖ betreffend Informationen Dritter im Zusammenhang mit Meldungen und Analysen (vgl. Art. 4 Abs. 1bis E-ISG) Rechnung getragen.

Busse bei Verletzung der Meldepflicht

Eindeutig am meisten Widerstand ausgelöst hat der Vorschlag, eine Sanktion bei Nichtbefolgung der Meldepflicht einzuführen. Vor einer Sanktionierung informiert das NCSC die Betroffenen zuerst über ihre Meldepflicht, bevor es die Meldung des Angriffs über eine Verfügung (mit Bussandrohung bei Nichtbefolgung) einfordert. Zusätzlich wurde eine Bestimmung aufgenommen, die das NCSC verpflichtet, den Meldepflichtigen mitzuteilen, wenn alle Informationen vorliegen, die für die Erfüllung der Meldepflicht notwendig sind (vgl. Art. 74e Abs. 5 E-ISG). Dieses Vorgehen gewährleistet, dass Sanktionierungen wegen Unklarheiten bei der Auslegung der Meldepflicht ausgeschlossen sind. Erst wenn die Meldepflichtigen trotz dieser Verfügung ihren Pflichten nicht nachkommen, d.h. einen konkreten Cyberangriff auch nicht nachträglich melden, ist eine Sanktionierung in Form einer Busse vorgesehen (vgl. Art. 74h E-ISG).

Trotzdem wird bezweifelt, dass eine Busse das richtige Instrument für die Durchsetzung der Meldepflicht darstellt, und 13 Teilnehmende verlangen eine Streichung des entsprechenden Artikels (Art. 74h VE-ISG). Diesem Anliegen wird nicht entsprochen. Ein wesentlicher Mehrwert der Einführung einer Meldepflicht gegenüber dem System der freiwilligen Meldungen besteht darin, dass alle betroffenen Organisationen zum Informationsaustausch verpflichtet werden und es nicht mehr möglich ist,

von der Frühwarnung zu profitieren, ohne selber einen Beitrag dazu zu leisten. Verweigert sich eine meldepflichtige Behörde oder Organisation aktiv an der Beteiligung bei diesem Informationsaustausch, braucht es die Möglichkeit einer Sanktionierung.

3 Rechtsvergleich, insbesondere mit dem europäischen Recht

Seit der Verabschiedung der NIS-Richtlinie[17] im Juli 2016 sind EU-Mitgliedsstaaten verpflichtet, eine Meldepflicht für Cybervorfälle umzusetzen. Die Frist für die Umsetzung ist im Mai 2018 abgelaufen. Die Meldepflicht betrifft «Anbieter wesentlicher Dienste», worunter gemäss Artikel 4 NIS-Richtlinie private Unternehmen oder öffentliche Einrichtungen fallen, die in den Bereichen Gesundheitswesen, Verkehr, Energie, Banken und Finanzmarktinfrastrukturen, digitale Infrastruktur und Wasserversorgung eine wichtige Rolle bei der Gewährleistung der Sicherheit spielen. Am 16. Mai 2022 haben sich Parlament und Kommission der EU über einen Entwurf zur Revision der NIS-Richtlinie (NIS2) geeinigt. Neu werden acht weitere Sektoren der NIS unterstellt (Abwasser, Abfallentsorgung, öffentliche Verwaltung, Postdienste, Ernährung, Industrie, Chemikalien, Raumfahrt). Der Adressatenkreis der NIS-Richtlinie entspricht damit weitegehend den gemäss dieser Vorlage definierten Meldepflichtigen.

In Bezug auf den Umfang der Meldepflicht lässt die NIS-Richtlinie den Mitgliedstaaten der EU relativ viel Spielraum offen. Meldepflichtig sind gravierende Vorfälle, wobei Artikel 14 festhält, dass bei der Beurteilung insbesondere die Zahl der betroffenen Nutzer, die Dauer des Sicherheitsvorfalls und die geografische Ausbreitung zu berücksichtigen sind. Im Unterschied zu unserer Vorlage beschränkt sich die NIS-Richtlinie jedoch nicht auf die Einführung einer Meldepflicht. Sie verpflichtet die Anbieter wesentlicher Dienste zugleich dazu, Sicherheitsvorkehrungen zu ergreifen. Dazu gehören die Risikovorsorge, die Gewährleistung der Sicherheit von Netz- und Informationssystemen und Massahmen, welche die Auswirkungen von Sicherheitsvorfällen so gering wie möglich halten (Art. 14 NIS-Richtlinie).

Die vorliegende Vorlage (E-ISG) beschränkt sich darauf, die gesetzlichen Grundlagen für solche Anforderungen im Stromsektor zu schaffen. In den übrigen Sektoren muss zunächst geklärt werden, ob der Bund die Kompetenz hat, rechtsverbindliche Normen für die Cybersicherheit festzulegen und in welchen Bereichen welche Anforderungen gestellt werden sollen.

17 Richtlinie (EU) 2016/1148 des europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. L 194 vom 19.7.2016, S. 1.

4 Grundzüge der Vorlage

4.1 Die beantragte Neuregelung

Das Hauptmotiv für die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen ist bei der Frühwarnung und bei der besseren Übersicht zur Bedrohungslage zu verorten. Da Angreiferinnen und Angreifer oft ähnliche Vorgehensweisen und Angriffsmuster für mehrere kritische Infrastrukturen in verschiedenen Sektoren verwenden, kann die Meldepflicht wesentlich dazu beitragen, durch frühzeitiges Erkennen der Angriffsmethoden und entsprechende Warnungen die Cybersicherheit von kritischen Infrastrukturen zu stärken. Durch die grössere Anzahl von Meldungen, die aufgrund der Meldepflicht beim NCSC eingehen werden, ist eine akkuratere Beurteilung der Bedrohungslage möglich.

Die Meldepflicht umfasst nur Cyberangriffe, die ein erhebliches Schadenspotenzial aufweisen. Nicht meldepflichtig sind Cybervorfälle, die auf menschliches Fehlverhalten, also beispielsweise eine unbeabsichtigte fehlerhafte Manipulation eines Mitarbeitenden, zurückzuführen sind. Schliesslich wurde auch davon abgesehen, die Meldepflicht auf Schwachstellen in Informatikmitteln auszudehnen. Schwachstellen werden meist durch Dritte (Sicherheitsforscherinnen und Sicherheitsforscher) entdeckt. Diese können über Anreize (z.B. Bug-Bounty-Programme) motiviert werden, die Schwachstellen zu melden. Meldepflichten hätten in diesem Umfeld hingegen wohl eher eine gewisse abschreckende Wirkung.

Trotz Einführung der Meldepflicht für Cyberangriffe ist es weiterhin möglich, Meldungen zu Cybervorfällen und Schwachstellen freiwillig zu melden. Diese Möglichkeit steht jeder Person offen und ist nicht auf kritische Infrastrukturen beschränkt.

Mit der Einführung der Meldepflicht für Cyberangriffe werden gleichzeitig die Aufgaben des NCSC auf Gesetzesstufe geregelt, welche aktuell nur in der Cyberrisikenverordnung vom 27. Mai 2020[18] (CyRV) definiert sind.

4.2 Abstimmung von Aufgaben und Finanzen

Das NCSC führt bereits heute eine Anlaufstelle, welche auf freiwilliger Basis Meldungen zu Cybervorfällen entgegennimmt. Es baut dabei auf der langjährigen Erfahrung von MELANI auf, welche diese Aufgabe seit 2004 ausgeführt hat.

Das NCSC nutzt für die Entgegennahme von freiwilligen Meldungen bereits ein elektronisches Meldeformular. Das elektronische Meldesystem des NCSC lässt sich auch für die Entgegennahme von Meldungen in Erfüllung der Meldepflicht verwenden. Für die nötigen Abstimmungen mit anderen Stellen, welche ebenfalls Meldungen entgegennehmen (z.B. EDÖB, Eidgenössische Finanzmarktaufsicht [FINMA], Eidgenössisches Nuklearsicherheitsinspektorat [ENSI]), und für die Konfiguration des Meldeformulars fällt ein Initialaufwand an, der jedoch über die bestehenden Ressourcen des NCSC aufgefangen werden kann. Für die Umsetzung der Vorlage muss das NCSC jedoch sicherstellen können, dass die in Erfüllung der Meldepflicht eingegangenen

18 SR **120.73**

Meldungen korrekt erfasst, quittiert und dokumentiert werden und die sich daraus ergebenden Informationen zur Cyberbedrohung zum Zweck der Frühwarnung an die richtigen Stellen weitergeleitet werden. Dieser zusätzliche Aufwand muss beim weiteren Ausbau des NCSC berücksichtigt werden.

Nach einem Cyberangriff wird das NCSC die betroffene kritische Infrastruktur bei der Vorfallbewältigung unterstützen. Auch diese Unterstützungsleistung ist dank der langjährigen Erfahrung des NCSC (und früher von MELANI) bereits gut eingespielt. Dennoch ist zu erwarten, dass sich der Aufwand für das NCSC durch die Einführung der Meldepflicht erhöhen wird. Erstens ist davon auszugehen, dass mehr Meldungen eingehen, und zweitens ist das NCSC neu nach Artikel 74*a* Absatz 3 in der Pflicht, mindestens eine erste Einschätzung und Empfehlungen zur Bewältigung des Vorfalls abzugeben. Das technische Analyseteam des NCSC (GovCERT) muss deshalb ebenfalls weiter ausgebaut werden.

4.3 Umsetzungsfragen

4.3.1 Notwendigkeit einer gesetzlichen Grundlage

Aus dem Legalitätsprinzip (Art. 5 Abs. 1 der Bundesverfassung[19] [BV]) und den Bestimmungen zur Gesetzgebung (Art. 164 Abs. 1 BV) ergibt sich, dass die Meldepflicht für Cyberangriffe mindestens in den Grundzügen auf Gesetzesebene zu regeln ist. Entsprechend enthält die Vorlage die wesentlichen Elemente der Meldepflicht für Cyberangriffe. Dazu zählen der Auslöser und Umfang der Meldepflicht (Cyberangriffe mit Schadenspotential), der Adressatenkreis der Meldepflichtigen (Betreiberinnen kritischer Infrastrukturen, die in bestimmten Bereichen tätig sind), die Frist und der Inhalt der Meldung sowie deren Verwendung durch das NCSC. Die Meldepflicht stellt für die meldepflichtigen Betreiberinnen kritischer Infrastrukturen einen Eingriff in die Rechte von Privaten und bei kantonaler oder kommunaler Trägerschaft in die föderalistische Autonomie dar. Die Meldepflicht ist aber kein Eingriff von grosser Tragweite und hat kaum finanzielle Auswirkungen auf die betroffenen Unternehmen.

4.3.2 ISG als geeignete Rechtsgrundlage

Im Rahmen der Vorarbeiten wurde geprüft, ob die neuen Regelungen in einem eigenständigen Gesetz oder in einen bestehenden Erlass eingefügt werden sollen, dessen Zweck, Gegenstand und Anwendungsbereich mit einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen vereinbar ist..[20] Für die Verankerung der Meldepflicht kamen als gesetzliche Grundlagen insbesondere Erlasse in Betracht, die bereits Bestimmungen zum Schutz kritischer Infrastrukturen enthielten und den Schutz der öffentlichen Ordnung im Fokus hatten (BZG, Landesversorgungsgesetz vom 17. Juni 2016[21], Bundesgesetz vom 21. März 1997[22] über Massnahmen zur Wahrung der inneren Sicherheit, NDG und ISG).

19 SR **101**
20 Vgl. Bericht «Meldepflicht für schwerwiegende Sicherheitsvorfälle bei kritischen Infrastrukturen, Rechtliche Grundlagen» vom 25. November 2020.
21 SR **531**
22 SR **120**

Nach eingehender Prüfung erwies sich von diesen Erlassen nur das ISG als passendes Gefäss. Sein Ziel, die Sicherheit für die vom Bund bearbeiteten Informationen und eingesetzten Informatikmittel zu gewährleisten, hat einen direkten Bezug zur Cybersicherheit (obwohl das Gesetz den Begriff nicht verwendet). Dazu kommt, dass im ISG bereits Bestimmungen zur Unterstützung für kritische Infrastrukturen durch den Bund vorgesehen waren. Dieser Teil des Aufgabenbereichs des NCSC war damit bereits gesetzlich verankert. Damit war das ISG nicht nur geeignet, sondern eine ideale Basis, um die Meldepflicht für Cyberangriffe zu verankern. Dafür spricht auch, dass in den parlamentarischen Beratungen zum Gesetzesentwurf die Einführung einer Meldepflicht für Betreiberinnen von kritischen Infrastrukturen bei «erheblichen Vorfällen» diskutiert, aber im Juni 2020 von der Mehrheit des Nationalrats jedoch abgelehnt wurde, nachdem der Bundesrat darauf hingewiesen hat, dass dazu eine Vorlage erarbeitet werden wird.

4.3.3 Ausführungsbestimmungen

Für den Vollzug der Meldepflicht ist das NCSC zuständig. Der Bundesrat hat am 12. Mai 2022 bereits entschieden, dass dieses zu einem Bundesamt ausgebaut werden soll. Damit erhält das NCSC die nötige Organisationsform, um die Aufgaben aus der Vorlage wahrnehmen zu können.

Die gesetzlichen Vorgaben zu den Aufgaben des NCSC und der Meldepflicht für Cyberangriffe werden durch den Bundesrat in einer Verordnung konkretisiert werden. Der Bundesrat kann – gestützt auf Artikel 182 Absatz 2 BV – zu sämtlichen Artikeln des 5. Kapitels Vollzugs- oder Ausführungsbestimmungen im Sinne von gesetzesergänzenden Normen erlassen. Er braucht dafür keine Delegationsnorm, da ihm keine Rechtsetzungsbefugnisse übertragen werden, ausser bei der Inkraftsetzungskompetenz. Er kann somit frei entscheiden, welche Gesetzesbestimmungen auf Verordnungsebene zu präzisieren sind. Einzig bei den Ausnahmen von der Meldepflicht in Artikel 74*c* wird der Bundesrat verpflichtet, entlang den dort aufgeführten Kriterien Schwellenwerte zu definieren.

4.3.4 Vollzugstauglichkeit der Meldepflicht

Die Stellungnahmen aus der Vernehmlassung machen deutlich, dass die Akzeptanz einer Meldepflicht grundsätzlich hoch ist. Voraussetzung ist aber, dass für die Meldepflichtigen wenig Aufwand bei der Meldung sowie ein Mehrwert für ihre Cybersicherheit entstehen. Für die Erfüllung der Meldepflicht wird daher ein Online-Formular entwickelt, welches es ermöglicht, die nötigen Angaben rasch zu erfassen und elektronisch ans NCSC zu übermitteln. Das NCSC hat bereits Erfahrung in der Bereitstellung von Meldeportalen, da es seit 2020 freiwillige Meldungen von Bevölkerung und Unternehmen entgegennimmt. Es kann sicherstellen, dass die Verfahren zur Meldung so einfach wie möglich gestaltet werden und wird dazu den direkten Austausch mit den Meldepflichtigen suchen.

Ein Cyberangriff auf eine kritische Infrastruktur kann neben der Meldepflicht an das NCSC weitere meldepflichtige Vorgänge betreffen und damit gleichzeitig mehrere Meldepflichten auslösen. Es sind beispielsweise folgende Überschneidungen denkbar:

– Für kritische Infrastrukturen, die im Finanzmarktsektor unter der Aufsicht der FINMA tätig sind, gilt bereits seit dem 1. September 2020 eine Meldepflicht für Cybervorfälle gegenüber der FINMA..[23]

– Ein Cyberangriff auf eine kritische Infrastruktur kann zu einer Verletzung der Datensicherheit führen, die je nach Schwere der Verletzung gegenüber dem EDÖB meldepflichtig ist (vgl. Art. 24 nDSG).

– Löst ein Cyberangriff Funktionsstörungen bei der kritischen Infrastruktur aus, z.B. einen radioaktiven Vorfall in einer Kernanlage, dann ist dieser Störfall in der Regel meldepflichtig (ENSI, Nationale Alarmzentrale usw.).

Die neu einzuführende Meldepflicht für Cyberangriffe wird die bestehenden Meldepflichten nicht ersetzen; letztere gelten unverändert weiter. Deshalb ist es wichtig, dass der Aufwand für die Meldepflichtigen auch dann vertretbar ist, wenn sie gleichzeitig weitere Meldepflichten erfüllen müssen. Aus diesem Grunde wird das NCSC ein System für die elektronische Erfassung der Meldung zur Verfügung stellen (Formular, Meldemaske oder Ähnliches), das die Meldepflichtigen für die Weiterleitung von Informationen an weitere Meldestellen nutzen können, sofern diese dazu Hand bieten. Auf diese Weise trägt das NCSC dazu bei, dass Synergien mit bestehenden Meldepflichten genutzt werden können, sofern sich diese auf den Cyberangriff oder dessen Auswirkungen beziehen.

Die Meldepflichtigen können selber entscheiden, ob sie die elektronisch erfasste Meldung ans NCSC, Teile davon oder Zusatzangaben an weitere Meldestellen schicken wollen oder nicht. Wichtig ist, dass die spezifischen Angaben für die Erfüllung der jeweiligen Meldepflicht nur für die betreffende Meldestelle zugänglich sind. Meldepflichtige können mit der Erfassung ihrer Angaben und Weiterleitung steuern, welche Meldestelle welche Angaben erhält.

5 Erläuterungen zu einzelnen Artikeln

5.1 Allgemeine Erläuterungen

Die gesetzlichen Grundlagen der Meldepflicht für Cyberangriffe sollen – abgesehen vom Titel des Erlasses und wenigen Anpassungen im 1. Kapitel – im 5. Kapitel des ISG eingefügt werden. Das 5. Kapitel wurde grundlegend überarbeitet, um darin auch die Aufgaben des NCSC – die über die Meldepflicht hinausgehen und nicht spezifisch auf kritische Infrastrukturen ausgerichtet sind – aufnehmen zu können. Entsprechend wurde auch die Kapitelüberschrift angepasst («5. Kapitel: Massnahmen des Bundes zum Schutz der Schweiz vor Cyberrisiken»).

Die wesentlichen Regelungsinhalte der gesetzlichen Bestimmungen wurden unter den vorstehenden Ziffern teilweise bereits ausführlich beschrieben und begründet. Die Kommentierung der nachfolgenden Artikel beschränkt sich daher auf Ergänzungen dazu. Für diejenigen Bestimmungen, die nur formell angepasst wurden, sind weiterhin

23 Vgl. FINMA, Aufsichtsmitteilung 05/2020 vom 7. Mai 2020, die sich auf Artikel 29 Absatz 2 des Finanzmarktaufsichtsgesetzes (SR 956.1) stützt.

die Ausführungen in der Botschaft vom 22. Februar 2017[24] zum Informationssicherheitsgesetz massgebend.

5.2 Die Bestimmungen im Einzelnen

Titel

Der Titel «Bundesgesetz über die Informationssicherheit beim Bund» wurde in «Bundesgesetz über die Informationssicherheit» geändert. Zwar betreffen die Bestimmungen über die Informationssicherheit hauptsächlich den Bund, die Cybersicherheit in der Schweiz als Aufgabe des NCSC, die im 5. Kapitel geregelt ist, beschränkt sich aber nicht nur auf den Bund. Die Einführung der Meldepflicht für Cyberangriffe erfolgt landesweit und erfasst auch kantonale Behörden und interkantonale Organisationen.

1. Kapitel: Allgemeine Bestimmungen

Im ersten Kapitel betreffen die Anpassungen Artikel 1, 2, 4 und 5. Die restlichen Artikel wurden nicht verändert.

Artikel 1 Zweck

Der Zweckartikel des ISG wurde in Absatz 1 ergänzt, indem eine Unterteilung in die Buchstaben a und b vorgenommen wurde. In Buchstabe a wurde die ursprüngliche Formulierung übernommen, während in Buchstabe b die Zweckbestimmung in Bezug auf Cyberbedrohungen ergänzt wurde. Diese erweiterte Zweckbestimmung dient dazu, den durch die Einführung einer Meldepflicht für Cyberangriffe und der gesetzlichen Regelung der Aufgaben des NCSC eingefügten Aspekten Rechnung zu tragen.

Artikel 2 Verpflichtete Behörden und Organisationen

Hier wurde der Verweis in Absatz 5 auf die Bestimmungen, die für kritische Infrastrukturen gelten, angepasst, da Kapitel 5 neu mit Artikel 73*a* beginnt und mit Artikel 79 aufhört. Es wurde keine inhaltliche Anpassung dieses Artikels vorgenommen.

Artikel 4 Verhältnis zu anderen Erlassen des Bundes

In der Vernehmlassung zum Vorentwurf wurde von mehreren Seiten angeregt, dass für Meldungen ans NCSC die Vertraulichkeit gewährleistet sein muss und aus diesem Grund das NCSC vom Geltungsbereich des BGÖ auszunehmen sei.

Diesem Anliegen wurde teilweise entsprochen, indem in Artikel 4 ISG, der das Verhältnis des ISG zum BGÖ regelt, ein Absatz 1bis eingefügt wurde, der den Zugang zu Informationen von Dritten, von denen das NCSC in seiner Funktion als Meldestelle Kenntnis erhält, sei es durch Meldungen oder deren Analysen, ausschliesst. Es wurde aber darauf verzichtet, das NCSC insgesamt vom Anwendungsbereich des BGÖ auszunehmen.

Das NCSC ist darauf angewiesen, dass die Meldenden sich auf die vertrauliche Behandlung der Meldungen durch das NCSC verlassen können. Das Vertrauensverhält-

24 BBl **2017** 2953, hier 3062 ff.

nis ist eine wichtige Voraussetzung, damit die kritischen Infrastrukturen die neue Meldepflicht für Cyberangriffe erfüllen. Die Gewährleistung der vertraulichen Behandlung hat durch die Einführung der Meldepflicht an Bedeutung gewonnen, da die Anzahl der Meldungen ans NCSC zunehmen wird.

Seit der Verabschiedung der CyRV (Mai 2020) und der ursprünglichen Fassung des ISG (Dezember 2020) hat sich der Aufgabenbereich des NCSC erweitert, insbesondere durch die Meldepflicht.

Es ist für die Aufgabenerfüllung des NCSC in seiner Funktion als Meldestelle – und in Anbetracht der steigenden Anzahl an Meldungen – unabdingbar, dass der Zugang gemäss BGÖ zu Informationen Dritter, von denen das NCSC im Zusammenhang mit Meldungen und Analysen Kenntnis erhält, ausgeschlossen wird. Dagegen unterstehen Informationen von Behörden oder Organisationen, die ihrerseits dem BGÖ unterstehen, weiterhin dem Zugangsrecht gemäss BGÖ.

Eine Ausnahmeregelung gilt im Übrigen auch für die Meldepflicht für Cybervorfälle im Finanzmarktsektor, deren Meldestelle die FINMA als Aufsichtsbehörde ist. Im Gegensatz zum NCSC wurde die FINMA vollständig vom BGÖ ausgenommen (vgl. Art. 2 Abs. 2 BGÖ). Beim NCSC wird demgegenüber lediglich das Zugangsrecht in Bezug auf Informationen Dritter, die es in seiner Funktion als Meldestelle erhält, ausgeschlossen. Im Übrigen geht das BGÖ somit weiterhin dem ISG vor (Art. 4 Abs. 1 ISG).

Artikel 5 Begriffe

Die Begriffsdefinitionen in den Buchstaben a, b und c wurden nicht verändert. Im Zusammenhang mit der Meldepflicht für Cyberangriffe gemäss Art. 74*a* ff. ist anzumerken, dass die Definition von kritischen Infrastrukturen in Buchstabe c weit gefasst ist. Sie lässt sich nicht direkt als Grundlage für den Adressatenkreis der Meldepflicht verwenden.

Der Begriffskatalog wird durch vier zusätzliche Definitionen (d. Cybervorfall, e. Cyberangriff, f. Cyberbedrohung und g. Schwachstelle) ergänzt. Diese Begriffe sind für die Einführung der Meldepflicht von unmittelbarer Bedeutung, weshalb eine Legaldefinition notwendig ist. Die neu eingeführten Definitionen entsprechen den Definitionen der international anerkannten Normen. [25]

Buchstabe d: Cybervorfall

Die Definition des Cybervorfalls macht deutlich, dass es sich dabei um den Oberbegriff für alle Ereignisse handelt, welche die Schutzziele der Informationssicherheit gemäss Artikel 6 Absatz 2 ISG, d.h. die Vertraulichkeit, Verfügbarkeit oder Integrität von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigen. Die Integrität von Informationen ist gewährleistet, wenn ihre Unversehrtheit und Richtigkeit gewahrt ist. Die Nachvollziehbarkeit bedeutet, dass man sehen kann, wer die Informationen wann und wie bearbeitet hat (vgl. Ausführungen in der Botschaft vom 22. Februar 2027[26] zum Informationssicherheitsgesetz).

25 Insbesondere ISO 27000; ISO/IEC 29147:2018; NIST.
26 BBl **2017** 2953, hier 3016

Ein Cybervorfall schliesst sowohl Ereignisse ein, welche von Unbefugten absichtlich ausgelöst wurden (Cyberangriffe) als auch jene, welche von Befugten unbeabsichtigt verursacht wurden (z.B. durch Fehlmanipulationen), oder solche, die durch Fehlfunktionen der Informatikmittel entstehen. Zu letzteren zählen auch Fehler in den algorithmischen Entscheidungssystemen (Künstliche Intelligenz, KI).

Das wesentliche Merkmal des Cybervorfalls ist die Beeinträchtigung der Vertraulichkeit, Verfügbarkeit oder Integrität von Informationen[27] oder die Nachvollziehbarkeit ihrer Bearbeitung. Ereignisse, die zwar das Potential einer Beeinträchtigung der Schutzziele haben, diese aber faktisch nicht tangieren, stellen keine Cybervorfälle im Sinne dieses Gesetzes dar, sondern sind Cyberbedrohungen gemäss Buchstabe f. Diese Einschränkung und Abgrenzung bei der Definition des Cybervorfalls ist nötig, da Organisationen und Unternehmen täglich zahlreiche Ereignisse feststellen, welche die Schutzziele theoretisch gefährden, in der Praxis aber durch technische Schutzmassnahmen erfolgreich abgewehrt werden können (z.B. Phishing-Versuche, Spammails, etc.). Erst durch die tatsächliche Beeinträchtigung der Schutzziele wird das Ereignis zum Cybervorfall.

Buchstabe e: Cyberangriff

Cyberangriffe sind eine mögliche Erscheinungsform des Cybervorfalls. Ein Cybervorfall gilt dann als Cyberangriff, wenn er absichtlich ausgelöst wurde – unabhängig davon, ob es sich dabei um interne Mitarbeitende oder eine externe Quelle handelt (oder beides). Entscheidend ist nicht die Frage, von wo der Angriff ausgeführt wurde (intern/extern), sondern ob die Angreiferin oder der Angreifer absichtlich die Schutzziele Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit beeinträchtigt (vgl. Definition zu Cybervorfall in Buchstabe d) hat. Die Definition von Cyberangriff impliziert, dass darunter nur erfolgreiche Angriffe fallen, d.h. solche, die nicht oder nicht vollständig abgewehrt werden konnten.

Die Abgrenzung des Cyberangriffs zum Cybervorfall ist deshalb von Bedeutung, weil Cyberangriffe mehrmals nach derselben Vorgehensweis ausgeführt werden können. Die Übersicht über diese Angriffsmethoden ist daher für die Frühwarnung von kritischen Infrastrukturen essentiell.

Aus diesem Grunde wird die Meldepflicht auf Cyberangriffe beschränkt, während andere Cybervorfälle (die z.B. von Mitarbeitenden durch eine Fehlmanipulation unabsichtlich ausgelöst wurden) und Cyberbedrohungen (z.B. nicht erfolgreiche Angriffsversuche oder Schwachstellen) weiterhin freiwillig und von jeder Person gemeldet werden können. Cyberangriffe sind dann meldepflichtig, wenn sie kritische Teilsektoren betreffen (Art. 74*b*) und einen bestimmten Schweregrad aufweisen (Art. 74*d*).

27 «Informationen» werden im ISG als Oberbegriff verwendet, unter den auch Personendaten fallen.

Buchstabe f: Cyberbedrohung

Eine Cyberbedrohung umfasst jeden Umstand oder jedes Ereignis mit dem Potenzial, einen Cybervorfall zu ermöglichen. Darunter fallen also auch alle erfolgreich abgewehrten Ereignisse, wie beispielsweise Phishing-Versuche. Die Begriffsdefinition basiert auf den international gebräuchlichen Definitionen für «Cyberthreat».[28]

Der Begriff «Cyberbedrohung» ist dem bisher häufig verwendeten Begriff «Cyberrisiko» vorzuziehen. Ein Cyberrisiko ist bei näherer Betrachtung keine Cyberbedrohung, sondern bildet nur die Einschätzung ihrer Eintrittswahrscheinlichkeit und ihres Schadenmasses ab.

Buchstabe g: Schwachstelle

Der Begriff «Schwachstelle» – d.h. eine Cyberbedrohung, die auf Schwächen oder Fehler in Informatikmitteln zurückzuführen ist – wird ebenfalls neu in die Begriffsdefinitionen aufgenommen. Eine Schwachstelle ist eine Erscheinungsform der Cyberbedrohung.

Die Definition von «Schwachstelle» orientiert sich an der Definition von «vulnerability» des US-amerikanischen *National Institute of Standards and Technology* (NIST).[29] Ursachen einer Schwachstelle können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb oder der Organisation liegen. Bisweilen wird in den Definitionen zu Schwachstellen («vulnerability») auch der Anfälligkeitsgrad («degree of vulnerability») unterschieden.[30] Hier wurde aber darauf verzichtet, verschiedene Stufen von Anfälligkeit zu unterscheiden.

Eine Schwachstelle kann selber den Cybervorfall verursachen (z. B. wenn Fehlfunktionen zu einer unzureichenden Verschlüsselung von Daten führen und dadurch direkt deren Vertraulichkeit gefährden). In aller Regel führt eine Schwachstelle in Informatikmitteln aber nur zu einer erhöhten Anfälligkeit für Cybervorfälle, z.B. indem sie als Einfallstor für Cyberangriffe genutzt werden kann.[31]

28 NIST: Cyber Threat - Glossary | CSRC (nist.gov); ISO: ISO/IEC TS 27100:2020(en), Information technology — Cybersecurity — Overview and concepts; ENISA: Glossary — ENISA (europa.eu).

29 Das *National Institute of Standards and Technology* des *U.S. Department of Commerce* (NIST) hat auf seiner Webseite folgende Definition: «Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source». Im Glossar von CISA bei der NICCS (*National Initiative for Cybersecurity Careers and Studies*) wird deutlich, dass «weakness" eine Vorstufe von «vulnerability» ist.

30 Vgl. Glossar von CISA: «Vulnerability (expressing degree of vulnerability): qualitative or quantitative expression of the level of susceptibility to harm when a threat or hazard is realized».

31 Vgl. die Definition von NISTIR 7511 Rev. 4 zu vulnerability: «error, flaw, or mistake in computer software that permits or causes an unintended behavior to occur».

2. Kapitel: Allgemeine Massnahmen

1. Abschnitt: Grundsätze

Am Schluss den 1. Abschnitts des zweiten Kapitels wurde ein neuer Artikel 10*a* eingefügt, der nichts mit der Einführung der Meldepflicht oder der Verankerung der Aufgaben des NCSC zu tun hat. Er wurde nachträglich ins ISG aufgenommen, weil für die Bearbeitung von Personendaten im Rahmen der Informationssicherheit eine materiell-gesetzliche Grundlage fehlte, die im Zuge der Teilrevision zur Meldepflicht ergänzt werden soll.

Artikel 10a Bearbeitung von Personendaten

Im Rahmen des Managements der Informationssicherheit, zum Beispiel bei der Ausbildung oder bei Audits, werden regelmässig Personendaten bearbeitet. Für die Bearbeitung dieser Daten genügt in der Regel eine Rechtsgrundlage auf Stufe der Verordnung. Die Bewältigung von Sicherheitsvorfällen setzt hingegen die Bearbeitung von Daten über potenzielle Täterinnen oder Täter voraus, die in Verbindung mit administrativen oder strafrechtlichen Verfolgungen und Sanktionen stehen können und deshalb als besonders schützenswerte Personendaten im Sinne von Artikel 3 Buchstabe c des geltenden Datenschutzgesetzes vom 19. Juni 1992[32] (DSG) bzw. von Artikel 5 Buchstabe c nDSG gelten. Bei Inkrafttreten des teilrevidierten Entwurfs gilt bereits das neue Datenschutzrecht, weshalb bereits darauf verwiesen wird.

Das Datenschutzgesetz verlangt für die Bearbeitung von besonders schützenswerten Personendaten eine Rechtsgrundlage auf Gesetzebene, die bislang fehlte und die nun mit Artikel 10*a* geschaffen wird. Bei den besonders schützenswerten Personendaten handelt es sich insbesondere um Daten über die Identität, die Handlungen, das Vorgehen und die Beweggründe von potenziellen Täterinnen und Tätern. Es werden auch Daten von Personen bearbeitet, die lediglich vom Vorfall betroffen sein können, weil sie beispielsweise einen Schaden erleiden.

Für die Bearbeitung der Personendaten muss gemäss dem DSG das Prinzip der Verhältnismässigkeit eingehalten werden, weshalb die besonders schützenswerten Personendaten nur zwei Jahren nach der Bewältigung der Informationssicherheitsverletzung oder Behebung der Schwachstelle aufbewahrt werden dürfen. Die Höchstfrist für die Bearbeitung der besonders schützenswerten Personendaten beträgt 10 Jahre, da kein festgelegtes Verfahren wie beispielsweise bei der Strafprozessordnung gesetzlich geregelt ist.

Artikel 10*a* regelt nicht die Bearbeitung von Personendaten durch das NCSC. Diese richtet sich nach den Artikeln 75 ff.

Artikel 23 Sicherheitszonen

Absatz 3

Redaktionelle Änderung im französischen Text.

32 SR **235.1**

3. Kapitel: Personensicherheitsprüfung

Artikel 44 Rechtsschutz

Absatz 2

Redaktionelle Änderung.

5. Kapitel: Massnahmen des Bundes zum Schutz der Schweiz vor Cyberbedrohungen

Im vierten Kapitel des ISG wurden keine Anpassungen vorgenommen.

Im fünften Kapitel wurden neben der Meldepflicht für Cyberangriffe auf kritische Infrastrukturen auch grundsätzliche Bestimmungen zu den Aufgaben des NCSC aufgenommen. Zur besseren Übersicht wurde das 5. Kapitel daher neu in drei Abschnitte gegliedert: «1. Abschnitt: Allgemeine Bestimmungen», «2. Abschnitt: Pflicht zur Meldung von Cyberangriffen» und «3. Abschnitt: Datenschutz und Informationsaustausch».

1. Abschnitt: Allgemeine Bestimmungen

Die Bestimmungen im 1. Abschnitt enthalten allgemeine Grundsätze, z.B. zum Meldeverfahren und dem Umgang des NCSC mit Meldungen, die auch für die Meldepflicht (2. Abschnitt) und den Datenschutz und Informationsaustausch (3. Abschnitt) gelten.

Artikel 73a Grundsatz

Absatz 1

In Absatz 1 wird die Analysetätigkeit des NCSC als Voraussetzung für seine Aufgabenerfüllung beschrieben. Die technischen Analysen des NCSC beinhalten auch das weitflächige Suchen nach infizierten Webseiten oder Schwachstellen.

Absatz 2

In Absatz 2 werden die Aufgaben es NCSC unter den Buchstaben a bis e aufgeführt. Es handelt sich um eine nicht abschliessende Aufzählung. Die einzelnen Aufgaben sowie die Zusammenarbeit mit Behörden im In- und Ausland werden in weiteren Artikeln konkretisiert und dort kommentiert.

Artikel 73b Meldungen

Das NCSC betreibt seit dem 1. Januar 2020 eine nationale Anlaufstelle für Cyberbedrohungen (vgl. Art. 12 Abs. 1 Bst. a CyRV), die Meldungen zu Cybervorfällen und Cyberbedrohungen erfasst und bearbeitet. Die Meldestelle des NCSC wurde auf der Grundlage von MELANI aufgebaut, welche seit 2004 Meldungen entgegennahm. Die Meldestelle wird von Unternehmen und Bevölkerung rege genutzt. Im Jahr 2021 gingen 21 714 Meldungen bei ihr ein.

Absatz 1

In seiner Funktion als Meldestelle nimmt das NCSC sowohl freiwillige Meldungen zu Cybervorfällen und Cyberbedrohungen entgegen wie auch Meldungen zu Cyberangriffen, die unter die Meldepflicht fallen. Dieser zweite Aspekt wird im Gesetz nicht explizit erwähnt, da Cyberangriffe eine Erscheinungsform von Cybervorfällen sind.

Cybervorfälle und Cyberbedrohungen, insbesondere Schwachstellen, können dem NCSC nicht nur von den Betroffenen selber, sondern auch von Dritten – und falls gewünscht auch anonym – gemeldet werden. Meldende müssen sich vergewissern, dass sie zur Meldung ans NCSC befugt sind, insbesondere, wenn sie für Dritte melden. Absatz 1 bildet keine Erlaubnisnorm im Sinne eines Whistleblower-Tatbestands. Vertragliche oder gesetzliche Geheimhaltungspflichten sind zu beachten.

Die Strafbarkeit für die Entdeckung von Schwachstellen durch das unbefugte Eindringen in fremde Informatikmittel (Hacken).[33] gilt weiterhin. Es ist nicht angezeigt, für Meldungen von Schwachstellen einen «Legal Safe Harbor» einzuführen, weil damit auch kriminelle Hackerinnen und Hacker – und nicht nur Sicherheitsforscher – straflos blieben bzw. sich durch eine Meldung von der Strafbarkeit befreien könnten. Der Tatbestand des Hackens bleibt somit weiterhin strafbar. Die Mitarbeitenden des NCSC sind gemäss Artikel 73*d* Absatz 3 von der Anzeigepflicht nach Artikel 22*a* BPG befreit. Überdies können Hackerinnen und Hacker oder Sicherheitsforscherinnen und Sicherheitsforscher dem NCSC entdeckte Schwachstellen anonym melden.

Absatz 2

Das NCSC analysiert die Meldungen und beurteilt, welche Bedeutung sie für den Schutz der Schweiz vor Cyberbedrohungen haben. Sofern die Meldungen nicht anonym erfolgen und die Meldenden dies wünschen, kann das NCSC basierend auf diesen Analysen Einschätzungen zum Vorfall und Empfehlungen für das weitere Vorgehen abgeben.

Das NCSC behandelt die Meldungen vertraulich. Die Vertraulichkeit der Meldungen ist eine wichtige Voraussetzung, damit überhaupt Meldungen eingehen und der Meldestelle Vertrauen entgegengebracht wird. Aus diesem Grunde wurde für Mitarbeitende des NCSC die Anzeigepflicht für Straftaten wegbedungen (vgl. 73*d* Abs. 3) und Informationen, welche das NCSC in seiner Funktion als Meldestelle von Dritten erhält, sind vom Zugangsrecht nach BGÖ ausgenommen (vgl. Art. 4 Abs. 1bis).

Absatz 3

Schwachstellen in Informatikmitteln erhöhen die Anfälligkeit für Cybervorfälle und stellen eine Cyberbedrohung dar (vgl. Art. 5 Bst. f und g). Schwachstellen können dem NCSC freiwillig gemeldet werden. Es besteht keine Meldepflicht für Schwachstellen.

33 Vgl. sog. «Hackertatbetand» in Art. 143bis StGB (SR **311.0**).

Wird dem NCSC eine Schwachstelle gemeldet, so informiert es den Herstellerinnen der betroffenen Soft- oder Hardware gemäss dem Verfahren der «Coordinated Vulnerability Disclosure».[34], damit dieser die Schwachstelle beheben und den Nutzerinnen und Nutzern eine Lösung, z.B. als «Fix» oder «Patch», zur Verfügung stellen kann. Der Begriff «Hersteller» ist funktional zu verstehen und umfasst beispielsweise auch Entwickler von Software.

Das NCSC setzt den Herstellern zur Behebung der Schwachstelle eine Frist mit dem Hinweis, dass ein Nichtbefolgen im Beschaffungsverfahren zum Ausschluss vom Verfahren oder Widerruf des Zuschlags führen kann.[35] und das NCSC die Schwachstelle nach Fristablauf veröffentlichen kann.

Wenn die Herstellerin eine Lösung für eine Schwachstelle anbietet, die nicht direkt von ihm eingespielt wird, ist es Sache der Nutzerinnen und Nutzer, ob sie diese umsetzen wollen oder nicht. Eine Pflicht, Schwachstellen zu schliessen, kommt einem starken Eingriff in die Wirtschaftsfreiheit gleich und ist nur mit erheblichem Aufwand kontrollierbar. Technisch ist es auch nicht bei jedem System sinnvoll Sicherheitsupdates in jedem Fall umzusetzen. Es wurde deshalb davon abgesehen, solche Pflichten einzuführen.

Artikel 73c Veröffentlichung von Informationen aus Meldungen

Absatz 1

Das NCSC kann Informationen zu Cybervorfällen veröffentlichen, sofern die Informationen keine Daten über natürliche oder juristische Personen enthalten. Diese Informationen dürfen nur dann Aufschluss über die betroffene natürliche oder juristische Person geben, sofern diese dazu einwilligt und es sich um missbräuchlich verwendete Identifikationsmerkmale und Adressierungselemente handelt, wie beispielsweise im Falle des Missbrauchs von Logos bei Phishing-Angriffen. Bei der missbräuchlichen Verwendung von Identifikationsmerkmalen sind in der Regel neben der jeweiligen Organisation oder Behörde, der das Logo gehört, auch Privatpersonen (z.B. die Kundschaft) betroffen. Das NCSC wird hier die Einwilligung der betroffenen Organisation oder Behörde einholen, deren Logo missbraucht wurde, um die Öffentlichkeit über diesen Missbrauch informieren zu können.

Absatz 2

Die rasche Veröffentlichung einer Schwachstelle mit Nennung der betroffenen Hard- oder Software kann notwendig sein, um weitere Cyberangriffe zu verhindern. Das NCSC wurde im September 2021 von der US-Organisation MITRE als Fachstelle für Schwachstellen, im Fachjargon auch als «Common Vulnerabilities and Exposure (CVE)» bezeichnet, anerkannt und autorisiert, diesen eine eindeutige Identifikationsnummer gemäss internationalem Referenzsystem zu vergeben, um öffentlich bekannt gewordene Schwachstellen im Bereich der Cybersicherheit zu identifizieren, zu definieren und zu katalogisieren.

34 Die «Coordinated Vulnerability Disclosure» wird auch als «Responsible Vulnerability Disclosure» bezeichnet.

35 Vgl. die Ergänzung in Artikel 44 Absatz 1 Buchstabe f^{bis} BöB.

Bei der Veröffentlichung von Schwachstellen wird der Prozess der «Coordinated Vulnerability Disclosure» eingehalten. Dieses Verfahren entspricht der gängigen Best Practice, die auch Bug-Bounty-Programme beachten. Den Herstellern wird vor der Veröffentlichung Zeit zur Behebung der Schwachstelle gewährt und das NCSC setzt dazu eine konkrete Frist.

Häufig erübrigt sich die Veröffentlichung einer Schwachstelle, wenn sie von der Herstellerin behoben wurde, insbesondere in Fällen, bei denen allfällige Patches automatisch eingespielt werden. In Einzelfällen kann es allerdings sinnvoll sein, die Öffentlichkeit auf eine Schwachstelle aufmerksam zu machen, selbst wenn diese von der Herstellerin behoben wurde. Eine Veröffentlichung ist in diesem Fall nur mit dem Einverständnis des Herstellers möglich. Falls die Herstellerin die Schwachstelle nicht behebt, kann das NCSC diese ohne sein Einverständnis veröffentlichen. Das NCSC sieht von einer Veröffentlichung ab, wenn dies dem Schutz vor Cyberbedrohungen nicht dient, z. B. wenn sie dazu führen würde, Angreiferinnen und Angreifer über mögliche Angriffsvektoren zu informieren, bevor sie diese entdeckt haben («zero day exploits»).

Absatz 2 bildet die gesetzliche Grundlage, damit das NCSC die betroffene Hard- und Software – und damit implizit deren Herstellerin – namentlich nennen darf, wenn dieser die Schwachstelle nicht fristgerecht behoben hat.

Artikel 73d Weiterleitung von Informationen

Diese Bestimmung definiert die Voraussetzungen, unter welchen es dem NCSC erlaubt ist, sicherheitsrelevante Informationen, die im Zusammenhang mit einer Meldung oder deren Analyse anfallen, an Behörden und Organisationen weiterzuleiten (Absätze 1 bis 3).

Enthalten diese Informationen gesetzliche oder vertragliche Geheimnisse, so muss sich der betreffende Mitarbeitende des NCSC, der die Weiterleitung verantwortet, nach dem Verfahren von Artikel 320 des Strafgesetzbuches[36] (StGB) vom Amtsgeheimnis entbinden lassen, um sich nicht strafbar zu machen (Absatz 4).

Absatz 1

Die Voraussetzungen für die Weiterleitung von Informationen an Behörden und Organisationen, die im Bereich der Cybersicherheit tätig sind, sind kumulativ zu erfüllen. Eine Weiterleitung setzt somit voraus, dass die betreffenden Informationen den betreffenden Cyberfachpersonen beim Schutz vor Cyberbedrohungen dienen müssen und, sofern die Informationen Aufschluss über die betroffene natürliche oder juristische Person geben, diese ihr Einverständnis erteilt hat.

Für die Weiterleitung an Cyberfachpersonen wird – im Gegensatz zur Veröffentlichung solcher Informationen gemäss Artikel 73*c* Absatz 1 – kein Identitätsmissbrauch vorausgesetzt.

36 SR **311.0**

Absatz 2

Der NDB hat gemäss Artikel 6 Absätze 1 Buchstabe a, 2 und 5 NDG den Auftrag, Bedrohungen der inneren und äusseren Sicherheit frühzeitig zu erkennen und zu verhindern, die Bedrohungslage zu beurteilen und kritische Infrastrukturen vor Bedrohungen zu warnen. Für diese Aufgaben des NDB können Informationen aus Meldungen zu Cybervorfällen und deren Analyse durch das NCSC sicherheitsrelevant sein. Das NCSC leitet deshalb Informationen, welche für diese Aufgaben des NDB nötig sind, an den NDB weiter. Die Weiterleitung an den NDB betrifft nur Informationen, die im Zusammenhang mit der Meldung eines Cybervorfalls und dessen Analyse stehen, nicht aber Informationen zu gemeldeten Schwachstellen

Absatz 3

Die für Bundesangestellte geltende Anzeigepflicht (vgl. Art. 22*a* BPG) gilt für Mitarbeitende des NCSC, wenn sie im Zusammenhang mit einer Meldung oder deren Analyse Hinweise auf eine mögliche schwere Straftat erhalten, nur gegenüber der Leiterin oder dem Leiter des NCSC. Diese Ausnahmeregelung war notwendig, weil die Anzeigepflicht in einem Spannungsfeld zum Grundsatz der vertraulichen Behandlung von Meldungen durch das NCSC steht. Für den Fall, dass Mitarbeitende des NCSC ausserhalb des Melde- und Analyseverfahrens Hinweise auf eine Straftat entdecken, gilt die Anzeigepflicht natürlich weiterhin.

Die Leiterin oder der Leiter des NCSC darf bei Verdacht auf eine schwere Straftat gestützt auf Informationen aus Meldungen oder deren Analyse die Strafverfolgungsbehörden einschalten. Das NCSC führt dabei keinerlei Ermittlungstätigkeiten durch.

Dieses Anzeigerecht für Ausnahmefälle wurde beispielsweise für Situationen vorgesehen, bei denen im Zuge der Analyse eines Vorfalls kinderpornographisches Material entdeckt wird. Die Leiterin oder der Leiter des NCSC wägt vor einer allfälligen Strafanzeige das Interesse des Staates an einer Strafverfolgung gegen das Interesse der meldenden Person an der Vertraulichkeit der Informationen ab.

Die Problematik, dass sich die meldende Person selber belastet, wird im Rahmen der Meldepflicht geregelt. Anstelle eines Selbstbelastungszwangsverbots wie im Datenschutzrecht (vgl. Art. 24 Abs. 6 nDSG) wird auf Gesetzesstufe bereits statuiert, dass zur Erfüllung der Meldepflicht eine strafrechtliche Selbstbelastung ausgeschlossen wird (vgl. Ausführungen zu Art. 74*e* Abs. 4).

Absatz 4

Für die Ausnahmefälle, in denen eine Weiterleitung von Informationen an den NDB oder die Strafverfolgungsbehörden gemäss den Absätzen 2 und 3 in Frage kommt, müssen sich die für die Weiterleitung zuständigen Mitarbeitenden des NCSC gemäss den Vorgaben von Artikel 320 StGB vom Amtsgeheimnis entbinden lassen, sofern die Informationen strafrechtlich geschützte Geheimnisse enthalten.

Artikel 74 Unterstützung für Betreiberinnen von kritischen Infrastrukturen

Zu den Aufgaben des NCSC, die in Artikel 73*a* im Sinne einer nicht abschliessenden Übersicht erwähnt werden, gehört neben der Entgegennahme und Bearbeitung von Meldungen (vgl. Art. 73*b* bis 73*d*) auch die Unterstützung von Betreiberinnen von

kritischen Infrastrukturen nach Buchstabe e, deren Leistungsumfang in Artikel 74 konkretisiert wird.

Dabei ist zu beachten, dass die Definition für kritische Infrastrukturen gemäss Artikel 5 Buchstabe c ISG sehr weit gefasst ist und daher eine gewisse Unschärfe besteht, wann ein Unternehmen oder eine Organisation als kritische Infrastruktur gilt und wann nicht.

Ferner gelten für kritische Infrastrukturen nach Artikel 2 Absätze 1 bis 3 ISG (z.B. Bundesbehörden) noch weitere Bestimmungen des ISG, die für andere kritische Infrastrukturen, wie z.B. die Migros, nicht gelten.

Absätze 1 und 2

Das NCSC unterstützt die Betreiberinnen von kritischen Infrastrukturen beim Schutz vor Cyberbedrohungen. Es stellt den Betreiberinnen kritischer Infrastrukturen zu diesem Zweck Hilfsmittel unentgeltlich zur Verfügung. Den Betreiberinnen kritischer Infrastrukturen ist es freigestellt, ob sie die Unterstützung des NCSC in Anspruch nehmen wollen. Die Hilfsmittel werden mithin zur freien Nutzung angeboten.

Die wichtigsten Hilfsmittel werden beispielhaft aufgelistet (Buchstaben a bis c). Es handelt sich um eine nicht abschliessende Aufzählung.

Buchstabe a

Der gegenseitige Informationsaustausch ist ein sehr wichtiges Mittel zum Schutz der kritischen Infrastrukturen vor Cyberbedrohungen. Die hohe Dynamik bei der Entwicklung der Bedrohungslage und die Notwendigkeit von möglichen Schutzmassnahmen bedingen, dass die Verantwortlichen stets über den aktuellsten Wissensstand verfügen. Dieser lässt sich am effizientesten im Austausch mit anderen Verantwortlichen erreichen. Das NCSC bietet in Fortführung der bewährten Zusammenarbeit über MELANI den Betreiberinnen kritischer Infrastrukturen eine Plattform für diesen Informationsaustausch. Das NCSC nutzt diesen geschützten Informationskanal auch dazu, die kritischen Infrastrukturen frühzeitig über Angriffsmuster zu informieren, die noch nicht öffentlich bekannt sind und vom NCSC aus Sicherheitsgründen auch nicht veröffentlicht werden können.

Buchstabe b

Das NCSC stellt den Betreiberinnen von kritischen Infrastrukturen technische Informationen zu aktuellen Cyberbedrohungen (z.B. Schwachstellen) sowie Empfehlungen zu präventiven und reaktiven Massnahmen gegen Cybervorfälle zur Verfügung. Diese unter Buchstabe b erwähnten Hilfsmittel beschränken sich auf Inhalte, die für kritische Infrastrukturen allgemein nützlich sein können. Es wird keine unternehmensspezifische Beratung durchgeführt.

Buchstabe c

Als weiteres Hilfsmittel bietet das NCSC auch technische Instrumente und Anleitungen für die Früherkennung von Cybervorfällen. Solche Instrumente können beispielsweise Detektionsregeln für die Erkennung von potenziell schädlichen Netzwerkflüssen und Dateien sein, Listen mit technischen Indikatoren für bereits erfolgte oder

versuchte Angriffe («Indicators of Compromise») oder spezialisierte Anwendungen für die Entdeckung von Angriffsmusstern und den Schutz vor solchen Angriffen

Diese Hilfsmittel werden teilweise so konzipiert, dass sie für alle kritischen Infrastrukturen hilfreich sind. Sie können aber auch spezifisch für gewisse Gruppen von kritischen Infrastrukturen oder für bestimmte Tätigkeitsbereiche zugeschnitten sein. Sie ersetzen nicht die Schutzdispositive der jeweiligen Infrastruktur, sondern müssen in diese eingebunden werden.

Absatz 3

Das NCSC kann Betreiberinnen kritischer Infrastrukturen bei der Bewältigung von Cybervorfällen und der Behebung von Schwachstellen mit technischer Beratung unterstützen. Die Unterstützung des NCSC für die kritischen Infrastrukturen erfolgt auf Anfrage und in enger Zusammenarbeit mit den Betroffenen.

Das NCSC kann Betreiberinnen zudem auch technisch unterstützen, wenn Cybervorfälle die Funktionsfähigkeit der betroffenen kritischen Infrastruktur gefährden. Die technische Unterstützung durch das NCSC ist vom Umfang her auf eine Notfallmassnahme beschränkt. Weitergehende Massnahmen, insbesondere zur Wiederherstellung der Cybersicherheit im Allgemeinen, sind Sache der betroffenen kritischen Infrastruktur und nicht Aufgabe des NCSC. Die Unterstützung erfolgt subsidiär zu den IT-Leistungen, die auf dem Markt erhältlich sind, sofern es sich um private Betreiberinnen handelt. Entscheidend ist dabei die Trägerschaft, nicht die Rechtsform der kritischen Infrastruktur. Die subsidiäre Unterstützung für private Betreiberinnen soll verhindern, dass das NCSC den Wettbewerb im Markt für IT-Leistungen verzerrt.

Ist die betroffene kritische Infrastruktur meldepflichtig gemäss Artikel 74*b* und 74*c*, dann hat sie Anspruch auf die technische Unterstützung des NCSC (vgl. Art. 74*a* Abs. 4). Auch in diesem Fall gilt der Vorbehalt, dass bei privatrechtlichen Organisationen keine Konkurrenzierung des IT-Dienstleistungsmarkts durch das NCSC erfolgen darf. Es unterstützt private Meldepflichtige bei der Vorfallbewältigung, wenn keine gleichwertige Marktleistung zeitnah verfügbar ist.

Absatz 4

Bei Cybervorfällen, insbesondere in Form von Cyberangriffen, soll das NCSC die Möglichkeit haben, zur Vorfallbewältigung oder zur Schadensbegrenzung auf die Systeme der betroffenen kritischen Infrastruktur zuzugreifen. Dies unter dem Vorbehalt, dass die Betreiberin der kritischen Infrastruktur ihr Einverständnis erteilt. Es ist Sache der Betreiberin, zu prüfen, ob allfällige Geheimhaltungspflichten diesem Einverständnis entgegenstehen. In der Praxis kommt es nur in Ausnahmefällen vor, dass das NCSC direkt auf die Informatikmittel zugreift. In den meisten Fällen verläuft die Zusammenarbeit zwischen NCSC und den IT-Fachpersonen der kritischen Infrastrukturen so, dass das NCSC Empfehlungen erteilt, nach welchen Indikatoren in den Systemen gesucht werden soll.

2. Abschnitt: Pflicht zur Meldung von Cyberangriffen auf kritische Infrastrukturen

Artikel 74a Grundsätze

In diesem Artikel wird der Umfang der Meldepflicht, der Meldevorgang, die Unterstellung unter die Meldepflicht sowie die Unterstützung des NCSC bei der Vorfallbewältigung geregelt. Das NCSC übt – wie bei freiwilligen Meldungen zu Cybervorfällen und -bedrohungen – auch für meldepflichtige Cyberangriffe die Funktion einer Meldestelle aus.

Absatz 1

Der Gegenstand und Adressatenkreis der Meldepflicht sowie die Meldestelle wird in Absatz 1 statuiert. Meldepflichtige müssen Cyberangriffe auf ihre Informatikmittel dem NCSC melden. Der Kreis der Meldepflichtigen wird in Artikel 74*b* aufgeführt und die Ausnahmen dazu werden in den Ausführungsbestimmungen gemäss Artikel 74*c* präzisiert werden.

Meldepflichtig sind Cyberangriffe nach Artikel 74*d* nur, wenn sie die Informatikmittel der Meldepflichtigen selber betreffen. So sind zum Beispiel die Anbieterinnen von Internetdienstleistungen nicht für Meldungen bei Vorfällen ihrer Kundinnen und Kunden zuständig.

Die Meldepflicht wird auch erfüllt, wenn Meldepflichtige einen Dritten, z.B. die Betreiberin ihrer Informatikmittel, mit der Meldung beauftragen. Falls dieselbe IT-Dienstleisterin für mehrere Meldepflichtige tätig ist, kann sie sich von mehreren Meldepflichtigen beauftragen lassen, allfällige Cyberangriffe auf ihre jeweiligen Informatikmittel an das NCSC zu melden. Aufgrund der kurzen Meldefrist von 24 Stunden (vgl. Art. 74*e* Abs. 1) werden Meldepflichtige allfällige Dritte vorausschauend beauftragen müssen, da bei Entdeckung eines Cyberangriffs für die Meldung wenig Zeit bleibt und die Vorfallbewältigung bereits viele Ressourcen binden dürfte.

Wenn Meldepflichtige Dritte mit der Meldung beauftragen, übertragen sie damit nicht die Meldepflicht per se. Ihre Meldepflicht bleibt bestehen. Versäumt der beauftragte Dritte, einen Cyberangriff ans NCSC zu melden, so muss die Meldepflichtige eine allfällige Verletzung der Meldepflicht verantworten.

Absatz 2

Da gemäss der Aufzählung in Artikel 74*b* Absatz 1 die Meldepflicht sehr viele verschiedene Bereiche erfasst, ist zu erwarten, dass selbst bei einer Präzisierung auf Verordnungsebene für gewisse Organisationen Unklarheiten verbleiben, ob sie der Meldepflicht unterstellt sind oder nicht. Damit diese Ungewissheit den Betroffenen nicht zum Nachteil gereicht und die Einführung der Meldepflicht ihre Wirksamkeit nicht einbüsst, erteilt das NCSC – soweit möglich mit einem elektronischen Fragebogen – Auskunft, ob Grenzfälle von der Meldepflicht erfasst sind oder nicht. Wird diese Einordnung des NCSC vom Betroffenen bezweifelt oder bestritten, wird das NCSC eine anfechtbare Verfügung mit Rechtsmittelbelehrung erlassen.

Absatz 3

Die Unterstellung unter die Meldepflicht soll für die Betroffenen nicht nur mit wenig Aufwand verbunden sein, sondern auch konkrete Vorteile bringen. Entsprechend haben Meldepflichtige, die einen Cyberangriff auf ihre Informatikmittel entdecken und diesen form- und fristgerecht ans NCSC melden, Anspruch auf die Unterstützung des NCSC bei der Vorfallbewältigung gemäss Artikel 74 Absatz 3. Bei beschränkten Kapazitäten wird das NCSC folglich Meldepflichtige vorrangig unterstützen.

Der Anspruch auf Unterstützung durch das NCSC garantiert den Meldepflichtigen, dass der Nutzen der Meldepflicht eine allfällige Mehrbelastung überwiegt und sie nicht nur einen Gegenwert erhalten, sondern allenfalls auch einen Mehrwert.

Absatz 4

Die Meldepflicht bezweckt, dass das NCSC Angriffsmuster auf kritische Infrastrukturen frühzeitig erkennen und dadurch mögliche Betroffene warnen und ihnen geeignete Präventions- und Abwehrmassnahmen empfehlen kann. Die Empfehlung von Präventions- und Abwehrmassnahmen gehört zu den gesetzlichen Aufgaben des NCSC.

Das NCSC hat keine Aufsichtsfunktion über die Meldepflichtigen; die Meldepflicht für Cyberangriffe ist daher auch kein Kontrollinstrument[37]. Für das NCSC bildet die Meldepflicht ein wertvolles Instrument, um frühzeitig über Angriffe im Bilde zu sein und somit die Cybersicherheit von kritischen Infrastrukturen durch gezielte Abwehr- und Präventionsmassnahmen verbessern zu können.

Aus dem Zweck der Meldepflicht ergibt sich, dass sie auf Cyberangriffe beschränkt sein muss. Meldungen zu Cybervorfällen, welche durch Fehlmanipulationen oder -funktionen entstehen, sind für Warnungen zum Schutz der Cybersicherheit nicht relevant. Meldungen zu Cyberbedrohungen, namentlich Schwachstellen, fallen ebenfalls nicht unter die Meldepflicht (vgl. 4.1).

Obschon ein Cyberangriff in aller Regel auch die Datensicherheit verletzt, verfolgt die Meldepflicht für Cyberangriffe einen anderen Zweck als die datenschutzrechtliche Meldepflicht (vgl. Art. 24 nDSG). Während die Meldepflichten im Bereich der Flug- oder Nuklearsicherheit eine lückenlose Erfassung möglichst aller, also auch kleiner Fehler im Sinne einer Sicherheitskultur anstreben, hat die Meldepflicht für Cyberangriffe keine eigenen Fehler zum Gegenstand, weshalb auch die «just culture»[38] bei der Sanktionierung keine Anwendung findet.

Artikel 74b Meldepflichtige Behörden und Organisationen

Grundsätzlich erfasst der Geltungsbereich der Meldepflicht jene Bereiche, welche aus Sicht der Cybersicherheit besonders lohnende Ziele für Cyberangriffe darstellen. Die

37 Anders liegt der Fall im Finanzmarktsektor in Bezug auf die Meldepflicht an die FINMA, da diese zugleich Aufsichtsbehörde über die Meldepflichtigen ist.

38 Gemäss der Webseite https://www.justculture.ch/was-ist-just-culture ist «just culture» eine Kultur, in der operative Mitarbeitende oder andere Personen nicht für Handlungen, Unterlassungen oder Entscheidungen, die ihrer Erfahrung und Ausbildung entsprechen, bestraft werden, jedoch Grobfahrlässigkeit, vorsätzliche Verstösse und destruktives Handeln nicht toleriert werden.

abschliessende Aufzählung in Artikel 74*b* orientiert sich an den kritischen Teilsektoren der Nationalen Strategie zum Schutz kritischer Infrastrukturen 2018–2022[39] (SKI), bzw. den Erkenntnissen des für die Umsetzung der SKI-Strategie zuständigen Bundesamts für Bevölkerungsschutz (BABS).

Da die Definition für kritische Infrastrukturen sehr breit gefasst ist,[40] ist davon auszugehen, dass fast alle Meldepflichtigen zugleich zu den kritischen Infrastrukturen nach Artikel 5 Buchstabe c ISG zählen.

Der Geltungsbereich der Meldepflicht wird, soweit möglich, mit Verweisen auf bestehende rechtliche Grundlagen konkretisiert. In Bereichen, in welchen kein solcher Verweis möglich ist – da keine rechtlichen Grundlagen bestehen, die für eine solche Eingrenzung geeignet sind – wird der betreffende Bereich möglichst genau bezeichnet. Dieses Vorgehen soll dafür sorgen, dass bereits auf Gesetzesstufe Klarheit darüber herrscht, wer der Meldepflicht unterstellt ist.

Angesichts des weit gefassten Adressatenkreises ist nicht damit zu rechnen, dass die Aufzählung in den kommenden Jahren ergänzt werden muss. In den Ausführungsbestimmungen kann der Bundesrat den Adressatenkreis der einzelnen Bereiche weiter konkretisieren und präzisieren. Sollte die Unterstellung unter die Meldepflicht dennoch in Einzelfällen unklar sein, so ist das NCSC befugt, diese Frage für einen konkreten Grenzfall nach Rücksprache mit dem BABS und den sektoriellen Aufsichts- und Regulierungsbehörden verfügungsweise zu entscheiden (vgl. Art. 74*a* Abs. 2).

Ferner wird der Bundesrat Ausnahmen von der Meldepflicht innerhalb gewisser Bereiche mittels Schwellenwerten festlegen. Der Bundesrat ist also verpflichtet, die Verhältnismässigkeit der Meldepflicht sicherzustellen, indem er diejenigen Organisationen von der Meldepflicht befreit, die für das Funktionieren der Wirtschaft beziehungsweise das Wohlergehen der Bevölkerung nicht essentiell sind (vgl. Art. 74*c*).

Absatz 1

Buchstabe a: Hochschulen

Hochschulen sind für den Bildungs- und Wirtschaftsstandort Schweiz von grosser Bedeutung. Insbesondere ihre Forschung ist ein Treiber der Innovation. Dadurch sind Hochschulen aber auch ein attraktives Ziel für Cyberangriffe. Der Meldepflicht unterstellt sind die kantonalen Universitäten, die Eidgenössischen Technischen Hochschulen, die Fachhochschulen und die pädagogischen Hochschulen.

Buchstabe b: Behörden

Cyberangriffe auf Behörden aller föderalen Ebenen sind meldepflichtig, da es wichtig ist zu wissen, wie oft und durch wen Behörden angegriffen werden. So können die

39 BBI **2018** 503

40 Art. 5 Bst. c ISG enthält folgende Definition für kritische Infrastrukturen: «Trinkwasser- und Energieversorgung, Informations-, Kommunikations- und Transportinfrastrukturen sowie weitere Prozesse, Systeme und Einrichtungen, die essenziell für das Funktionieren der Wirtschaft beziehungsweise das Wohlergehen der Bevölkerung sind».

Abwehrdispositive jeweils auf die relevanten Bedrohungen ausgerichtet werden. Zu den Behörden zählen auch das Bundesparlament sowie die kantonalen Parlamente.

Die Gruppe Verteidigung als Verwaltungseinheit des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport ist von der Meldepflicht ausgenommen, wenn die Armee Assistenzdienst nach Artikel 67 oder Aktivdienst nach Artikel 76 des Militärgesetzes vom 3. Februar 1995[41] leistet. In diesen Fällen könnte die Meldepflicht militärische Geheimnisse gefährden oder die Zusammenarbeit mit Partnerorganisationen erschweren.

Buchstabe c: Organisationen der Sicherheit und Rettung, der Trinkwasserversorgung, der Abwasserversorgung und der Abfallentsorgung

Organisationen, welche öffentlich-rechtliche Aufgaben in bestimmten Bereichen wahrnehmen, sind der Meldepflicht unterstellt. Buchstabe c zählt auf, welche Tätigkeiten damit konkret gemeint sind. Im Bereich Sicherheit und Rettung liegt der Fokus auf den Blaulichtorganisationen (Polizei, Feuerwehr, Sanität- und Rettungsdienste). Daneben sind auch Organisationen der Trinkwasserversorgung, der Abwasseraufbereitung und der Abfallentsorgung meldepflichtig. Die Meldepflicht gilt dabei nur für das hoheitliche Handeln dieser Behörden und Organisationen.

Buchstabe d: Energieversorgung, -handel, -messung und -steuerung

Die Versorgung mit Energie ist für die Wirtschaft und Gesellschaft essentiell. Verschiedene Angriffe auf die Stromversorgung oder auf Pipelines in anderen Staaten haben gezeigt, dass diese Infrastrukturen gezielt angegriffen werden, sei es aus politischen Motiven oder um möglichst hohe Summen zu erpressen. Unternehmen mit Tätigkeiten, die für die Versorgung mit Energie wichtig sind, werden deshalb der Meldepflicht unterstellt. Gemäss Artikel 6 Absatz 1 des Energiegesetzes vom 30. September 2016[42] umfasst die Energieversorgung «Gewinnung, Umwandlung, Lagerung und Speicherung, Bereitstellung, Transport, Übertragung sowie Verteilung von Energieträgern und Energie bis zur Endverbraucherin und zum Endverbraucher, einschliesslich der Ein-, Aus- und Durchfuhr». Zusätzlich werden auch Unternehmen erfasst, die in den Bereichen Energiehandel, -messung oder -steuerung tätig sind.

Bewilligungsinhaber gemäss dem Kernenergiegesetz vom 21. März 2003[43] (KEG) sind von der Meldepflicht für Cyberangriffe ausgenommen, sofern ein Cyberangriff auf eine Kernanlage erfolgt. Sie haben im Hinblick auf die nukleare Aufsicht bereits umfangreiche Meldepflichten für Vorkommnisse im Sicherheits- und Sicherungsbereich an das ENSI, u.a. auch für Cyberangriffe auf Kernanlagen (vgl. Art. 22 Abs. 2 Bst. f KEG i.V.m. Art. 38 Abs. 3 und Art. 39 Abs. 2 der Kernenergieverordnung vom 10. Dezember 2000[44]).

Als Bundesbehörde, welche die schweizerischen Kernanlagen beaufsichtigt, verfügt das ENSI über eine sektorielle Meldestelle, die auch im Cyberbereich jederzeit über

41 SR **510.10**
42 SR **730.0**43 SR **732.1**
43 SR **732.1**
44 SR **732.11**.

eine in Bereitschaft stehende und mit technisch ausgebildetem Fachpersonal ausgestattete Organisation verfügt. Die festgelegten Prozesse für die Meldungen sind etabliert und praxiserprobt, damit sie bei Vorkommnissen in einer Kernanlage zuverlässig funktionieren.

Auf eine zusätzliche Meldepflicht für Bewilligungsinhaber nach KEG wird in diesem eng umschriebenen Bereich verzichtet, um die Gefahr auszuschliessen, dass im Ereignisfall die etablierten, im Bereich der nuklearen Sicherheit sensiblen Prozesse gestört werden könnten. Dafür wird das ENSI mit der Einführung von Artikel 102 Absatz 2 KEG verpflichtet, allfällige Meldungen zu einem Cyberangriff auf eine Kernanlage, der die Voraussetzungen von Artikel 74*d* erfüllt, dem NCSC weiterzuleiten.

Buchstabe e: Banken, Versicherungen und Finanzmarktinfrastrukturen

Die Unternehmen des Finanzsektors sind stark betroffen von Cyberangriffen, da sie auf Grund der beträchtlichen finanziellen Mittel, welche sie verwalten, ein attraktives Ziel für Kriminelle darstellen. Für die Verlässlichkeit des Finanzplatzes Schweiz ist es wichtig, dass solche Angriffe gemeldet werden. Die bereits bestehende Meldepflicht für Cyberangriffe gegenüber der Finanzmarktaufsicht FINMA bleibt parallel zur neuen Meldepflicht ans NCSC bestehen. Die FINMA und das NCSC werden sich beim Meldevorgang abstimmen, damit der Aufwand für die Meldepflichtigen so gering wie möglich ausfällt.

Buchstabe f: Gesundheitseinrichtungen

Als Spital gilt gemäss Artikel 4 Absatz 1 Buchstabe l der Medizinprodukteverordnung vom 1. Juli 2020[45] eine Gesundheitseinrichtung, in der durch ärztliche und pflegerische Hilfeleistungen stationäre Behandlungen von Krankheiten oder stationäre Massnahmen der medizinischen Rehabilitation oder stationäre medizinische Massnahmen zum Zwecke der Ästhetik durchgeführt werden. Meldepflichtig sind aber gemäss Artikel 39 Absatz 1 Buchstabe e des Bundesgesetzes vom 18. März 1994[46] über die Krankenversicherung (KVG) nur diejenigen Spitäler, die auf der Spitalliste ihres Kantons aufgeführt sind.

Die in den kantonalen Spitallisten aufgeführten Spitäler für Akutsomatik, Rehabilitation und Psychiatrie gewährleisten die Deckung des Bedarfs an medizinischer Grundversorgung auf dem jeweiligen Kantonsgebiet. In die Spitalliste können gemäss Artikel 39 Absatz 3 KVG auch Geburtshäuser sowie Pflegeheime aufgenommen werden. Die Meldepflicht für Cyberangriffe soll für alle gelisteten Gesundheitseinrichtungen gelten, weil es zu verhindern gilt, dass die Grundversorgung durch solche Angriffe beeinträchtigt wird. Führen Cyberangriffe auf Gesundheitseinrichtungen oder auf das Bundesamt für Gesundheit dazu, dass Daten in elektronischen Patientendossiers gefährdet sind, ist jene Organisation meldepflichtig, welche vom Cyberangriff betroffen worden ist.

45 SR **812.213**
46 SR **832.10**

Buchstabe g: medizinische Laboratorien

Laboratorien, die mikrobiologische Untersuchungen zur Erkennung von übertragbaren Krankheiten durchführen, sind für die Gesundheitsversorgung wichtig. Bei ihren Analysen und in der Zusammenarbeit mit den Grundversorgern sind sie in grossem Ausmass von funktionierenden IT-Infrastrukturen abhängig. Cyberangriffe auf solche Laboratorien sollen deshalb meldepflichtig sein.

Buchstabe h: Herstellung, Inverkehrbringen und Einfuhr von Arzneimitteln

Für die medizinische Versorgung der Bevölkerung ist die Herstellung, der Vertrieb und die Einfuhr von Arzneimitteln von grosser Bedeutung. Unternehmen, welche in diesen Bereichen tätig sind und eine Bewilligung nach dem Heilmittelgesetz vom 15. Dezember 2000[47] haben, werden daher der Meldepflicht unterstellt.

Buchstabe i: Sozialversicherungen

Organisationen, die Leistungen zur Absicherung gegen die Folgen von Krankheit, Unfall, Arbeits- und Erwerbsunfähigkeit, Alter, Invalidität und Hilflosigkeit erbringen, sind ebenfalls meldepflichtig. Der Begriff «Sozialversicherungen» wird im Gesetzestext nicht erwähnt, da er nicht gesetzlich definiert wird.

Die Meldepflicht wird anhand der Leistungen für Risiken umschrieben, die in den Allgemeinen Bestimmungen des Bundesgesetzes vom 6. Oktober 2000[48] über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG) erfasst sind, um möglichst alle Zweige der Sozialversicherungen abzudecken. Die Meldepflicht ist aber nicht auf Sozialversicherungen beschränkt, die dem ATSG unterstellt sind. Es wurde auf die Aufzählung einzelner Gesetze (z.B. Bundesgesetz vom 19. Juni 1959[49] über die Invalidenversicherung, Bundesgesetz vom 20. Dezember 1946[50] über die Alters- und Hinterlassenenversicherung) verzichtet, um nicht nur gesetzliche, sondern auch überobligatorische Leistungen, beispielsweise der beruflichen Vorsorge oder der Zusatzversicherung zur obligatorischen Krankenkasse, abzudecken.

Bei der beruflichen Vorsorge (im Sinne der 2. Säule) werden alle registrierten und nicht registrierten Vorsorgeeinrichtungen (inkl. Auffangeinrichtungen), die Freizügigkeitseinrichtungen und der Sicherheitsfond erfasst.

Die freiwillige Selbstvorsorge (Säule 3a und 3b) wird in aller Regel von Banken und Versicherungen angeboten, die ihrerseits der Meldepflicht unterstehen.

Auf Verordnungsstufe kann der Bundesrat auch im Falle der Sozialversicherungen Einschränkungen für den Kreis der Meldepflichtigen vornehmen und beispielsweise den Adressatenkreis der meldepflichtigen Vorsorge- und Freizügigkeitseinrichtungen durch geeignete Kriterien einschränken (vgl. Art. 74*c* sowie die Ausführungen unter 4.3.3).

47 SR **812.21**
48 SR **830.1**
49 SR **831.20**
50 SR **831.10**

Buchstabe j: Schweizerische Radio- und Fernsehgesellschaft (SRG)

Die Schweizerische Radio- und Fernsehgesellschaft (SRG) hat den Auftrag, die gesamte Bevölkerung inhaltlich umfassend mit gleichwertigen Radio- und Fernsehprogrammen in den drei Amtssprachen zu versorgen. Sie hat zudem gemäss Artikel 24 Absätze 1 Buchstabe a und 4 Buchstabe a des Bundesgesetzes vom 24. März 2006[51] über Radio und Fernsehen den Auftrag, zur freien Meinungsäusserung durch umfassende, vielfältige und sachgerechte Information, insbesondere über politische, wirtschaftliche und soziale Zusammenhänge, beizutragen. Damit geht ihr Auftrag deutlich über die Bekanntmachungspflichten der übrigen konzessionierten Medien hinaus und machen die SRG zu einem lohnenden Ziel für einen Cyberangriff. Daher rechtfertigt es sich, nur die SRG der Meldepflicht zu unterstellen.

Buchstabe k: Nachrichtenagenturen von nationaler Bedeutung

Eine Nachrichtenagentur ist von nationaler Bedeutung und kann gemäss Art. 44*a* der Radio- und Fernsehverordnung vom 9. März 2007[52] durch den Bund unterstützt werden, wenn ihre Berichterstattung alle vier Sprachregionen abdeckt und sie regelmässig in drei Landessprachen erfolgt (vgl. Art. 18 Bst. a des Sprachengesetzes vom 5. Oktober 2007[53] i.V.m. Art. 13 Abs. 2 der Sprachenverordnung vom 4. Juni 2010[54]). Konkret gibt es in der Schweiz nur noch die Nachrichtenagentur Keystone-SDA (siehe Covid-19-Verordnung elektronische Medien vom 20. Mai 2020[55]).

Buchstabe l: Anbieterinnen von Postdiensten

Unternehmen, welche Kundinnen und Kunden in eigenem Namen Postdienste anbieten, unterliegen ebenfalls der Meldepflicht, sofern sie bei der Postkommission gemäss Artikel 4 Absatz 1 des Postgesetzes vom 17. Dezember[56] registriert sind. Der Bundesrat kann auf Verordnungsebene kleinere Unternehmen von der Meldepflicht ausnehmen. Es wäre beispielsweise eine analoge Einschränkung denkbar, wie sie in Artikel 4 Absatz 2 des Postgesetzes für Unternehmen vorgesehen ist, die einen geringen Umsatz erzielen.

Buchstabe m: Öffentlicher Verkehr (Personentransport plus Eisenbahngüterverkehr)

Mit dem Verweis auf die beiden einschlägigen Bundesgesetze (Eisenbahngesetz vom 20. Dezember 1957[57] und Personenbeförderungsgesetz vom 20. März 2009[58] [PBG]) werden die wichtigsten Bereiche des öffentlichen Personenverkehrs, des Schienengüterverkehrs und die Eisenbahninfrastruktur erfasst. Nicht unter die Bestimmung fallen somit kleinere Bus- oder Seilbahnunternehmen, die über eine kantonale Bewilligung nach Artikel 7 PBG verfügen. Ebenfalls nicht erfasst wird der grenzüberschreitende Personenverkehr. Die eigenständige Auflistung der Eisenbahnunternehmen ist erforderlich, weil der Schienengüterverkehr keiner Konzessionspflicht untersteht.

51 SR **784.40**
52 SR **784.401**
53 SR **441.1**
54 SR **441.11**
55 SR **784.402**
56 SR **783.0**
57 SR **742.101**
58 SR **745.1**

Buchstabe n: Unternehmen der Zivilluftfahrt

Unternehmen der Zivilluftfahrt, die über eine Bewilligung des Bundesamtes für Zivilluftfahrt verfügen (z.B. die Betriebsbewilligung gemäss Artikel 27 des Luftfahrtgesetzes vom 21. Dezember 1948[59] [LFG]), sowie die Landesflughäfen gemäss Sachplan Infrastruktur Luftfahrt (SIL) sollen der Meldepflicht für Cyberangriffe unterstellt werden.

Im Luftfahrtgesetz werden nur die Landesflughäfen Zürich und Genf erwähnt (vgl. Art. 37*u* Abs. 2 LFG) nicht aber Basel. Es schien daher notwendig, auf den SIL zu verweisen, um alle Landesflughäfen erfassen zu können. Der Bundesrat verabschiedet für jeden Landesflughafen (Zürich, Basel, Genf) ein SIL-Objektblatt. Die Plangenehmigung für Flughäfen bewilligt das Eidgenössische Departement für Umwelt, Verkehr, Energie und Kommunikation (vgl. Art. 37 ff. LFG).

Buchstabe o: Hafen Basel und Rheinschifffahrt

Die Schweizerischen Rheinhäfen bilden den Zugang der Schweiz zu den Weltmeeren. Sie sind für die Versorgung der Schweiz mit Gütern aller Art von grosser Bedeutung. Die Meldepflicht für Cyberangriffe gilt deshalb für die Schifffahrt auf dem Rhein zur Güterbeförderung nach dem Seeschifffahrtsgesetz vom 23. September 1953[60] und für die für den Betrieb und die Funktion vom Hafen Basel relevanten Prozesse.

Buchstabe p: Unentbehrliche Güter des täglichen Bedarfs

In die Versorgung der Bevölkerung mit unentbehrlichen Gütern des täglichen Bedarfs, insbesondere Lebensmittel, ist eine Vielzahl von Akteurinnen eingebunden. Neben den Produzentinnen und Importeurinnen spielen auch die Verarbeiterinnen, die Verteilzentren und die Detailhändlerinnen eine bedeutende Rolle. Nicht alle dieser Akteurinnen sind gleichbedeutend für die Versorgungssicherheit der Schweiz. Deshalb wurde bereits auf Gesetzesstufe eine Einschränkung auf Unternehmen vorgenommen, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen führen würde.

Die Meldepflicht für Cyberangriffe soll somit nur für jene Akteurinnen gelten, welche in dieser Hinsicht eine wichtige Bedeutung haben. Der Bundesrat wird daher die Meldepflicht im Bereich der Versorgung mit unentbehrlichen Gütern des täglichen Bedarfs auf Verordnungsebene gemäss den Kriterien von Artikel 74*c* einschränken.

Buchstabe q: Anbieterinnen von Fernmeldediensten

Gemäss Artikel 3 Buchstabe c des Fernmeldegesetzes vom 30. April 1997[61] (FMG) ist eine fernmeldetechnische Übertragung ein elektrisches, magnetisches, optisches oder anderes elektromagnetisches Senden oder Empfangen von Informationen über Leitungen oder Funk. Als fernmeldetechnische Übertragung gilt auch das Anbieten von Übertragungskapazität.

59 SR **748.0**
60 SR **747.30**
61 SR **784.10**

Wer eine Übertragung von Informationen für Dritte erbringt, gilt grundsätzlich als Fernmeldedienstanbieterin. Meldepflichtig sind Fernmeldedienstanbieterinnen, welche gemäss Artikel 4 FMG registriert sind.

Buchstabe r: Registerbetreiberinnen und Registrare von Internet-Domains

Durch Internet-Domain-Namen ist es möglich, jeder Website eine einmalige Adresse zuzuweisen. Solche Namen, wie zum Beispiel bakom.ch, werden vor allem für den Zugriff auf Websites oder den Versand von E-Mails verwendet.

Internet-Domains werden global bei der *Internet Corporation for Assigned Names and Numbers* (ICANN) verwaltet. Der Bund verwaltet Domain-Namen der ersten Ebene mit Bezug zur Schweiz gemäss Artikel 28*b* ff. FMG .

Das Bundesamt für Kommunikation übt die Funktion als Registerbetreiberin aus; es hat diese Aufgabe allerdings an SWITCH delegiert. Es kann unter bestimmten Voraussetzungen als Registrar tätig sein, wenn kein befriedigendes Marktangebot besteht. Für die Domains «.ch» und «.swiss» ist die Registerbetreiberin («registry») für die zentrale technische und operationelle Verwaltung der Domains zuständig, während die Funktion des Registrars, die von mehreren Unternehmen ausgeübt werden kann, gemäss Verordnung vom 5. November 2014[62] über Internet-Domains (VID) die Domain-Namen im freien Wettbewerb vermarkten.

Registrare, die einen Registrarvertrag mit der Registerbetreiberin abgeschlossen haben, können Domain-Namen für ihre Kundinnen und Kunden beantragen und verwalten. Die Registrare fungieren so als exklusive Schnittstelle zwischen der Registerbetreiberin und der gesuchstellenden Person (vgl. Art. 24 Abs. 1 und Anhang Bst. m VID).

Buchstabe s: Politische Rechte

Dienste und Infrastrukturen im Bereich der politischen Rechte umfassen Systeme, welche zur Sammlung und Auszählung von Unterschriften zu Volksbegehren sowie zur Vorbereitung, Durchführung und Nachbereitung von Urnengängen eingesetzt werden.

Darunter sind beispielsweise Systeme zur elektronischen Stimmabgabe (E-Voting), Systeme zur Führung von Stimmregistern und zur Ermittlung und Übermittlung der Ergebnisse von Urnengängen gemeint. Hinzu kommen allfällige künftige Systeme zur elektronischen Unterschriftensammlung (E-Collecting). Zu den weiteren Diensten und Infrastrukturen gehören beispielsweise Unternehmen, welche mit dem Druck des Stimmmaterials beauftragt werden.

Buchstabe t: Digitale Dienste

Die Meldepflicht gilt für Anbieterinnen und Betreiberinnen von Cloudcomputing (z.B. Software-as-a-Service, SaaS), von Suchmaschinen, von digitalen Sicherheits- und Vertrauensdiensten sowie von Rechenzentren, sofern sie einen Sitz in der Schweiz haben.

62 SR **784.104.2**

Der Begriff «Vertrauensdienst» umfasst analog zum EU-Recht[63] Dienste in den Bereichen elektronische Signatur, Siegel und Zeitstempel, Zustellung elektronischer Einschreiben, Zertifikate für die Authentifizierung sowie (Auf-)Bewahrungsdienste für elektronische Signatur, Siegel und Zertifikate. Als Vertrauensdienst gilt somit beispielsweise auch die E-ID.

Mit Sicherheitsdienst sind insbesondere Lösungen für die Verschlüsselung von Informationen gemeint oder den Informatikmitteln zum Schutz vor Cyberangriffen dienen (Spamfilter, Antiviren-Programme, Firewalls).

Buchstabe u: Herstellerinnen von Hard- und Software

Cyberangriffe auf kritische Infrastrukturen, die über deren Lieferketten erfolgen, sind zu einer relevanten Bedrohung geworden. Dabei stehen insbesondere die Zulieferinnen von Hard- und Software im Fokus. Die Angreiferinnen und Angreifer manipulieren dabei die Informatikmittel bereits vor der Auslieferung an die Endkundinnen, damit sie später Zugriff auf die Systeme erhalten. Für die Cybersicherheit sind deshalb Cyberangriffe auf die Herstellerinnen der Hard- und Software kritischer Infrastrukturen von grosser Bedeutung.

Besonders relevant sind Cyberangriffe auf Herstellerinnen, wenn diese über Fernwartungszugänge zu den Systemen verfügen. Fernwartungszugänge erlauben Herstellerinnen, die über entsprechende Berechtigungen verfügen, zum Zweck der Wartung oder zur Störungsbeseitigung von aussen – d. h. in der Regel über das Internet – auf IT- und OT-Komponenten im lokalen Netz zuzugreifen. Angreiferinnen und Angreifer können versuchen, über solche legitimen Zugänge direkt in die Systeme der kritischen Infrastrukturen einzudringen.

Neben dem Kriterium des Fernwartungszugangs sind Herstellerinnen von Hard- und Software auch dann meldepflichtig, wenn ihre Produkte in besonders heiklen Bereichen zum Einsatz kommen. Dies betrifft Hard- und Software zur Steuerung und Überwachung von physischen Geräten, Prozessen und Ereignissen (sog. Betriebstechnik oder Operational Technology). Dazu zählen insbesondere industrielle Steuerungssysteme (Industrial Control Systems) und Automationslösungen, die Steuerungs- und Regelfunktionen aller Art übernehmen. Weitere Beispiele sind Laborgeräte, z.B. automatisierte Mikroskope oder Analysewerkzeuge, Logistiksysteme, wie Barcodescanner mit Kleinrechner, oder Gebäudeleittechnik (Ziff. 1).

Ebenfalls im Fokus steht Hard- und Software, welche zur Gewährleistung der öffentlichen Sicherheit eingesetzt wird (Ziff. 2). Zu denken ist hier insbesondere an die Kommunikation von Blaulichtorganisationen oder die Systeme für die polizeiliche Ermittlung.

63 Die Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (kurz: eIDAS-Verordnung), ABl. L 257 vom 28.8.2014, S. 73, definiert in Art. 3 Ziff. 16 den Vertrauensdienst.

Absatz 2

Für Grossunternehmen, Konglomerate und Konzerne mit Tätigkeitsbereichen, die teilweise unter die Aufzählung von Absatz 1 fallen, gilt die Meldepflicht für Cyberangriffe nicht für alle ihre Tätigkeiten, sondern ausschliesslich dann, wenn sie einen Bereich betreffen, der in Absatz 1 erwähnt wird. Betreibt beispielsweise ein Unternehmen der Lebensmittelversorgung gleichzeitig noch Freizeitparks oder ein Finanzinstitut ein Museum, dann sind diese Unternehmen nur dann meldepflichtig, wenn ein Cyberangriff die Informatikmittel betreffen, welch für die Aufgaben der Lebensmittelversorgung respektive der Finanzdienstleistungen relevant sind.

Absatz 3

Bei international tätigen Unternehmen und Organisationen stellt sich die Frage, ob sie auch für Cyberangriffe auf Informatikmittel, die sich im Ausland befinden, meldepflichtig werden. Dies ist dann zu bejahen, wenn diese Unternehmen und Organisationen einen Sitz in der Schweiz haben, eine Tätigkeit in einem Bereich nach Absatz 1 ausüben und die vom Cyberangriff betroffenen Informatikmittel für die Ausübung dieser Tätigkeit in der Schweiz dienen.

Artikel 74c Ausnahmen von der Meldepflicht

Der Adressatenkreis der Meldepflicht nach Artikel 74*b* ist breit gefasst. Er kann auch Organisationen und Behörden umfassen, welche für sich alleine betrachtet, d.h. aufgrund ihrer Grösse oder ihres Versorgungsgrades, nicht von essentieller Bedeutung für das Funktionieren der Wirtschaft beziehungsweise das Wohlergehen der Bevölkerung sind, obschon sie in einem kritischen Teilsektor tätig sind, der in Artikel 74*b* Absatz 1 erwähnt wird.

Artikel 74*c* legt daher fest, dass der Bundesrat den Adressatenkreis auf Verordnungsebene weiter einschränken muss. Ein Ausschluss von der Meldepflicht ist dann vorgesehen, wenn ein Funktionsausfall bei einer Organisation oder einer Behörde nur geringe Auswirkungen auf die Wirtschaft oder das Wohlergehen der Bevölkerung hat. Messbar sind solche Auswirkungen namentlich an der Anzahl der betroffenen Personen.

Artikel 74d Zu meldende Cyberangriffe

Der Umfang der Meldepflicht, d.h. welche Art von Cyberangriffen zu melden sind, ist auf Gesetzesebene zu verankern. Die Buchstaben a bis d enthalten die entsprechenden Kriterien, die bestimmen, welche Cyberangriffe zum Zweck der Frühwarnung und Beurteilung der Bedrohungslage besonders relevant und deshalb meldepflichtig sind. Die Kriterien sind so gewählt, dass sie für die Unternehmen möglichst direkt feststellbar sind. Die Kriterien werden auf Verordnungsstufe, sofern notwendig, weiter präzisiert.

Buchstabe a

Die Gefährdung der Funktionsfähigkeit ist das einzige Kriterium, das sich nicht an der Relevanz für Cybersicherheit, sondern an den Auswirkungen orientiert. Es wurde

deshalb als Schwelle für meldepflichtige Cyberangriffe aufgenommen, weil das Schadenspotential auch ausschlaggebend ist für den Anspruch auf Unterstützung bei der Vorfallsbewältigung durch das NCSC (vgl. Art. 74*a* Abs. 4 i.V.m. Art. 74 Abs. 3).

Buchstabe b

Die Manipulation von Informationen ist ein Kriterium, das einen Cyberangriff meldepflichtig macht. Zur Manipulation zählen beispielsweise die Verschlüsselung von Informationen der betroffenen Organisation.

Buchstabe c

Falls ein Cyberangriff längere Zeit unentdeckt blieb, kann eine Ausspionierung, z. B. für Industriespionage, oder die Vorbereitung für weitere Angriffe nicht ausgeschlossen werden. Erkenntnisse über Angriffe, welche absichtlich so ausgeführt werden, dass eine Entdeckung möglichst schwierig ist, sind für die Warnung von anderen Betreiberinnen kritischer Infrastrukturen von besonderer Relevanz.

Buchstabe d

In Buchstabe d wird statuiert, dass bei strafrechtlich relevanten Begleitumständen ein Cyberangriff immer zu melden ist. Viele Cyberkriminelle versuchen über die Androhung oder Durchführung von Angriffen die Betreiberinnen kritischer Infrastrukturen, deren Kundinnen und Kunden oder einzelne Mitarbeitende zu erpressen (beispielsweise 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 kompromittierenden Informationen über Einzelpersonen).

Cyberangriffe mit strafrechtlich relevanten Begleitumständen sind dann zu melden, wenn die Erpressung, Drohung oder Nötigung einen Bezug zum meldepflichtigen Unternehmen hat und sich auf dessen Geschäftstätigkeit negativ auswirken kann. Die Meldung solcher Angriffe ist wichtig, damit eingeschätzt werden kann, wie stark die Bedrohung kritischer Infrastrukturen durch Cyberkriminelle ist.

Artikel 74e Frist und Inhalt der Meldung

Absatz 1

Es ist für die Frühwarnung und die Prävention entscheidend, dass Angriffe unmittelbar nach deren Entdeckung gemeldet werden. Eine Meldefrist von 24 Stunden trägt diesem Ziel Rechnung. Innerhalb von 24 Stunden müssen nur die bis dahin bekannten Informationen gemeldet werden; die Meldung kann später ergänzt werden.[64]

Absatz 2

Der Inhalt der Meldung, d.h. die wesentlichen Informationen, die für die Erfüllung der Meldepflicht notwendig sind, werden in Absatz 2 gesetzlich verankert. Der kon-

64 Vgl. FINMA-Aufsichtsmitteilung 05/2020, online abrufbar unter www.finma.ch > Dokumente > Finma-Aufsichtsmitteilung 05/2020.

krete Umfang und Gehalt der zu meldenden Informationen wird in den Ausführungsbestimmungen präzisiert werden. Das NCSC wird im Meldeformular zudem detailliert beschreiben, was unter den einzelnen Informationen zu verstehen ist. Unter «Art und Ausführung des Cyberangriffs» werden beispielsweise die «Indicator of Compromise» (IOC) verstanden. Dazu zählen namentlich IP-Adressen oder DNS-Records von bekannten Angriffsinfrastrukturen (beispielsweise von Botnetzen oder von Command and Control-Servern, URL zu verdächtigen Seiten, hash-Werte von Malware, Virensignaturen, Anomalien im Netzwerkverkehr oder verdächtiges Verhalten von Software. Die Formulierung betreffend der «ergriffenen Massnahmen» lehnt sich an die Formulierung in Artikel 24 Absatz 2 nDSG an.

Zur Erfüllung der Meldepflicht sind keine Informationen notwendig, die allfällige Berufs- oder Geschäftsgeheimnisse der Meldepflichtigen betreffen und verletzten würden oder sie selber inkriminieren könnten (vgl. Abs. 4).

Absatz 3

Um den Aufwand für die Meldenden so gering wie möglich zu halten, werden zum Zeitpunkt der Entdeckung des Cyberangriffs nur zwingend notwendige Informationen verlangt. Bei Cyberangriffen ist sehr oft längere Zeit unklar, wie gravierend der Angriff ist und was genau passiert ist. Wenn diese Informationen zum Zeitpunkt der Meldung nur unvollständig vorliegen, sollen die Betroffenen daher die Möglichkeit haben, die gemäss Absatz 2 verlangten Angaben erst dann zu übermitteln, wenn sie über einen ausreichenden Kenntnisstand dazu verfügen. Dieses zweistufige Vorgehen entspricht auch der Meldepflicht für Cyberangriffe an die FINMA. Auf die Verankerung einer zweiten Meldefrist wurde bewusst verzichtet, damit die Betroffenen sich auf die Vorfallbewältigung konzentrieren können. Anstelle der zweiten Frist ist vorgesehen, dass das NCSC die Meldepflichtigen informiert, wann alle notwendigen Informationen vorliegen und die Meldepflicht als erfüllt gilt (vgl. Abs. 5).

Absatz 4

In der Regel enthalten die Angaben, die im Rahmen der Meldepflicht an das NCSC zu übermitteln sind, keine Informationen, die die Meldepflichtige bzw. die meldende Person strafrechtlich belasten könnten. Damit der Grundsatz des Selbstbelastungszwangsverbots gewahrt ist, wird bereits auf Gesetzesstufe auf diesen Umstand hingewiesen; ein entsprechender Hinweis ist auch im Meldeformular vorgesehen.

Absatz 5

Damit für die Meldepflichtigen Klarheit besteht, ob die von ihnen gelieferten Informationen vollständig und präzise genug sind, teilt das NCSC ihnen mit, wenn die Informationen in demjenigen Umfang und derjenigen Klarheit vorliegen, die zur Erfüllung der Meldepflicht notwendig sind.

Artikel 74f Übermittlung der Meldung

Absatz 1

Damit die Meldepflicht mit möglichst geringem Aufwand erfüllt werden kann, wird das NCSC verpflichtet, ein sicheres elektronisches System zur Übermittlung der Meldungen, z.B. durch ein Meldeformular, zur Verfügung zu stellen. Dieses wird ähnlich wie das bestehende Formular für freiwillige Meldungen zu Cybervorfällen und Cyberbedrohungen aufgebaut sein. Das Meldeformular wird im Gesetzestext angesichts der technologischen Entwicklung generisch mit «System zur Übermittlung der Meldung» umschrieben.

Das NCSC wird die Möglichkeit schaffen, sich vorgängig zu registrieren, so dass Unternehmen oder Organisationen Angaben zu sich selber bei einer Meldung nicht mehr zusätzlich erfassen müssen. Damit wird das «Once-only-Prinzip», wonach die Daten des Meldenden nur einmal erfasst werden müssen, im Rahmen der Meldepflicht umgesetzt. Eine automatisierte Meldung via «Application Programming Interface» (API) ist nicht sinnvoll, da auf diese Weise zu viele Informationen an das NCSC übermittelt werden. Es ist Aufgabe der Meldepflichtigen, dem NCSC nur die gewünschten Informationen im Zusammenhang mit dem Cyberangriff zu übermitteln.

Abgesehen von diesem Meldeformular bleibt es jedoch in jedem Fall zulässig, das NCSC auf andere Weise (Mail, telefonisch) über den Cyberangriff in Kenntnis zu setzen.

Absätze 2 und 3

Das NCSC wird das Meldesystem – auf Wunsch und in Zusammenarbeit mit weiteren Meldestellen – so ausgestalten, dass die Meldenden die Möglichkeit erhalten, die Meldung des Cyberangriffs oder seiner Auswirkungen (z.B. auf die Datensicherheit oder auf die Funktionsfähigkeit der kritischen Infrastruktur) als Ganzes oder lediglich Teile davon an weitere Behörden zu übermitteln (Abs. 2) oder sogar zusätzliche Angaben, die für die weiteren Meldepflichten benötigt werden, zu erfassen (Abs. 3). Diese Weiterleitungsfunktion soll dazu dienen, den Aufwand der Meldenden möglichst gering zu halten. Bei Zusammentreffen von mehreren Meldepflichten können die Meldenden die entsprechenden Behörden rasch, zeitnah und ohne grossen Aufwand informieren.

Wichtig ist dabei, dass gemäss Absatz 2 die Meldung oder Teile davon nur von den Meldepflichtigen selber übermittelt werden können. Sie alleine bestimmen, welche Behörde – ausser dem NCSC – die Meldung des Cyberangriffes oder seiner Auswirkungen erhalten soll.

Gemäss Absatz 3 besteht auch die Möglichkeit, dass die Meldepflichtigen zur Erfüllung einer anderen Meldepflicht allfällige zusätzlichen Angaben, die für die Meldung an das NCSC nicht notwendig sind, erfassen können, um diese Angaben an eine oder mehrere Meldestellen zu übermitteln. Diese zusätzlichen Informationen, welche die Meldenden für andere Stellen und Behörden im Meldesystem des NCSC erfassen, werden von diesem nur übermittelt, aber nicht gespeichert. Das NCSC selber hat keine Zugriffsmöglichkeit auf diese Informationen.

Das NCSC bietet anderen, interessierten Meldestellen die Möglichkeit, das elektronische Formular gemäss ihren jeweiligen Meldepflichten zu ergänzen, um den Aufwand

der Meldepflichtigen zu verringern und Synergien nutzen zu können. Die bestehenden Meldepflichten werden dadurch weder ersetzt noch wird das NCSC zur Meldestelle für andere Meldepflichten. Durch die Weiterleitungsfunktion wird dem Bedürfnis eines «One-stop-Shop» insofern Rechnung getragen, als dass überschneidende Meldepflichten durch einen einzigen Meldevorgang erfüllt werden können. Das NCSC übernimmt bei der Weiterleitung von Informationen an andere Meldestellen aber keine aktive Rolle; die Weiterleitung erfolgt ausschliesslich durch die Meldepflichtigen.

Artikel 74g Verletzung der Meldepflicht

Absatz 1

Im Falle einer Verletzung der Meldepflicht macht das NCSC in einem ersten Schritt die Meldepflichtigen auf die Pflichtverletzung aufmerksam. Diese haben somit nochmals Gelegenheit, ihren Pflichten innert einer angemessenen Frist nachzukommen. Sollten dazu Missverständnisse vorliegen, dann können diese geklärt werden.

Um solchen Missverständnissen vorzubeugen, kann das NCSC bereits anlässlich der Meldung weitere Informationen bei den Meldepflichtigen einholen, falls die Angaben in der Meldung unvollständig oder unpräzis sind. Es informiert die Meldepflichtigen, sobald alle Informationen vorliegen und die Meldepflicht erfüllt ist (vgl. Art. 74*e* Abs. 5).

Bei einer allfälligen Verletzung der Meldepflicht wird das NCSC somit pragmatisch vorgehen und die betroffenen Meldepflichtigen zunächst über die Pflichtverletzung informieren. Das NCSC ist zu dieser ersten Kontaktaufnahme verpflichtet. Diese Informationspflicht ist eine Voraussetzung für den Erlass einer Verfügung nach Absatz 2.

Absatz 2

In einem zweiten Schritt, d.h. wenn Meldepflichtige trotz offensichtlicher Pflichtverletzung innert der gesetzten Frist nichts unternehmen, erlässt das NCSC eine Verfügung mit Bussandrohung. Das NCSC konkretisiert die verletzten Pflichten in der Verfügung so weit, dass für die Meldepflichtigen kein Zweifel besteht, was sie zu tun haben. Dies erleichtert auch die Arbeit der kantonalen Strafverfolgungsbehörden, die im Falle der Missachtung dieser Verfügung auf Anzeige des NCSC hin den Sachverhalt ermitteln und ein Urteil bzw. einen Strafbefehl erlassen müssen (vgl. Art. 74*h*).

Artikel 74h Missachten von Verfügungen des NCSC

Es wurde eine Bussenregelung getroffen, die weitgehend den Mechanismus übernimmt, der im revidierten Datenschutzgesetzt (Art. 60 ff. nDSG) bei Pflichtverletzungen oder im Falle der Missachtung von Verfügungen des Beauftragten vorgesehen wird. Wie in der Botschaft vom 15. September 2017.[65] zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz ausgeführt wurde, gilt auch hier, dass sich diejenige Person strafbar macht, die innerhalb der kritischen Infrastruktur hätte dafür sorgen müssen,

65 BBl **2017** 6974, hier 6980 und 7103 f.

dass der Verfügung des NCSC Folge geleistet wird (vgl. Art. 29 StGB). Die Einhaltung der Meldepflicht, die eigentlich dem Unternehmen obliegt, wird der natürlichen Person zugerechnet.

Der Verweis auf Artikel 6 Bundesgesetzes vom 22. März 1974[66] über das Verwaltungsstrafrecht adressiert eine strafrechtliche Verantwortung an die Leitungsebene von Unternehmen, also an Führungspersonen, die Entscheidungs- und Weisungsbefugnisse haben. Dies ermöglicht eine sachgerechte Zuweisung der strafrechtlichen Verantwortung bei den meldepflichtigen Unternehmen. Es ist Sache der internen Betriebsorganisation, die entsprechenden Verantwortlichkeiten zu regeln.

Absatz 1

Die Obergrenze der Busse wurde auf 100 000 Franken angesetzt, um der Bedeutung von kritischen Infrastrukturen für das ordnungsgemässe Funktionieren von Gesellschaft, Wirtschaft und Staat gebührend Rechnung zu tragen und die Verantwortung ihrer Betreiberinnen für die Gewährleistung der Cybersicherheit zu verdeutlichen. Der Höchstbetrag der Busse rechtfertigt sich auch dadurch, dass die Busse erst als Ultima Ratio nach einer Kaskade von Massnahmen zum Zug kommt. Angesichts der heterogenen Niveaus der Cybersicherheit in den einzelnen Sektoren und der zusätzlichen Anforderungen durch die neu eingeführte Meldepflicht für Cyberangriffe wurde bewusst darauf verzichtet, die Bussobergrenze des revidierten Datenschutzgesetzes von 250 000 Franken zu übernehmen. Dazu kommt, dass auch die Interessenlage und Zuordnung der Verantwortlichkeit bei Datenschutzverletzungen anders gelagert ist. Eine Bussandrohung von 100 000 Franken sollte ausreichen, um die Verantwortlichen der meldepflichtigen kritischen Infrastrukturen zu pflichtkonformem Verhalten zu bewegen.

Bei der Festlegung der Busse werden die persönlichen Verhältnisse der betroffenen Person entsprechend den strafrechtlichen Grundsätzen berücksichtigt.

Absätze 2 und 3

Bei der Bussauferlegung an Geschäftsbetriebe wurde die Regelung des revidierten Datenschutzgesetzes sinngemäss übernommen (Art. 64 nDSG). Die Höhe der Busse für Geschäftsbetriebe von 20 000 Franken bei einer maximalen Bussandrohung von 100 000 Franken entspricht derselben Ratio wie im Datenschutzrecht (250 000 Franken resp. 50 000 Franken).

Bis zu einem Betrag von 20 000 Franken kann die Busse somit direkt dem meldepflichtigen Unternehmen anstelle der verantwortlichen natürlichen Person auferlegt werden, um aufwändige Ermittlungen zu vermeiden. Angesichts des Höchstbetrages von 100 000 Franken wurde der Betrag für diese «Bagatellfälle» auf 20 000 Franken angesetzt.

Wenn man bedenkt, dass die Meldepflicht auf die bedeutendsten kritischen Infrastrukturen fokussiert, die vielfach auch einen entsprechenden Marktanteil beanspruchen, gibt es kaum Argumente, um den Höchstbetrag von 20 000 Franken tiefer anzusetzen.

66 SR **313.0**

Es gibt auch keine Möglichkeit, die Busse für das Unternehmen höher anzusetzen und beispielsweise auf einen bestimmten Prozentsatz des Umsatzes festzulegen. Die Strafbarkeit von Unternehmen ist in der Schweiz stets subsidiär zur persönlichen Strafbarkeit (vgl. auch Art. 29 und 102 StGB). Die Auferlegung der Busse an das Unternehmen ist somit nur in Bagatellfällen zulässig.

Absatz 4

Aus Transparenzgründen wird in Absatz 4 – analog zu Artikel 65 nDSG – auf die Zuständigkeit der kantonalen Strafverfolgungsbehörden hingewiesen, sollte einer Verfügung des NCSC keine Folge geleistet werden. Es wurde darauf verzichtet, das Anzeigerecht des NCSC zu erwähnen, da sich dieser Umstand aus dem Kontext ergibt.

3. Abschnitt: Datenschutz und Informationsaustausch

Die Artikel 75 bis 79, die neu unter dem 3. Abschnitt zusammengefasst werden, mussten sowohl sprachlich wie auch inhaltlich angepasst werden, um der gesetzlichen Verankerung der Aufgaben des NCSC zu entsprechen. Das NCSC löst mit seiner Meldestelle die gemeinsam durch das damalige Informatiksteuerungsorgan des Bundes und den NDB betriebene MELANI ab. Da der NDB einen gesetzlichen Auftrag zur Beurteilung der Bedrohungslage und zur Frühwarnung von Betreiberinnen kritischer Infrastrukturen hat, muss die Zusammenarbeit des NCSC mit dem NDB und die Weitergabe von Informationen und Daten soweit notwendig im ISG geregelt werden.

Artikel 75 Bearbeitung von Personendaten

Die Bestimmung von Artikel 75 wurde bei der Revision des 5. Kapitels inhaltlich dahingehend erweitert, dass das NCSC nun eine Grundlage zur Bearbeitung von Personendaten hat, auch wenn diese nicht mit Adressierungselementen verbunden sind. Zudem wurden mehrere systematische und formelle Anpassungen gemacht, z. B. durch Einfügen der Bezeichnung «NCSC».

Absatz 1

Anstelle der generischen Umschreibung der zuständigen Bundesstellen wurde das NCSC eingefügt und der Absatz 1 mit Absatz 2 verbunden. Wie bisher gilt, dass nicht nur Personendaten, sondern im Zusammenhang mit Adressierungselementen, auch besonders schützenswerte Personendaten bearbeitet werden dürfen. Als Adressierungselement gilt gemäss der Definition in Artikel 3 Buchstabe f FMG eine «Abfolge von Ziffern, Buchstaben oder Zeichen oder andere Informationen zur Identifikation von Personen, Computerprozessen, Maschinen, Geräten oder Fernmeldeanlagen, die an einem fernmeldetechnischen Kommunikationsvorgang beteiligt sind».

In den Buchstaben a und b wurde das Verb gestrichen; in Buchstabe a wurde zudem der Begriff «Cybersicherheit» eingefügt. Für die Ausführungen zu den besonders schützenswerten Personendaten gemäss Buchstaben a und b wird auf die Botschaft zum ISG verwiesen.[67]

67 BBl **2017** 2953, hier 3060 ff.

Absatz 2

Die Formulierung in Absatz 2 übernimmt im Wesentlichen den Inhalt der früheren Absätze 3 und 4, wurde aber vom Passiv ins Aktiv geändert, wodurch deutlicher wird, dass die Datenbearbeitung vom NCSC vorgenommen wird. Zusätzlich wurden die Voraussetzungen konkretisiert, die vorliegen müssen, wenn das NCSC die betroffene Person über die Datenbearbeitung bzw. den Identitätsmissbrauch nicht informiert.

Artikel 76 Zusammenarbeit im Inland

Dieser Artikel bildet die gesetzliche Grundlage für den Informationsaustausch zwischen dem NCSC und den Betreiberinnen von kritischen Infrastrukturen (Absatz 1 und 2) sowie zwischen dem NCSC und den Fernmeldedienstanbieterinnen (Absatz 3 und 4) – sofern diese nicht als kritische Infrastrukturen gelten.

Inhaltlich entspricht Artikel 76 weitgehend der vom Parlament am 18. Dezember 2020 verabschiedeten Version. Es wurden neben sprachlichen Anpassungen (z.B. durch Einfügen von «Cyberbedrohungen» und «NCSC») auch systematische Änderungen vorgenommen: Absätze 1 und 2 beschreiben den Informationsaustausch zwischen dem NCSC und den kritischen Infrastrukturen; Absätze 3 und 4 (neu) den Informationsaustausch zwischen dem NCSC und den Fernmeldedienstanbieterinnen.

Absätze 1 und 2

Der in Absatz 1 und 2 geregelte Informationsaustausch zwischen dem NCSC und den Betreiberinnen von kritischen Infrastrukturen ist nicht auf die meldepflichtigen kritischen Infrastrukturen beschränkt, sondern steht allen interessierten kritischen Infrastrukturen mit Sitz in der Schweiz offen. Das bedeutet, dass nicht nur Meldepflichtige gemäss Artikel 74*b*, sondern auch gemäss Artikel 74*c* von der Meldepflicht ausgenommene kritische Infrastrukturen am Informationsaustausch teilnehmen können.

Für den Informationsaustausch mit den kritischen Infrastrukturen, der über einen geschützten Kommunikationskanal erfolgt, verwendet das NCSC das «Traffic Light Protocol» (TLP), d.h. die international gängige Einteilung von schutzwürdigen Informationen in vier Kategorien, die deren Verwendung sowie eine allfällige Weitergabe regeln.

Der Umfang des Informationsaustauschs zwischen dem NCSC und den kritischen Infrastrukturen wurde gegenüber der ursprünglichen Fassung erweitert, da die Beschränkung auf Adressierungselemente und damit verbundene Personendaten nicht sachgerecht war. Zur Frühwarnung sowie zur Abwehr von unmittelbaren Cyberangriffen ist das NCSC darauf angewiesen, dass es kritischen Infrastrukturen auch Personendaten bekanntgeben kann, die nicht im Zusammenhang mit Adressierungselementen stehen. Den kritischen Infrastrukturen muss es erlaubt sein, dem NCSC Personendaten bekannt zu geben, die keinen unmittelbaren Zusammenhang mit einem Cybervorfall haben (so wie in Absatz 3 ursprünglich vorgesehen), sondern beispielsweise mit Cyberbedrohungen in Verbindung stehen. Diese Ergänzung steht im Einklang mit der Botschaft zum ISG, die festhielt, dass kritische Infrastrukturen Informationen «im Zusammenhang mit Gefahren und Vorfällen» an MELANI melden und dabei «zur Abwehr von Gefahren und entsprechend zur Verhinderung von Schäden Angaben über von ihnen erbrachte Dienstleistungen, Vermittlungen und andere Vorgänge machen»

dürfen.[68]. Die vorliegende Revision des 5. Kapitels wurde zum Anlass genommen, den Gesetzestext zu präzisieren. Damit wird sichergestellt, dass das NCSC mit den kritischen Infrastrukturen alle Informationen, einschliesslich Personendaten, austauschen kann, die für die frühzeitige Warnung sowie zur Abwehr von Cyberbedrohungen erforderlich sind.

Absätze 3 und 4

Der Informationsaustausch zwischen dem NCSC und den Fernmeldedienstanbieterinnen wurde in Absatz 3 und 4 explizit geregelt, da zwar die meisten, aber wohl nicht alle Fernmeldedienstanbieterinnen als kritische Infrastrukturen gelten.

Der in der ursprünglichen Fassung enthaltene zweite Satz von Absatz 3, wonach MELANI Daten nur mit ausdrücklicher Einwilligung der Datenlieferantinnen zu Strafverfolgungszwecken weitergeben durfte, wurde gestrichen. Diese Regelung wurde durch das Anzeigerecht der Leiterin oder des Leiters des NCSC überflüssig (vgl. Art. 73*d* Abs. 3).

Artikel 76a Unterstützung für Behörden

Diese Bestimmung wurde neu eingefügt. Sie regelt, welche Informationen das NCSC anderen Behörden in welchem Umfang und zu welchem Zweck zur Verfügung stellt. Sie klärt die Rollenteilung zwischen dem NCSC und dem NDB (Absatz 1) sowie den Inhalt und die Art und Weise der Informationsübermittlung an den NDB, die Strafverfolgungsbehörden und die kantonalen Stellen, die für Cybersicherheit zuständig sind (Absätze 2 bis 4).

Ein wichtiger Aspekt bei der Zusammenarbeit des NCSC mit diesen Behörden bilden die vom NCSC gesammelten Informationen über die Angreiferinnen und Angreifer selber sowie über deren Methoden und Taktiken. Nur diese Informationen werden den Behörden zugänglich gemacht.

Absatz 1

Im ersten Absatz dieser Bestimmung wird statuiert, dass das NCSC dem NDB bei seinen Aufgaben durch spezifische Auswertungen zu Anzahl, Art und Ausmass von Cyberangriffen sowie durch technische Analysen von Cyberbedrohungen behilflich ist. Diese «Lagebilder» enthalten keine konkreten, fallspezifischen Personendaten oder Informationen, sondern beschränken sich auf statistische und technische Auswertungen, die für die Beurteilung der Bedrohungslage und die Frühwarnung notwendig sind. Der NDB ist gestützt auf Artikel 6 Absatz 2 NDG zuständig für die Beurteilung der Bedrohungslage. Über die Meldestelle – und die zusätzlichen Meldungen in Erfüllung der Meldepflicht – verfügt das NCSC über wichtige Informationsquellen zur Bedrohungslage durch Cybervorfälle. Es kann dem NDB deshalb Informationen zu Anzahl, Art und Ausmass der Cyberangriffe liefern und ihn durch technische Analysen zu Angriffen beziehungsweise mit den Erkenntnissen aus solchen Analysen unterstützen.

68 BBl **2017** 2953, hier 3062 f.

Absätze 2, 3 und 4

In den Absätzen 2 bis 4 werden Inhalt und Umfang sowie die Art und Weise des Informationsaustausches des NCSC mit dem NDB, den Strafverfolgungsbehörden und den kantonalen Cybersicherheitsstellen geregelt.

Inhaltlich besteht die Unterstützung des NCSC darin, dass es den Behörden Zugriff auf Informationen über die Angreiferinnen und Angreifer selber und über deren Methoden und Taktiken gewährt. Diese Informationen können rein technischer Natur sein (z.B. Angriffsmuster oder Hashwerte von Malware) und keine Personendaten enthalten. Es werden zwischen diesen Behörden aber auch Informationen ausgetauscht, die personenbezogen sind oder über die ein Personenbezug hergestellt werden kann. Konkret handelt sich um Adressierungselemente (wie Domain-Name, IP-Adresse, missbräuchlich verwendete Mailadressen) oder Angaben zu Finanztransaktionen (Bankkonten, IBAN-Nummer usw.). Für den Informationsaustausch in Bezug auf diese Personendaten wird hier eine Rechtsgrundlage geschaffen.

Die berechtigten Behörden nach den Absätzen 2 bis 4 können auf die genannten Informationen selbstständig zugreifen. Dieses Vorgehen ist aufgrund der grossen Anzahl von Cyberangriffen und damit verbundenen technischen Informationen angezeigt, damit Abgleich zeitnah möglich sind.

Eine Weiterleitung von anderen Informationen, die das NCSC im Zusammenhang mit Meldungen zu Cybervorfällen erhalten hat, erfolgt nur in Ausnahmefällen und bleibt an die Bedingungen nach Artikel 73*c* gebunden.

Artikel 77 Internationale Zusammenarbeit

Diese Bestimmung wurde gegenüber der ursprünglichen Fassung nur formell angepasst. Neu wird das NCSC namentlich genannt. Ferner wurde der Begriff «Daten» durch den Oberbegriff «Informationen» ersetzt und der Aufgabenbereich der ausländischen Stellen präzisiert. Letztere müssen nicht «für den Schutz kritischer Infrastrukturen» (ursprüngliche Fassung), sondern für die «Cybersicherheit» zuständig sein. Die ursprüngliche Formulierung war zu unspezifisch und hätte den Informationsaustausch mit international bedeutenden Organisationen, die im Bereich Cybersicherheit tätig sind, behindern können.

Absätze 1 und 2

Der Inhalt der Informationen, die das NCSC an diese Organisationen weiterleitet, beschränkt sich auf die Identität und die Vorgehensweise der Angreiferinnen und Angreifer. Der Umfang ist mithin derselbe wie bei der Unterstützung der Behörden gemäss Artikel 76*a*. Die Übermittlung der Informationen durch das NCSC erfolgt selbstverständlich unter Einhaltung des Datenschutzrechts.

Die ausländischen und internationalen Cybersicherheitsorganisationen müssen die Informationen des NCSC betreffend Angriffsmerkmale und -methoden bestimmungsgemäss verwenden. Dies wird vom NCSC mittels Verwendung des TLP sichergestellt. Diese international gängige Einteilung von schutzwürdigen Informationen legt für jede Schutzstufe fest, welche Bedingungen für die Verwendung und Weitergabe gelten.

Bei Inkrafttreten dieser Teilrevision gilt bereits das neue Datenschutzrecht, weshalb im Entwurf bereits darauf verwiesen wird.

Absatz 3

Der Vorbehalt zur Amts- und Rechtshilfe in Absatz 3 wurde gestrichen.

Mit der Einführung der Meldepflicht hat sich der Kontext des 5. Kapitels geändert. Die vertrauliche Behandlung der Meldungen durch das NCSC hat noch mehr Gewicht erhalten. Die Meldungen an das NCSC sowie deren Analysen, soweit sie auf Informationen Dritter beruhen, wurden deshalb vom Geltungsbereich des Öffentlichkeitsgesetzes ausgenommen (vgl. Art. 4 Abs. 1bis). Aus demselben Grund wurde auch die Anzeigepflicht für Straftaten für Mitarbeitende der Meldestelle auf die Leiterin oder den Leiter des NCSC beschränkt. Ebenfalls nur für Ausnahmefälle besteht ein Weiterleitungsrecht für Informationen im Zusammenhang mit gemeldeten Cybervorfällen, sofern diese in erheblichem Masse sicherheits- oder strafrelevant sind (Art. 73*d*).

Vor diesem Hintergrund kann der Vorbehalt in Bezug auf die Amts- und Rechtshilfe zu Missverständnissen führen. Das NCSC kann nur dann Amtshilfe leisten, wenn eine materielle Bestimmung dies vorsieht. Auch in diesen Fällen kann es nur Informationen herausgeben, wenn dem keine Geheimhaltungsbestimmungen entgegenstehen. Faktisch wird das NCSC daher nur in seltenen Fällen Amtshilfe leisten können.

Artikel 78 Informationssystem zur Unterstützung von kritischen Infrastrukturen

Dieser Artikel wurde durch die Revision des DSG überflüssig und daher aufgehoben.

Die Zwecke der Datenbearbeitung durch das NCSC ergeben sich aus seinen Aufgaben, die in den aufgeführten Artikeln ausreichend beschrieben sind. Sie geben vor, für was die Informationssysteme des NCSC bei der Bearbeitung von Personendaten verwendet werden dürfen.

Artikel 79 Datenaufbewahrung und -archivierung

Absatz 1 wurde strenger formuliert als die ursprünglich vom Parlament verabschiedete Version[69].

Es wurde präzisiert, dass Personendaten höchstens fünf Jahre ab der letzten Verwendung zur Erkennung von Cyberbedrohungen oder zur Bewältigung von Cybervorfällen, aufbewahrt werden. Der Hintergrund für diese Regelung ist, dass gewisse technische Informationen zu Cybervorfällen, wie z.B. Domain-Name, IP-Adresse oder missbrauchte Mailadressen, für den Abgleich von neu gemeldeten Cybervorfällen und die Analyse von Angriffsmethoden und -mustern eine zentrale Bedeutung haben. Ohne diese Vergleichsdaten kann das NCSC seine Analysen nicht oder nicht zielorientiert durchführen, was eine Grundvoraussetzung für seine Aufgabenerfüllung ist.

Das NCSC ist also auch bei längerer Nichtverwendung von Datensätzen darauf angewiesen, dass es diese zu Vergleichszwecken noch abrufen kann. In der Botschaft zum

69 «Die Stellen nach Artikel 74 Absatz 5 bewahren Personendaten nur so lange auf, wie dies zur Abwehr von Gefahren oder zur Erkennung von Vorfällen zweckmässig ist, höchstens jedoch fünf Jahre» (Art. 79 Abs. 1, Version vom 18. Dezember 2020).

ISG[70] wurde diesbezüglich erwähnt, dass Angriffsvektoren über mehrere Jahre Gültigkeit haben können. Da diese technischen Daten aber auch personenbezogene Elemente enthalten und damit als Personendaten dem Datenschutz unterstehen – und eine Anonymisierung die Aufgabenerfüllung beträchtlich behindern oder gar verunmöglichen würde –, wurde die Aufbewahrungsdauer ab der letzten Verwendung klar eingegrenzt.

Aus Gründen des Datenschutzes wurde im zweiten Teil des Satzes eingefügt, dass besonders schützenswerte Personendaten höchstens zwei Jahre ab der letzten Verwendung aufbewahrt werden. Diese Präzisierung war in der ursprünglichen Fassung nicht enthalten.

Artikel 80 Bestimmungen des Bundesrats

Dieser Artikel wurde aufgehoben.

Die Kompetenz, Ausführungsbestimmungen zu erlassen, kommt dem Bundesrat auch ohne Gesetzesvorbehalt zu (vgl. 4.3.3).

Bundesgesetz vom 21. Juni 2019[71] über das öffentliche Beschaffungswesen

In der Vernehmlassung des Vorentwurfs wurde angeregt, dass Herstellerinnen von Hard- oder Software, die eine entdeckte Schwachstelle nicht fristgerecht beheben, im Rahmen des öffentlichen Beschaffungsrechts für dieses Fehlverhalten zur Verantwortung gezogen werden sollen.[72]

Neben dem öffentlichen Interesse, die Cybersicherheit durch offene Schwachstellen nicht zu gefährden, besteht auch ein öffentliches Interesse daran, allfällige säumige Herstellerinnen von Aufträgen der öffentlichen Hand auszuschliessen. Angebote mit Produkten, die nicht behobene Schwachstellen beinhalten, können zwar schon unter der aktuellen Rechtslage ausgeschlossen werden. Solche Produkte, die nicht (mehr) den Anforderungen entsprechen (die z.B. nicht behobene Schwachstellen enthalten) weisen einen Mangel auf und erfüllen daher die technischen Spezifikationen nicht (mehr), falls der Mangel für den vorgesehenen oder erwartbaren Zweck relevant ist. Technische Spezifikationen und die gängigen Industriestandards sind aber zwingend jederzeit zu erfüllen. Die betroffenen Angebote können über Artikel 44 Absatz 1 Buchstabe a resp. b BöB ausgeschlossen werden.[73]

Eine explizite Ausschlussmöglichkeit als direkte Folge eines unkooperativen Verhaltens seitens der Herstellerinnen im Prozess der «Coordinated Vulnerability Disclosure» ist aber dennoch nötig. Nur wenn Herstellerinnen sich auch wirklich um die Behebung einer Schwachstelle bemühen, ist es sinnvoll, sie zuerst über die Schwachstelle zu informieren.

70 BBl **2017** 2953, hier 3064
71 SR **172.056.1**
72 Vgl. Eingabe von CH++.
73 Vgl. Trüeb (Hrsg.) (2020): Handkommentar zum Schweizerischen Beschaffungsrecht, darin Locher zu Art. 44, N12 und N 13.

Durch die Ergänzung des Kriterienkatalogs des Artikels 44 Absatz 1 durch den Buchstaben f^{bis} wird die Möglichkeit geschaffen, Anbieterinnen als direkte Folge eines unkooperativenen Verhaltens bei der Schliessung von Schwachstellen von künftigen Aufträgen auszuschliessen oder bestehende Verträge aufzulösen.

Damit die zentralen Beschaffungsstellen, die Verantwortlichen für die Informatiksicherheit und für das Vertragsmanagement frühzeitig über offene Schwachstellen in Hard- oder Software informiert werden, können sie am Informationsaustausch des NCSC mit den kritischen Infrastrukturen teilnehmen.

Abschliessend ist zu erwähnen, dass die neu eingeführte Bestimmung im BöB nur auf Bundesebene Geltung haben wird. Sie läuft insofern dem Hauptziel der kürzlich erfolgen Totalrevision des BöB – der Harmonisierung des BöB mit der interkantonalen Vereinbarung über das öffentliche Beschaffungswesen (IVöB 2019) – entgegen.

Änderung des Datenschutzgesetzes vom 25. September 2020[74]

Damit der EDÖB bei der Analyse einer eingetretenen Verletzung der Datensicherheit, die der Verantwortliche ihm gestützt auf Artikel 24 nDSG und Artikel 19 DSV gemeldet hat, die technischen Fachspezialistinnen und Fachspezialisten des NCSC miteinbeziehen kann, wird in Artikel 24 Absatz 5bis nDSG vorgesehen, dass der EDÖB die Meldung einer Verletzung der Datensicherheit an das NCSC weiterleiten kann.

Die Weiterleitung kann jegliche Angaben gemäss Artikel 19 Absatz 1 DSV enthalten, muss sich aber gleichzeitig auf die für das NCSC für die Analyse des Vorfalls notwendigen Daten beschränken. Dabei kann die Mitteilung des EDÖB an das NCSC auch Personendaten enthalten, einschliesslich besonders schützenswerter Personendaten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen des meldepflichtigen Verantwortlichen. Die für die Analyse eines Vorfalls notwendigen Informationen werden im Einzelfall selektiert, jedoch können unter Umständen damit auch indirekt Informationen über ein laufendes Verfahren an das NCSC gelangen. Daher ist eine gesetzliche Grundlage für die Bekanntgabe von besonders schützenswerten Personendaten zu schaffen.

Vorausgesetzt ist, dass der Verantwortliche, der zur Meldung an den EDÖB verpflichtet ist, vorgängig sein Einverständnis zur Weiterleitung gegeben hat. Ausserdem darf die Weiterleitung nicht dazu führen, dass Artikel 24 Absatz 6 nDSG umgangen wird, wonach die Meldung nur mit Einverständnis der meldepflichtigen Person im Rahmen eines Strafverfahrens verwendet werden darf. Dies bedeutet, dass sich ein Verantwortlicher auch im Falle einer Weiterleitung seiner Meldung an das NCSC auf das datenschutzrechtliche Verwertungsverbot berufen können wird. Der neue Absatz 5bis in Artikel 24 nDSG ermöglicht dem EDÖB keine systematische Weiterleitung von Meldungen an das NCSC. Vielmehr darf der EDÖB von dieser Möglichkeit nur in Einzelfällen Gebrauch machen, in denen das technische Fachwissen des NCSC für die Abklärung eines Vorfalls erforderlich ist.

Dieses Weiterleitungsrecht für Informationen des EDÖB an das NCSC beschränkt sich auf einen einseitigen Informationsaustausch. Das NCSC seinerseits liefert dem

74 SR **235.1,** AS **2022** 491

EDÖB keine Informationen aus Meldungen, selbst wenn diese Datenschutzverletzungen beinhalten. Das NCSC stellt aber ein elektronisches System zur Verfügung, das den Meldenden die Weiterleitung der Meldung oder Teilen davon erlaubt. Die meldende Person erhält somit die Möglichkeit, das Formular zur Meldung des Cyberangriffs auch zur Meldung einer Datensicherheitsverletzung an den EDÖB zu nutzen.

Das revidierte Datenschutzgesetz wird voraussichtlich im September 2023, d.h. kurz nach Inkrafttreten des ISG (ohne diese Vorlage), in Kraft treten. Ab diesem Zeitpunkt bis zum Inkrafttreten des revidierten 5. Kapitels ISG (diese Vorlage) frühestens Ende 2023 wird die in Artikel 24 Absatz 5^{bis} vorgesehene Regelung bereits auf Verordnungsebene gelten (vgl. Art. 41 Abs. 1 der Datenschutzverordnung vom 31. August 2022.[75]). Mit Inkraftsetzung dieser Vorlage wird der Bundesrat jene Verordnungsbestimmung aufheben.

Stromversorgungsgesetz vom 23. März 2007.[76] (StromVG)

Eine durch das Bundesamt für Energie beauftragte Studie hat in diesem für die wirtschaftliche Versorgung und die Sicherheit des Landes entscheidenden Sektor einen hohen Regulierungsbedarf bei der Cybersicherheit festgestellt..[77] Die Erkenntnisse zeigen, dass über Jahre verfügbare und subsidiär verankerte Branchenrichtlinien nicht zu einem angemessenen Schutz vor Cyberbedrohungen führten. Der Schutz vor Cyberbedrohungen, der neu in Artikel 8*a* des Stromversorgungsgesetzes explizit verankert werden soll, dient der Versorgungssicherheit.

Die zu treffenden Massnahmen gemäss Absatz 1 sollen Cybervorfälle und damit insbesondere Funktionsstörungen der entsprechenden Anlagen verhindern respektive möglichst rasch beheben. Die Pflicht trifft neben den Netzbetreibern, die direkt via Steuertechnologie Einfluss auf den Netzbetrieb ausüben, auch die Erzeuger (bspw. Betreiber von Wind- oder Wasserkraftanlagen) und die Speicherbetreiber, zumal diese über die Ein- und Ausspeisung massgeblichen Einfluss auf die Versorgungssicherheit ausüben können. Bei der Frage, welcher Schutz als angemessen gilt, kommt es auf den Einfluss des entsprechenden Akteurs auf die Versorgungssicherheit an (bspw. Netzebene, Anschlussleistung, Kraftwerksleistung, Anzahl betroffener Endverbraucher).

Für die Überwachung der Einhaltung von Artikel 8*a* ist aufgrund ihrer subsidiären Generalkompetenz die Eidgenössische Elektrizitätskommission (ElCom) zuständig (Art. 22 Abs. 1 StromVG). Der Bundesrat wird entsprechende Ausführungsbestimmungen erlassen, insbesondere zum Schutzniveau und der Auditierung (bspw. Dokumentationspflichten zuhanden der ElCom). Dabei wird er sich im Sinne des Subsidiaritätsprinzips (Art. 3 Abs. 2 StromVG) an einschlägigen Branchenrichtlinien orientieren (bspw. am Handbuch des Verbands Schweizerischer Elektrizitätsunter-

75 SR **235.11**, AS **2022** 568
76 SR **734.7**
77 Vgl. Bericht vom 28. Juni 2021 über die Cyber-Sicherheit und Cyber Resilienz für die Schweizer Stromversorgung, online abrufbar unter www.bfe.admin.ch > Versorgung > Digitalisierung im Energiesektor > Strategie Cyber Security für die Schweizer Stromversorgung.

nehmen über den Grundschutz für «Operational Technology» in der Stromversorgung, Ausgabe Juli 2018, zurzeit in Überarbeitung), welche er auch für verbindlich erklären kann.

Die Bestimmung in Absatz 2 ermöglicht es dem Bundesrat, gewisse Dienstleister der Elektrizitätsversorgung der Pflicht nach Absatz 1 zu unterstellen. Denkbar ist dies zum Beispiel in den Bereichen Handel, Messung, Steuerung, Flexibilität, Datenbearbeitung oder Elektromobilität. Dabei kommen mit Blick auf den Zweck der Bestimmung lediglich Akteure in Frage, die einen massgebenden Einfluss auf die Versorgungssicherheit ausüben. Dies ist namentlich der Fall, wenn sie im Rahmen ihrer Dienstleistungen auf die Leitsysteme einer Vielzahl von Elektrizitätsversorgungsunternehmen zugreifen können und damit eine grosse Anzahl von Endverbrauchern betroffen wäre, oder wenn Dienstleister etwa im Bereich Elektromobilität oder dezentraler Produktion über Aggregation eine grosse Leistung im Energieversorgungssystem steuern.

Der Bundesrat kann ferner gestützt auf Absatz 2 Ausnahmen vorsehen, beispielsweise für Verteilnetzbetreiber mit wenigen Endverbrauchern oder Produzenten mit geringer Kraftwerksleistung. Denkbar sind daneben auch Ausnahmen für Unternehmen, die bereits aufgrund anderer spezialrechtlicher Vorgaben Massnahmen im Cyberbereich zu treffen haben (bspw. im Bahnstrombereich). Hier bedarf es einer entsprechenden Koordination auf Verordnungsstufe.

Kernenergiegesetz vom 21. März 2003[78]

Mit der Einführung von Artikel 102 Absatz 2 KEG (neu) schafft der Gesetzgeber eine explizite gesetzliche Grundlage, damit das ENSI als sektorielle Meldestelle eine Meldung zu einem Cyberangriff auf eine Kernanlage, welcher die Voraussetzungen von Artikel 74*d* des ISG erfüllt, an die sektorübergreifende Meldestelle NCSC weiterleitet. Damit erhält das NCSC die Meldung zum Cyberangriff, ohne die für Kernanlagen etablierten Prozesse zu beeinflussen.

Finanzmarktaufsichtsgesetz vom 22. Juni 2007[79] *(FINMAG)*

Im Finanzmarktsektor besteht ebenfalls eine Meldepflicht für Cyberangriffe, wobei die Aufsichtsbehörde FINMA diese Meldungen entgegennimmt. Da für Finanzmarktakteurinnen im Falle von Cyberangriffen somit parallele Meldepflichten bestehen, wird das NCSC das elektronische Meldesystem so einrichten, dass Meldende das Meldeformular für das NCSC auch für die FINMA verwenden können.

Abgesehen von den parallelen Meldepflichten muss die FINMA bei Cyberangriffen im Bedarfsfall befugt sein, dem NCSC nicht öffentliche Informationen zu übermitteln, sofern dies zur Aufgabenerfüllung des NCSC notwendig ist. Zu diesem Zweck wird Artikel 39 Absatz 1 FINMAG das NCSC in der Aufzählung ergänzt und so die gesetzliche Grundlage zur Informationsübermittlung an den NCSC geschaffen.

78 SR **732.1**
79 SR **956.1**

6 Auswirkungen

6.1 Auswirkungen auf den Bund

Das NCSC führt bereits heute eine Anlaufstelle, welche auf freiwilliger Basis Meldungen zu Cybervorfällen entgegennimmt. Es baut dabei auf die langjährige Erfahrung von MELANI auf, welche diese Aufgabe seit 2004 spezifisch für Meldungen von kritischen Infrastrukturen ausgeführt hat.

6.1.1 Finanzielle Auswirkungen

Das NCSC betreibt für die Entgegennahme von Meldungen bereits heute ein elektronisches Meldeformular. Dieses lässt sich so anpassen, dass es auch für die Entgegennahme von Meldungen in Erfüllung der Meldepflicht verwendet werden kann. Für die nötigen Abstimmungen mit anderen Stellen, welche ebenfalls Meldungen entgegennehmen (z.B. EDÖB, FINMA, ENSI) und für die Konfiguration des Meldeformulars fällt ein Initialaufwand an, der jedoch über die bestehenden Ressourcen des NCSC aufgefangen werden kann. Für den späteren Betrieb muss das NCSC jedoch sicherstellen, dass die in Erfüllung der Meldepflicht eingegangenen Meldungen korrekt erfasst, quittiert und dokumentiert werden und die Meldung zum Zweck der Frühwarnung an die richtigen Stellen weitergeleitet werden. Dieser zusätzliche Aufwand muss beim weiteren Ausbau des NCSC berücksichtigt werden.

6.1.2 Personelle Auswirkungen

Nach einem Cyberangriff wird das NCSC die Betreiberin der betroffenen kritischen Infrastruktur bei der Vorfallbewältigung unterstützen. Auch diese Unterstützungsleistung ist dank der langjährigen Erfahrung des NCSC (und früher von MELANI) bereits gut eingespielt. Dennoch ist zu erwarten, dass sich der Aufwand für das NCSC durch die Einführung der Meldepflicht erhöht. Erstens ist damit zu rechnen, dass mehr Meldungen eingehen, und zweitens ist das NCSC neu in der Pflicht, mindestens eine erste Einschätzung und Empfehlungen zur Bewältigung des Vorfalls abzugeben. Das technische Analyseteam des NCSC (GovCERT) muss deshalb ebenfalls weiter ausgebaut werden. Der dadurch entstehende personelle Zusatzaufwand kann zum heutigen Zeitpunkt noch nicht hinreichend genau abgeschätzt werden. Er kann auch nicht losgelöst von der künftigen Ausrichtung der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken und der Organisationsform des NCSC beurteilt werden, die vom Bundesrat aktuell geklärt wird. Er wird bis zum Erlass der Ausführungsbestimmungen konkretisiert und dann beantragt werden.

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

Den Kantonen und Gemeinden werden mit dieser Vorlage keine neuen Aufgaben zugewiesen, sie sind aber von der Meldepflicht aus zwei Gründen betroffen. Erstens unterstehen die Kantons- und Gemeindebehörden selber gemäss Artikel 74*b* Buchstabe b der Meldepflicht und zweitens haben viele der meldepflichtigen Unternehmen kantonale oder kommunale Trägerschaften.

Im Gegenzug profitieren Kantone und Gemeinden aber auch von den Leistungen des NCSC, um sich besser vor Cyberbedrohungen schützen zu können. Bereits zum heutigen Zeitpunkt sind zahlreiche Kantone und Städte in den Informationsaustausch zwischen kritischen Infrastrukturen und dem NCSC integriert.

6.3 Auswirkungen auf die Volkswirtschaft, die Gesellschaft und die Umwelt

Direkte Auswirkungen auf die Volkswirtschaft, die Gesellschaft und die Umwelt sind nicht zu erwarten. Von der Einführung einer Meldepflicht für Cyberangriffe werden die Volkswirtschaft und Gesellschaft indirekt profitieren, da die Verbesserung der Cybersicherheit von kritischen Infrastrukturen auch dazu dient, die Cybersicherheit in der Schweiz insgesamt besser schützen zu können. Weiter trägt die Meldepflicht dazu bei, dass dank frühzeitiger Präventions- und geeigneter Abwehrmassnahmen verhindert werden kann, dass Cyberangriffe auf kritische Infrastrukturen Funktionsstörungen und -ausfälle von essentiellen Dienstleistungen verursachen, die das ordnungsgemässe Funktionieren von Wirtschaft und Staat gefährden.

Die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen hat kaum oder nur vernachlässigbare Auswirkungen auf die Volkswirtschaft oder auf die betroffenen Unternehmen. Es kann daher auf eine Regulierungsfolgenabschätzung verzichtet werden.

Die Meldepflicht hilft, Transparenz über die Bedrohung durch Cyberangriffe zu schaffen, und trägt dazu bei, die Bevölkerung für Cyberbedrohungen zu sensibilisieren. Eine erhöhte Cyberkompetenz der Bevölkerung ist eine wichtige Voraussetzung für die erfolgreiche Digitalisierung der Gesellschaft.

7 Rechtliche Aspekte

7.1 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 Konvention[80] 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.

7.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz

Die Einführung einer 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.

7.3 Erlassform

Als Gesetzesgrundlage für die Einführung der Meldepflicht scheint eine Ergänzung des bereits verabschiedeten ISG ideal, zumal dieses nicht nur durch Zweck, Gegenstand und Anwendungsbereich im Grundsatz mit der Meldepflicht für kritische Infrastrukturen vereinbar ist, sondern auch die formell-gesetzliche Grundlage für das NCSC als Meldestelle bildet. Aus systematischer Sicht kann die Meldepflicht für Cyberangriffe sowie die Aufgaben des NCSC zum Schutz der Cybersicherheit im 5. Kapitel eingefügt werden.

Für die Ausführungsbestimmungen zur Meldepflicht wird noch zu entscheiden sein, ob für diese eine eigenständige Verordnung geschaffen oder bestehende Verordnungen ergänzt werden sollen.

7.4 Unterstellung unter die Ausgabenbremse

Mit der Vorlage werden weder neue Subventionsbestimmungen (die Ausgaben über einem der Schwellenwerte nach sich ziehen) geschaffen noch neue Verpflichtungskredite oder Zahlungsrahmen (mit Ausgaben über einem der Schwellenwerte) beschlossen.

80 Rz. 25 der Gesetzestechnischen Richtlinien des Bundes, online abrufbar www.bk.admin.ch > Dokumentation > Rechtsetzungsbegleitung > Gesetzestechnische Richtlinien GTR

7.5 Einhaltung des Subsidiaritätsprinzips und des Prinzips der fiskalischen Äquivalenz

Bei der Zuweisung und Erfüllung staatlicher Aufgaben ist der Grundsatz der Subsidiarität zu beachten (Artikel 5*a* BV). Gemäss Artikel 43*a* Absatz 1 BV übernimmt der Bund nur die Aufgaben, welche die Kraft der Kantone übersteigen oder einer einheitlichen Regelung durch den Bund bedürfen. Gleichzeitig hat der Bund von seinen Kompetenzen einen schonenden Gebrauch zu machen und den Kantonen ausreichend Raum für die Aufgabenerfüllung zu überlassen.

Eine Meldepflicht für Cyberangriffe auf kritische Infrastrukturen kann nicht wirkungsvoll umgesetzt werden, wenn sie nicht landesweit und sektorenübergreifend gilt. Ohne einheitliches Meldeverfahren und zentrale Meldestelle ist Cyberangriffen, die sich über geografische und sektorielle Grenzen hinweg ereignen, nicht beizukommen. Entsprechend der verfassungsmässigen Kompetenz des Bundes wurde die Meldepflicht auf Cyberangriffe bei kritischen Infrastrukturen beschränkt, da deren Auswirkungen eine Bedrohung für die Landessicherheit und das ordnungsgemässe Funktionieren des Staates darstellen können. Die Einführung der Meldepflicht stellt deshalb eine Massnahme dar, die mit dem Subsidiaritätsprinzip (Artikel 5*a* i.V.m. 43*a* BV) vereinbar ist.

Nach dem in Artikel 43*a* Absätze 2 und 3 BV statuierten Prinzip der fiskalischen Äquivalenz trägt das Gemeinwesen, in dem der Nutzen einer staatlichen Leistung anfällt deren Kosten; das Gemeinwesen, das die Kosten einer staatlichen Leistung trägt, kann über die Leistungen bestimmen. Im Zusammenhang mit der Einführung der Meldepflicht ist dieses Prinzip gewahrt, da die Kosten für den Betrieb der zentralen Meldestelle beim Bund anfallen werden. Für die kritischen Infrastrukturen ändert sich mit der Einführung der Meldepflicht wenig: Sie können wie bisher auf die Unterstützung des NCSC bei der Vorfallbewältigung zählen. Im Vergleich zu freiwilligen Meldungen zu Cybervorfällen entsteht durch die Meldepflicht nur ein geringer Mehraufwand. Somit entstehen auch bei kritischen Infrastrukturen, die von Kantonen und Gemeinden betrieben werden, keine eigentlichen Zusatzkosten durch die Meldepflicht.

7.6 Delegation von Rechtsetzungsbefugnissen

Die für die Einführung der Meldepflicht für Cyberangriffe wesentlichen Eckwerte sollen gemäss dem vorliegenden Vernehmlassungsentwurf auf Gesetzesstufe verankert werden.

Der Bundesrat wird dazu Ausführungsbestimmungen erlassen, um die gesetzlichen Bestimmungen, sofern nötig, zu konkretisieren. Insbesondere obliegt es dem Bundesrat nach Artikel 74*c* E-ISG den Adressatenkreis der Meldepflicht weiter einzuschränken. Das Gesetz definiert die dafür anzuwendenden Kriterien, es muss aber durch den Bundesrat pro Sektor festgelegt werden, welche Kriterien wie angewendet werden (Beispielsweise über die Definition von geeigneten Schwellenwerten).

7.7 Datenschutz und Öffentlichkeitsprinzip

Die Vernehmlassungsvorlage hat die datenschutzrechtlichen Vorgaben im Wesentlichen unverändert übernommen, wie sie vom Parlament im 5. Kapitel des ISG ursprünglich im Zusammenhang mit der Unterstützung für kritische Infrastrukturen verabschiedet wurden.

Neu wurde in das ISG eine Bestimmung aufgenommen (Art. 4 Abs. 1bis), gemäss welcher Informationen Dritter, die dem NCSC im Rahmen der Meldepflicht übermittelt wurden oder von denen das NCSC durch die Analyse solcher Meldungen Kenntnis erhalten hat, nicht nach dem Öffentlichkeitsgesetz zugänglich gemacht werden dürfen.

Der EDÖB ist mit dieser Bestimmung nicht einverstanden. Diese Ausnahme würde gemäss Einschätzung des EDÖB das Öffentlichkeitsprinzip verletzen, indem es den Bürgerinnen und Bürgern den Zugang zu Informationen verwehrt, die in direktem Zusammenhang mit der Erfüllung einer zentralen Aufgabe des NCSC stehen. Dies erschwere die öffentliche Kontrolle in einem sensiblen Bereich. Zudem reiche die breite Palette an Ausnahmen im Öffentlichkeitsgesetz aus, um die verschiedenen Interessen zu schützen, so dass die Einführung einer neuen Ausnahme überflüssig ist. Der EDÖB kann nicht erkennen, wie die Anwendung des Öffentlichkeitsgesetzes die Funktion des NCSC als Meldestelle beeinträchtigen könnte.

Beilagen (Erlassentwürfe)