Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Bundesrat

Vernehmlassung zur Einführung einer Meldepflicht für Cyberangriffe eröffnet

Bern, 12.01.2022 - An seiner Sitzung vom 12. Januar 2022 hat der Bundesrat die Vernehmlassung zur Vorlage für die Einführung einer Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen eröffnet. Die Vorlage schafft die gesetzlichen Grundlagen für die Meldepflicht und definiert die Aufgaben des Nationalen Zentrums für Cybersicherheit (NCSC), welches als zentrale Meldestelle für Cyberangriffe vorgesehen ist. Die Vernehmlassung dauert bis zum 14. April 2022.

Cyberangriffe sind zu einer ernsthaften Bedrohung der Sicherheit und Wirtschaft der Schweiz geworden. Täglich finden Angriffe auf Unternehmen und Behörden statt. Das NCSC erhält im Durchschnitt wöchentlich über 300 Meldungen zu erfolgreichen oder versuchten Cyberangriffen. Diese Meldungen an das NCSC erfolgen auf freiwilliger Basis durch Unternehmen, Behörden und Privatpersonen. Sie helfen den zuständigen Bundesbehörden, die Bedrohungslage einzuschätzen und aktuelle Angriffsmuster frühzeitig zu erkennen. Der Bundesrat will nun das Meldewesen stärken, indem er die Betreiberinnen und Betreiber kritischer Infrastrukturen verpflichtet, dem NCSC Cyberangriffe zu melden. Über die Meldepflicht soll sichergestellt werden, dass das NCSC aufgrund der umfassenden Informationen über ein übersichtlicheres Lagebild verfügt und dadurch andere Betreibende kritischer Infrastrukturen frühzeitig vor Cyberangriffen warnen kann.

Meldepflicht für kritische Infrastrukturen

Die Meldepflicht für die Betreiberinnen und Betreiber kritischer Infrastrukturen soll für Cyberangriffe gelten, die ein erhebliches Schadenspotential aufweisen. Dies sind insbesondere Angriffe, die die Funktionsfähigkeit von kritischen Infrastrukturen gefährden oder mit Erpressung, Drohung oder Nötigung verbunden sind. Als zentrale Meldestelle ist das NCSC vorgesehen. Um eine Meldung so einfach wie möglich vorzunehmen, wird das NCSC ein elektronisches Meldeformular zur Verfügung stellen. Dies erlaubt, Meldungen einfach zu erfassen und die Meldungen auf Wunsch direkt weiteren Stellen zu übermitteln.

Pflicht des Bundes zur Unterstützung bei Cyberangriffen

Die Vorlage verpflichtet aber nicht nur die Unternehmen zur Mitwirkung beim Schutz vor Cyberangriffen, sondern definiert auch die Aufgaben des Bundes bei der Unterstützung der Wirtschaft und Bevölkerung. Zu diesem Zweck wird das NCSC beauftragt, die Öffentlichkeit vor Cyberbedrohungen zu warnen und sie für Cyberrisiken zu sensibilisieren. Auch soll das NCSC Meldungen zu Vorfällen und Schwachstellen entgegennehmen, technische Analysen durchführen und den Meldenden Empfehlungen zum weiteren Vorgehen abgeben. Betreiberinnen und Betreiber kritischer Infrastrukturen, zu denen auch kantonale und kommunale Behörden gehören, unterstützt das NCSC zudem bei der Bewältigung von Cybervorfällen. Diese Unterstützung soll im Sinne einer ersten Hilfe erfolgen und nur soweit gehen, dass sie nicht in Konkurrenz stehen zu Dienstleistungen, die am Markt erhältlich sind.

Bis anhin wurden diese Aufgaben des Bundes beim Schutz vor Cyberrisiken auf Basis der bestehenden Aufträge wahrgenommen, waren jedoch nicht auf Gesetzesstufe definiert. Mit der Verankerung der Meldepflicht im Informationssicherheitsgesetz (ISG) sollen nun auch die Aufgaben des NCSC, insbesondere auch dessen Zuständigkeit als Meldestelle, im ISG festgelegt werden.

Die Vernehmlassung zur Vorlage dauert bis zum 14. April 2022.

Adresse für Rückfragen

Kommunikation,
Eidgenössisches Finanzdepartement EFD
Tel. +41 58 462 60 33, info@gs-efd.admin.ch

Dokumente

Gesetz (PDF, 321 kB)

Erläuternder Bericht (PDF, 696 kB)

Brief an die Kantone (PDF, 149 kB)

Brief an die Organisationen (PDF, 167 kB)

Liste der Vernehmlassungsadressaten - Liste des destinataires - Elenco dei destinatari (PDF, 172 kB)

Herausgeber

Der Bundesrat
https://www.admin.ch/gov/de/start.html

Eidgenössisches Finanzdepartement
http://www.efd.admin.ch

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
http://www.vbs.admin.ch

https://www.admin.ch/content/gov/de/start/dokumentation/medienmitteilungen.msg-id-86768.html/

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Nationales Zentrum für Cybersicherheit (NCSC)

Bern, 12.01.2022

Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen

Änderung des Bundesgesetzes über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) vom 18. Dezember 2020

Erläuternder Bericht
zur Eröffnung des Vernehmlassungsverfahrens

Inhaltsverzeichnis

Übersicht

In den letzten Jahren haben Cybervorfälle bei Privaten, in Unternehmen und auch bei Behörden stark zugenommen, mit teilweise gravierenden Auswirkungen. Der vorliegende Vernehmlassungsentwurf sieht die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen vor. 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.

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

Der nun vorliegende Vernehmlassungsentwurf sieht vor, dass die gesetzliche Grundlage für die Meldepflicht ins Informationssicherheitsgesetz (ISG), das am 18. Dezember 2020 vom Parlament verabschiedet wurde, aufgenommen werden soll. Zusätzlich zur Meldepflicht sollen im ISG auch die Aufgaben des nationalen Zentrums für Cybersicherheit (NCSC) und dessen Funktion als Meldestelle verankert werden.

Inhaltlich soll die Meldepflicht nur für Cyberangriffe gelten, die ein gewisses Schadenspotential aufweisen. Sie gilt für Betreiberinnen kritischer Infrastrukturen, worunter jene Prozesse, Systeme und Einrichtungen zu verstehen sind, die essenziell für das Funktionieren der Wirtschaft beziehungsweise das Wohlergehen der Bevölkerung sind. Die Funktion als zentrale Meldestelle übernimmt das NCSC, das auch freiwillige Meldungen zu Cybervorfällen und Schwachstellen in Informatikmitteln entgegennimmt.

Erläuternder Bericht

1 Ausgangslage

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[1] und erteilte 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 2) und zum Schutz der Schweiz vor Cyberrisiken (NCS 2018–2022, Massnahme 9) sowie den Expertenbericht zur Zukunft der Datenbearbeitung und Datensicherheit[2]. 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[3] erteilte der Bundesrat dem 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 Nationale Zentrum für Cybersicherheit (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[4] 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

1.2.1 Ausbau des freiwilligen Informationsaustausches

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 ein freiwilliger Austausch funktioniert, braucht es ein gut etabliertes 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 Akteuren eine ausreichende Vertrauensbasis hergestellt werden kann. In

1 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 (Postulatsbericht).
2 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.
3 Vgl. Bericht «Meldepflicht für schwerwiegende Sicherheitsvorfälle bei kritischen Infrastrukturen, Rechtliche Grundlagen» vom 25. November 2020, Beilage 01 zum BRA vom 11.12.2020.
4 17.3508 Mo. Eder «Schaffung eines Cybersecurity-Kompetenzzentrums auf Stufe Bund».

der Konsequenz hat sich der Informationsaustausch über die letzten Jahre so entwickelt, dass mit einigen Unternehmen und Organisationen die etablierte Zusammenarbeit weiterhin gut funktioniert, eine Ausweitung dieses Modells aber nicht mehr realistisch ist.

Beim Meldeeingang kann dieser Fokus auf wenige Unternehmen 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 ist, sich darauf zu verlassen, wichtige Meldungen 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 Verhältnis zu anderen Meldepflichten und Informationsaustausch unter den Behörden

Die Einführung einer Meldepflicht für Cyberangriffe tangiert bereits bestehende Meldepflichten und führt zur Frage, wie und wann die beim NCSC eingegangenen Meldungen an andere Behörden weitergeleitet werden können.

Beim Verhältnis zu bereits bestehenden Meldepflichten wurde überprüft, ob es möglich ist, die Meldepflicht für Cyberangriffe in diesen zu verankern und darauf zu verzichten, eine sektorübergreifende Meldepflicht einzuführen. Diese Variante wurde verworfen, da die Regelungen zu Sicherheitsvorfällen in den verschiedenen Sektoren uneinheitlich sind und teilweise gar keine solchen bestehen. Wenn an einer Meldepflicht für Cyberangriffe gegenüber einer zentralen Meldestelle festgehalten wird, muss jedoch geklärt werden, welche Meldungen wann bei wem erfasst werden müssen. Hier gilt, dass die Meldepflicht für Cyberangriffe die bestehenden Meldepflichten nicht ersetzt, sondern nur ergänzt. Gleichzeitig wurde darauf geachtet, dass die gesetzlichen Grundlagen eine gleichzeitige Erfüllung verschiedener Meldepflichten erlauben. Der Aufwand für die Erfüllung der verschiedenen 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 (nachfolgend: nDSG)[5], 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 gleichzeitig mit der Übermittlung an das NCSC anderen Meldestellen weiterzuleiten, um damit anderweitige Meldepflichten zu erfüllen. Umgekehrt wird das NCSC auch Meldungen zu Cyberangriffen entgegennehmen, welche in Erfüllung einer anderweitigen Meldepflicht abgegeben wurden, sofern sie die benötigten Inhalte umfasst. Damit soll verhindert werden, dass Betroffene den gleichen Vorfall unterschiedlichen Stellen über unterschiedliche Verfahren melden müssen.

Klärungsbedürftig ist in diesem Zusammenhang auch der Informationsaustausch zwischen den Behörden. 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 beibehalten werden. Eine Weiterleitung von Meldungen oder Teilen davon erfolgt nur mit Einverständnis der Betreiberin der betroffenen kritischen Infrastruktur oder anonymisiert.

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

5 Bundesgesetz vom 25. September 2020 über den Datenschutz (Datenschutzgesetz, DSG, SR **235.1**), BBl 2020 7639.

schwere Straftat enthält. Zwar ist das NCSC von der Anzeigepflicht gemäss Artikel 22*a* des Bundespersonalgesetzes vom 24. März 2000[6] 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. Die Weiterleitung an die Strafverfolgungsbehörden wird keine strafrechtlichen Konsequenzen für die Betreiberin der kritischen Infrastruktur haben, da sich das Strafverfahren in der Regel ausschliesslich gegen die Angreifer richten wird. Sollte die Betreiberin der kritischen Infrastruktur ausnahmsweise selber Gegenstand der Strafverfolgung werden, so darf die Meldepflicht nicht dazu führen, dass sie sich durch die Meldung selber belasten muss. Es wurde daher eine Bestimmung aufgenommen, um dem Selbstbelastungsverbot als zentralem Grundsatz der Strafverfolgung Rechnung zu tragen. Vorbild dafür war die Regelung, die für die Meldepflicht bei Verletzungen der Datensicherheit im revidierten Datenschutzrecht vorgesehen ist (vgl. Art. 24 Abs. 6 nDSG).

Der zweite Fall einer zulässigen Weiterleitung betrifft Informationen, welche für den Nachrichten dienst des Bundes (NDB) für seine Aufgaben der frühzeitigen Erkennung und Verhinderung von Bedrohungen der inneren oder äusseren Sicherheit, für die Beurteilung der Bedrohungslage oder für die nachrichtendienstliche Frühwarnung zum Schutz von kritischen Infrastrukturen nach Artikel 6 Absatz 1 Buchstabe a, Absatz 2 und 5 des Nachrichtendienstgesetzes vom 25. September 2015 (NDG)[7] relevant sind. Dadurch ist sichergestellt, dass der NDB als zuständige Behörde für die Frühwarnung von kritischen Infrastrukturen und für die Einschätzung der Bedrohungslage die nötigen Informationen erhält.

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 Unterstützung bei der Bewältigung des Angriffs. Diese sollen im Sinne einer ersten Hilfe erfolgen und nur soweit gehen, dass sie nicht in Konkurrenz stehen zu Dienstleistungen, die am Markt erhältlich sind. Für Betreiberinnen kritischer Infrastrukturen 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.

Der dritte Faktor zur Durchsetzung der Meldepflicht besteht in negativen Anreizen in Form einer Busse. Wenn es trotz Rücksprache mit der kritischen Infrastruktur zu einer Verletzung der Melde- oder Auskunftspflicht kommen sollte, besteht 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. Als Vorlage für diese verwaltungsrechtliche Sanktionsmöglichkeit diente das revidierte Datenschutzgesetz, das in Artikel 63 f. eine ähnliche Regelung für den Fall einer Missachtung von Verfügungen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) enthält.

Aufgrund der langbewährten Zusammenarbeit mit den kritischen Infrastrukturen geht das NCSC davon aus, dass diese Bestimmung weitgehend symbolischen Charakter hat und in erster Linie dazu dient, der Meldepflicht die nötige Beachtung zu verschaffen.

6 SR **172.220.1**
7 SR **121**

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

Die Vorlage wurde in der Botschaft vom 29. Januar 2020 zur Legislaturplanung 2019–2023[8] und im Bundesbeschluss vom 21. September 2020 über die Legislaturplanung 2019–2023[9] angekündigt. In der Botschaft LP 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 LP 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 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 leiste[10].

In der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken 2018–2022 werden die Abklärungen sowie der Entscheid über die Einführung der Meldepflicht für Cyberangriffe in Massnahme 9 aufgeführt. Diese Massnahme 9 wird mit der vorliegenden Vernehmlassungsvorlage vollständig umgesetzt[11].

8 BBl 2020 1777, hier 1866.
9 BBl 2020 8385, hier 8392.
10 Voranschlag 2022 mit IAFP 2023–2025, Band 2B, S. 11 ff., abrufbar unter: «www.efv.admin.ch > Finanzberichte > Finanzberichte > Voranschlag mit integriertem Aufgaben- und Finanzplan» https://www.efv.admin.ch/dam/efv/de/dokumente/Finanzberichte/finanzberichte/va_iafp/2022/va2b-2022.pdf.download.pdf/VA2B-6-8-d.pdf.
11 Vgl. Bericht zum Umsetzungsstand der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022 vom August 2021, S. 10, 15 f. (: «www.ncsc.admin.ch > NCSC Strategie > Berichte und Studien» https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/strategie/Bericht-Umsetzungsstand_NCS_2021_DE.pdf.download.pdf/Bericht-Umsetzungsstand_NCS_2021_DE.pdf).

2 Rechtsvergleich, insbesondere mit dem europäischen Recht

Seit der Verabschiedung der EU-Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) 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 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[12]. Der Adressatenkreis entspricht damit weitegehend den in der Vernehmlassungsvorlage definierten meldepflichtigen kritischen Infrastrukturen.

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 zur erarbeiteten Vernehmlassungsvorlage 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).

Die Vernehmlassungsvorlage beschränkt sich darauf, die gesetzlichen Grundlagen für solche Anforderungen im Stromsektor zu schaffen. Eine durch das Bundesamt für Energie (BFE) beauftragte Studie hat in diesem für die wirtschaftliche Versorgung und die Sicherheit des Landes entscheidenden Sektor einen hohen Handlungsbedarf bei der Cybersicherheit festgestellt.[13] 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.

12 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 (europa.eu).

13 Strategie Cyber Security für die Schweizer Stromversorgung vom 28. Juni 2021, «Strategie Cyber Security für die Schweizer Stromversorgung vom 28. Juni 2021, www.bfe.admin.ch > Versorgung > Digitalisierung im Energiesektor» https://www.bfe.admin.ch/bfe/de/home/news-und-medien/publikationen.exturl.html/aHR0cHM6Ly9wdWJkYi5iZmUuYWRtaW4uY2gvZGUvcHVibGljYX/Rpb24vZG93bmxvYWQvMTA1MjQ=.html.

3 Grundzüge der Vorlage

3.1 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 Angreifer oft mehrmals 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.

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 Mitarbeiters, zurückzuführen sind. Schliesslich wurde auch davon abgesehen, die Meldepflicht auf Schwachstellen in Informatikmitteln auszudehnen. Unabhängig von der 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 (CyRV)[14] definiert sind. Dies ist einerseits nötig, da das NCSC die Funktion der Meldestelle übernimmt. Andererseits wird mit dieser der Neuorganisation der Bundesverwaltung im Bereich Cybersicherheit Rechnung getragen, insbesondere der Gründung des NCSC, die erst während der parlamentarischen Debatten zum ISG erfolgte.

3.2 Abstimmung von Aufgaben und Finanzen

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

Das NCSC nutzt für die Entgegennahme von Meldungen 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 die Umsetzung der Vorlage muss das NCSC jedoch sicherstellen können, 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.

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 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.

14 SR **120.73**

3.3 Umsetzungsfragen

3.3.1 Notwendigkeit einer gesetzlichen Grundlage

Aus dem Legalitätsprinzip (Art. 5 Abs. 1 der Bundesverfassung, BV[15]) und den Bestimmungen zur Gesetzgebung von Artikel 164 Absatz 1 BV ergibt sich, dass die Meldepflicht für Cyberangriffe mindestens in den Grundzügen auf Gesetzesebene zu regeln ist. Entsprechend enthält die Vernehmlassungsvorlage 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), der Inhalt der Meldungen sowie deren Verwendung durch das NCSC. Die Meldepflicht stellt für die meldepflichtigen Betreiberinnen kritischen Infrastrukturen einen Eingriff in Rechte von Privaten oder, bei kantonaler oder kommunaler Trägerschaft, in deren föderalistische Autonomie dar. Die Meldepflicht ist aber nicht ein Eingriff von grosser Tragweite und hat kaum finanzielle Auswirkungen auf die betroffenen Unternehmen.

3.3.2 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[16]. 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[17], LVG[18], BWIS[19], NDG und ISG[20]). 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 KI-Betreibende 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.

3.3.3 Ausführungsbestimmungen

Die gesetzlichen Vorgaben werden durch eine Verordnung konkretisiert. Diese wird die Aufgaben des NCSC und die Zusammenarbeit mit weiteren Stellen genauer umschreiben und präzisieren, wer wann welche Cyberangriffe über welche Verfahren zu melden hat. Die Verordnung wird jene Bestimmungen der heutigen CyRV integrieren, welche das Verhältnis des Bundes zur Öffentlichkeit und insbesondere zu den Betreiberinnen kritischer Infrastrukturen betreffen. Bei den Bestimmungen zum Adressatenkreis ist jeweils zu prüfen, ob eine Präzisierung in der Verordnung zur Meldepflicht oder in sektorspezifischen Verordnungen zu bevorzugen ist.

15 SR **101**
16 Vgl. Bericht «Meldepflicht für schwerwiegende Sicherheitsvorfälle bei kritischen Infrastrukturen, Rechtliche Grundlagen» vom 25. November 2020, Beilage 01 zum BRA vom 11.12.2020.
17 SR **520.1**
18 SR **531**
19 SR **120**
20 Bundesgesetz vom 18. Dezember 2020 über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG), BBl *2020* 9975.

3.3.4 Vollzugstauglichkeit der Meldepflicht

Das NCSC hat im April 2021 unter Betreiberinnen kritischer Infrastrukturen und Behörden eine Umfrage zur geplanten Einführung einer Meldepflicht für Cyberangriffe durchgeführt. Diese hat ergeben, dass die Akzeptanz gegenüber einer Meldepflicht grundsätzlich hoch ist, wenn es gelingt, diese so umzusetzen, dass ein geringer bürokratischer Aufwand entsteht. Abbildung 1 verdeutlicht die hohe grundsätzliche Zustimmung der Befragten.

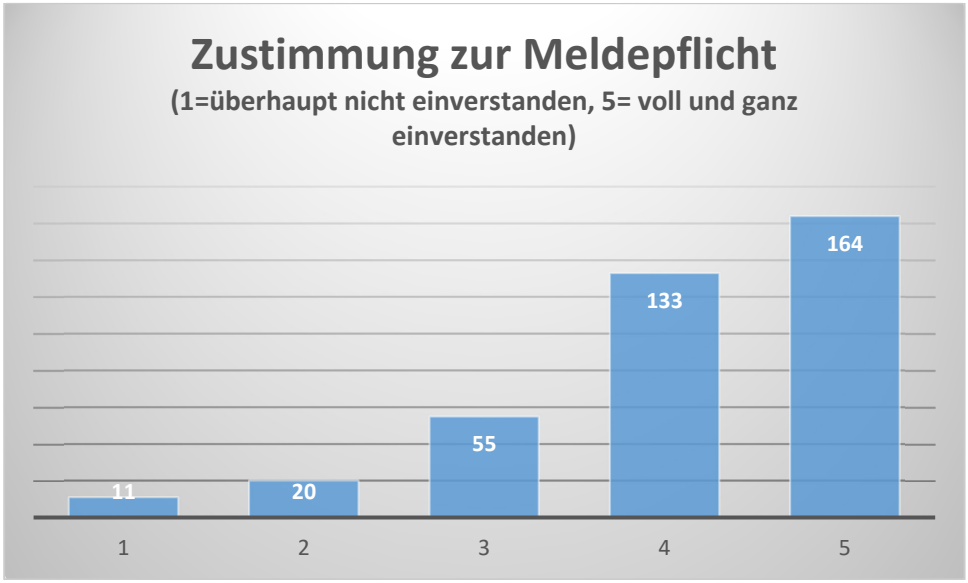

Abbildung 1 Beurteilung der Meldepflicht

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 Mai 2020 eine Meldepflicht für Cybervorfälle gegenüber der FINMA[21]. Damit wird ein Cyberangriff in aller Regel sowohl der FINMA wie auch dem NCSC zu melden sein.

- Ein Cyberangriff auf eine kritische Infrastruktur kann zu einer Verletzung der Datensicherheit, die je nach Schwere der Verletzung gegenüber dem EDÖB meldepflichtig ist[22].

- Löst ein Cyberangriff Funktionsstörungen bei der kritischen Infrastruktur aus, z.B. einen radioaktiven Vorfall in einer Kernanlage, dann ist dieser Störfall ebenfalls meldepflichtig (ENSI, NAZ 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). Die Meldepflichtigen können selber entscheiden, ob sie die elektronisch erfasste Meldung mit möglichen Zusatzangaben an weitere Meldestellen schicken wollen. Sofern andere Meldestellen Hand bieten, könnte die Erfassung der Meldung auch so gegliedert werden, dass neben den allgemeinen Angaben zur kritischen Infrastruktur

21 Vgl. Artikel 29 FINMAG. Die allgemeine Meldepflicht umfasst auch Cybervorfälle (vgl. FINMA, Aufsichtsmitteilung 05/2020 vom 7.Mai 2020).
22 Artikel 24 nDSG.

die spezifischen Angaben für die Erfüllung der jeweiligen Meldepflicht nur für die betreffende Meldestelle bestimmt wären. Meldepflichtige würden mit der Erfassung und Weiterleitung steuern, welche Meldestelle welche Angaben erhält.

4 Erläuterungen zu einzelnen Artikeln

Die gesetzlichen Grundlagen der Meldepflicht für Cyberangriffe, sollen – abgesehen von 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 in der Botschaft zum ISG (BBl 2017 3062 ff.) und unter den vorstehenden Ziffern teilweise bereits ausführlich beschrieben und begründet. Die Kommentierung der nachfolgende Artikel beschränkt sich daher auf Ergänzungen dazu.

1. Kapitel: Allgemeine Bestimmungen

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

Artikel 1 Zweck

Der Zweckartikel des ISG wurde in Absatz 1 ergänzt und zu diesem Zweck eine Unterteilung in Buchstabe a und b vorgenommen. In Buchstabe a wurde die ursprüngliche Formulierung übernommen, während in Buchstabe b die Zweckbestimmung in Bezug auf Cyberrisiken ergänzt wurde. Diese erweiterte Zweckbestimmung dient dazu, den durch die Einführung einer Meldepflicht für Cyberangriffe und der gesetzlichen Regelung der Aufgaben des NCSC eingefügten Aspekte 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 5 Begriffe

Die Begriffsdefinitionen in Buchstabe a, b und c wurden nicht verändert.

Buchstabe d

Die neu aufgenommene Definition von «Cybervorfall» wurde aus Artikel 3 Buchstabe b CyRV übernommen und leicht angepasst. Die Definition umfasst auch den Missbrauch von Informatikmitteln, wie dies z.B. bei Phishing-Versuchen der Fall ist.

Buchstabe e

Neu definiert wurde der Begriff «Cyberangriff», der eine mögliche Erscheinungsform des Cybervorfalls darstellt. Der Begriff «Cyberangriff» ist als Abgrenzung zum Oberbegriff «Cybervorfall» deshalb von Bedeutung, weil nur die Angriffe auf kritische Infrastrukturen meldepflichtig sind, während Cybervorfälle und Schwachstellen freiwillig und von jeder Person gemeldet werden können.

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

Im zweiten, dritten und vierten Kapitel 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 3 Abschnitte gegliedert.

1. Abschnitt: Allgemeine Bestimmungen

Artikel 73a Grundsatz

In diesem Artikel werden die Aufgaben des NCSC unter Buchstabe a bis f beschrieben. Es handelt sich um eine nicht abschliessende Aufzählung. Im Zusammenhang mit der Entgegennahmen und Bearbeitung von Meldungen (Buchstabe e) ist zu präzisieren, dass es hier sowohl um die freiwilligen Meldungen zu Cybervorfällen und Schwachstellen geht wie auch um die Meldungen zu Cyberangriffe auf kritische Infrastrukturen, die meldepflichtig sind.

Die einzelnen Aufgaben sowie die Zusammenarbeit mit Behörden im In- und Ausland bilden Gegenstand von weiteren Artikeln, die deren Inhalt konkretisieren.

Artikel 73b Bearbeitung von Meldungen zu Cybervorfällen und Schwachstellen

Das NCSC betreibt seit dem 1. Januar 2020 eine nationale Anlaufstelle für Cyberrisiken (vgl. Art. 12 Abs. 1 Bst. a CyRV), die Meldungen zu Cybervorfällen und Schwachstellen erfasst und bearbeitet. Die Meldestelle des NCSC wurde auf der Grundlage von MELANI aufgebaut, welche seit 2004 Meldungen entgegennimmt. Die Meldestelle des NCSC wird von Unternehmen und Bevölkerung rege genutzt. Im Jahr 2020 gingen 10'834 Meldungen bei ihr ein[23].

Das NCSC wurde am 28. September 2021 Teil des weltweiten Netzwerks zur Verwaltung von Schwachstellen in Informatiksystemen und ist seither berechtigt, den gemeldeten Schwachstellen eine eindeutige Identifikationsnummer gemäss internationalem Referenzsystem zu vergeben[24]. Es ist deshalb wichtig zu präzisieren, dass das NCSC neben Meldungen zu Cybervorfällen auch solche zu Schwachstellen entgegennimmt.

Absatz 1

Cybervorfälle und Schwachstellen können dem NCSC nicht nur von den Betroffenen selber, sondern auch von Dritten – und falls gewünscht auch anonym – gemeldet werden. Das NCSC analysiert die Vorfälle und beurteilt, welche Bedeutung sie für den Schutz der Schweiz vor Cyberrisiken haben. Sofern die Meldungen nicht anonym erfolgen, kann das NCSC auf Wunsch der Meldenden basierend auf diesen Analysen auch Einschätzungen zum Vorfall und Empfehlungen für das weitere Vorgehen abgeben. Zudem verwendet das NCSC die Meldungen für statistische Zwecke und für die Warnung der Öffentlichkeit vor Cyberbedrohungen. Dabei werden keine Angaben der Meldenden oder der Betroffenen publiziert.

Das NCSC behandelt die Meldungen vertraulich. Diese Vertraulichkeit der Meldungen ist eine wichtige Voraussetzung, damit überhaupt Meldungen eingehen und der Meldestelle Vertrauen entgegengebracht wird.

Absatz 2

Das NCSC kann Informationen zu Cybervorfällen veröffentlichen oder an interessierte Behörden und Organisationen weiterleiten, sofern die Informationen keine Personendaten oder Daten juristischer Personen enthalten. Eine Veröffentlichung von Personendaten im Falle von Cybervorfällen ist ausgeschlossen. Weiterhin möglich ist die Veröffentlichung von Informationen aus der Meldung mit Zustimmung der betroffenen Person oder Organisation, wie beispielsweise im Falle des Missbrauchs von Logos bei Phishing-Angriffen.

23 Vgl. Bericht zum Umsetzungsstand der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022, verfasst im August 2021, S. 5 («www.ncsc.admin.ch > NCSC Strategie > Berichte und Studien» https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/strategie/Bericht-Umsetzungsstand_NCS_2021_DE.pdf.download.pdf/Bericht-Umsetzungsstand_NCS_2021_DE.pdf).

24 Vgl. Medienmitteilung des NCSC vom 28. September 2021: «www.ncsc.admin.ch > Dokumentation > Medienmitteilungen > Newslist > NCSC ist neu Teil des weltweiten Netzwerks zur Verwaltung von Schwachstellen in Informatiksystemen» https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/medienmitteilungen/newslist.msg-id-85280.html.

Absatz 3

Bei Schwachstellen hingegen kann die schnelle Veröffentlichung der Schwachstelle mit Nennung der betroffenen Soft- oder Hardware notwendig sein, um weitere Cyberangriffe zu verhindern. Das Ausnutzen von Schwachstellen ist eine der häufigsten Vorgehensweisen bei Cyberangriffen. Nur mit diesen Informationen ist es den Nutzenden der Soft- oder Hardware möglich, umgehend die nötigen Massnahmen zum Schutz vor Cyberangriffen zu ergreifen. Absatz 3 bildet die gesetzliche Grundlage, damit das NCSC bei der Veröffentlichung der Schwachstellen die betroffene Hard- und Software – und damit implizit deren Hersteller – namentlich nennen darf.

Artikel 73c Weiterleitung von Informationen

Artikel 73*c* definiert die Voraussetzungen, unter welchen es dem NCSC erlaubt ist, gewisse Informationen, die in einer Meldung enthalten sind, an den NDB oder die Strafverfolgungsbehörden weiterzuleiten (Absatz 1 und 2). Schliesslich wird auch der Umgang mit Informationen geregelt, sollte sich ein Strafverfahren gegen eine meldende Person richten (Absatz 3).

Absatz 1

Absatz 1 hält fest, dass es dem NCSC erlaubt ist, Informationen an den NDB weiterzuleiten, wenn diese Informationen der Früherkennung und Verhinderung von Bedrohungen der inneren oder äusseren Sicherheit, für die Beurteilung der Bedrohungslage oder für die nachrichtendienstliche Frühwarnung zum Schutz von kritischen Infrastrukturen nach Artikel 6 Absätzen 1 Buchstabe a, 2 und 5 NDG relevant sind. Diese Weiterleitung ist nötig, damit der NDB seine Aufgaben auch in Bezug auf Cyberbedrohungen erfüllen kann. Sie beschränkt sich jedoch auf die dafür nötigen Informationen.

Absatz 2

Absatz 2 regelt die Weitergabe von Informationen an die Strafverfolgungsbehörden. Die für Bundesangestellte geltende Anzeigepflicht entfällt für Informationen, welche das NCSC bei der Meldung eines Cybervorfalls oder bei dessen Analyse erhält, da diese Anzeigepflicht in einem Spannungsfeld zum Grundsatz der vertraulichen Behandlung der Meldung steht. Die Leiterin oder der Leiter des NCSC ist jedoch berechtigt, Informationen an die Strafverfolgungsbehörden weiterzuleiten. Sie oder er wägt dabei das Interesse des Staates an einer Strafverfolgung gegen das Interesse der meldenden Person an der Vertraulichkeit der Meldung ab. Diese Möglichkeit der Weiterleitung der Meldung nach entsprechender Interessenabwägung wurde vorgesehen, damit das NCSC bei schweren Straftaten an die Strafverfolgungsbehörden gelangen kann.

Absatz 3

Über die Bestimmung von Absatz 3 wird sichergestellt, dass die meldende Person in einem gegen sie selber gerichteten Strafverfahren nicht gegen ihren Willen durch Informationen aus der Meldung belastet wird. In der Regel wird sich ein Strafverfahren gegen die Verursacher des Cybervorfalls, d.h. gegen die Angreifer, richten und nicht gegen die meldende Person. Sollte sich ein Strafverfahren ausnahmsweise gegen das Opfer eines Cyberangriffs richten, wurde eine analoge Regelung wie in Artikel 24 Absatz 6 nDSG aufgenommen. Diese Bestimmung setzt im Bereich der Meldepflicht bei Cyberangriffen den Grundsatz des Selbstbelastungszwangsverbots um (nemo tenetur). Sie ist also insbesondere für diejenigen Meldungen von Bedeutung, die in Erfüllung der Meldepflicht für Cyberangriffe erfolgen. Darüber hinaus soll dieses Privileg aber auch für freiwillige Meldungen gelten.

Absatz 4

Für die Ausnahmefälle, in denen eine Weiterleitung von Informationen an den NDB oder Strafverfolgungsbehörden gemäss Absätzen 1 und 2 in Frage kommt, muss sich das NCSC gemäss den Vorgaben von Art. 320 StGB vom Amtsgeheimnis entbinden lassen, sofern die Informationen strafrechtlich geschützte Geheimnisse sind.

Artikel 74 Unterstützung für Betreiberinnen von kritischen Infrastrukturen

Ergänzend zu den allgemeinen Aufgaben in Artikel 73*a* und der Bearbeitung von Meldungen zu Cybervorfällen und Schwachstellen gemäss Artikel 73*b* erbringt das NCSC für Betreiberinnen von kritischen Infrastrukturen weitergehende Leistungen beim Schutz vor Cyberrisiken (Absatz 1). Dabei ist zu beachten, dass die Definition für kritische Infrastrukturen gemäss Artikel 5 ISG sehr weit gefasst ist und daher eine gewisse Unschärfe besteht, wann eine Organisation als kritische Infrastruktur gilt und wann nicht. Das NCSC orientiert sich dabei an den in der Strategie zum Schutz kritischer Infrastrukturen (SKI)[25] aufgelisteten Sektoren und Teilsektoren.

Absatz 2

Das NCSC stellt den Betreiberinnen kritischer Infrastrukturen zu diesem Zweck Hilfsmittel zur Verfügung. Die wichtigsten davon werden in diesem Absatz beispielhaft aufgelistet. Es handelt sich um eine nicht abschliessende Aufzählung.

Buchstabe a

Der gegenseitige Informationsaustausch ist ein sehr wichtiges Mittel zum Schutz vor Cyberrisiken. 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.

Buchstabe b

Informationen zu aktuellen Cyberrisiken und Schwachstellen sowie Empfehlungen für präventive Massnahmen beschränken sich auf Inhalte, die für kritische Infrastrukturen allgemein nützlich sein können. Es wird keine unternehmensspezifische Beratung durchgeführt.

Buchstabe c

Hilfsmittel und Anleitungen für die Früherkennung werden teilweise so konzipiert, dass sie allgemein 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 einzelner Unternehmen, sondern müssen in diese eingebunden werden.

Absatz 3

Bei Cybervorfällen unterstützt das NCSC die Betreiberinnen kritischer Infrastrukturen mit technischer Beratung. Die technische Unterstützung durch das NCSC 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. Es gilt ferner für alle Betreiberinnen, dass die Unterstützung durch das NCSC nur dann erfolgt, wenn sie zeitkritisch ist und ein erheblicher Schaden droht.

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 natürlich unter dem Vorbehalt, dass die Betreiberin der kritischen Infrastruktur ihr Einverständnis erteilt. Die Betreiberin ist gegenüber dem NCSC von ihren Geheimhal-

25 Nationale Strategie zum Schutz kritischer Infrastrukturen 2018-2022: «www.babs.admin.ch > Weitere Aufgabenfelder > Schutz kritischer Infrastrukturen > Nationale SKI-Strategie» https://www.bAbsatzadmin.ch/de/aufgabenbabs/ski/nationalestrategie.html.

tungspflichten entbunden. Der zweite Satz bildet die gesetzliche Grundlage dafür, dass die Betreiberin dem NCSC den Zugriff auf ihre Informationen und Informatikmittel erlauben kann, ohne ihre gesetzlichen und vertraglichen Geheimhaltungspflichten zu verletzen.

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

Artikel 74a Meldepflicht

In diesem Artikel wird die Meldepflicht in den Grundzügen definiert. Es wird festgehalten, dass Betreiberinnen kritischer Infrastrukturen im Falle von Cyberangriffen der Meldepflicht unterstellt sind und dass sie die Meldung des Cyberangriffs nach dessen Entdeckung so rasch wie möglich dem NCSC zu erstatten haben. Es ist für die Frühwarnung und die Prävention entscheidend, dass Angriffe unmittelbar nach deren Entdeckung gemeldet werden. In Artikel 74*e* wird präzisiert, dass die Anforderung der Unverzüglichkeit nicht für die gesamten verlangten Angaben gilt, sondern nur für die Erstmeldung auf der Basis der zu diesem Zeitpunkt verfügbaren Informationen.

Artikel 74b Bereiche

Die Definition kritischer Infrastrukturen nach Artikel 5 ist breit gefasst. Sie ist nicht eindeutig genug, um zu bestimmen, welche Unternehmen oder Organisationen als kritische Infrastruktur gelten und darum unter die Meldepflicht fallen. Art. 74*b* listet deshalb konkret auf, für welche Unternehmen und Organisationen die Meldepflicht gelten soll. Grundlage für die Auflistung sind die in der Nationalen Strategie zum Schutz kritischer Infrastrukturen aufgeführten kritischen Teilsektoren. Der Geltungsbereich der Meldepflicht wird für diese Bereiche, soweit möglich, mit Verweisen auf bestehende rechtliche Grundlagen bestimmt. 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 stellt sicher, dass ausreichende Klarheit darüber besteht, wer der Meldepflicht unterstellt ist.

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 Ebene sind meldepflichtig, da es wichtig ist zu wissen, wie oft und durch wen Behörden angegriffen werden. So können die Abwehrdispositive jeweils auf die relevanten Bedrohungen ausgerichtet werden. Die Meldepflicht gilt dabei nur für das hoheitliche Handeln dieser Behörden und Organisationen.

Buchstabe c: Organisationen mit öffentlich-rechtlichen Aufgaben

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.

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 Infra-

strukturen 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.

Buchstabe e: Banken, Versicherungen und Finanzmarktinfrastrukturen

Die Unternehmen des Finanzsektors sind stark betroffen von Cyberangriffen, da sie auf Grund der hohen 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 dazu bestehen. Die FINMA und das NCSC werden sich so abgleichen, dass der Aufwand für die Meldepflichtigen so gering wie möglich ausfällt.

Buchstabe f: Digitale Dienste

Als Anbieterinnen digitaler Dienste gelten jene Unternehmen, welche im Internet Dienste anbieten, die in der Schweiz von einer grossen Zahl von Nutzenden beansprucht werden, eine hohe Bedeutung für die digitale Wirtschaft haben oder Sicherheits- und Vertrauensdienste beinhalten. Dies sind insbesondere Anbieterinnen von Online-Marktplätzen von bedeutender Grösse, Cloudcomputing und Suchmaschinen. Die Aufzählung ist nicht abschliessend. Als «weitere digitale Dienste» fallen insbesondere Dienstleistungen in den Bereichen Identitätsmanagement, Signaturen oder E-Voting in Betracht. Ferner werden auch Registrare von Domain-namen und Betreiberinnen von Rechenzentren erwähnt. Auf Verordnungsstufe werden Kriterien wie die Anzahl Nutzende, Anzahl Mitarbeitende, Umsatz oder Art der Tätigkeiten festgelegt, um zu konkretisieren, welche digitalen Dienste der Meldepflicht unterstehen.

Buchstabe g: Spitäler

Die Kantone führen Spitallisten. Die dort aufgeführten kantonalen und ausserkantonalen Spitäler gewährleisten die Deckung des Bedarfs an medizinischer Grundversorgung auf dem jeweiligen Kantonsgebiet. Die Meldepflicht für Cyberangriffe soll für diese Spitäler gelten, weil es zu verhindern gilt, dass die Grundversorgung durch solche Angriffe beeinträchtigt wird.

Buchstabe h: 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 i: Herstellung, Inverkehrbringen bzw. Vertrieb sowie Einfuhr von Arzneimitteln und Medizinprodukten

Für die medizinische Versorgung der Bevölkerung ist die Herstellung, der Vertrieb und der Import von Arzneimittel von grosser Bedeutung. Unternehmen, welche in diesen Bereichen tätig sind, werden daher der Meldepflicht unterstellt. Zusätzlich sind auch Hersteller oder Distributoren von Medizinprodukten meldepflichtig.

Buchstabe j: Sozialversicherungen

Die Leistungen der Sozialversicherungen wurden in Anlehnung an die definierten Risiken in den Allgemeinen Bestimmungen des Bundesgesetzes über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG; SR 830.1) umschrieben, um möglichst alle Zweige der Sozialversicherungen abzudecken. Es wurde auf die Aufzählung einzelner Gesetze (z.B. IVG, AHVG) verzichtet, um nicht nur gesetzliche, sondern auch überobligatorische Leistungen, beispielsweise der beruflichen Vorsorge oder der Zusatzversicherung zur obligatorischen Krankenkasse, abzudecken. Bei der beruflichen Vorsorge werden alle registrierten und nicht registrierten Vorsorge- und Freizügigkeitseinrichtungen erfasst, jedoch nicht die gebundene oder freiwillige Selbstvorsorge (Säule 3a und 3b). Diese

letztgenannten Vorsorgemöglichkeiten werden in aller Regel von Banken und Versicherungen angeboten, die ihrerseits der Meldepflicht unterstehen.

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.

Buchstabe k: Anbieterinnen von Fernmeldediensten

Eine fernmeldetechnische Übertragung ist elektrisches, magnetisches, optisches oder anderes elektromagnetisches Senden oder Empfangen von Informationen über Leitungen oder Funk (Art. 3 Bst. c des Fernmeldegesetzes vom 30. April 1997, FMG[26]). Als fernmeldetechnische Übertragung gilt auch das Anbieten von Übertragungskapazität und die so genannten Over the Top (OTT)-Dienste. Bei Letzteren handelt es sich um Übertragungen von Informationen über Internetdienste. Bekannte Beispiele für solche Dienste sind Skype (Microsoft), WhatsApp (Facebook), Facetime (Apple), Hangouts (Google), Signal und Threema.

Buchstabe l: Schweizerische Radio- und Fernsehgesellschaft (SRG)

Die SRG hat den Auftrag, die gesamte Bevölkerung inhaltlich umfassend mit gleichwertigen Radio- und Fernsehprogrammen in den drei Amtssprachen zu versorgen (Art. 24 Abs. 1 Bst. a des Radio- und Fernsehgesetzes vom 24. März 2006, RTVG)[27]. Sie hat zudem den Auftrag, zur freien Meinungsäusserung durch umfassende, vielfältige und sachgerechte Information insbesondere über politische, wirtschaftliche und soziale Zusammenhänge beizutragen (Art. 24 Abs. 4 Bst. a RTVG). Damit geht ihr Auftrag deutlich über die Bekanntmachungspflichten der übrigen konzessionierten Medien hinaus. Cyberangriffe auf die SRG können die Erfüllung dieser Aufträge gefährden.

Buchstabe m: Nachrichtenagenturen von nationaler Bedeutung

Eine Nachrichtenagentur ist von nationaler Bedeutung gemäss Artikel 44a der Radio- und Fernsehverordnung vom 9. März 2007[28], 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[29] i.V.m. Art. 13 Abs. 2 der Sprachenverordnung vom 4. Juni 2010[30]). Konkret gibt es in der Schweiz nur noch die Nachrichtenagentur Keystone-SDA (siehe Covid-19-Verordnung elektr. Medien)[31].

Buchstabe n: 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 2010[32] registriert sind. Der Bundesrat kann auf Verordnungsebene kleinere Unternehmen von der Meldepflicht ausnehmen. Es wäre beispielsweise eine analoge Einschränkung denkbar, wie sie in Art. 4 Abs. 2 des Postgesetzes für Unternehmen vorgesehen ist, die einen geringen Umsatz erzielen.

Buchstabe o: Öffentlicher Verkehr (Personentransport plus Eisenbahngüterverkehr)

Mit dem Verweis auf das Bundesgesetz vom 18. Juni 2010[33] über die Sicherheitsorgane der Transportunternehmen im öffentlichen Verkehr wird nur der wichtigste Bereich des öffentlichen Verkehrs, d.h. der konzessionierte Personenverkehr sowie der Güterverkehr und die Infrastruktur der Eisenbahn erfasst.

26 SR **784.10**
27 SR **784.40**
28 SR **784.401**
29 SR **441.1**
30 SR **441.11**
31 SR **784.402**
32 SR **783.0**
33 SR **745.2**

Buchstabe p: Unternehmen der Zivilluftfahrt

Die Bestimmung unterstellt alle Unternehmen mit einer Bewilligung des Bundesamts für Zivilluftfahrt der Meldepflicht für Cyberangriffe.

Buchstabe q: Rheinschifffahrt

Die Schweizerischen Rheinhäfen bilden den Zugang der Schweiz zu den Weltmeeren und 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[34] und für die für den Betrieb und die Funktion vom Hafen Basel relevanten Prozesse.

Buchstabe r: Unentbehrliche Güter des täglichen Bedarfs

In die Versorgung der Bevölkerung mit unentbehrlichen Gütern des täglichen Bedarfs, insbesondere Lebensmittel, ist eine Vielzahl von Akteuren eingebunden. Neben den Produzenten und Importeuren spielen auch die Verarbeiter, die Verteilzentren und die Detailhändler eine bedeutende Rolle. Nicht alle dieser Akteure sind gleichbedeutend für die Versorgungssicherheit der Schweiz. Die Meldepflicht für Cyberangriffe soll nur für jene Akteure 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 gemäss den Kriterien von Art. 74*c* auf Verordnungsebene einschränken.

Buchstabe s: Hersteller von Hard- und Software

Vermehrt wird festgestellt, dass kritische Infrastrukturen über die Hersteller von Hard- und Software angegriffen werden. Die Cyberangreifer manipulieren dabei die Hard- und Software bereits vor der Auslieferung an die Endkunden, damit sie später Zugriff auf die Systeme erhalten. Für die Cybersicherheit sind deshalb die Hersteller von Hard- und Software von grosser Bedeutung.

Besonders relevant sind Cyberangriffe auf Hersteller von Software, wenn diese über Fernwartungszugänge verfügen. Angreifer können versuchen, über solche legitimen Zugänge direkt in die Systeme der kritischen Infrastrukturen einzudringen. Neben dem Kriterium des Fernwartungszugangs sind Hersteller von Hard- und Software dann meldepflichtig, wenn ihre Produkte in besonders heiklen Bereichen zum Einsatz kommen. Dies betrifft Hard- und Software zur Steuerung und Überwachung von Systemen (Industrial Control Systems) (Ziff. 1) sowie zum Betrieb von Medizintechnik und Fernmeldeanlagen (Ziff. 2). Der Fokus liegt sodann auch auf Hard- und Software, welche zur Gewährleistung der öffentlichen Sicherheit eingesetzt wird (Ziff. 3). Zu denken ist hier insbesondere an die Kommunikation von Blaulichtorganisationen oder die Systeme für die polizeiliche Ermittlung. Zudem sollen die Hersteller von Hard- und Software mit besonders heiklen Funktionen (IT-Sicherheit, Verschlüsselung, Identifikation, Zugriffs- und Zutrittsberechtigung) (Ziff. 4) der Meldepflicht unterstellt werden, da eine Manipulation solcher Produkte, die gerade beim erhöhtem Schutzbedarf eingesetzt werden, in jedem Fall heikel ist.

Artikel 74c Ausnahmen von der Meldepflicht

Der Adressatenkreis der Meldepflicht nach Art. 74*b* ist breit gefasst und kann auch Unternehmen umfassen, welche für sich alleine betrachtet nicht von essentieller Bedeutung für das Funktionieren der Wirtschaft beziehungsweise das Wohlergehen der Bevölkerung sind, obschon sie in einem kritischen Teilsektor tätig sind. Art. 74*c* legt daher fest, dass der Bundesrat den Adressatenkreis weiter einschränkt. Er verwendet dazu die aufgelisteten Kriterien. Ein Ausschluss von der Meldepflicht wird vorgenommen, wenn ein Unternehmen oder Kategorien von Unternehmen nur eine geringe Risikoexposition gegenüber Cyberangriffen haben, weil ein solcher als unwahrscheinlich beurteilt werden kann oder die Unternehmen in ihrem Betrieb nur in geringem Ausmass von Informatikmittel abhängen (Buchstabe a). Ein Ausschluss kann auch erfolgen, wenn ein Ausfall oder eine Störung

34 SR **747.30**

der Unternehmen nur geringe Auswirkungen auf die Wirtschaft oder das Wohlergehen der Bevölkerung haben. Messbar sind solche Auswirkungen an der Anzahl der betroffenen Personen, der Substituierbarkeit der Dienstleistung oder dem volkswirtschaftlichen Schadenspotential (Buchstabe b).

Artikel 74d Zu meldende Cyberangriffe

Absatz 1

Der Umfang der Meldepflicht, d.h. welche Art von Cyberangriffen zu melden sind, ist auf Gesetzesebene zu verankern. In Absatz 1 enthalten die Buchstaben a bis d die entsprechenden Kriterien, um bei einem Cyberangriff auf ein erhebliches Schadenspotential oder eine hohe Relevanz für den Schutz anderer kritischer Infrastrukturen schliessen zu können. Erfüllt ein Cyberangriff eines der Kriterien, so ist er meldepflichtig. Die Kriterien sind auf Verordnungsebene bei Bedarf weiter zu präzisieren.

Absatz 2

In Absatz 2 wird statuiert, dass bei strafrechtlich relevanten Begleitumstände ein Cyberangriff immer zu melden ist. Viele Cyberkriminelle versuchen über die Androhung oder Durchführung von Angriffen Betreiberinnen kritischer Infrastrukturen oder einzelne Mitarbeitende dieser Unternehmen zu erpressen (Beispielsweise über die Verschlüsselung mittels Ransomware, der Androhung von Angriffen auf die Verfügbarkeit mittels DDoS-Attacken oder der Androhung der Veröffentlichung von kompromittierenden Informationen über Einzelpersonen). Solche Angriffe sind zu melden, damit eingeschätzt werden kann, wie stark die Bedrohung kritischer Infrastrukturen durch Cyberkriminelle ist.

Artikel 74e Inhalt der Meldung

Die wesentlichen Angaben, die für die Erfüllung der Meldepflicht notwendig sind, werden in Absatz 1 gesetzlich verankert. Der konkrete Inhalt der einzelnen Angaben wird in den Ausführungsbestimmungen präzisiert werden.

Absatz 2 präzisiert die Unverzüglichkeit der Meldungserstattung *(«so rasch als möglich»*) gemäss Artikel 74*a* dahingehend, dass sich diese nur auf die bereits bekannten Informationen bezieht. 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 1 verlangten Angaben erst dann zu übermitteln, wenn sie über einen ausreichenden Kenntnisstand dazu verfügen.

Artikel 74f Übermittlung der Meldung

Absatz 1

Damit die Meldepflicht mit möglichst geringem Aufwand erfüllt werden kann, wird das NCSC verpflichtet, ein sicheres elektronisches Meldeformular zur Verfügung zu stellen. Das Meldeformular wird im Gesetzestext angesichts der technologischen Entwicklung generisch mit «System zur Übermittlung der Meldung» umschrieben. 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.

Absatz 2

Das Meldesystem bietet den Meldenden die Möglichkeit, die Meldung des Cyberangriffs oder seiner Auswirkungen (z.B. auf die Datensicherheit oder auf die Funktionsfähigkeit der kritischen Infrastruktur) als Ganzes oder Teile davon an weitere Stellen und Behörden zu übermitteln. Für diese Übermittlung via Meldesystem des NCSC an weitere Stellen und Behörden wird diesen gegenüber keine gesetzliche Meldepflicht vorausgesetzt; sie steht auch für freiwillige Meldungen an Drittstellen offen. Wichtig ist dabei, dass die Übermittlung der Meldung nur von der Betreiberin der betroffenen kritischen Infrastruktur übermittelt werden kann. Sie alleine bestimmt, welche Stelle oder Behörde –

ausser dem NCSC – die Meldung des Cyberangriffes oder seiner Auswirkungen erhalten soll. Das NCSC leitet keine Meldungen an andere Stellen und Behörden weiter. Vorbehalten sind die Ausnahmefälle in Artikel 73*c* Absatz 1 und 2.

Absatz 3

Das NCSC kann das Meldesystem – auf Wunsch und in Zusammenarbeit mit weiteren Meldestellen – so ausgestalten, dass die meldepflichtige Betreiberin einer kritischen Infrastruktur allfällige zusätzliche Angaben erfassen kann, die für die Meldung an das NCSC nicht notwendig sind, um diese an eine oder mehrere weitere Meldestellen zu übermitteln. Diese Funktion soll dazu dienen, den Aufwand der Meldenden möglichst gering zu halten. Sie hilft ihnen, insbesondere bei Zusammentreffen von mehreren Meldepflichten, die entsprechenden Stellen und Behörden möglichst rasch, zeitnah und ohne grossen Aufwand informieren zu können. Diese zusätzlichen Informationen, die die Meldenden für andere Stellen und Behörden im Meldesystem des NCSC erfassen, werden von diesem nur übermittelt, ohne diese zu speichern. Das NCSC selber hat keine Zugriffsmöglichkeit auf diese Informationen.

Artikel 74g Auskunftspflicht

Die Auskunftspflicht ist auf Informationen beschränkt, die benötigt werden, um das Angriffsmuster und die Angriffsmethode eines gemeldeten Cyberangriffs identifizieren (Frühwarnung) und damit Auswirkungen des Cyberangriffs auf andere kritische Infrastrukturen verhindern zu können.

Artikel 74h Verletzung der Melde- oder Auskunftspflicht

Absatz 1

Im Falle einer Verletzung der Melde- oder Auskunftspflicht macht das NCSC in einem ersten Schritt die Betreiberin der kritischen Infrastruktur auf die Pflichtverletzung aufmerksam. Diese hat somit nochmals Gelegenheit, ihren Pflichten nachzukommen. Sollten dazu Missverständnisse vorliegen, dann können diese geklärt werden. Das NCSC ist zu dieser ersten Kontaktaufnahme verpflichtet. Sie ist eine Voraussetzung für den Erlass einer Verfügung nach Absatz 2.

Absatz 2

In einem zweiten Schritt, d.h. wenn die Betreiberin trotz offensichtlicher Pflichtverletzung nichts unternimmt, erlässt das NCSC eine Verfügung mit Bussandrohung. Das NCSC konkretisiert die verletzten Pflichten in der Verfügung soweit, dass für die Betreiberin der kritischen Infrastruktur kein Zweifel besteht, was sie zu tun oder zu lassen hat. Dies erleichtert auch die Arbeit der 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. Artikel 74*i*).

Artikel 74i Widerhandlungen gegen Verfügungen des NCSC

Dieser Artikel übernimmt weitgehend die Regelung, die in Artikel 63 ff. nDSG im Falle der Missachtung von Verfügungen des Beauftragten durch Geschäftsbetriebe vorgesehen wird. Wie in der Botschaft zum revidierten Datenschutzgesetz[35] ausgeführt wurde, gilt auch hier, dass sich diejenige Person strafbar macht, die innerhalb der kritischen Infrastruktur hätte dafür sorgen müssen, dass der Verfügung des NCSC Folge geleistet wird (vgl. Artikel 29 StGB[36]). Die verletzte Pflicht, die dem Unternehmen obliegt, wird der natürlichen Person zugerechnet. Der Verweis auf Artikel 6 des Bundesgesetzes vom 22. März 1974[37] 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 kritischen Infrastrukturen.

35 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl *2017* 6974, 6980, 7103 f.
36 SR **311.0**
37 SR **313.0**

Absatz 1

Die Obergrenze der Busse wurde auf 100'000 Franken angesetzt, um der Bedeutung von kritischen Infrastrukturen für das ordnungsgemässe Funktionieren von Wirtschaft und Staat gebührend Rechnung zu tragen und deren Verantwortung für die Gewährleistung ihrer 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 von 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. Eine Bussandrohung von 100'000 Franken sollte ausreichen, um die Verantwortlichen der kritischen Infrastrukturen zu pflichtkonformem Verhalten zu bewegen.

Absatz 2 und 3

Bei der Bussauferlegung an Geschäftsbetriebe wurde die Regelung des revidierten Datenschutzgesetzes sinngemäss übernommen (Art. 64 nDSG). Bis zu einem Betrag von 20'000 Franken kann die Busse somit direkt der kritischen Infrastruktur 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, um die kritischen Infrastrukturen als solche in die Pflicht zu nehmen und auf weitere Untersuchungen betreffend die Verantwortlichen zu verzichten. 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.

Absatz 4

Aus Transparenzgründen wird in Absatz 4 – analog zu Art. 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 (ISB) 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

Absatz 1

Anstelle der generischen Umschreibung der zuständigen Bundesstellen wurde das NCSC eingefügt und verdeutlicht, dass das NCSC nicht nur Personendaten, sondern im Zusammenhang mit Adressierungselementen auch besonders schützenswerte Personendaten bearbeiten darf. Als Adressierungselement gilt gemäss 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 Buchstabe a der Begriff «Cybersicherheit» eingefügt.

Absatz 2

Die Formulierung in Absatz 2 übernimmt im Wesentlichen den alten Absatz 3, wurde aber von passiv auf aktiv geändert, wodurch deutlicher wird, dass die Datenbearbeitung vom NCSC vorgenommen wird. Zusätzlich wurden die Voraussetzungen konkretisiert, die vorliegen müssen, wenn die betroffene Person über die Datenbearbeitung nicht informiert wird.

Absatz 3

In Absatz 3 wurde inhaltlich präzisiert, dass die vom Missbrauch von Adressierungselementen betroffene Person über diesen Umstand zu informieren ist.

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).

Es wurden auch formelle Anpassungen vorgenommen. So wurde beispielsweise in jedem Absatz präzisiert, dass die Zusammenarbeit unter dem Vorbehalt steht, dass sie zum Schutz von kritischen Infrastrukturen vor Cyberrisiken erforderlich ist.

Absatz 1 und 2

Der in Absatz 1 geregelte Informationsaustausch zwischen dem NCSC und den Betreiberinnen von kritischen Infrastrukturen ist nicht auf die meldepflichtigen kritischen Infrastrukturen beschränkt, sondern richtet sich an alle interessierten kritischen Infrastrukturen mit Sitz in der Schweiz.

Absatz 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.

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 bestimmt insbesondere den Inhalt und Umfang sowie die Art und Weise des Informationsaustausches des NCSC mit dem NDB, den Strafverfolgungsbehörden und den kantonalen Stellen, die für Cybersicherheit zuständig sind (Absätze 2 bis 4). Ein wichtiger Aspekt bei der Zusammenarbeit des NCSC mit diesen Behörden ist der Austausch von Informationen über die Angreifer selber und über deren Methoden und Taktiken.

Absatz 1

Im ersten Absatz dieser Bestimmung wird im Gegensatz zu den nachfolgenden Absätzen nicht der gegenseitige Informationsaustausch geregelt, sondern der Grundsatz statuiert, dass das NCSC dem NDB bei seinen Aufgaben durch spezifische Auswertungen zu Anzahl, Art und Ausmass von Cyberangriffen sowie technischen Analysen von Cyberrisiken 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 Meldepflicht verfügt das NCSC über eine wichtige Informationsquelle zur Bedrohungslage durch Cybervorfälle. Es muss dem NDB deshalb Informationen übermitteln können zur Anzahl, Art und Ausmass der Cyberangriffe. Zudem muss es den NDB mit technischen Analysen zu Angriffen unterstützen und diesem Erkenntnisse aus solchen Analysen weiterleiten können.

Absatz 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 Cybersicherheits-Stellen geregelt. Ein wichtiger Aspekt bei der Zusammenarbeit des NCSC mit diesen Behörden ist, wie bereits erwähnt, der Austausch von Informationen über die Angreifer selber und über deren Methoden und Taktiken. 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 für die ein Personenbezug hergestellt werden kann. Für den Informationsaustausch in Bezug auf diese Personendaten wird hier eine Rechtsgrundlage geschaffen. Konkret handelt sich um Adressierungselemente (wie Domainname, IP-Adresse, missbräuchlich verwendete Mailadressen) oder Angaben zu Finanztransaktionen (Bankkonten, IBAN-Nummer usw.).

Die berechtigten Behörden nach Absatz 2 bis 4 können auf die genannten Informationen auch im Abrufverfahren zugreifen. Dieses Vorgehen ist aufgrund der grossen Anzahl von Cyberangriffen und damit verbundenen technischen Informationen angezeigt. Eine Weiterleitung von Meldungen an den NDB oder die Strafverfolgungsbehörden mit Informationen zu den Betroffenen erfolgt nur in Ausnahmefällen und bleibt an die Bedingungen nach Artikel 73*c* Absatz 1 und 2 gebunden.

Artikel 77 Internationale Zusammenarbeit

Diese Bestimmung wurde formell angepasst, indem das NCSC namentlich eingefügt wurde. Ferner wurde der Begriff «Daten» durch den Oberbegriff «Informationen» ersetzt, wo nicht spezifisch Personendaten gemäss Artikel 75 gemeint sind. Zum Umfang, Inhalt und Zweck des Informationsaustausches wurde konkretisierend eingefügt, dass er mit Stellen zulässig ist, die für die Cybersicherheit zuständig sind. Damit wurde die Formulierung «für den Schutz kritischer Infrastrukturen» durch «Cybersicherheit» ersetzt, da die erste Formulierung zu eng ist für die international bedeutenden Organisationen, die im Bereich Cybersicherheit tätig sind.

Artikel 78 Informationssystem zur Unterstützung von kritischen Infrastrukturen

Dieser Artikel wurde in Anwendung der geänderten Rechtsgrundlagen durch die Revision des DSG gestrichen. 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

Dieser Artikel wurde nur in Bezug auf Absatz 1 leicht angepasst. Es wurde präzisiert, dass Personendaten höchstens fünf Jahre ab der letzten Verwendung aufbewahrt werden können. Der Hintergrund für diese Regelung ist, dass gewisse technische Informationen zu Cybervorfällen, wie z.B. Domainname, 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, die eine Grundvoraussetzung für seine Aufgabenerfüllung sind. Da diese technischen Daten aber auch personenbezogene Elemente enthalten und damit als Personendaten dem Datenschutz unterstehen, muss die Aufbewahrungsdauer klar eingegrenzt werden. Aus Gründen des Datenschutzes wurde im zweiten Teil des Satzes präzisiert, dass besonders schützenswerte Personendaten höchstens zwei Jahre ab der letzten Verwendung aufbewahrt werden.

Artikel 80 Bestimmungen des Bundesrats

Dieser Artikel wurde gestrichen. Durch die erfolgten Konkretisierungen im Gesetzestext werden die in diesem Abschnitt vorgesehenen Delegationen an den Bundesrat obsolet. Die Kompetenz, Ausführungsbestimmungen zu erlassen, kommt dem Bundesrat auch ohne Gesetzesvorbehalt zu. Ferner sind die in Buchstabe c (Verantwortung für den Datenschutz und Datensicherheit) vorgesehenen Ausführungsbestimmungen bereits durch die Artikel 33 und 8 Absatz 3 nDSG abgedeckt.

Anhang 1 (Artikel 89 Änderung anderer Erlasse)

Die Auflistung der Änderungen anderer Erlasse gemäss Artikel 89 in Anhang 1 wird wie folgt ergänzt.

Bundesgesetz vom 23. März 2007 über die Stromversorgung[38]

Der Schutz vor Cyberrisiken, der neu in Artikel 8a 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, Leistung, Anzahl betroffener Endverbraucher).

Der Bundesrat wird auf Verordnungsebene entsprechende Vorgaben, insbesondere zum Schutzniveau und der Auditierung festlegen. Dabei kann er sich an einschlägigen Fachnormen orientieren (bspw. am Handbuch des VSE Grundschutz für «Operational Technology» in der Stromversorgung, Ausgabe Juli 2018, zurzeit in Überarbeitung), welche er auch für verbindlich erklären kann. Für kleinere Akteure sind entsprechende Ausnahmen oder Erleichterungen vorzusehen.

Als weitere Beteiligte im Sinne von Absatz 2 kommen mit Blick auf den Zweck der Bestimmung lediglich Akteure in Frage, die einen massgebenden Einfluss auf die Versorgungssicherheit ausüben, namentlich entsprechend grosse Dienstleister im Elektrizitätssektor, beispielsweise in den Bereichen Handel, Messung, Steuerung, Flexibilität, Datenbearbeitung oder Elektromobilität.

Änderung des Datenschutzgesetzes vom 25. September 2020[39]

Damit der EDÖB bei der Analyse einer eingetretenen Verletzung der Datensicherheit, die der Verantwortliche ihm gestützt auf Artikel 24 nDSG und Artikel 19 E-VDSG 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 E-VDSG 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 revDSG umgangen wird, wonach die Meldung nur mit Einverständnis der meldepflichtigen Person im Rahmen eines Strafverfahrens verwendet werden darf. 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, wo das technische Fachwissen des NCSC für die Abklärung eines Vorfalls erforderlich ist, Gebrauch machen.

38 SR **734.7**
39 Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) vom 25. September 2020, BBl *2020* 7639.

5 Auswirkungen

5.1 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.

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.

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.

Dieser Mehrbedarf ist bei den laufenden Arbeiten zum Ausbau des NCSC zu berücksichtigen. Er kann nicht vollständig losgelöst von den anderen Aufgaben des NCSC hinreichend abgeschätzt werden, weshalb das Ergebnis der aktuell noch laufenden Wirksamkeitsüberprüfung der Cyberorganisation des Bundes abgewartet wird. Der Ressourcenbedarf wird in Kenntnis des Ergebnisses dieser Vernehmlassung für die Botschaft der Änderung des ISG konkretisiert.

5.2 Auswirkungen auf Kantone und Gemeinden

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 74b 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 Cyberrisiken schützen zu können. Bereits zum heutigen Zeitpunkt sind zahlreiche Kantone und Städte in den Informationsaustausch zwischen kritischen Infrastrukturen und dem NCSC integriert.

5.3 Auswirkungen auf die Volkswirtschaft und die Gesellschaft

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 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 (RFA) verzichtet werden.

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

6 Rechtliche Aspekte

6.1 Verfassungsmässigkeit

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

Die kritischen Infrastrukturen haben eine hohe Sicherheitsrelevanz für Gesellschaft, Wirtschaft und Staat. Die potenziell schwerwiegenden und landesweiten Auswirkungen von Cyberangriffen auf kritische Infrastrukturen gefährden die Wohlfahrt des Landes und stellen eine Bedrohung für die innere und äussere Sicherheit dar. Die Einführung einer Meldepflicht dient mithin zur Wahrung der wirtschaftlichen, gesellschaftlichen und staatlichen Stabilität. Sie bildet die Grundlage dafür, dass die Ereignisbewältigung koordiniert und rasch eingeleitet werden kann. Die Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen hat ferner zum Ziel, anhand der Meldungen eine Analyse der Bedrohungslage zwecks Frühwarnung und Gefahrenabwehr zu erstellen. Aus dem Zweck der Meldepflicht ergibt sich, dass sie in ihrem Umfang auf Cyberangriffe auf kritische Infrastrukturen beschränkt werden soll. Das Melderecht bei Cybervorfällen und Schwachstellen, das jedermann 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[40] Artikel 173 Absatz 2 BV zitiert. Das Informationssicherheitsgesetz erwähnt in seinem Ingress – neben Artikel 54 Absatz 1, 60 Absatz 1, 101, 102 Absatz 1 und 173 Absatz 1 Buchstaben a und b – auch Artikel 173 Absatz 2 als massgebende Kompetenzgrundlage. Es besteht somit kein Bedarf für die Ergänzung von Verfassungsbestimmungen im Ingress des ISG.

6.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz

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.

6.3 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 formellgesetzliche 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 die bestehende Cyberrisikenverordnung ergänzt soll.

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

6.4 Unterstellung unter die Ausgabenbremse

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

6.5 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.

6.6 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 Art. 74c 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.

6.7 Datenschutz

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.

Bei der Erarbeitung der Vernehmlassungsvorlage wurde der EDÖB konsultiert. Es wurden dabei auch Koordinationsmöglichkeiten mit der Meldepflicht bei Verletzung der Datensicherheit diskutiert.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

BBl 2020
www.bundesrecht.admin.ch
Massgebend ist die signierte elektronische Fassung

Bundesgesetz über die Informationssicherheit beim Bund

(Informationssicherheitsgesetz, ISG)

Änderung vom ...

Die Bundesversammlung der Schweizerischen Eidgenossenschaft,
nach Einsicht in die Botschaft des Bundesrates vom ...,
beschliesst:

I

Das Informationssicherheitsgesetz vom 18. Dezember 2020[1] wird wie folgt geändert:

Art. 1 Abs. 1

[1] Dieses Gesetz soll:

a. die sichere Bearbeitung der Informationen, für die der Bund zuständig ist, sowie den sicheren Einsatz der Informatikmittel des Bundes gewährleisten;

b. die Widerstandsfähigkeit der Schweiz gegenüber Cyberrisiken erhöhen.

Art. 2 Abs. 5

[5] Für Organisationen des öffentlichen und privaten Rechts, die kritische Infrastrukturen betreiben, die aber nicht unter die Absätze 1–3 fallen, gelten die Artikel 73*a*–79. Die Spezialgesetzgebung kann weitere Teile dieses Gesetzes für anwendbar erklären.

SR **126**
[1] SR **126** [BBl **2020** 9975]

Art. 5 Bst. d–e

In diesem Gesetz bedeuten:

d. *Cybervorfall:* Ereignis beim Betrieb von Informatikmitteln, das dazu führen kann, dass die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist;

e. *Cyberangriff:* Cybervorfall, der von Unbefugten absichtlich ausgelöst wurde.

Gliederungstitel vor Art. 73a

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

1. Abschnitt: Allgemeine Bestimmungen

Art. 73a Grundsatz

Zum Schutz der Schweiz vor Cyberrisiken nimmt das nationale Zentrum für Cybersicherheit (NCSC) insbesondere folgende Aufgaben wahr:

a. Sensibilisierung der Öffentlichkeit auf Cyberrisiken;

b. Warnung vor Cyberrisiken und Schwachstellen von Informatikmitteln;

c. Veröffentlichung von Informationen zur Cybersicherheit sowie von Anleitungen für präventive und reaktive Massnahmen gegen Cyberrisiken;

d. technische Analysen zur Bewertung und Abwehr von Cyberrisiken;

e. Entgegennahme und Bearbeitung von Meldungen zu Cybervorfällen und Schwachstellen von Informatikmitteln;

f. Unterstützung von Betreiberinnen von kritischen Infrastrukturen.

Art. 73b Bearbeitung von Meldungen zu Cybervorfällen und Schwachstellen

[1] Werden dem NCSC Cybervorfälle oder Schwachstellen von Informatikmitteln gemeldet, so analysiert es diese auf ihre Bedeutung für den Schutz der Schweiz vor Cyberrisiken. Es gibt auf Wunsch der meldenden Person eine Empfehlung zum weiteren Vorgehen ab, sofern dafür keine weiteren Analysen und Abklärungen erforderlich sind.

[2] Das NCSC kann Informationen zu Cybervorfällen veröffentlichen oder an interessierte Behörden und Organisationen weiterleiten, sofern dies dazu dient, Cyberangriffe zu verhindern oder zu bekämpfen. Diese Informationen dürfen Personendaten und Daten juristischer Personen enthalten, sofern es sich um missbräuchlich verwendete Identifikationsmerkmale und Adressierungselemente handelt und die betroffene Person einwilligt.

[3] Werden dem NCSC Schwachstellen gemeldet, so informiert es umgehend den Hersteller und setzt ihm zur Behebung der Schwachstelle eine angemessene Frist. Behebt der Hersteller die Schwachstelle nicht innert dieser Frist, so veröffentlicht das NCSC die Schwachstelle unter Angabe der betroffenen Soft- oder Hardware, sofern dies zum Schutz vor Cyberrisiken beiträgt.

Art. 73c Weiterleitung von Informationen

[1] Ergeben sich aus der Meldung eines Cybervorfalls oder dessen Analyse Informationen, die für das frühzeitige Erkennen und Verhindern von Bedrohungen der inneren oder äusseren Sicherheit, für die Beurteilung der Bedrohungslage oder für die nachrichtendienstliche Frühwarnung zum Schutz von kritischen Infrastrukturen nach Artikel 6 Absätze 1 Buchstabe a, 2 und 5 des Nachrichtendienstgesetzes vom 25. September 2015[2] (NDG) relevant sind, so leitet das NCSC diese Informationen an den NDB weiter.

[2] Für Mitarbeitende des NCSC entfällt die Anzeigepflicht gemäss Artikel 22*a* des Bundespersonalgesetzes vom 24. März 2000[3], wenn sie im Zusammenhang mit der Meldung eines Cybervorfalls oder dessen Analyse Hinweise auf eine mögliche Straftat erhalten. Die Leiterin oder der Leiter des NCSC kann Anzeige erstatten, sofern dies aufgrund der Schwere der möglichen Straftat geboten scheint.

[3] Informationen, die von einer Person im Rahmen einer Meldung dem NCSC bekanntgegeben wurden, dürfen in einem Strafverfahren gegen diese Person nur mit deren Einverständnis verwendet werden.

[4] Informationen, die strafrechtlich geschützte Geheimnisse offenbaren, darf das NCSC nur nach den Vorgaben von Artikel 320 StGB[4] weiterleiten.

Art. 74 Unterstützung von Betreiberinnen von kritischen Infrastrukturen

[1] Das NCSC unterstützt die Betreiberinnen von kritischen Infrastrukturen beim Schutz vor Cyberrisiken.

[2] Es stellt ihnen dazu insbesondere folgende Hilfsmittel zur Verfügung:

a. ein Kommunikationssystem für den sicheren Informationsaustausch;

b. technische Informationen zu aktuellen Cyberrisiken und Schwachstellen sowie Empfehlungen für präventive Massnahmen;

c. technische Instrumente und Anleitungen zur Erkennung von Cybervorfällen, die auf den erhöhten Schutzbedarf von kritischen Infrastrukturen ausgerichtet sind.

[3] Es berät und unterstützt sie bei der Bewältigung von Cybervorfällen und der Behebung von Schwachstellen, wenn für die kritische Infrastruktur ein unmittelbares Risiko von gravierenden Auswirkungen besteht und, sofern es sich um private

2 SR **121**
3 SR **172.220.1**
4 SR **311.0**

Betreiberinnen handelt, die Beschaffung gleichwertiger Unterstützung auf dem Markt nicht rechtzeitig möglich ist.

[4] Es kann zur Analyse eines Cybervorfalls mit dem Einverständnis der betroffenen Betreiberin auf deren Informationen und Informatikmittel zugreifen. Das Einverständnis kann unabhängig von allfälligen Geheimhaltungspflichten gewährt werden.

Gliederungstitel vor Art. 74a

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

Art. 74a Meldepflicht

Die Betreiberinnen von kritischen Infrastrukturen müssen dem NCSC Cyberangriffe nach deren Entdeckung so rasch als möglich melden, damit das NCSC Angriffsmuster frühzeitig erkennen, mögliche Betroffene warnen und ihnen geeignete Präventions- und Abwehrmassnahmen empfehlen kann.

Art. 74b Bereiche

Die Meldepflicht gilt für:

a. Hochschulen nach Artikel 2 Absatz 2 des Hochschulförderungs- und -koordinationsgesetzes vom 30. September 2011[5];

b. Bundes-, Kantons- oder Gemeindebehörden sowie interkantonale, kantonale und interkommunale Organisationen;

c. Organisationen mit öffentlich-rechtlichen Aufgaben in den Bereichen Sicherheit und Rettung, Trinkwasserversorgung, Abwasseraufbereitung und Abfallentsorgung;

d. Unternehmen, die in den Bereichen Energieversorgung nach Artikel 6 Absatz 1 des Energiegesetzes vom 30. September 2016[6], Energiehandel, -messung oder -steuerung tätig sind;

e. Unternehmen, die dem Bankengesetz vom 8. November 1934[7], dem Versicherungsaufsichtsgesetz vom 17. Dezember 2004[8] oder dem Finanzmarktinfrastrukturgesetz vom 19. Juni 2015[9] unterstehen;

f. Anbieterinnen von Online-Marktplätzen, Cloudcomputing, Suchmaschinen und weiteren digitalen Diensten sowie Registrare von Domain-Namen und Betreiberinnen von Rechenzentren, die in der Schweiz:

    1. von einer grossen Zahl von Nutzenden beansprucht werden,

    2. eine hohe Bedeutung für die digitale Wirtschaft haben, oder

5 SR **414.20**
6 SR **730.0**
7 SR **952.0**
8 SR **961.01**
9 SR **958.1**

3. Sicherheits- und Vertrauensdienste anbieten;

g. Spitäler, die auf der kantonalen Spitalliste nach Artikel 39 Absatz 1 Buchstabe e des Bundesgesetzes vom 18. März 1994[10] über die Krankenversicherung aufgeführt sind;

h. medizinische Laboratorien mit einer Bewilligung nach Artikel 16 Absatz 1 des Epidemiengesetzes vom 28. September 2012[11];

i. Unternehmen, die für die Herstellung, das Inverkehrbringen und die Einfuhr von Arzneimitteln eine Bewilligung nach dem Heilmittelgesetz vom 15. Dezember 2000[12] (HMG) haben oder Medizinprodukte nach Artikel 4 Absatz 1 Buchstabe b HMG herstellen oder vertreiben;

j. Organisationen, die Leistungen der Sozialversicherungen zur Absicherung der Folgen von Krankheit, Unfall, Arbeits- und Erwerbsunfähigkeit, Alter, Invalidität und Hilflosigkeit erbringen;

k. Anbieterinnen von Fernmeldediensten nach Artikel 3 Buchstabe b FMG;

l. die Schweizerische Radio- und Fernsehgesellschaft;

m. Nachrichtenagenturen von nationaler Bedeutung;

n. Anbieterinnen von Postdiensten, die bei der Postkommission nach Artikel 4 Abs. 1 des Postgesetzes vom 17. Dezember 2010[13] registriert sind;

o. Transportunternehmen, die dem Bundesgesetz vom 18. Juni 2010[14] über die Sicherheitsorgane der Transportunternehmen im öffentlichen Verkehr unterstehen;

p. Unternehmen der Zivilluftfahrt, die über eine Bewilligung des Bundesamtes für Zivilluftfahrt verfügen;

q. Unternehmen, die nach dem Seeschifffahrtsgesetz vom 23. September 1953[15] Güter auf dem Rhein befördern sowie Unternehmen, die die Registrierung, Ladung oder Löschung im Hafen Basel betreiben;

r. Unternehmen, die die Bevölkerung mit unentbehrlichen Gütern des täglichen Bedarfs versorgen;

s. Hersteller von Hard- und Software, deren Produkte von kritischen Infrastrukturen genutzt werden, sofern die Hard- oder Software einen Fernwartungszugang hat oder zu einem der folgenden Zwecken eingesetzt wird:

1. Steuerungstechnik und Überwachung von Systemen,

2. Betrieb von Medizinprodukten und Fernmeldeanlagen,

3. Gewährleistung der öffentlichen Sicherheit,

10 SR **832.10**
11 SR **818.101**
12 SR **812.21**
13 SR **783.0**
14 SR **745.2**
15 SR **747.30**

4. IT-Sicherheit, Verschlüsselung, Identifikation, Zugriffs- und Zutrittsberechtigung.

Art. 74c Ausnahmen von der Meldepflicht

Der Bundesrat nimmt bestimmte Kategorien von Betreiberinnen von kritischen Infrastrukturen von der Meldepflicht aus, wenn durch Cyberangriffe auf ihre Infrastrukturen ausgelöste Funktionsausfälle oder Fehlfunktionen:

a. unwahrscheinlich sind, insbesondere wegen einer geringen Abhängigkeit von Informatikmitteln; oder

b. nur geringe Auswirkungen auf das Funktionieren der Wirtschaft beziehungsweise das Wohlergehen der Bevölkerung haben, insbesondere, weil sie:

   1. nur eine geringe Anzahl Personen betreffen,
   2. von anderen kritischen Infrastrukturen aufgefangen werden, oder
   3. nur ein geringes volkswirtschaftliches Schadenspotenzial haben.

Art. 74d Zu meldende Cyberangriffe

[1] Ein Cyberangriff auf eine kritische Infrastruktur muss gemeldet werden, wenn Anzeichen dafür bestehen, dass:

a. die Funktionsfähigkeit der betroffenen kritischen Infrastruktur oder einer anderen kritischen Infrastruktur gefährdet ist;

b. ein fremder Staat ihn ausgeführt oder veranlasst hat;

c. er zu einem Abfluss oder zur Manipulation von Informationen geführt hat oder führen könnte; oder

d. er länger als 30 Tage unentdeckt blieb.

[2] Ein Cyberangriff auf eine kritische Infrastruktur muss immer gemeldet werden, wenn er mit Erpressung, Drohung oder Nötigung gegenüber der Betreiberin einer kritischen Infrastruktur oder ihren Mitarbeitenden verbunden ist.

Art. 74e Inhalt der Meldung

[1] Die Meldung muss Informationen zur kritischen Infrastruktur, zur Art und Ausführung des Cyberangriffs, zu seinen Auswirkungen und zum geplanten weiteren Vorgehen der Betreiberin der kritischen Infrastruktur enthalten.

[2] Sind zum Zeitpunkt der Meldung nicht alle erforderlichen Informationen bekannt, so ergänzt die Betreiberin der kritischen Infrastruktur die Meldung, sobald sie an neue Informationen gelangt.

Art. 74f Übermittlung der Meldung

[1] Für die elektronische Meldung von Cyberangriffen stellt das NCSC ein sicheres System zur Übermittlung der Meldung an das NCSC zur Verfügung.

[2] Das System muss der Betreiberin einer kritischen Infrastruktur ermöglichen, die Meldung des Cyberangriffs oder seiner Auswirkungen gesamthaft oder in Teilen an weitere Stellen und Behörden zu übermitteln.

[3] Benötigt eine Stelle oder Behörde Informationen, die über Art. 74e hinausgehen, kann die Betreiberin diese über das System direkt an die betreffende Stelle oder Behörde übermitteln.

Art. 74g Auskunftspflicht

Die Betreiberin der kritischen Infrastruktur muss dem NCSC ergänzende Auskünfte zu den Inhalten der Meldung nach Artikel 74*e* erteilen, die es zur Erfüllung seiner Aufgaben in Bezug auf die Abwehr weiterer Cyberangriffe auf kritische Infrastrukturen benötigt.

Art. 74h Verletzung der Melde- oder Auskunftspflicht

[1] Bestehen Anzeichen für eine Verletzung der Melde- oder Auskunftspflicht, so informiert das NCSC die Betreiberin der kritischen Infrastruktur darüber.

[2] Kommt die Betreiberin trotz dieser Information ihrer Pflicht nicht nach, so erlässt das NCSC eine Verfügung über die umzusetzenden Pflichten, setzt ihr darin eine Frist und verweist auf die Bussandrohung nach Artikel 74*i*.

Art. 74i Widerhandlungen gegen Verfügungen des NCSC

[1] Mit Busse bis zu 100 000 Franken wird bestraft, wer einer vom NCSC unter Hinweis auf die Strafdrohung dieses Artikels erlassenen rechtskräftigen Verfügung oder dem Entscheid einer Rechtsmittelinstanz vorsätzlich nicht Folge leistet.

[2] Bei Widerhandlungen in Geschäftsbetrieben ist Artikel 6 des Bundesgesetzes vom 22. März 1974[16] über das Verwaltungsstrafrecht (VStrR) anwendbar.

[3] Fällt eine Busse von höchstens 20 000 Franken in Betracht und würde die Ermittlung der nach Artikel 6 VStrR strafbaren Personen Untersuchungsmassnahmen bedingen, die im Hinblick auf die verwirkte Strafe unverhältnismässig wären, so kann die Behörde von einer Verfolgung dieser Personen absehen und an ihrer Stelle den Geschäftsbetrieb zur Bezahlung der Busse verurteilen.

[4] Bei einer Widerhandlung gegen eine Verfügung des NCSC obliegt die Verfolgung und die Beurteilung den Kantonen.

16 SR **313.0**

Gliederungstitel vor Art. 75

3. Abschnitt: Datenschutz und Informationsaustausch

Art. 75 Bearbeitung von Personendaten

[1] Das NCSC kann zur Erfüllung seiner Aufgaben Personendaten bearbeiten, einschliesslich Adressierungselementen nach Artikel 3 Buchstabe f FMG[17] und damit zusammenhängenden besonders schützenswerte Personendaten, die Informationen enthalten über:

a. religiöse, weltanschauliche oder politische Ansichten enthalten; die Bearbeitung ist nur zulässig, wenn sie für die Bewertung von konkreten Bedrohungen und Gefahren im Bereich der Cybersicherheit erforderlich ist;

b. administrative oder strafrechtliche Verfolgungen und Sanktionen enthalten.

[2] Es kann die Personendaten bearbeiten, ohne dass dies für die betroffenen Personen erkennbar ist, falls sonst der Zweck der Bearbeitung gefährdet wäre oder die Information der betroffenen Person nur mit unverhältnismässigem Aufwand erreicht werden könnte.

[3] Liegen konkrete Hinweise auf den Missbrauch einer Identität oder auf die unberechtigte Verwendung von Adressierungselementen vor, so informiert es die Personen, deren Identität oder Adressierungselemente missbraucht werden; vorbehalten bleiben die Artikel 18*a* Absatz 4 Buchstabe b und 18*b* DSG[18].

Art. 76 Zusammenarbeit im Inland

[1] Das NCSC kann den Betreiberinnen von kritischen Infrastrukturen Personendaten bekanntgeben, sofern dies zum Schutz von kritischen Infrastrukturen vor Cyberrisiken erforderlich ist.

[2] Die Betreiberinnen von kritischen Infrastrukturen können dem NCSC Personendaten bekanntgeben, sofern dies zum Schutz von kritischen Infrastrukturen vor Cyberrisiken erforderlich ist.

[3] Das NCSC kann den Fernmeldedienstanbieterinnen Adressierungselemente und damit zusammenhängende Personendaten bekanntgeben, sofern dies zum Schutz von kritischen Infrastrukturen vor Cyberrisiken erforderlich ist.

[4] Die Fernmeldedienstanbieterinnen können dem NCSC Adressierungselemente und damit zusammenhängende Personendaten bekanntgeben, sofern dies zum Schutz von kritischen Infrastrukturen vor Cyberrisiken erforderlich ist.

Art. 76a Unterstützung für Behörden

[1] Das NCSC unterstützt den NDB beim frühzeitigen Erkennen und Verhindern von Bedrohungen der inneren oder äusseren Sicherheit, bei der Beurteilung der Bedrohungslage und bei der nachrichtendienstlichen Frühwarnung zum Schutz von kriti-

17 SR **784.10**
18 SR **235.1**

schen Infrastrukturen nach Artikel 6 Absätze 1 Buchstabe a, 2 und 5 NDG[19] mit Auswertungen zu Anzahl, Art und Ausmass von Cyberangriffen sowie technischen Analysen von Cyberrisiken.

[2] Es gewährt dem NDB Zugriff auf Informationen im Abrufverfahren, die Aufschluss über die Identität und die Vorgehensweise der Verursacherinnen und Verursacher von Cyberangriffen geben.

[3] Es gewährt den Strafverfolgungsbehörden Zugriff auf Informationen im Abrufverfahren, die Aufschluss über die Identität und die Vorgehensweise der Verursacherinnen und Verursacher von Cyberangriffen geben.

[4] Es kann den kantonalen Stellen, die für die Cybersicherheit zuständig sind, Zugriff auf Informationen im Abrufverfahren gewähren, die für den Schutz kantonaler Behörden und kantonaler kritischer Infrastrukturen vor Cyberrisiken erforderlich sind.

Art. 77 Internationale Zusammenarbeit

[1] Das NCSC kann mit ausländischen und internationalen Stellen, die für die Cybersicherheit zuständig sind, Informationen austauschen, wenn sie diese zur Erfüllung von Aufgaben benötigen, die denjenigen des NCSC entsprechen. Umfasst der Informationsaustausch auch Personendaten nach Artikel 75, ist Artikel 6 DSG[20] zu beachten.

[2] Der Informationsaustausch nach Absatz 1 ist nur dann zulässig, wenn die ausländischen und internationalen Stellen die bestimmungsgemässe Verwendung gewährleisten.

[3] Werden die Informationen für ein rechtliches Verfahren im Ausland benötigt, so gelten die Bestimmungen über die Amts- und Rechtshilfe.

Art. 78
Aufgehoben

Art. 79 Abs. 1

[1] Das NCSC bewahrt Personendaten nur so lange auf, wie dies zur Abwehr von Gefahren oder zur Erkennung von Vorfällen zweckmässig ist, höchstens jedoch fünf Jahre ab der letzten Verwendung; bei besonders schützenswerten Personendaten beträgt die Frist zwei Jahre.

Art. 80
Aufgehoben

19 SR **121**
20 SR **235.1**

II

Die nachstehenden Erlasse werden wie folgt geändert:

1. Stromversorgungsgesetz vom 23. März 2007[21]

Art. 8a Schutz vor Cyberrisiken

[1] Die Netzbetreiber, die Erzeuger und die Speicherbetreiber treffen Massnahmen für einen angemessenen Schutz ihrer Anlagen vor Cyberrisiken.

[2] Der Bundesrat kann diese Pflicht auf weitere Beteiligte ausdehnen.

2. Datenschutzgesetz vom 25. September 2020[22]

Art. 24 Abs. 5bis

[5bis] Der EDÖB kann die Meldung mit dem Einverständnis des meldepflichtigen Verantwortlichen zur Analyse des Vorfalls an das Nationale Zentrum für Cybersicherheit weiterleiten. Die Mitteilung kann Personendaten enthalten, einschliesslich besonders schützenswerter Personendaten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen betreffend den meldepflichtigen Verantwortlichen.

III

[1] Dieses Gesetz untersteht dem fakultativen Referendum.

[2] Der Bundesrat bestimmt das Inkrafttreten.

21 SR **734.7**
22 SR **235.1,** BBl 2020 7639

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Vorsteher des Eidgenössischen Finanzdepartements EFD

Bern, 12. Januar 2022

Adressaten:
die politischen Parteien
die Dachverbände der Gemeinden, Städte und Berggebiete
die Dachverbände der Wirtschaft
die interessierten Kreise

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe: Eröffnung des Vernehmlassungsverfahrens

Sehr geehrte Damen und Herren

Der Bundesrat hat am 12. Januar 2022 das EFD beauftragt, bei den Kantonen, den politischen Parteien, den gesamtschweizerischen Dachverbänden der Gemeinden, Städte und Berggebiete, den gesamtschweizerischen Dachverbänden der Wirtschaft und den interessierten Kreisen zur Einführung einer Meldepflicht für Cyberangriffe und der damit verbundenen Änderung des Informationssicherheitsgesetzes (ISG) ein Vernehmlassungsverfahren durchzuführen.

Die Vernehmlassung dauert bis am **14. April 2022**.

Cyberrisiken sind zu einer der wichtigsten Bedrohungen der Sicherheit und der Wirtschaft der Schweiz geworden. Es ist von grosser Bedeutung, dass Angriffe auf Schweizer Unternehmen und Behörden frühzeitig erkannt und die Bedrohungslage möglichst genau eingeschätzt werden kann. Dazu soll mit der Ihnen unterbreiteten Vorlage eine Meldepflicht für Betreiberinnen kritischer Infrastrukturen eingeführt werden. Die Meldepflicht soll es dem Nationalen Zentrum für Cybersicherheit (NCSC) ermöglichen, eine verbesserte Übersicht über Cyberangriffe in der Schweiz zu gewinnen, Betroffene bei der Bewältigung von Cyberangriffen zu unterstützen und alle anderen Betreiberinnen kritischer Infrastrukturen zu warnen. Mit der Einführung einer Meldepflicht schliesst die Schweiz eine Lücke im Dispositiv der Cybersicherheit. Meldepflichten für Cyberangriffe sind in vielen Ländern bereits etabliert und gelten seit 2018 in allen EU-Mitgliedstaaten.
Die Vorlage ist auf die bestehenden Meldepflichten (insbesondere der neu eingeführten datenschutzrechtlichen Meldepflicht) abgestimmt und so ausgestaltet, dass sie für die betroffenen Unternehmen und Behörden einen möglichst geringen Mehraufwand bedeutet. Die Schaffung einer zentralen Meldestelle auf Bundesebene (NCSC) ist dabei unumgänglich, da nur eine zentrale Stelle sicherstellen kann, dass die Meldepflicht die Zwecke der Frühwarnung und der besseren Übersicht über die Bedrohungslage erfüllt. Die Vorlage schafft auch die Grundlage für eine Zusammenarbeit des NCSC mit anderen Stellen, insbesondere mit den Strafvollzugsbehörden.

Wir laden Sie ein, zu den Ausführungen im erläuternden Bericht und insbesondere zur Umsetzung der vorgeschlagenen Regelungen Stellung zu nehmen.

Das Vernehmlassungsverfahren wird elektronisch durchgeführt. Die Vernehmlassungsunterlagen können bezogen werden über die Internetadresse:

https://www.fedlex.admin.ch/de/consultation-procedures/ongoing

Wir sind bestrebt, die Dokumente im Sinne des Behindertengleichstellungsgesetzes (BehiG; SR 151.3) barrierefrei zu publizieren. Wir ersuchen Sie daher, Ihre Stellungnahmen, wenn möglich, elektronisch (**bitte nebst einer PDF-Version auch eine Word-Version**) innert der Vernehmlassungsfrist an folgende Email-Adresse zu senden:

ncsc@gs-efd.admin.ch

Wir bitten Sie, im Hinblick auf allfällige Rückfragen die bei Ihnen zuständigen Kontaktpersonen und deren Koordinaten anzugeben.

Für Rückfragen und allfällige Informationen stehen Ihnen Herr Manuel Suter, Geschäftsstelle NCSC (Tel. 058 461 43 20) und Frau Angelika Spiess, Rechtsdienst GS-EFD (Tel. 058 467 68 03) zur Verfügung.

Freundliche Grüsse

Ueli Maurer

Liste der Vernehmlassungsadressaten
Liste des destinataires consultés
Elenco dei destinatari della consultazione

Art. 4 Abs. 3 Vernehmlassungsgesetz (SR 172.061)

1. Kantone / Cantons / Cantoni

Staatskanzlei des Kantons Zürich	Neumühlequai 10 Postfach 8090 Zürich
Staatskanzlei des Kantons Bern	Postgasse 68 3000 Bern 8
Staatskanzlei des Kantons Luzern	Bahnhofstrasse 15 6002 Luzern
Standeskanzlei des Kantons Uri	Rathausplatz 1 6460 Altdorf
Staatskanzlei des Kantons Schwyz	Regierungsgebäude Bahnhofstrasse 9 Postfach 1260 6431 Schwyz
Staatskanzlei des Kantons Obwalden	Rathaus 6061 Sarnen
Staatskanzlei des Kantons Nidwalden	Dorfplatz 2 Postfach 1246 6371 Stans
Staatskanzlei des Kantons Glarus	Rathaus 8750 Glarus
Staatskanzlei des Kantons Zug	Seestrasse 2 Regierungsgebäude am Postplatz 6300 Zug
Chancellerie d'Etat du Canton de Fribourg	Rue des Chanoines 17 1701 Fribourg
Staatskanzlei des Kantons Solothurn	Rathaus Barfüssergasse 24 4509 Solothurn
Staatskanzlei des Kantons Basel-Stadt	Marktplatz 9 4001 Basel
Landeskanzlei des Kantons Basel-Landschaft	Regierungsgebäude Rathausstrasse 2 4410 Liestal

Staatskanzlei des Kantons Schaffhausen	Beckenstube 7 8200 Schaffhausen
Kantonskanzlei des Kantons Appenzell Ausserrhoden	Regierungsgebäude 9102 Herisau
Ratskanzlei des Kantons Appenzell Innerrhoden	Marktgasse 2 9050 Appenzell
Staatskanzlei des Kantons St. Gallen	Regierungsgebäude 9001 St. Gallen
Standeskanzlei des Kantons Graubünden	Reichsgasse 35 7001 Chur
Staatskanzlei des Kantons Aargau	Regierungsgebäude 5001 Aarau
Staatskanzlei des Kantons Thurgau	Regierungsgebäude Zürcherstrasse 188 8510 Frauenfeld
Cancelleria dello Stato del Cantone Ticino	Piazza Governo 6 6501 Bellinzona
Chancellerie d'Etat du Canton de Vaud	Place du Château 4 1014 Lausanne
Chancellerie d'Etat du Canton du Valais	Planta 3 1950 Sion
Chancellerie d'Etat du Canton de Neuchâtel	Le Château Rue de la Collégiale 12 2000 Neuchâtel
Chancellerie d'Etat du Canton de Genève	Rue de l'Hôtel-de-Ville 2 Case postale 3964 1211 Genève 3
Chancellerie d'Etat du Canton du Jura	2, rue de l'Hôpital 2800 Delémont
Konferenz der Kantonsregierungen (KdK) Conférence des gouvernements cantonaux (CdC) Conferenza dei Governi cantonali (CdC)	Sekretariat Haus der Kantone Speichergasse 6 Postfach 3001 Bern

2. In der Bundesversammlung vertretene politische Parteien / partis politiques représentés à l'Assemblée fédérale / partiti rappresentati nell'Assemblea federale

Die Mitte Le Centre Alleanza del Centro	Generalsekretariat Hirschengraben 9 Postfach 3001 Bern
Eidgenössisch-Demokratische Union EDU Union Démocratique Fédérale UDF Unione Democratica Federale UDF	Postfach 3602 Thun
Ensemble à Gauche EAG	Case postale 2070 1211 Genève 2
Evangelische Volkspartei der Schweiz EVP Parti évangélique suisse PEV Partito evangelico svizzero PEV	Nägeligasse 9 Postfach 3001 Bern
FDP. Die Liberalen PLR. Les Libéraux-Radicaux PLR. I Liberali Radicali	Generalsekretariat Neuengasse 20 Postfach 3001 Bern
Grüne Partei der Schweiz GPS Parti écologiste suisse PES Partito ecologista svizzero PES	Waisenhausplatz 21 3011 Bern
Grünliberale Partei Schweiz glp Parti vert'libéral Suisse pvl Partito verde liberale svizzero pvl	Monbijoustrasse 30 3011 Bern
Lega dei Ticinesi (Lega)	Via Monte Boglia 3 Case postale 4562 6904 Lugano
Partei der Arbeit PDA Parti suisse du travail PST	Postfach 8721 8036 Zürich
Schweizerische Volkspartei SVP Union Démocratique du Centre UDC Unione Democratica di Centro UDC	Generalsekretariat Postfach 8252 3001 Bern
Sozialdemokratische Partei der Schweiz SPS Parti socialiste suisse PSS Partito socialista svizzero PSS	Zentralsekretariat Theaterplatz 4 Postfach 3001 Bern

3. Gesamtschweizerische Dachverbände der Gemeinden, Städte und Berggebiete / associations faîtières des communes, des villes et des régions de montagne qui œuvrent au niveau national / associazioni mantello nazionali dei Comuni, delle città e delle regioni di montagna

Schweizerischer Gemeindeverband Association des Communes Suisses Associazione dei Comuni Svizzeri	Laupenstrasse 35 3008 Bern
Schweizerischer Städteverband Union des villes suisses Unione delle città svizzere	Monbijoustrasse 8 Postfach 3001 Bern
Schweizerische Arbeitsgemeinschaft für die Berggebiete Groupement suisse pour les régions de montagne Gruppo svizzero per le regioni di montagna	Seilerstrasse 4 Postfach 3001 Bern

4. Gesamtschweizerische Dachverbände der Wirtschaft / associations faîtières de l'économie qui œuvrent au niveau national / associazioni mantello nazionali dell'economia

economiesuisse Verband der Schweizer Unternehmen Fédération des entreprises suisses Federazione delle imprese svizzere Swiss business federation	Hegibachstrasse 47 Postfach 8032 Zürich
Schweizerischer Gewerbeverband (SGV) Union suisse des arts et métiers (USAM) Unione svizzera delle arti e mestieri (USAM)	Schwarztorstrasse 26 Postfach 3001 Bern
Schweizerischer Arbeitgeberverband Union patronale suisse Unione svizzera degli imprenditori	Hegibachstrasse 47 Postfach 8032 Zürich
Schweiz. Bauernverband (SBV) Union suisse des paysans (USP) Unione svizzera dei contadini (USC)	Laurstrasse 10 5201 Brugg
Schweizerische Bankiervereinigung (SBV) Association suisse des banquiers (ASB) Associazione svizzera dei banchieri (ASB) Swiss Bankers Association	Postfach 4182 4002 Basel
Schweiz. Gewerkschaftsbund (SGB) Union syndicale suisse (USS) Unione sindacale svizzera (USS)	Monbijoustrasse 61 Postfach 3000 Bern 23

Kaufmännischer Verband Schweiz Société suisse des employés de commerce Società svizzera degli impiegati di commercio	Hans-Huber-Strasse 4 Postfach 1853 8027 Zürich
Travail.Suisse	Hopfenweg 21 Postfach 5775 3001 Bern

5. Weitere interessierte Kreise / autres milieux concernés / altre cerchie interessate

Schweizerische Informatikkonferenz (SIK) Conférence suisse sur l'informatique (CSI) Conferenza svizzera sull'informatica (CSI)	Haus der Kantone Speichergasse 6 3011 Bern sekretariat@sik.swiss
Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD)	Haus der Kantone Speichergasse 6 3011 Bern info@kkjpd.ch
Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren (GDK)	Haus der Kantone Speichergasse 6 3011 Bern office@gdk-cds.ch
Regierungskonferenz Militär, Zivilschutz, Feuerwehr	Haus der Kantone Speichergasse 6 3011 Bern Alexander.Krethlow@rkmzf.ch
Schweizerische Staatsanwälte-Konferenz	Haus der Kantone Speichergasse 6 3011 Bern info@ssk-cps.ch
Bau-, Planungs- und Umweltdirektoren-Konferenz BPUK	Haus der Kantone Speichergasse 6 3011 Bern info@bpuk.ch
Verein eCH Association eCH	Mainaustrasse 30 Postfach 8034 Zürich info@ech.ch
Geschäftsstelle eJustice.CH Secrétariat eJustice.CH Segreteria eJustice.CH	Postfach 3134 3001 Bern info@eJustice.ch
digitalswitzerland	Waisenhausplatz 14 3011 Bern info@digitalswitzerland.ch

Schweizer Informatik Gesellschaft SI	Schwarztorstrasse 31 3007 Bern admin@s-i.ch
Geschäftsstelle Digitale Schweiz (GDS) Direction opérationnelle Suisse numérique (GDS) Direzione operativa Svizzera digitale (GDS)	Zukunftstrasse 44 2501 Biel / Bienne www.digitaldialog.swiss
privatim, Konferenz der schweizerischen Datenschutzbeauftragten privatim, Conférence des Préposé(e) suisses à la protection des données	c/o Dr. Beat Rudin, Advokat, Postfach 205 4010 Basel kommunikation@privatim.ch
eHealth Suisse	Schwarzenburgstrasse 157 3003 Bern info@e-health-suisse.ch
asut – Schweizerischer Verband der Telekommunikation	Hirschengraben 8 3011 Bern info@asut.ch
ASIP – Schweizerischer Pensionskassenverband	Kreuzstrasse 26 8008 Zürich info@asip.ch
Stiftung Auffangeinrichtung BVG	Elias-Canetti-Strasse 2 8050 Zürich
Verein Vorsorge Schweiz VVS	Aeschengraben 29 4051 Basel info@verein-vorsorge.ch
Inter-pension Interessengemeinschaft autonomer Sammel- und Gemeinschaftseinrichtungen	Gartenstrasse 2 3063 Ittigen info@inter-pension.ch
PK-Netz 2. Säule	Monbijoustrasse 61 3007 Bern info@pk-netz.ch
Konferenz der kantonalen BVG- und Stiftungsaufsichtsbehörden	Sekretariat Monica Schiesser Aeberhard m.schiesser@gmx.ch
IV-Stellen-Konferenz (IVSK)	Sempacherstrasse 15 6003 Luzern Schweiz
Konferenz der kantonalen Ausgleichskassen (KKAK)	Genfergasse 10 3011 Bern info@ahvch.ch
Vereinigung der Verbandsausgleichskassen (VVAK)	Kapellenstrasse 14 Postfach 3001 Bern info@vvak.ch

Seilbahnen Schweiz	Giacomettistrasse 1 3006 Bern info@seilbahnen.org
Verband Schweizerischer Schifffahrtsunternehmen VSSU	Mythenquai 333 8038 Zürich info@vvssu.ch
RAILplus AG	Hintere Bahnhofstrasse 85 5001 Aarau info@railplus.ch
swissnuclear	Postfach 1663 4601 Olten info@swissnuclear.ch
SwissGrid AG	Bleichemattstrasse 31 5001 Aarau info@swissgrid.ch

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bern, 2. Dezember 2022

Vorentwurf zur Änderung des Bundesgesetzes vom 18. Dezember 2020 über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG)

Bericht über die Ergebnisse der Vernehmlassung

Inhaltsverzeichnis

1 Ausgangslage

Am 12. Januar 2022 hat der Bundesrat den Vorentwurf zur Änderung des Informationssicherheitsgesetzes vom 18. Dezember 2020 (ISG) sowie den erläuternden Bericht verabschiedet und das Eidgenössische Finanzdepartement (EFD) beauftragt, ein Vernehmlassungsverfahren durchzuführen. Die Vernehmlassung dauerte vom 12. Januar bis zum 14. April 2022. Die Liste aller Vernehmlassungsteilnehmenden mit den nachfolgend verwendeten Abkürzungen findet sich im Anhang. Es sind 99 Stellungnahmen eingegangen:

99	Total eingegangene Stellungnahmen
25	Kantonsregierungen
4	Kantonale Konferenzen
7	Parteien
1	Gesamtschweizerischer Dachverband der Gemeinden, Städte und Berggebiete
4	Gesamtschweizerische Dachverbände der Wirtschaft
19	Betroffene Unternehmen
39	Weitere interessierte Kreise

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

2 Gegenstand des Vernehmlassungsentwurfs

Ziel des Vorentwurfs ist es, im Informationssicherheitsgesetz (ISG), das am 18. Dezember 2020 vom Parlament verabschiedet wurde, die gesetzliche Grundlage für eine Meldepflicht für Cyberangriffe auf kritische Infrastrukturen zu schaffen.

Inhaltlich soll die Meldepflicht nur für Cyberangriffe gelten, die ein gewisses Schadenspotential aufweisen. Nicht meldepflichtig sind Cybervorfälle, die auf menschliches Fehlverhalten, also beispielsweise eine unbeabsichtigte fehlerhafte Manipulation eines Mitarbeitenden, zurückzuführen sind. Es wurde auch davon abgesehen, die Meldepflicht auf Schwachstellen in Informatikmitteln auszudehnen. Die Meldepflicht gilt für Betreiberinnen kritischer Infrastrukturen, die in kritischen Teilsektoren tätig sind. Die Funktion als zentrale Meldestelle übernimmt das NCSC, das auch freiwillige Meldungen zu Cybervorfällen und Schwachstellen in Informatikmitteln entgegennimmt.

Die gesetzlichen Grundlagen der Meldepflicht für Cyberangriffe, sollen – abgesehen von 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 – welche aktuell nur in der Cyberrisikenverordnung (CyRV)[2] definiert sind – und dessen Funktion als Meldestelle für meldepflichtige Cyberangriffe zu regeln.

Durch Einführung einer Meldepflicht können Cyberangriffe künftig 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.

Nicht Gegenstand dieser Vorlage ist die Einführung von verbindlichen Mindeststandards für die Cybersicherheit für Betreiberinnen kritischer Infrastrukturen sowie von Anforderungen an die Produktesicherheit von IT-Produkten.

1 www.fedlex.admin.ch > Vernehmlassungen > Abgeschlossene Vernehmlassungen > 2022 > EFD
2 SR **120.73**

3 Ergebnisse der Vernehmlassung

3.1 Gesamtbeurteilung der Vorlage

89 Vernehmlassungsteilnehmende der Vernehmlassungsteilnehmenden **begrüssen** grundsätzlich die **Zielsetzungen und Stossrichtungen des Vorentwurfs**, wobei teilweise auch Vorbehalte angebracht werden.

Positive Stellungnahmen (von insgesamt 102 Stellungnahmen)	**89**
Kantonsregierungen	25
Kantonale Konferenzen	4
Parteien	6
Gesamtschweizerische Dachverbände der Gemeinden, Städte und Berggebiete	1
Gesamtschweizerische Dachverbände der Wirtschaft	3
Betroffene Unternehmen	17
Weitere interessierte Kreise	33

7 Vernehmlassungsteilnehmende haben sich ausdrücklich **gegen den Vorentwurf ausgesprochen**.

Negative Stellungnahmen (von insgesamt 102 Stellungnahmen)	**7**
Kantonsregierungen	-
Kantonale Konferenzen	-
Parteien	1
Gesamtschweizerische Dachverbände der Gemeinden, Städte und Berggebiete	-
Gesamtschweizerische Dachverbände der Wirtschaft	1
Betroffene Unternehmen	2
Weitere interessierte Kreise	3

Die Bundesanwaltschaft, SwissDigital und die Piratenpartei haben inhaltliche Änderungsvorschläge gemacht, aber auf eine Bewertung der Vorlage verzichtet.
Folgende Vernehmlassungsteilnehmende haben explizit auf eine Stellungnahme verzichtet: Kanton Obwalden, Schweizerische Staatsanwälte-Konferenz, Stiftung Auffangeinrichtung BVG.

3.2 Zusammenfassung der Vernehmlassungsantworten und hauptsächliche Kritikpunkte

Alle Kantone (mit Ausnahme des Kantons Obwalden, der auf eine Stellungnahme verzichtet hat), 4 kantonale Konferenzen (KKJPD, KKPKS, RK MZF, GDK), 6 Parteien (SP, SVP, FDP, Die Mitte, die Grünen und GLP), der Schweizerische Städteverband, 3 gesamtschweizerische Dachverbände der Wirtschaft (economiesuisse, Swiss Banking, SGB), 17 Unternehmen (Abraxas, Axpo, Flughafen ZH, Flughafen GE, Helvetia Versicherungen, Migros, die Post, Raiffeisen, Romande Energie, SBB, Salt, Sunrise, Suva, Swisscom, Swissgrid, Switch, TPG), 34 interessierte Organisationen (AEROSUISSE, asut, AEIS, Verband der Auslandsbanken in der Schweiz, Centre Patronal, CH++, Digitale Gesellschaft, digitalswitzerland, eAHV, eGov-Schweiz, FER, GEM, Härting Rechtsanwälte, IG eHealth, Inter-pension, ASIP, Operation Libero, Pour Demain, privatim, santésuisse, ISSS, RAILplus, SVV, Swico, swissICT, Swissmem, Trust Valley, SVGW, UniBe, VAV, VUD, VöV, VSE, UniZH/UNIL NFP 77, UniGE) und die Gemeinde Gachnang **begrüssen die Zielsetzungen und die Stossrichtungen des Vorentwurfs.**

Die meisten Stellungnahmen zugunsten des Vorentwurfs verlangen ausdrücklich, dass die Meldepflicht **keine hohen Kosten** für die öffentliche Verwaltung oder die Privatwirtschaft (namentlich Unternehmen, die einen Cybervorfall melden) mit sich bringt, dass die Umsetzung der Meldepflicht unbürokratisch erfolgt und dass der **administrative Aufwand gering bleibt.** Alle Teilnehmenden wünschen Präzisierungen und viele äussern Vorbehalte zu gewissen Bestimmungen.

Die **Präzisierungen** betreffen insbesondere die Begriffe (Art. 5), die Liste der Bereiche, die der Meldepflicht unterstehen (Art. 74*b*), und die Ausnahmen von der Meldepflicht (Art. 74*c*), die Definition der zu meldenden Cyberangriffe (Art. 74*d*) sowie die Modalitäten für die Übermittlung der Meldung (Art. 74*f*).

Insbesondere zu den Strafen bei Verletzung der Meldepflicht (Art. 74*h* und Art. 74*i*) wurden **Vorbehalte** geäussert. 24 Institutionen, die sich an der Vernehmlassung beteiligt haben, **lehnen jegliche Möglichkeit von Sanktionen ab.** Sie begründen ihre Ablehnung hauptsächlich damit, dass Bussen grundsätzlich nicht das richtige Instrument seien, um die Einhaltung der Meldepflicht zu erwirken. Sie vertreten die Ansicht, dass die Umsetzung der Meldepflicht eher durch Anreize im Sinne von Unterstützungsleistungen gefördert werden müsste.

Diese Vernehmlassung hat ausserdem gezeigt, dass der Schutz von Informationen aus Meldungen – insbesondere von Personendaten – von grosser Bedeutung ist. Tatsächlich wurden hinsichtlich der **Weiterleitung personenbezogener Daten an die Nachrichtendienste sowie an die Strafverfolgungsbehörden** von sechs Vernehmlassungsteilnehmenden (Swico, Privatim, Piratenpartei, digitale Gesellschaft, Romande Energie, Verein Unternehmensdatenschutz) Bedenken geäussert.

Zudem wünschen sich einige Vernehmlassungsteilnehmende, dass der Vorentwurf erweitert werde. Es gehe nicht nur um die Einführung einer Meldepflicht. Das NCSC müsse zudem die Befugnis haben, den Betreiberinnen von kritischen Infrastrukturen **Mindeststandards** aufzuerlegen und die Umsetzung von Massnahmen wie die **Installation von Sicherheitsupdates** zu verlangen. In diesem Zusammenhang wird auch vorgeschlagen, dass die Betreiberinnen von kritischen Infrastrukturen den Artikeln 6 bis 10 ISG unterstellt sein sollen.

Weiter begrüssen die Teilnehmenden die Tatsache, dass auch Schwachstellen dem NCSC gemeldet werden können, dass dieses zunächst die Hersteller der betreffenden Produkte gemäss den **«Coordinated Vulnerability Disclosure»**-Grundsätzen informiert und ihnen eine Frist setzt, um die Schwachstellen zu beheben. Es wird gewünscht, dass die Institutionen, die Schwachstellen melden, strafrechtlich nicht verfolgt werden dürfen, und dass die Hersteller, die diese Schwachstellen nicht innert der vom NCSC gesetzten Frist beheben, von öffentlichen Beschaffungen ausgeschlossen werden können.

SVP, SGV, scienceindustries, swissuniversities, Coop, Swiss Airlines und eine Einzelperson **lehnen** den Vorentwurf in seiner aktuellen Form **ab.** Die Bundesanwaltschaft (BA) hat sich nicht ausdrücklich für oder gegen den Vorentwurf geäussert.

3.3 Anträge und Bemerkungen zum Vorentwurf

3.3.1 Vorbemerkung

Im Folgenden werden die Bemerkungen, Änderungsvorschläge und Kritikpunkte zu den einzelnen Bestimmungen aufgeführt. Es werden jeweils lediglich die in einer Stellungnahme vorgebrachten Hauptargumente erwähnt. Besonders ausführliche Stellungnahmen werden nur insoweit wiedergegeben, als sie konkrete materielle Änderungen fordern. Weitere Einzelheiten können den im Internet publizierten Stellungnahmen entnommen werden.
Stillschweigende Zustimmung bzw. der Verzicht auf eine Rückmeldung zu einem Artikel wird nicht erwähnt. Dies soll die Leserschaft aber nicht darüber hinwegtäuschen, dass trotz zahlreicher kritischer Stimmen zu einzelnen Bestimmungen eine Mehrzahl der Vernehmlassungsteilnehmenden

mit weiten Teilen der vorgeschlagenen Gesetzesbestimmungen grundsätzlich einverstanden ist. Zur Gesetzessystematik sind keine Stellungnahmen eingegangen.

3.3.2 Anträge und Bemerkungen zu den einzelnen Bestimmungen

3.3.2.1 Titel

Der **Kanton Thurgau** regt an, den Titel des Erlasses anzupassen, da der aktuelle Titel «Bundesgesetz über die Informationssicherheit beim Bund» suggeriere, dass sich sein Geltungsbereich auf den Bund beschränke. Das sei mit der Einführung einer Meldepflicht nicht mehr der Fall.

3.3.2.2 Artikel 1 Absatz 1 (Zweck)

> [1] Dieses Gesetz soll:
>
> a. die sichere Bearbeitung der Informationen, für die der Bund zuständig ist, sowie den sicheren Einsatz der Informatikmittel des Bundes gewährleisten;
>
> b. die Widerstandsfähigkeit der Schweiz gegenüber Cyberrisiken erhöhen.

Zum vorliegenden Artikel sind 4 Reaktionen eingegangen, die im Wesentlichen konzeptuelle Anpassungen betrafen.

❖ **Allgemeine Bemerkungen zu Artikel 1 Absatz 1**

Migros schlägt vor, Artikel 1 mit einer Regelung zum räumlichen Geltungsbereich zu ergänzen.

Laut dem **Kanton TG** ist die Trennung in Buchstabe a und Buchstabe b in diesem Fall nicht sinnvoll.

❖ **Zustimmung zu Artikel 1 Absatz 1**

Swiss Banking begrüsst die Tatsache, dass Artikel 1 ausdrücklich die «Widerstandsfähigkeit der Schweiz gegenüber Cyberrisiken» einschliesst. Dadurch untermauere Artikel 1 die in Artikel 73*a* ff. festgelegten Aufgaben des NCSC.

❖ **Änderungsanträge und Anregungen zu Artikel 1 Absatz 1**

- **<u>Zu Buchstabe a</u>**

ISSS und Härting Rechtsanwälte verlangen, Artikel 1 wie folgt zu ergänzen: «die sichere Bearbeitung der Informationen, für die der Bund zuständig ist, sowie den sicheren Einsatz der Informatikmittel des Bundes gewährleisten, [*es sei denn eine Spezialgesetzgebung sehe eine gesonderte Zuständigkeit vor*]».

- **<u>Zu Buchstabe b</u>**

Swico verlangt, den Begriff «Cyberrisiken» durch «Bedrohungen» zu ersetzen, da der Begriff «Cyberrisiken» laut **Swico** nicht definiert werden kann.

3.3.2.3 Artikel 2 Absatz 5 (Geltungsbereich)

> [5] Für Organisationen des öffentlichen und privaten Rechts, die kritische Infrastrukturen betreiben, die aber nicht unter die Absätze 1–3 fallen, gelten die Artikel 73*a*–79. Die Spezialgesetzgebung kann weitere Teile dieses Gesetzes für anwendbar erklären.

Zum vorgeschlagenen Geltungsbereich sind 5 allgemeine Bemerkungen eingegangen.

❖ **Allgemeine Bemerkungen zu Artikel 2 Absatz 5**

Swissmem sowie UniZH/UNIL NFP 77 haben betont, dass neben den Artikeln 73*a*–79 auch Artikel 6 ISG zu berücksichtigen sei.

UniZH/UNIL NFP 77 ist der Ansicht, dass es sinnvoll wäre, die Möglichkeit vorzusehen, das NCSC beizuziehen, um festzustellen, ob eine Betreiberin dem Gesetz oder der Meldepflicht unterstellt ist, wie dies beispielsweise in der VÜPF vorgesehen ist (siehe insbesondere Art. 51 VÜPF).

Der **Kanton GE** verlangt eine Definition des Begriffs «kritisch».

❖ **Änderungsanträge und Anregungen zu Artikel 2 Absatz 5**

ISSS und Härting Rechtsanwälte bitten um eine Ergänzung von Artikel 2 Absatz 5 wie folgt: «*…* die kritische Infrastrukturen *[gemäss Artikel 74b]* betreiben, *…*»*,* um zu präzisieren, dass von kritischen Infrastrukturen im Sinne des ISG die Rede ist.

3.3.2.4 Artikel 5 Buchstaben d und e (Begriffe)

In diesem Gesetz bedeuten: d. *Cybervorfall:* Ereignis beim Betrieb von Informatikmitteln, das dazu führen kann, dass die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist; e. *Cyberangriff:* Cybervorfall, der von Unbefugten absichtlich ausgelöst wurde.

23 Vernehmlassungsteilnehmende haben sich zu den beiden Definitionen geäussert und Änderungsanträge gestellt.

❖ **Allgemeine Bemerkungen zu Artikel 5**

Economiesuisse, IG eHealth, die Post und VUD sind der Ansicht, dass die Begriffe «Cybervorfall» und «Cyberangriff», wie sie in diesem Artikel gemeint sind, genauer definiert werden müssten.

Digital Law Center UniGE verlangt, dass Cyberangriffe und Cybervorfälle so definiert werden, dass sie auch ohne Verletzung der Datensicherheit oder anderer gesetzlicher oder regulatorischer Bestimmungen entsprechend eingestuft werden können.

❖ **Änderungsanträge und Anregungen zu Artikel 5**

IG eHealth, ISSS, Härting Rechtsanwälte, der Kanton GE und die Post vertreten die Meinung, dass eine Definition der Begriffe «Schwachstelle» und «Cyberrisiko» in diesen Artikel aufzunehmen sei.

Die **Gemeinde Gachnang** erachtet es als notwendig, das Präfix «Cyber» zu definieren.

- **<u>Zu Buchstabe d</u>**

Pour Demain schlägt vor, die künstliche Intelligenz im Rahmen der Definition von «Cybervorfall» explizit zu erwähnen.

Migros, Sunrise, TPG und digitalswitzerland verlangen, dass der Satz «das dazu führen kann» geändert wird. Die letzten drei sind der Ansicht, dass er durch folgenden Satz ersetzt werden sollte**:** «das dazu führt». Migros hingegen fordert eine bessere Definition.

Santésuisse meint, dass die Definition nicht hinreichend genau sei und dass sich solche Ereignisse auch ohne Cyberangriff als Auslöser zutragen könnten, beispielsweise durch den Ausfall von IT-Komponenten oder durch Programmierfehler. Diese Ereignisse dürften nicht unter die Meldepflicht fallen.

UniZH/UNIL NFP 77 sind der Ansicht, dass die vorliegende Definition von «Cybervorfall» und die in Artikel 3 Buchstabe b CyRV vorgesehene Definition aufeinander abzustimmen seien. Zudem erachten **UniZH/UNIL NFP 77** den Ausdruck «beim Betrieb von Informatikmitteln» als nicht optimal, da er jegliches passives Verhalten ausschliesst und so als zu restriktiv empfunden werden könne.

- **<u>Zu Buchstabe e</u>**

Swissgrid fragt, ob die Definition von «Unbefugten» nur externe oder auch interne Personen umfasse.

3.3.2.5 Artikel 73*a* Grundsatz

Zum Schutz der Schweiz vor Cyberrisiken nimmt das nationale Zentrum für Cybersicherheit (NCSC) insbesondere folgende Aufgaben wahr: a. Sensibilisierung der Öffentlichkeit auf Cyberrisiken; b. Warnung vor Cyberrisiken und Schwachstellen von Informatikmitteln; c. Veröffentlichung von Informationen zur Cybersicherheit sowie von Anleitungen für präventive und reaktive Massnahmen gegen Cyberrisiken; d. technische Analysen zur Bewertung und Abwehr von Cyberrisiken; e. Entgegennahme und Bearbeitung von Meldungen zu Cybervorfällen und Schwachstellen von Informatikmitteln; f. Unterstützung von Betreiberinnen von kritischen Infrastrukturen.

16 Vernehmlassungsteilnehmende haben sich zum Teil sehr ausführlich zu den vorgeschlagenen Grundsätzen geäussert. 2 Teilnehmende sind mit dem aktuellen Wortlaut von Artikel 73*a* einverstanden, 5 verlangen, dass zur obigen Liste eine Aufgabe hinzugefügt wird, und 9 weitere haben Bemerkungen gemacht und andere Änderungen beantragt.

- ❖ **Allgemeine Bemerkungen zu Artikel 73*a***

CH++ begrüsst den Artikel, ist aber der Meinung, dass als Aufgabe des NCSC die «aktive Erkennung von Schwachstellen und Bedrohungen» zum vorliegenden Artikel hinzugefügt werden müsste.

Die **Gemeinde Gachnang** begrüsst den Artikel, spricht sich aber dafür aus, im Artikel 73*a* die Aufgaben um ein «regelmässiges Reporting zwecks Qualitätssicherung und Erfolgskontrolle» zu ergänzen.

Migros verlangt eine nicht abschliessende Liste von Beispielen, um die Absicht von Artikel 73*a* zu untermauern.

Der **Kanton BE** verlangt die Ergänzung von Artikel 73*a* um einen zweiten Absatz: «Das NCSC arbeitet bei der Erfüllung dieser Aufgaben mit den Polizeibehörden der Kantone zusammen».

Swisscom begrüsst diesen Artikel, hält es aber für notwendig, dass für das NCSC neben den bereits erwähnten Aufgaben und Kompetenzen im Gesetz festgehalten wird, dass es nicht nur den Bund, sondern auch die Wirtschaft und die Bevölkerung unterstützt.

- ❖ **Zustimmung zu Artikel 73*a***

Swico, SuisseDigita und swissICT loben die Schaffung rechtlicher Grundlagen für die Aufgaben des NCSC explizit.

- ❖ **Änderungsanträge und Anregungen zu Artikel 73*a***

- **<u>Zu Buchstabe b</u>**

Pour Demain ist der Ansicht, dass die mit der KI verbundenen Risiken zu den oben erwähnten Aufgaben des NCSC hinzugefügt werden müssten.

- **Zu Buchstabe c**

Swiss Banking und Raiffeisen begrüssen den Artikel, erachten aber die «Anleitungen für präventive und reaktive Massnahmen gegen Cyberrisiken» nur als sinnvoll, wenn sie nicht verpflichtend sind.

- **Zu Buchstabe f**

Die Grünen fordern, dass die «Unterstützung von Betreiberinnen von kritischen Infrastrukturen» (Art. 73*a* Bst. f) breiter gedacht wird, als die Definitionen das bisher vorsehen.

3.3.2.6 Artikel 73*b* Bearbeitung von Meldungen zu Cybervorfällen und Schwachstellen

[1] Werden dem NCSC Cybervorfälle oder Schwachstellen von Informatikmitteln gemeldet, so analysiert es diese auf ihre Bedeutung für den Schutz der Schweiz vor Cyberrisiken. Es gibt auf Wunsch der meldenden Person eine Empfehlung zum weiteren Vorgehen ab, sofern dafür keine weiteren Analysen und Abklärungen erforderlich sind.
[2] Das NCSC kann Informationen zu Cybervorfällen veröffentlichen oder an interessierte Behörden und Organisationen weiterleiten, sofern dies dazu dient, Cyberangriffe zu verhindern oder zu bekämpfen. Diese Informationen dürfen Personendaten und Daten juristischer Personen enthalten, sofern es sich um missbräuchlich verwendete Identifikationsmerkmale und Adressierungselemente handelt und die betroffene Person einwilligt.
[3] Werden dem NCSC Schwachstellen gemeldet, so informiert es umgehend den Hersteller und setzt ihm zur Behebung der Schwachstelle eine angemessene Frist. Behebt der Hersteller die Schwachstelle nicht innert dieser Frist, so veröffentlicht das NCSC die Schwachstelle unter Angabe der betroffenen Soft- oder Hardware, sofern dies zum Schutz vor Cyberrisiken beiträgt.

21 Teilnehmende haben sich dazu geäussert. Im Allgemeinen hat Absatz 3 am meisten Reaktionen hervorgerufen.

❖ **Allgemeine Bemerkungen zu Artikel 73*b***

Scienceindustries ist der Meinung, dass die Umsetzung der Meldepflicht bedinge, dass sie einen Mehrwert für die betroffenen Unternehmen darstelle, einen verhältnismässigen und subsidiären Ansatz verfolge, keine Mehrkosten für die Schweizer Wirtschaft auslöse und auf einer kooperativen Grundlage beruhe.

Die Grünen, die Digitale Gesellschaft und die Piratenpartei begrüssen Artikel 73*b,* vertreten aber die Ansicht, dass das NCSC bestimmte Mindestanforderungen erfüllen müsse, um seine Verpflichtungen in Bezug auf diesen Artikel einhalten zu können: Es müsse über umfassendere Kompetenzen verfügen bei schweren Vorfällen und ein Responsible-Disclosure-Verfahren für die kritischen Infrastrukturen einrichten.

Die Grünen und CH++ verlangen, dass das NCSC gegenüber Herstellern und Betreiberinnen Leitlinien sowie verbindliche Standardfristen erlassen kann, die sie verpflichten, Schwachstellen rasch zu beheben und Schäden zu begrenzen.

Der Kanton VD verlangt, den Artikel 73*b* mit der Medizinprodukteverordnung (MepV) abzustimmen.

❖ **Änderungsanträge und Anregungen**

- **Zu Absatz 1**

Laut **UniZH/UNIL NFP 77** ist die Formulierung «sofern dafür keine weiteren Analysen und Abklärungen erforderlich sind» nicht klar. Sie sei zu ersetzen durch «wenn Cybervorfälle oder Schwachstellen dem NCSC gemeldet werden», damit keine Beschränkung auf eine Meldung vorliegt, die mit der Meldung von Cyberangriffen durch die betreffende Person verwechselt werden könnte.

- **Zu Absatz 2**

Den Grünen und CH++ zufolge müsste das NCSC, ausser bei gerechtfertigten Ausnahmen eine Verpflichtung zur Veröffentlichung von Cybervorfällen einführen. **ISSS, Härting Rechtsanwälte, VSE, VöV, Swissgrid, der Kanton GE und RAILplus** bestehen hingegen darauf, dass Personendaten sowie Daten von juristischen Personen nur mit ausdrücklicher und vorgängiger Einwilligung veröffentlicht werden dürfen und dass die Umstände, unter denen der Cybervorfall veröffentlicht werden muss, sowie die bereitzustellenden Informationen aus Gründen des Datenschutzes und der Geheimhaltung vertraulicher Daten genauer zu regeln sind.

UniZH/UNIL NFP 77 sind der Ansicht, dass die Einwilligung von der Person stammen müsste, die die Daten teilt, und nicht von den betroffenen Personen. Denn das Einholen der Einwilligung sämtlicher betroffener Personen könne unverhältnismässig aufwendig sein.

- **Zu Absatz 3**

Die Piratenpartei begrüsst, dass in Artikel 73*b* Absatz 3 die Sicherheitslücken unverzüglich mit den Betreiberinnen kritischer Infrastrukturen geteilt werden, und bittet darum, hinzuzufügen, dass diese sie nicht für offensive Cyberspiele gemäss NDG missbrauchen dürfen. Ebenso müssten Hacker im Rahmen von Responsible Disclosure automatisch Straffreiheit erhalten.

CH++ schlägt vor, dass Hersteller, welche nicht auf Schwachstellenmeldungen reagieren, von öffentlichen Beschaffungen ausgeschlossen werden können sollen.

UniZH/UNIL NFP 77 vertreten die Meinung, dass es sinnvoll wäre, Absatz 3 neben der Veröffentlichung mit einer Sanktionsmöglichkeit auszustatten, während **die Post** hingegen erklärt, dass sich Sanktionen negativ auf die Anzahl Meldungen auswirken könnten.
Der **Kanton GE** beantragt, «Hersteller» durch «Hersteller und/oder Herausgeber» zu ersetzen.

Nach Ansicht **der Digitalen Gesellschaft** muss das NCSC, wenn es Kenntnis über eine Sicherheitslücke betreffend ein Drittprodukt hat, bei der nicht davon auszugehen ist, dass sie dem Hersteller bereits bekannt ist, diese Sicherheitslücke dem betreffenden Hersteller im Rahmen eines Responsible-Disclosure-Verfahrens unverzüglich melden. Zudem müssten dem NCSC der **Digitalen Gesellschaft** zufolge Mittel zur Verfügung gestellt werden, die es ihm erlauben, bei den Organisationen, die eine Sicherheitslücke melden, auf deren Behebung zu bestehen.

Laut **ISSS und Härting Rechtsanwälte** müssen Meldungen von Schwachstellen, die das NCSC den Herstellern zukommen lässt, vom Öffentlichkeitsprinzip ausgeschlossen sein.

Pour Demain und Operation Libero sind der Ansicht, dass die Fristen auch für die Betreiberinnen festgelegt werden müssten, um die effektive Durchführung von Sicherheitsupdates zu gewährleisten.

SSV und VUD äussern Bedenken, dass eine vorzeitige Veröffentlichung der Schwachstelle mit Angabe der betroffenen Software oder des betreffenden Materials für die meldende Stelle zu einem zusätzlichen Risiko führen könnte. Daher schlägt **VUD** vor, dass sämtliche Informationen und Kommunikationsmassnahmen des NCSC dem Gesetzesvorbehalt unterstellt werden müssen, dass sie Cyberangriffe nicht fördern oder erleichtern.

3.3.2.7 Artikel 73*c* Weiterleitung von Informationen

[1] Ergeben sich aus der Meldung eines Cybervorfalls oder dessen Analyse Informationen, die für das frühzeitige Erkennen und Verhindern von Bedrohungen der inneren oder äusseren Sicherheit, für die Beurteilung der Bedrohungslage oder für die nachrichtendienstliche Frühwarnung zum Schutz von kritischen Infrastrukturen nach Artikel 6 Absätze 1 Buchstabe a, 2 und 5 des Nachrichtendienstgesetzes vom 25. September 2015 (NDG) relevant sind, so leitet das NCSC diese Informationen an den NDB weiter.
[2] Für Mitarbeitende des NCSC entfällt die Anzeigepflicht gemäss Artikel 22a des Bundespersonalgesetzes vom 24. März 2000, wenn sie im Zusammenhang mit der Meldung eines Cybervorfalls oder dessen Analyse Hinweise auf eine mögliche Straftat erhalten. Die Leiterin oder der Leiter des NCSC kann Anzeige erstatten, sofern dies aufgrund der Schwere der möglichen Straftat geboten scheint.
[3] Informationen, die von einer Person im Rahmen einer Meldung dem NCSC bekanntgegeben wurden, dürfen in einem Strafverfahren gegen diese Person nur mit deren Einverständnis verwendet werden.
[4] Informationen, die strafrechtlich geschützte Geheimnisse offenbaren, darf das NCSC nur nach den Vorgaben von Artikel 320 StGB weiterleiten.

25 Teilnehmende haben sich zu diesem Artikel geäussert. Er wurde viel diskutiert und es sind viele Änderungsanträge eingegangen. 2 Stellen begrüssen Artikel 73*c* Absatz 3, während 3 andere Artikel 73*c* Absatz 2 ablehnen.

❖ Allgemeine Bemerkungen zu Artikel 73*c*

Privatim fordert, dass die an den NDB oder an die Strafverfolgungsbehörden übermittelten Daten nach der Übermittlung an diese Stellen von den Servern des NCSC gelöscht werden.

Der Kanton GR verlangt, dass das Zusammenspiel von «Geheimhaltungsverpflichtungen der Betreiberinnen» und «Weiterleitung von Informationen im Rahmen der Meldepflicht» expliziter formuliert wird.

Swico begrüsst den Artikel zwar, verlangt aber, dass präzisiert wird, dass nur sicherheitsrelevante Informationen kommuniziert werden.

❖ Zustimmung zu Artikel 73*c*

AEROSUISSE begrüsst den vorliegenden Gesetzestext.

Der Kanton AG begrüsst die Lösung, bei welcher die Mitarbeitenden des NCSC von der Anzeigepflicht ausgenommen werden und dem NCSC ein Anzeigerecht erteilt wird.

Die Grünen und CH++ begrüssen Artikel 73*c* Absatz 3.

❖ Ablehnung von Artikel 73*c*

Die Piratenpartei und eGov-Schweiz sind nicht damit einverstanden, dass der NDB die im Rahmen der Meldepflicht an das NCSC übermittelten Daten bearbeitet.

Der Kanton BE und die KKJPD verlangen die Streichung von Artikel 73*c* Absatz 2, da sie der Meinung sind, dass das NCSC weiterhin sämtliche Offizialdelikte an die Strafverfolgungsbehörden weiterleiten solle.

Der Kanton NW fordert, Artikel 73*c* Absatz 2 zu streichen, da der Artikel seiner Ansicht nach potenziell willkürlich sei.

❖ Änderungsanträge und Anregungen zu Artikel 73*c*

- **Zu Absatz 1**

Die **GLP** verlangt, in Artikel 73*c* Absatz 1 explizit festzuhalten, dass anonyme Meldungen beim NCSC möglich sind.

Die Grünen und VUD beantragen, dass die Daten anonym an das NCSC übermittelt werden können und dass dies rechtlich geregelt wird.

- **Zu Absatz 2**

Der Kanton SZ ist der Ansicht, dass das NCSC sicherstellen müsse, dass schwere Verstösse konsequent zur Anklage gebracht würden.

Die Kantone BL, NW und SZ haben ob der mit einer solchen Bestimmung verbundenen potenziellen Willkür Bedenken.

- **Zu Absatz 3**

Digitalswitzerland, Sunrise, VUD, swissICT und asut sind der Meinung, dass ein Risiko bestehe, dass die meldende Person sich selbst belaste, und verlangen daher eine Anpassung des Textes.

Digitalswitzerland beantragt, dass Artikel 73*c* Absatz 3 wie folgt geändert wird: «Informationen, die dem NCSC im Rahmen einer Meldung bekanntgegeben wurden und die meldende Person selbst belasten könnten, dürfen in einem Strafverfahren gegen diese Person nur mit Einverständnis dieser Person verwendet werden».

VUD schlägt vor, die Pflicht zur Einholung des Einverständnisses auf sämtliche Mitarbeitenden und Organe eines Unternehmens oder einer Organisation, die einen Cybervorfall melden, auszudehnen.

3.3.2.8 Artikel 74 Unterstützung von Betreiberinnen von kritischen Infrastrukturen

[1] Das NCSC unterstützt die Betreiberinnen von kritischen Infrastrukturen beim Schutz vor Cyberrisiken.
[2] Es stellt ihnen dazu insbesondere folgende Hilfsmittel zur Verfügung:
a. ein Kommunikationssystem für den sicheren Informationsaustausch;
b. technische Informationen zu aktuellen Cyberrisiken und Schwachstellen sowie Empfehlungen für präventive Massnahmen;
c. technische Instrumente und Anleitungen zur Erkennung von Cybervorfällen, die auf den erhöhten Schutzbedarf von kritischen Infrastrukturen ausgerichtet sind.
[3] Es berät und unterstützt sie bei der Bewältigung von Cybervorfällen und der Behebung von Schwachstellen, wenn für die kritische Infrastruktur ein unmittelbares Risiko von gravierenden Auswirkungen besteht und, sofern es sich um private Betreiberinnen handelt, die Beschaffung gleichwertiger Unterstützung auf dem Markt nicht rechtzeitig möglich ist.
[4] Es kann zur Analyse eines Cybervorfalls mit dem Einverständnis der betroffenen Betreiberin auf deren Informationen und Informatikmittel zugreifen. Das Einverständnis kann unabhängig von allfälligen Geheimhaltungspflichten gewährt werden.

22 Vernehmlassungsteilnehmende haben sich konkret zu dieser Gesetzesbestimmung geäussert. Die meisten Anträge betreffen Textänderungen oder Klärungen. Eine einzige Stelle lehnt diesen Artikel ab.

- ❖ **Allgemeine Bemerkungen zu Artikel 74**

Die Grünen begrüssen, dass das NCSC die Betreiberinnen kritischer Infrastrukturen bei Cyberrisiken unterstützt.

Der SSV verlangt weitere Klärungen zur Unterstützung der Städte, insbesondere hinsichtlich der Einführung von Mitteln zur Erkennung und Identifikation von Cyberangriffen sowie deren Finanzierung.

Raiffeisen ist der Ansicht, dass der Einsatz der vom NCSC bereitgestellten Mittel freiwillig bleiben und keine Pflicht zur Nutzung dieser Mittel eingeführt werden solle.

UniBe verlangt, dass das NCSC die Betreiberinnen von kritischen Infrastrukturen über die von anderen Betreiberinnen von kritischen Infrastrukturen gemeldeten Cyberangriffe informiert.

❖ **Änderungsanträge und Bemerkungen zu Artikel 74**

- **Zu Abs. 2 Buchstabe a**

ISSS, Härting Rechtsanwälte und die Post fordern, dass das NCSC neben der Bereitstellung eines Kommunikationssystems für den gesicherten Informationsaustausch eine sichere Datenspeicherung gewährleistet.

- **Zu Abs. 2 Buchstabe b**

Der Kanton SH spricht sich für die Errichtung einer gemeinsamen Plattform für den Informationsaustausch aus.

- **Zu Abs. 2 Buchstabe c**

Die Post verlangt eine Umformulierung, damit eindeutig sichergestellt ist, dass der Einsatz solcher Techniken zwar empfohlen wird, dieser aber letztlich freiwillig und nicht verpflichtend ist.

- **Zu Absatz 3**

VSE begrüsst die Bestrebungen, die privatwirtschaftlichen Angebote nicht konkurrenzieren zu wollen, schlägt aber vor, dass das NCSC als GovCERT einen Schirm über die privatwirtschaftlichen CERT bildet und diese bei der Krisenbewältigung je nach Situation und Bedarf unterstützt. **VSE** verlangt zudem, dass relevantere Unterscheidungskriterien dafür festgelegt werden, wer Anspruch auf die Unterstützung des NCSC hat, und fordert die Anpassung von Artikel 74 Absatz 3 wie folgt: «Es berät und unterstützt sie bei der Bewältigung von Cybervorfällen und der Behebung von Schwachstellen, wenn für die kritische Infrastruktur ein unmittelbares Risiko von gravierenden Auswirkungen besteht».

UniZH/UNIL NFP 77 sind der Meinung, dass die Bestimmung die Schadensfolgen auf die Mitarbeitenden, die Begünstigten, die Leistungen sowie (teilweise) auf die Gesellschaft ausdehnen müsste.

Die Post und der Kanton GE fordern Präzisierungen zum Begriff «unmittelbares Risiko» und **die Post** zusätzlich zum Begriff «gravierende Auswirkungen».

- **Zu Absatz 4**

Für diesen Absatz verlangt **digitalswitzerland,** dass klarer erläutert wird, wie das NCSC die Geheimhaltungspflichten schützt.

ISSS und Härting Rechtsanwälte beantragen, dass der Text wie folgt ersetzt wird: «Es kann zur Analyse eines Cybervorfalls mit dem Einverständnis der betroffenen Betreiberin auf deren Informationen und Informatikmittel zugreifen. Der Zugriff kann gewährt werden ohne allfällige Geheimhaltungspflichten zu verletzen».

Nach Ansicht von **UniZH/UNIL NFP 77** muss die Bestimmung umformuliert werden, indem eingefügt wird, dass das NCSC die Vertraulichkeit gewährleistet und dass die Betreiberin kein Geheimnis verletzt, wenn sie die Informationen weiterleitet und dem NCSC für die Analyse eines Vorfalls Zugang zu ihren Informatikmitteln gewährt.

3.3.2.9 Artikel 74*a* Meldepflicht

Die Betreiberinnen von kritischen Infrastrukturen müssen dem NCSC Cyberangriffe nach deren Entdeckung so rasch als möglich melden, damit das NCSC Angriffsmuster frühzeitig erkennen, mögliche Betroffene warnen und ihnen geeignete Präventions- und Abwehrmassnahmen empfehlen kann.

27 Vernehmlassungsteilnehmende haben sich dazu geäussert, 14 davon haben betont, dass es wichtig sei, eine Meldefrist festzulegen.

- **Änderungsanträge und Bemerkungen zu Artikel 74*a***

Die Grünen, AEROSUISSE und economiesuisse verlangen explizit, dass durch die Meldepflicht keine zusätzlichen Kosten entstehen, weder für die nationale Wirtschaft noch für die meldenden Institutionen. Zudem sei der administrative Aufwand beim Meldeprozess auf ein Minimum zu beschränken.

Die Grünen, GLP, ISSS, Härting Rechtsanwälte und Pour Demain sind der Meinung, dass die Meldepflicht auch für Cyberangriffe und «allgemeine» Cybervorfälle sowie für Schwachstellen gelten müsse.

Sunrise und Switch sind der Ansicht, dass die Meldepflicht nur für Unternehmen gelten sollte, die Cyberangriffe auf ihre eigene Infrastruktur erlitten haben; keine Meldung von Dritten.

Die Digitale Gesellschaft beantragt, die Meldepflicht auf alle Sektoren der Schweizer Wirtschaft sowie auf die staatlichen Behörden und auf NGOs auszudehnen, während die **Piratenpartei** der Meinung ist, dass die Meldepflicht mindestens auf Organisationen auszuweiten sei, die im Auftrag des Staates Aufgaben ausführen, auf sämtliche Unternehmen, die einer ordentlichen Revision unterstehen oder gemäss Artikel 11*a* DSG Datensammlungen anmelden müssen.

eAHV ist der Ansicht, dass spezifiziert werden müsse, dass eine Meldung auch verschiedene betroffene Organisationen umfassen könne und dass die Meldung auch explizit durch Dritte erfolgen könne.

Die Piratenpartei und die Grünen finden, dass die KI im vorliegenden Gesetzestext behandelt werden müsse.

Die SP verlangt, dass die von Cyberangriffen betroffenen Personen vom NCSC so rasch als möglich gewarnt werden müssen.

Asut weist darauf hin, dass es schwierig sei, einen Internetprovider zu verpflichten, sämtliche Cyberangriffe zu melden, die über sein Netzwerk auf Betreiberinnen von kritischen Infrastrukturen erfolgten. Unter Umständen sei eine Meldung durch den Internetprovider wegen der Bestimmungen des Datenschutzgesetzes oder vertraglicher Vereinbarungen auch gar nicht möglich.

Der Verband der Auslandbanken in der Schweiz, CH++, Pour Demain, Swiss Banking, Scienceindustries, die Kantone FR, GR und UR, Raiffeisen, Switch und die Grünen betonen, dass es wichtig sei, explizite Fristen für die Meldung und die Kommunikation detaillierter Informationen an das NCSC festzulegen. **Swiss Banking** beantragt die Ergänzung des vorliegenden Textes um einen Absatz 2, der eine Meldefrist vorgibt, während **Raiffeisen und das Digital Law Center UniGE** empfehlen, die zweistufigen Meldefristen aus der FINMA-Aufsichtsmitteilung 05/2020 zu übernehmen.

Digitalswitzerland schlägt die Einführung des Begriffs des «Meldepflichtigen» vor, um eine höhere Präzision zu erreichen und jegliche Missverständnisse zu vermeiden.
Ausserdem halten es **digitalswitzerland und economiesuisse** für notwendig**,** das Vertrauen der Wirtschaft in den Nutzen dieses Artikels zu stärken, indem hervorgehoben wird, dass die Vorteile dieser Bestimmung unmittelbarer Natur sind und die Verpflichtungen überwiegen. Denn die Verhältnismässigkeit der Massnahmen sei insbesondere für KMU und Startups ein wichtiges Kriterium.

Der Flughafen ZH und Raiffeisen fordern, dass sich die Meldepflicht auf erfolgreiche Angriffe konzentriert. Daher schlägt **der Flughafen ZH** vor, den Text wie folgt zu ergänzen: «*... [erfolgreiche]* Angriffe *[im Sinne von Art. 74d] …».*

UniZH/UNIL NFP 77 verlangen, dass der Begriff «Entdeckung» durch «Erkennung» ersetzt wird und in der französischen Version der Begriff «celui-ci» klarer definiert wird.

3.3.2.10 Artikel 74*b* Bereiche

Die Meldepflicht gilt für:

a. Hochschulen nach Artikel 2 Absatz 2 des Hochschulförderungs- und -koordinationsgesetzes vom 30. September 2011;
b. Bundes-, Kantons- oder Gemeindebehörden sowie interkantonale, kantonale und interkommunale Organisationen;
c. Organisationen mit öffentlich-rechtlichen Aufgaben in den Bereichen Sicherheit und Rettung, Trinkwasserversorgung, Abwasseraufbereitung und Abfallentsorgung;
d. Unternehmen, die in den Bereichen Energieversorgung nach Artikel 6 Absatz 1 des Energiegesetzes vom 30. September 2016, Energiehandel, -messung oder -steuerung tätig sind;
e. Unternehmen, die dem Bankengesetz vom 8. November 1934, dem Versicherungsaufsichtsgesetz vom 17. Dezember 2004 oder dem Finanzmarktinfrastrukturgesetz vom 19. Juni 2015 unterstehen;
f. Anbieterinnen von Online-Marktplätzen, Cloudcomputing, Suchmaschinen und weiteren digitalen Diensten sowie Registrare von Domain-Namen und Betreiberinnen von Rechenzentren, die in der Schweiz:
    1. von einer grossen Zahl von Nutzenden beansprucht werden,
    2. eine hohe Bedeutung für die digitale Wirtschaft haben, oder
    3. Sicherheits- und Vertrauensdienste anbieten;
g. Spitäler, die auf der kantonalen Spitalliste nach Artikel 39 Absatz 1 Buch-stabe e des Bundesgesetzes vom 18. März 1994 über die Krankenversicherung aufgeführt sind;
h. medizinische Laboratorien mit einer Bewilligung nach Artikel 16 Absatz 1 des Epidemiengesetzes vom 28. September 2012;
i. Unternehmen, die für die Herstellung, das Inverkehrbringen und die Ein-fuhr von Arzneimitteln eine Bewilligung nach dem Heilmittelgesetz vom 15. Dezember 2000 (HMG) haben oder Medizinprodukte nach Artikel 4 Absatz 1 Buchstabe b HMG herstellen oder vertreiben;
j. Organisationen, die Leistungen der Sozialversicherungen zur Absicherung der Folgen von Krankheit, Unfall, Arbeits- und Erwerbsunfähigkeit, Alter, Invalidität und Hilflosigkeit erbringen;
k. Anbieterinnen von Fernmeldediensten nach Artikel 3 Buchstabe b FMG;
l. die Schweizerische Radio- und Fernsehgesellschaft;
m. Nachrichtenagenturen von nationaler Bedeutung;
n. Anbieterinnen von Postdiensten, die bei der Postkommission nach Artikel 4 Abs. 1 des Postgesetzes vom 17. Dezember 2010 registriert sind;
o. Transportunternehmen, die dem Bundesgesetz vom 18. Juni 2010 über die Sicherheitsorgane der Transportunternehmen im öffentlichen Verkehr unterstehen;
p. Unternehmen der Zivilluftfahrt, die über eine Bewilligung des Bundesamtes für Zivilluftfahrt verfügen;
q. Unternehmen, die nach dem Seeschifffahrtsgesetz vom 23. September 1953 Güter auf dem Rhein befördern sowie Unternehmen, die die Registrierung, Ladung oder Löschung im Hafen Basel betreiben;
r. Unternehmen, die die Bevölkerung mit unentbehrlichen Gütern des täglichen Bedarfs versorgen;
s. Hersteller von Hard- und Software, deren Produkte von kritischen Infrastrukturen genutzt werden, sofern die Hard- oder Software einen Fernwartungszugang hat oder zu einem der folgenden Zwecken eingesetzt wird:
    1. Steuerungstechnik und Überwachung von Systemen,

2. Betrieb von Medizinprodukten und Fernmeldeanlagen,
3. Gewährleistung der öffentlichen Sicherheit,
4. IT-Sicherheit, Verschlüsselung, Identifikation, Zugriffs- und Zutrittsberechtigung.

Dieser Artikel hat viele Reaktionen hervorgerufen. 39 Vernehmlassungsteilnehmende haben sich zu den vorgesehenen Bereichen für die Meldepflicht geäussert.

- **Allgemeine Bemerkungen zu Artikel 74*b***

Die Piratenpartei ist der Meinung, dass die in Artikel 74*b* genannten Bereiche auf die grossen Medienunternehmen ausgedehnt werden sollten.

Die SP beantragt, die Liste alle fünf Jahre zu überprüfen und allenfalls zu aktualisieren.

Economiesuisse verlangt, die Meldepflicht auf die Bereiche zu beschränken, deren Ausfall oder Beeinträchtigung zu nachhaltig wirkenden Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen führen würden.

Digitalswitzerland fordert eine Folgenabschätzung sowie einen abgestuften Regulierungsansatz, der sich an der Kritikalität der Unternehmen orientiert.

Scienceindustries, SGV, der Kanton UR und Swico fordern eine explizitere Liste, insbesondere indem klar festgelegt werde, was unter dem Begriff «kritische Infrastruktur» zu verstehen sei. In diesem Sinne schlägt **swissICT** eine qualitative Gewichtung nach «sehr kritisch» oder «kritisch» vor.

Der Kanton ZG und swissuniversities beantragen, die Liste zu revidieren und zu kürzen.

Coop und Migros schlagen vor, die Meldepflicht auf die als kritisch eingestuften Tätigkeiten im Unternehmen zu beschränken.

Der Kanton AG beantragt, den Artikel wie folgt zu ändern: «Objekte, Organisationen und Unternehmen, die von den zuständigen Stellen von Bund oder Kanton als kritische Infrastrukturen im Sinne des Bevölkerungsschutzes erfasst sind».

Der Kanton GR schlägt eine Vereinfachung der Umsetzung dieses Artikels vor. Es solle geprüft werden, ob eine Priorisierung und eine entsprechende zeitliche Staffelung vorzunehmen seien, um die Liste während einer Pilotphase zu reduzieren.

Der Kanton SZ fordert, dass die Betreiberinnen elektronischer Patientendossiers gemäss Artikel 10 des Bundesgesetzes über das elektronische Patientendossier vom 19. Juni 2015 (SR 816.1) ebenfalls der Meldepflicht unterstellt werden.

Der Kanton UR schlägt zudem vor, dass zusätzlich zur Meldepflicht die Meldung von Cybervorfällen für alle weiteren Organisationen empfohlen werden sollte.

Die Grünen regen an, diesen Bereich auf die Demokratie (politische Parteien im Parlament und Politikerinnen und Politiker in relevanten Ämtern) oder auf Presseagenturen auszuweiten.

- **Zustimmung zu Artikel 74*b***

Der Verband **eGov-Schweiz, die Kantone AI, GR und BE** sowie **privatim** halten die vorgeschlagene Bestimmung für angemessen.

- **Ablehnung von Artikel 74*b***

VUD lehnt den vorliegenden Artikel wegen Unverhältnismässigkeit ab und schlägt stattdessen vor, die Meldepflicht von vornherein auf Cyberangriffe zu begrenzen, welche kritische Infrastrukturen im Sinne von Artikel 5 Bst. c ISG erheblich gefährden und deshalb von nationalem Interesse sind.

❖ Änderungsanträge und Bemerkungen zu Artikel 74*b*

- **Buchstabe b (Behörden)**

Der SSV verlangt, dass die Zuständigkeit für die Meldepflicht der Gemeindebehörden geklärt wird.

- **Buchstabe c (Blaulicht, Wasser, Abwasser, Abfall)**

Laut dem **Kanton AI** sollte eine Meldung reichen, wenn die kantonalen und die kommunalen Behörden den gleichen Informatikanbieter haben.

- **Buchstabe f (Digitale Dienste)**

Digitalswitzerland schlägt aus Gründen der Klarheit vor, den Begriff «Online-Marktplätze» aus dem obenstehenden Text zu streichen.

SwissICT beantragt, dass bei Buchstabe f die Ziffern 1, 2 und 3 besser definiert werden.

Swissmem erklärt sich mit der vorliegenden Bestimmung einverstanden, wünscht sich jedoch eine klarere Unterscheidung zwischen einer Betreiberin oder einer Anbieterin von Dienstleistungen und einer Betreiberin von Dateninfrastrukturen (Cloud-Dienste).

Migros spricht sich für eine technologieneutral formulierte Definition aus.

Switch sowie UniZH/UNIL NFP 77 verlangen, den extraterritorialen Aspekt dieser Bestimmung insbesondere hinsichtlich der Anwendung schweizerischen Rechts zu erörtern.

UniZH/UNIL NFP 77 wünschen sich mehr Details dazu, welche Anbieter von verwandten Telekommunikationsleistungen davon ebenfalls betroffen sind.

Der Kanton GE fordert eine präzisere Definition des Begriffs «Sicherheits- und Vertrauensdienste».

Switch beantragt, dass die Verwaltung von .ch-Domainnamen in diese Bestimmung aufgenommen wird.

Den Grünen und CH++ zufolge stellt die Anzahl Nutzende keine gute Kennzahl für die Bedeutung der Zielgruppe dar.

Die Grünen und CH++ verlangen, dass der Begriff «digital» aus Ziffer 2 gestrichen wird.

- **Buchstabe g (Spitäler)**

Der Kanton GL bittet um mehr Details dazu, welche Spitäler (Grösse der Infrastrukturen) als kritische Infrastrukturen gelten, und verlangt, dass die Plattformen für das EPD ebenfalls der Meldepflicht unterstellt werden.

- **Buchstabe i (Arzneimittel)**

Scienceindustries verlangt eine genaue Definition und eine spezifische Bezeichnung für die Unternehmen, die dieser Bestimmung unterstellt sind.

- **Buchstabe j (Sozialversicherungen)**

Inter-pension ist der Ansicht, dass der Begriff «Sozialversicherungen» in der beruflichen Vorsorge (überobligatorische Leistungen) nicht klar definiert sei.

- **Buchstabe k (Fernmeldedienste)**

UniZH/UNIL NFP 77 legen nahe, dass dieser Artikel einen extraterritorialen Aspekt umfasse, weshalb die Anwendung schweizerischen Rechts vorzusehen sei (siehe z. B. die Theorie betreffend

die Auswirkungen gemäss Art. 3 revDSG). **SuisseDigital** weist darauf hin, dass Over-the-Top (OTT) Dienste keine Anbieterinnen von Fernmeldediensten sind. Es sind Präzisierungen nötig.

- **Buchstabe p (Zivilluftfahrt)**

AEROSUISSE sowie die Flughäfen GE und ZH fordern, dass der Text so angepasst wird, dass er die Liste der Fluggesellschaften, die der Meldepflicht unterstehen, nicht auf diejenigen reduziert, die über eine Bewilligung des Bundesamtes für Zivilluftfahrt verfügen.

- **Buchstabe r (Grundversorgung)**

Migros verlangt, dass einfach messbare Kriterien wie die Anzahl Mitarbeitende oder der Umsatz eingeführt wird, für die gewisse Erleichterungen oder Ausnahmen direkt im Gesetz vorgesehen werden.

Der Kanton GE und TPG fordern, in der französischen Fassung des Gesetzestextes den Begriff «chiffrage» anstelle von «cryptage» zu verwenden.

- **Buchstabe s (Hersteller Hard- und Software)**

Die Grünen und CH++ erachten die vorgeschlagene Bestimmung als angemessen und schlagen vor, die Lieferketten zu erwähnen.

eAHV findet, dass auch die Informationstechnologiehersteller der Exekutive zu erwähnen seien, deren Situation hier nicht klar definiert sei.

Economiesuisse vertritt die Meinung, dass die Tatsache, dass die Hersteller im vorliegenden Text erwähnt würden, die Unklarheit in Bezug auf die Instanzen, die der Meldepflicht unterständen, verstärke.

Der SSV macht sich Sorgen bezüglich der Anwendbarkeit dieser Bestimmung, insbesondere weil viele Hardware- und Softwarehersteller keinen Sitz in der Schweiz hätten.

Swico schlägt vor, die Ziffern 1–4 aus der Bestimmung zu streichen und stattdessen den Begriff «Fernwartungszugang» zu definieren, um damit auch die Lieferkettenproblematik zu lösen.

SwissICT verlangt hier eine Präzisierung, dass die Hersteller, die Software als Dienstleistung (SaaS) anbieten, keine kritischen Infrastrukturen betreiben.

Swissmem verlangt die Streichung von Artikel 74*b* Buchstabe s.

3.3.2.11 Artikel 74*c* Ausnahmen von der Meldepflicht

Der Bundesrat nimmt bestimmte Kategorien von Betreiberinnen von kritischen Infrastrukturen von der Meldepflicht aus, wenn durch Cyberangriffe auf ihre Infrastrukturen ausgelöste Funktionsausfälle oder Fehlfunktionen:

a. unwahrscheinlich sind, insbesondere wegen einer geringen Abhängigkeit von Informatikmitteln; oder
b. nur geringe Auswirkungen auf das Funktionieren der Wirtschaft beziehungsweise das Wohlergehen der Bevölkerung haben, insbesondere, weil sie:
   1. nur eine geringe Anzahl Personen betreffen,
   2. von anderen kritischen Infrastrukturen aufgefangen werden, oder
   3. nur ein geringes volkswirtschaftliches Schadenspotenzial haben.

Insgesamt 20 Vernehmlassungsteilnehmende haben sich zu den Ausnahmen geäussert. Es handelte sich dabei mehrheitlich um allgemeine Bemerkungen und um viele Anträge zur Anpassung der Formulierung dieses Artikels. Nur 5 Vernehmlassungsteilnehmende haben sich gegen die Aufnahme der Bestimmung in das Gesetz ausgesprochen.

❖ **Allgemeine Bemerkungen zu Artikel 74*c***

Swiss Banking beantragt, dass dieser Artikel wie folgt geändert wird: «Der Bundesrat legt auf Verordnungsstufe klare Kriterien fest, anhand derer die Infrastrukturen meldepflichtig werden. Sinn dieser Kriterien ist es, jene Betreiberinnen kritischer Infrastrukturen von der Meldepflicht auszunehmen, bei denen durch Cyberangriffe ausgelöste Funktionsausfälle oder Fehlfunktionen …».

SuisseDigital verlangt, dass die Ausnahmebestimmungen präziser definiert werden.

Swico erachtet die in diesem Artikel erwähnten Kriterien als schwer umsetzbar und beantragt, sie durch folgendes Kriterium zu ersetzen: «das Ausmass des Einflusses einer Beeinträchtigung». Zudem würde **Swico** dem vorliegenden Artikel einen weiteren Buchstaben hinzufügen: «c. weil mitigierende Massnahmen solche Cyberangriffe unschädlich machen».

VUD hält die Bestimmungen von Artikel 74*c* Buchstaben a und b für widersprüchlich oder unklar und verlangt eine Präzisierung, insbesondere für folgende Sätze: «… wegen einer geringen Abhängigkeit von Informatikmitteln …» und «… nur geringe Auswirkungen auf das Funktionieren der Wirtschaft beziehungsweise das Wohlergehen der Bevölkerung haben …».

Der Kanton BE beantragt das Einfügen einer zusätzlichen Bestimmung in den vorliegenden Text:
« Art. 74c^{bis} Bestimmungen des kantonalen Rechts
Die Kantone können
a. nach Anhörung des NCSC unter den Voraussetzungen des Artikels 74c kantonale oder kommunale Behörden oder Träger öffentlicher Aufgaben von der Meldepflicht ausnehmen,
b. die für die Meldung verantwortlichen Personen der kantonalen oder kommunalen Behörden oder Träger öffentlicher Aufgaben bestimmen.»

Migros bedauert das Fehlen einer risikobasierten Regelung.

Der Kanton LU und Switch beantragen, dass die kleinen Organisationen von der Meldepflicht befreit werden, da dieser Prozess laut dem **Kanton LU** zu kostenintensiv ist.

- **Zustimmung zu Artikel 74*c***

eGov-Schweiz und die Kantone AI und NW erachten diesen Artikel als angemessen.

- **Ablehnung von Artikel 74*c***

Die Grünen, CH++, Operation Libero sowie die Kantone TG und UR verlangen die Streichung dieses Artikels.

- **Änderungsanträge und Anregungen zu Artikel 74*c***

- **<u>Buchstabe a</u>**

Den Grünen, Operation Libero und Pour Demain zufolge scheint im 21. Jahrhundert eine geringe Abhängigkeit von Informatikmitteln immer weniger wahrscheinlich zu sein. Buchstabe a sei daher zu streichen.

Der Kanton GE vertritt die Meinung, dass diese Bestimmung im Widerspruch zum Datenschutzgesetz stehe.

- **<u>Buchstabe b</u>**

Laut **VUD** ist einzig und allein ausschlaggebend, ob ein Cyberangriff die nationale Sicherheit stark beeinträchtigt.

Dem Kanton GE zufolge widerspricht diese Bestimmung dem Zweck von Artikel 74*b,* der die Organisationen mit grosser Bedeutung aufführt.

Migros erachtet die in Buchstabe b vorgesehene Ausnahme als nicht praktikabel.

3.3.2.12 Artikel 74*d* Zu meldende Cyberangriffe

[1] Ein Cyberangriff auf eine kritische Infrastruktur muss gemeldet werden, wenn Anzeichen dafür bestehen, dass:

a. die Funktionsfähigkeit der betroffenen kritischen Infrastruktur oder einer anderen kritischen Infrastruktur gefährdet ist;
b. ein fremder Staat ihn ausgeführt oder veranlasst hat;
c. er zu einem Abfluss oder zur Manipulation von Informationen geführt hat oder führen könnte; oder
d. er länger als 30 Tage unentdeckt blieb.

[2] Ein Cyberangriff auf eine kritische Infrastruktur muss immer gemeldet werden, wenn er mit Erpressung, Drohung oder Nötigung gegenüber der Betreiberin einer kritischen Infrastruktur oder ihren Mitarbeitenden verbunden ist.

Die Definition der zu meldenden Cyberangriffe hat viele Reaktionen hervorgerufen, hauptsächlich allgemeine Bemerkungen oder konkrete Änderungsanträge.
Insgesamt 36 Teilnehmende haben sich geäussert, wovon sich 1 Stelle ausdrücklich für die Einführung dieser Gesetzesbestimmung ausgesprochen hat. 4 Teilnehmende lehnen den Artikel hingegen klar ab.

- **Allgemeine Bemerkungen zu Artikel 74*d***

AEROSUISSE erachtet es für die Rechtssicherheit der betroffenen Unternehmen als notwendig, klar festzulegen, dass Artikel 74*d* als Kriterium definiert, wann ein Angriff auf eine kritische Infrastruktur gemeldet werden muss.

Economiesuisse, eGov-Schweiz, der Kanton ZH, SuisseDigital und Santésuisse finden, dass dieser Artikel zwingend überarbeitet werden müsse, insbesondere weil die Kriterien zu weit gefasst und für die Unternehmen nur schwer fassbar oder anwendbar seien. So wäre es **economiesuisse** zufolge sinnvoller, eine kürzere (Positiv-)Liste der zu meldenden Vorfälle zur Verfügung zu stellen und die Meldepflicht auf erfolgreiche oder besonders schwerwiegende Versuche zu beschränken.

Der **Kanton GR** verlangt eine klare Liste der zu meldenden Fälle.

ISSS, Härting Rechtsanwälte und UniZH/UNIL NFP 77 fordern einen anderen Titel für diesen Artikel: «Zu meldende Cyberangriffe – und Vorfälle»

Privatim spricht sich für eine präzisere Definition aus, was unter «schwerwiegend» zu verstehen sei, vor allem da hier implizit gemeint sei, dass Vorfälle gemeldet werden müssten, auch wenn ihr Schweregrad noch nicht ermittelt werden könne. Sollte das NCSC also feststellen, dass es sich nicht um einen schwerwiegenden Sicherheitsvorfall handelt und keine Zustimmung der betreffenden Person(en) vorliegt, müssten die Personendaten unverzüglich gelöscht oder anonym verarbeitet werden.

Scienceindustries verlangt, im Text explizit anzugeben, dass sich die Meldepflicht auf Angriffe auf Anlagen in der Schweiz beschränkt und keine Anlagen im Ausland betrifft. **UniZH/UNIL NFP 77** fordern hingegen, dass diese Bestimmung auch die Anlagen im Ausland abdeckt.

Coop ist der Meinung, dass die vorgeschlagene Definition zu allgemein sei und keine klare Unterscheidung zulasse zwischen Vorfällen, die sich nicht oder nur wenig auf die Geschäftstätigkeit auswirkten, und solchen, die direkt den Betrieb kritischer Infrastrukturen betreffen oder ein hohes Risiko darstellen würden. Zudem sei nicht klar, welche der erfolgreichen oder fehlgeschlagenen Cyberangriffe zu melden seien.

Der Flughafen ZH fordert, nur erfolgreiche Cyberangriffe der Meldepflicht zu unterstellen.

Laut dem **Kanton AG** sollte das NCSC die Triage der zu meldenden Angriffe vornehmen. Denn auch «unwichtige» Meldungen könnten sich als wichtig erweisen.

❖ Zustimmung zu Artikel 74*d*

Der **VSE** spricht sich für diese Bestimmung aus.

❖ Ablehnung von Artikel 74*d*

Swiss Banking und Raiffeisen beantragen die Streichung dieses Artikels und schlagen vor, ihn durch einen mit der Formulierung der FINMA kompatiblen Wortlaut zu ersetzen: «Zu melden sind Cyberangriffe mit erheblichen Auswirkungen auf die Geschäftstätigkeit des Unternehmens, insbesondere erfolgreiche oder teilweise erfolgreiche Angriffe auf kritische Funktionen, deren Ausfall oder Störung den Schutz der Kundinnen und Kunden oder das Funktionieren der Märkte stark beeinträchtigen würde.»

SwissICT fordert die Streichung dieser Bestimmung, da praktisch jeder Cyberangriff zu melden sei.

VUD zufolge ist die gesetzgeberische Lösung, wonach die zu meldenden Ereignisse breit gefasst werden (Art. 5 Bst. d und e ISG), nur um die Meldepflicht danach wieder zu begrenzen (Art. 74*d* ISG), abzulehnen und der Artikel zu streichen.

❖ Änderungsanträge und Anregungen zu Artikel 74*d*

- **<u>Zu Absatz 1</u>**

Laut **ISSS** widerspricht die Tatsache, dass die Anzeichen für einen Cyberangriff gemäss Artikel 74*d* bereits der Meldepflicht unterstehen, der *ratio legis.* Die vorliegende Bestimmung sei wie folgt zu ändern: «[1] Ein Cyberangriff oder ein Cybervorfall auf eine kritische Infrastruktur muss gemeldet werden, wenn die ernsten Befürchtungen bestehen, dass:».

- **<u>Zu Absatz 1 Buchstabe a</u>**

Swissmem fordert, diese Bestimmung wie folgt zu ersetzen: «die Funktionsfähigkeit der betroffenen kritischen Infrastruktur oder einer anderen kritischen Infrastruktur wesentlich gefährdet ist;».

Da die Unternehmen häufig nicht in der Lage seien, eine Bedrohung zu beurteilen, sind **die Flughäfen GE und ZH, Swissgrid, santésuisse sowie der Kanton GE** der Ansicht, dass der folgende Text zu streichen sei: «oder einer anderen kritischen Infrastruktur».

- **<u>Zu Absatz 1 Buchstabe b</u>**

Economiesuisse, Coop, IG eHealth, Switch, der Kanton TG, ISSS, der Flughafen ZH, Axpo, UniZH/UNIL NFP 77, Scienceindustries, VUD, VöV und RAILplus stellen die Relevanz dieser zweiten Bedingung infrage, weil Cyberangriffe, die von Staaten ausgingen, häufig zu komplex seien, um überhaupt erkannt zu werden, und ihre Zuordnung ein politisches und kompliziertes Vorgehen darstelle. Daher beantragen **ISSS, Flughafen ZH, Axpo, UniZH/UNIL NFP 77, Scienceindustries, VUD, VöV und RAILplus** die Streichung dieser Bedingung. **RAILplus** schlägt vor, sie durch ein kumulatives Kriterium im Zusammenhang mit den Auswirkungen zu ersetzen (Beispiel: «Anzahl betroffener Nutzender oder Systeme»).

- **<u>Zu Absatz 1 Buchstabe c</u>**

Swissgrid ist der Meinung, dass die folgenden Punkte weiter ausgeführt werden müssten: «besonders schützenswerte Personendaten», «Informationen zu den kritischen Systemen», «Daten des Stromnetzbetriebs», «Infrastrukturen» und «Systeme des Kernbetriebs».

- **<u>Zu Absatz 1 Buchstabe d</u>**

Economiesuisse, der Flughafen ZH, SVV, VUD und Coop erachten die Frist von 30 Tagen als nicht sinnvoll.

IG eHealth beantragt, Punkt d (Cyberangriff bleibt länger als 30 Tage unentdeckt) keiner Meldepflicht zu unterstellen, wenn die Punkte a (Funktionsfähigkeit gefährdet) und c (möglicher Abfluss

oder zur Manipulation von Informationen) nicht erfüllt sind, d. h., der Angriff eine Bagatelle war oder einen tiefen bis mittleren Schweregrad aufwies.

Der SVV erachtet die Frist als nicht realistisch, weil dies implizieren würde, dass man auf einen Angriff reagieren müsste, von dem man noch keine Kenntnis habe und von dem man allenfalls nicht wissen könne, wann er eingetreten sei. Der **SVV** schlägt vor, Punkt d wie folgt zu ersetzen: «über einen längeren Zeitraum unentdeckt blieb».
Der Kanton TG beantragt, den vorliegenden Text wie folgt zu ersetzen:
«d. die direkt und unmittelbar für das Ziel des Cyberangriffs verwendeten Instrumente länger als 30 Tage unentdeckt blieben».

Migros sowie UniZH/UNIL NFP 77 zufolge sollte eine Zeitspanne für die «Nicht-Entdeckung» kein Einzel-Kriterium für eine Meldung darstellen.

- **<u>Zu Absatz 2</u>**

Laut **Scienceindustries** ist die Meldepflicht auf Erpressungen, Bedrohungen oder Zwang dahingehend zu beschränken, dass sie nur bei Vorliegen eines Bezuges zur Geschäftstätigkeit wirksam wird.

Der **SSV** ist der Ansicht, dass die abschliessend formulierte Aufzählung die Frage aufwirft, ob die Meldepflicht nicht auch dann gelten solle, wenn ein Cyberangriff mit Erpressung, Drohung oder Nötigung gegenüber Kunden und Kundinnen oder Patienten und Patientinnen einer Betreiberin verbunden sei.

Der Kanton BL beantragt, den Text zu ergänzen und den Tatbestand der Datenbeschädigung, der durch Verschlüsselung oder das Einschleusen von Malware verursacht wird, einzuschliessen.

Der Kanton GE weist darauf hin, dass die Institutionen, die gegen diesen Artikel verstossen, doppelt bestraft werden könnten.

UniZH/UNIL NFP 77 schlagen vor, den Text so zu ändern, dass eine Meldepflicht besteht, sobald «strafrechtlich relevante Handlungen» vorliegen statt nur bei Erpressungen.

3.3.2.13 Artikel 74*e* Inhalt der Meldung

[1] Die Meldung muss Informationen zur kritischen Infrastruktur, zur Art und Ausführung des Cyberangriffs, zu seinen Auswirkungen und zum geplanten weiteren Vorgehen der Betreiberin der kritischen Infrastruktur enthalten.
[2] Sind zum Zeitpunkt der Meldung nicht alle erforderlichen Informationen bekannt, so ergänzt die Betreiberin der kritischen Infrastruktur die Meldung, sobald sie an neue Informationen gelangt.

15 Vernehmlassungsteilnehmende haben sich zu dieser Bestimmung geäussert. Die meisten Anträge zum Gesetzestext betreffen die Klärung und eine detailliertere Beschreibung der Informationen, die nach Artikel 74*e* verlangt werden.

- ❖ **Allgemeine Bemerkungen zu Artikel 74*e***

Die Grünen sind der Meinung, dass Artikel 74*e* so zu überarbeiten sei, dass eine Automatisierung der Meldungen möglich sei.

Der Verband der Auslandbanken in der Schweiz findet, dass es möglich sein sollte, die Meldungen auf Englisch und in den Amtssprachen zu verfassen.

Economiesuisse fordert, dass die Anforderungen an die Meldung einfach bleiben müssen, um die Hindernisse für die Unternehmen zu minimieren. Zudem müssten die zu meldenden Fälle klar abgegrenzt werden.

SwissICT, die Post sowie die Kantone GR und TG verlangen eine präzisere Beschreibung der im Rahmen von Artikel 74*e* geforderten Informationen, evtl. mithilfe einer Liste.

SwissICT und die Post fordern, dass die gemäss Artikel 74*e* verlangten Informationen mit anderen Behörden abgestimmt werden (z. B. mit der FINMA).

Laut **Axpo** muss die Meldung unabhängig vom Informationsniveau umgehend erfolgen.

❖ **Zustimmung zu Artikel 74*e***

Swiss Banking begrüsst diese Bestimmung.

❖ **Änderungsanträge und Anregungen zu Artikel 74*e***

- **<u>Zu Absatz 1</u>**

ISSS und Härting Rechtsanwälte verlangen, dass die vorliegende Bestimmung wie folgt geändert wird: «Die Meldung muss Informationen zur kritischen Infrastruktur, zur Art und Ausführung des Cyberangriffs, des Cybervorfalles, zu seinen Auswirkungen und zum geplanten weiteren Vorgehen der Betreiberin der kritischen Infrastruktur enthalten».

Der Kanton GE beantragt, «und zum geplanten weiteren Vorgehen der Betreiberin der kritischen Infrastruktur» durch «oder zu den von der betroffenen Einrichtung bereits eingeleiteten Schritten» zu ersetzen.

UniZH/UNIL NFP 77 beantragen ebenfalls eine Änderung der Bestimmung wie folgt: «… oder zu den bereits eingeleiteten oder geplanten Schritten».

- **<u>Zu Absatz 2</u>**

Der Kanton GE beantragt, die vorliegende Bestimmung so zu ändern, dass die Meldung nicht nur durch die Betreiberin zu ergänzen ist, sobald sie an neue Informationen gelangt, sondern auch wenn solche Informationen eingeholt werden können.

3.3.2.14 Artikel 74*f* Übermittlung der Meldung

[1] Für die elektronische Meldung von Cyberangriffen stellt das NCSC ein sicheres System zur Übermittlung der Meldung an das NCSC zur Verfügung.

[2] Das System muss der Betreiberin einer kritischen Infrastruktur ermöglichen, die Meldung des Cyberangriffs oder seiner Auswirkungen gesamthaft oder in Teilen an weitere Stellen und Behörden zu übermitteln.

[3] Benötigt eine Stelle oder Behörde Informationen, die über Art. 74e hinausgehen, kann die Betreiberin diese über das System direkt an die betreffende Stelle oder Behörde übermitteln.

34 Teilnehmende haben sich zum Artikel 74*f* geäussert, wovon 4 (RAILplus, santésuisse, UniBE und die Post) den Text in der vorliegenden Form annehmen. Der Text wurde von keiner Stelle vollumfänglich abgelehnt. Die meisten Diskussionen betrafen die Zentralisierung der Übermittlungskanäle für die Informationen an das NCSC und an die im Gesetz bezeichneten Behörden.

❖ **Allgemeine Bemerkungen zu Artikel 74*f***

CH++ findet, dass in Artikel 74*f* explizit zu erwähnen sei, dass die Datenübermittlung über eine gesicherte Schnittstelle erfolge. Zudem sei ein API-basierter Ansatz, wie er von den Partnernetzwerken von Meta/Facebook oder AT&T erfolgreich praktiziert werde, durch das NCSC weiter zu verfolgen. Diesbezüglich sei eine geeignete Rechtsgrundlage zu schaffen.

Pour Demain und Operation Libero sind der Meinung, dass auch eine Informatikschnittstelle (API) für die Übermittlung automatisierter Meldungen an das NCSC zu erstellen sei.

Der SVV, swissuniversities, der Kanton ZH und Swico fordern, dass die Meldung in einer einfachen Form erfolgen kann.

Der Kanton GR verlangt eine Klarstellung, welche Informationen übermittelt werden, an welche Behörden sie gehen und wer sie einsehen kann.

UniZH/UNIL NFP 77 fordern, dass die Behörden keinen Zugriff auf Informationen haben sollen, die für andere Stellen bestimmt sind.

Swico verlangt einen möglichst freien Meldemechanismus, um etwa automatische Meldungen über RSS- oder API-Feeds oder über den bestehenden Datenaustausch über das System MISP zu ermöglichen, über die viele kritische Infrastrukturen verfügen. Zudem fordert **Swico,** dass der bestehende Kanal für die Übermittlung von Informationen zwischen GovCERT und den kritischen Infrastrukturen weiterhin für die Meldung von Cyberangriffen an das NCSC genutzt werden können sollte.

SwissICT ist der Ansicht, dass die Übermittlung von Informationen an andere Behörden neben dem NCSC nur für die Behörden eine Pflicht sei, nicht aber für die Unternehmen.

Raiffeisen begrüsst diese Bestimmung und wünscht die Ergänzung um folgenden Absatz: «Dieses System ist auch von den Bundesbehörden zu benutzen, die Meldepflichten im Zusammenhang von Cyberangriffen etablieren.»

Swissgrid verlangt, dass das System eine gleichzeitige Übermittlung von Meldedaten an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) erlaubt.

Switch fordert, dass die Meldungen ebenfalls über eine gemeinsame Sektor-CERT erfolgen können. Da dies vom Gesetz nicht explizit ausgeschlossen werde, gehe **Switch** davon aus, dass die betreffenden Organisationen die Freiheit hätten, sich entsprechend zu organisieren.

- **Zustimmung zu Artikel 74*f***

RAILplus, santésuisse, UniBE und die Post begrüssen den vorliegenden Text, insbesondere die Möglichkeit, Informationen über eine gesicherte Plattform zu übermitteln, die den höchsten Sicherheitsstandards entspricht, sowie die Tatsache, dass auch andere Mittel für die Meldung verwendet werden können, namentlich das bestehende Formular des NCSC, E-Mail oder Telefon.

- **Änderungsanträge und Anregungen zu Artikel 74*f***

- **<u>Zu Absatz 1</u>**

Der Kanton GE fordert, dass auf die Kostenlosigkeit des Systems hingewiesen wird.

- **<u>Zu Absatz 2</u>**

Der Verband der Auslandbanken in der Schweiz, Swiss Banking, die Grünen, CH++, asut, ISSS und GLP vertreten die Ansicht, dass bei der Umsetzung sicherzustellen sei, dass die Meldepflichten, die sich überlappen würden (DSG, FINMA usw.), durch ein einziges Meldeverfahren abgedeckt werden müssten. **GLP, VSE, digitalswitzerland, economiesuisse und die Digitale Gesellschaft** gehen noch weiter und schlagen die Einrichtung einer eidgenössischen Meldestelle vor, bei der sämtliche Meldepflichten mit einem einzigen Onlineformular erfüllt werden können.

ISSS und Härting Rechtsanwälte begrüssen die Schaffung einer einzigen Stelle im Rahmen der obigen Bestimmung, verlangen jedoch Klarstellungen, an wen welche Informationen weitergegeben werden dürfen und mit welchem Inhalt. So sei etwa nicht klar, ob Meldungen an das NCSC, die an den EDÖB weitergeleitet würden, ebenfalls unter dem Vorbehalt der Nichtbelastung im Strafverfahren nach Artikel 24 Absatz 6 revDSG fallen würden oder nicht. Da gemäss Artikel 74*g* das NCSC weitere Auskünfte verlangen könne, erweitere dies sodann den Umfang der Kommunikation gegenüber Dritten. Eine solche, oft auch sehr informelle Kommunikation auf technischer

Ebene solle nicht Gegenstand eines Strafverfahrens nach dem revDSG werden können, wenn denn Personendaten involviert seien. Es brauche folglich eine detailliertere Regelung, mit wem welche Informationen geteilt werden könnten und welche Konsequenzen dies haben könne oder eben nicht habe.

UniZH/UNIL NFP 77 weisen darauf hin, dass Artikel 73*c* anzupassen und ein expliziter Verweis aufzunehmen sei, wenn effektiv die Absicht bestehe, Artikel 73*c* Absätze 1, 2 und 3 E-ISG auf die Meldungen von Cyberangriffen anzuwenden. Dies diene dazu, dass das NCSC die Informationen bei Fällen gemäss Artikel 73*c* Absätze 1 und 2 rechtmässig an andere Behörden weiterleiten dürfe.

- **Zu Absatz 3**

ISSS und Härting Rechtsanwälte verlangen, dass dieser Absatz gestrichen wird, um sicherzustellen, dass andere Stellen und Behörden nur die Informationen erhalten, die sie rechtlich erhalten dürfen oder die im Rahmen des Zwecks der zugrunde liegenden Gesetzgebung gerechtfertigt sind.

Der Kanton GE beantragt, dass der Absatz verdeutlicht, dass die Stelle oder Behörde die betreffenden Informationen «berechtigterweise» benötigt.

3.3.2.15 Artikel 74*g* Auskunftspflicht

Die Betreiberin der kritischen Infrastruktur muss dem NCSC ergänzende Auskünfte zu den Inhalten der Meldung nach Artikel 74*e* erteilen, die es zur Erfüllung seiner Aufgaben in Bezug auf die Abwehr weiterer Cyberangriffe auf kritische Infrastrukturen benötigt.

9 Vernehmlassungsteilnehmende haben sich zu diesem Artikel geäussert; keiner hat dem Artikel in der vorliegenden Form zugestimmt.

- **Allgemeine Bemerkungen zu Artikel 74*g***

Laut **ISSS und Härting Rechtsanwälte** erweitert diese Bestimmung den Umfang der Kommunikation gegenüber Dritten. Es sei daher festzulegen, wie weit eine Auskunftspflicht gehen könne.

Scienceindustries ist der Meinung, dass die ergänzenden Auskünfte, die das NCSC einfordern dürfe, klar festzulegen sind.

SwissICT vertritt die Ansicht, dass die ergänzenden Informationen während eines Angriffs nur dann eingeholt werden dürften, wenn dies für die Sicherheit der jeweiligen Versorgung zwingend notwendig sei, um die Unternehmen, Institutionen, Behörden und Gemeinden in schwierigen Zeiten nicht noch mehr zu belasten.

Der **Kanton TG** verlangt eine nuanciertere Formulierung dieses Artikels, um es den Kantonen zu erlauben, auch ihre eigenen IT-Sicherheits-Richtlinien einzuhalten.

UniBE fordert Klarstellungen in Bezug auf die Erwartungen hinsichtlich des Inhalts und der zeitlichen Vorstellungen im Zusammenhang mit dieser Pflicht.

- **Ablehnung von Artikel 74*g***

VUD erachtet diese Bestimmung als zu vage und würde sie ersatzlos streichen, da der Inhalt dieser Meldung in Artikel 74*e* schon abschliessend geregelt sei.

- **Änderungsanträge und Anregungen zu Artikel 74*g***

Scienceindustries beantragt, die Bestimmung wie folgt zu ändern: « … kritischen Infrastruktur erteilt, wenn möglich, dem NCSC ergänzende Auskünfte zu den Inhalten der Meldung nach Artikel 74*e*, die ...».

Der **Kanton GE** verlangt, dass die Auskünfte dem NCSC «sobald wie möglich» zu erteilen seien.

3.3.2.16 Artikel 74*h* Verletzung der Melde- oder Auskunftspflicht

[1] Bestehen Anzeichen für eine Verletzung der Melde- oder Auskunftspflicht, so informiert das NCSC die Betreiberin der kritischen Infrastruktur darüber.

[2] Kommt die Betreiberin trotz dieser Information ihrer Pflicht nicht nach, so erlässt das NCSC eine Verfügung über die umzusetzenden Pflichten, setzt ihr darin eine Frist und verweist auf die Bussandrohung nach Artikel 74*i*.

Nur 4 Vernehmlassungsteilnehmende haben sich mit der Frage der Verletzung der Melde- oder der Auskunftspflicht auseinandergesetzt.

❖ Zustimmung zu Artikel 74*h*

Centre Patronal begrüsst den vorliegenden Gesetzestext.

❖ Ablehnung von Artikel 74*h*

Scienceindustries, Flughafen GE und **Digitalswitzerland** sprechen sich gegen diesen Artikel aus, da eine Meldepflicht ihrer Meinung nach ein Unternehmen dazu bringen könnte, gegen die Datenschutzgesetzgebung im Land, wo es seinen Sitz hat, zu verstossen oder die Auskunftspflicht in der Schweiz zu verletzen.

❖ Änderungsanträge und Anregungen zu Artikel 74*g*

UniZH/UNIL NFP 77 verlangt, dass dieser Artikel den betreffenden Institutionen das rechtliche Gehör gewähren muss.

3.3.2.17 Artikel 74*i* Widerhandlungen gegen Verfügungen des NCSC

[1] Mit Busse bis zu 100 000 Franken wird bestraft, wer einer vom NCSC unter Hinweis auf die Strafdrohung dieses Artikels erlassenen rechtskräftigen Verfügung oder dem Entscheid einer Rechtsmittelinstanz vorsätzlich nicht Folge leistet.

[2] Bei Widerhandlungen in Geschäftsbetrieben ist Artikel 6 des Bundesgesetzes vom 22. März 1974[3] über das Verwaltungsstrafrecht (VStrR) anwendbar.

[3] Fällt eine Busse von höchstens 20 000 Franken in Betracht und würde die Ermittlung der nach Artikel 6 VStrR strafbaren Personen Untersuchungsmassnahmen bedingen, die im Hinblick auf die verwirkte Strafe unverhältnismässig wären, so kann die Behörde von einer Verfolgung dieser Personen absehen und an ihrer Stelle den Geschäftsbetrieb zur Bezahlung der Busse verurteilen.

[4] Bei einer Widerhandlung gegen eine Verfügung des NCSC obliegt die Verfolgung und die Beurteilung den Kantonen.

30 der Vernehmlassungsteilnehmenden haben sich zu diesem Artikel geäussert, 13 davon haben die Streichung beantragt.

❖ Allgemeine Bemerkungen zu Artikel 74*i*

Den Grünen und CH++ zufolge soll der Artikel die Tatsache, dass die vorgesehenen Sanktionen auf Ebene der Leitung der Organisationen und nicht auf Ebene der Fachpersonen zum Tragen kommen, expliziter erläutern.

RAILplus schlägt vor, dass nur juristische Personen bestraft werden können sollten (unabhängig von der Höhe der Sanktion). Zudem verlangt **RAILplus,** dass die Situationen geregelt werden, in denen die Subunternehmer im Ausland ansässig sind.

[3] SR **313.0**

Die Piratenpartei und der Kanton GE erklären, dass der Gesetzgeber zur Sicherstellung verhältnismässiger Bussen die Abstufung im Verhältnis zum Umsatz des Unternehmens festlegen müsse (z. B. 4 % des Jahresumsatzes).

Die SP erachtet die Massnahmen in Artikel 74*i* als sinnvoll. Allerdings sei nach fünf Jahren zu prüfen, ob die in Artikel 74*i* genannten Sanktionsmöglichkeiten ausreichen würden und ob die Grundsätze der Gleichbehandlung und der Verhältnismässigkeit eingehalten worden seien.

Die Kantone SO und UR verlangen, dass eine Busse erst nach (schriftlicher) Konsultation des NCSC mit dem Urheber des Verstosses ausgesprochen wird.

UniZH/UNIL NFP 77 erachten die Höhe der Busse nicht als abschreckend, insbesondere im Vergleich zur Höhe gemäss DSG.

❖ **Ablehnung von Artikel 74*i***

AEROSUISSE, die Post, Raiffeisen, Swisscom, Sunrise, Switch, Coop, asut, economiesuisse, SuisseDigital, Scienceindustries, digitalswitzerland, Swico, ISSS, Härting Rechtsanwälte, Swiss Banking, Flughfen GE und Helvetia Versicherungen erachten die Durchsetzung der neuen Pflichten durch Strafbestimmungen als nicht sinnvoll und lehnen diese prinzipiell ab.

Des Weiteren sind **scienceindustries, die Kantone SO und TG, VöV und SGV** der Meinung, dass der Höchstbetrag der verhängten Bussen auf administrativer Ebene eine Gefahr für die Existenz darstelle, weil übertrieben hohe und unverhältnismässige Bussen drohen würden, besonders für kleine und mittelgrosse Unternehmen.

❖ **Änderungsanträge und Anregungen zu Artikel 74*i***

- **<u>Zu Absatz 1</u>**

Der VöV beantragt, den Text wie folgt zu ändern: «Mit Busse bis zu [*10 000*] Franken wird bestraft …».

- **<u>Zu Absatz 3</u>**

SwissICT findet, dass der Betrag von CHF 20 000 auf CHF 50 000 angehoben werden müsse. Einerseits würde dies in unwichtigen Fällen unverhältnismässige Ermittlungskosten vermeiden und andererseits würde dies es erlauben, sich im Rahmen von Artikel 64 Absatz 2 revDSG zu bewegen.

Der VöV beantragt, den Text wie folgt zu ändern: «Fällt eine Busse von höchstens [*5000*] Franken in Betracht ...».

3.3.2.18 Artikel 75 Bearbeitung von Personendaten

[1] Das NCSC kann zur Erfüllung seiner Aufgaben Personendaten bearbeiten, einschliesslich Adressierungselementen nach Artikel 3 Buchstabe f FMG[4] und damit zusammenhängenden besonders schützenswerte Personendaten, die Informationen enthalten über:

a. religiöse, weltanschauliche oder politische Ansichten enthalten; die Bearbeitung ist nur zulässig, wenn sie für die Bewertung von konkreten Bedrohungen und Gefahren im Bereich der Cybersicherheit erforderlich ist;

b. administrative oder strafrechtliche Verfolgungen und Sanktionen enthalten.

4 SR **784.10**

[2] Es kann die Personendaten bearbeiten, ohne dass dies für die betroffenen Personen erkennbar ist, falls sonst der Zweck der Bearbeitung gefährdet wäre oder die Information der betroffenen Person nur mit unverhältnismässigem Aufwand erreicht werden könnte.

[3] Liegen konkrete Hinweise auf den Missbrauch einer Identität oder auf die unberechtigte Verwendung von Adressierungselementen vor, so informiert es die Personen, deren Identität oder Adressierungselemente missbraucht werden; vorbehalten bleiben die Artikel 18a Absatz 4 Buchstabe b und 18b DSG[5].

Keine der befragten Instanzen wollte den Artikel in seiner jetzigen Form beibehalten.

❖ **Allgemeine Bemerkungen zu Artikel 75**

Privatim spricht sich für diesen Artikel aus, fragt sich aber, ob die Verarbeitung mit anonymisierten Daten erfolgen soll, wenn Daten ohne Personenbezug ausreichen.

Scienceindustries fordert, dass mögliche Konflikte mit der ausländischen Datenschutzgesetzgebung bei der Übermittlung von Personendaten berücksichtigt und rechtlich geregelt werden.

Die Post verlangt, dass die Verarbeitung vertraulicher Daten genauer geregelt wird, damit die Vertraulichkeit der Meldungen gewährleistet ist.

Swisscom und die Post verlangen im Zuge der vorliegenden Revision des ISG die Einführung einer Ausnahmeregelung, die im Sinne eines *lex specialis* Vorrang vor dem Öffentlichkeitsprinzip nach BGÖ hat.

Raiffeisen ist der Ansicht, dass die Meldungen gemäss der neuen Regelung das Berufsgeheimnis wahren müssten, und schlägt vor, einen Absatz hinzuzufügen: «Weitergegebene Informationen sind durch die Empfängerbehörde vertraulich zu behandeln. Sie dürfen nicht weitergegeben werden, wenn dadurch die Sicherheit des betroffenen Unternehmens oder der betroffenen Personen gefährdet würde.»

❖ **Ablehnung von Artikel 75**

Der **Kanton TG** vertritt die Meinung, dass das NCSC keinen Zugang zu Personendaten haben solle, und lehnt diesen Artikel daher ab.

❖ **Änderungsanträge und Anregungen zu Artikel 75**

- **<u>Zu Absatz 1</u>**

Egov-Schweiz findet, dass die Kompetenzen zur Bearbeitung von besonders schützenswerten Personendaten durch das NCSC gemäss Artikel 75, insbesondere in Verbindung mit den Möglichkeiten der Weitergabe im In- und im Ausland gemäss den Artikeln 76 und 77, problematisch seien. **Egov-Schweiz** geht daher davon aus, dass das NCSC bei Bedarf polizeiliche und geheimdienstliche Unterstützung herbeizieht und keine eigene Bearbeitung anstrebt.

Da das NCSC nicht die Aufgaben des NDB übernimmt und keine Strafverfolgungsbehörde ist, scheint **privatim** zufolge das Volumen an Personendaten, das gemäss Artikel 75 E-ISG verarbeitet wird, ohne weitere Beschränkungen (insbesondere über die unbedingte Notwendigkeit, die Aufgaben zu erfüllen) nicht verhältnismässig. **Privatim** empfiehlt, die erforderlichen Einschränkungen vorzusehen.

- **<u>Zu Absatz 1 Buchstabe a</u>**

Der Kanton GR fordert die Streichung dieser Bestimmung.

5 SR **235.1**

Die GLP kritisiert den Umfang der Personendaten, die das NCSC gemäss dem Vorentwurf verarbeiten darf, und verlangt, dass die Weitergabe besonders schützenswerter Daten zwischen NCSC, Strafverfolgungsbehörden und dem NDB spezifiziert wird. Hinzu komme, dass momentan keine besondere Aufsicht vorgesehen sei. Es sei daher nicht gewährleistet, dass diese Daten nicht missbräuchlich genutzt würden.

- **Zu Absatz 2**

Privatim findet, dass die Verteilung der Kompetenzen zwischen dem NCSC, den Strafverfolgungsbehörden und dem NDB deutlich mehr Aufmerksamkeit verdiene. Daher müsse Artikel 75 Absatz 2 ISG (Bearbeitung von Personendaten, ohne dass dies für die betroffenen Personen ersichtlich sei) auf laufende Strafverfahren beschränkt werden.

- **Zu Absatz 3**

Migros gibt an, dass die vorliegende Bestimmung mit den Bestimmungen von Artikel 24 revDSG in Einklang zu bringen sei.

3.3.2.19 Artikel 76 Zusammenarbeit im Inland

[1] Das NCSC kann den Betreiberinnen von kritischen Infrastrukturen Personendaten bekanntgeben, sofern dies zum Schutz von kritischen Infrastrukturen vor Cyberrisiken erforderlich ist.

[2] Die Betreiberinnen von kritischen Infrastrukturen können dem NCSC Personendaten bekanntgeben, sofern dies zum Schutz von kritischen Infrastrukturen vor Cyberrisiken erforderlich ist.

[3] Das NCSC kann den Fernmeldedienstanbieterinnen Adressierungselemente und damit zusammenhängende Personendaten bekanntgeben, sofern dies zum Schutz von kritischen Infrastrukturen vor Cyberrisiken erforderlich ist.

[4] Die Fernmeldedienstanbieterinnen können dem NCSC Adressierungselemente und damit zusammenhängende Personendaten bekanntgeben, sofern dies zum Schutz von kritischen Infrastrukturen vor Cyberrisiken erforderlich ist.

7 Teilnehmende haben sich zu diesem Gesetzestext geäussert.

❖ **Allgemeine Bemerkungen zu Artikel 76**

Scienceindustries ist der Meinung, dass zumindest in den Absätzen 1 und 2 einschränkend vorzusehen sei, dass die Weitergabe solcher Informationen, speziell an Mitbewerber in ähnlichen Märkten nicht ohne Zustimmung des Dateninhabers erfolgen dürfe.

Swico betont, wie wichtig die Beibehaltung der bereits bestehenden Kommunikationskanäle zwischen dem NCSC, den kritischen Infrastrukturen und weiteren Parteien sei.

VöV verlangt, dass das Verhältnis der Bestimmungen von Artikel 76 Absatz 1 zu Artikel 73*b* Absatz 2 sowie Artikel 73*c* so klargestellt wird, dass das NCSC den Betreiberinnen kritischer Infrastrukturen die Personendaten nur unter der Bedingung bekanntgibt, dass dies für den Schutz von kritischen Infrastrukturen vor Cyberrisiken erforderlich ist.

Der Kanton GE bittet um Klärung, ob es sich im vorliegenden Text um kritische Infrastrukturen im Sinne von Artikel 74*b* mit den (oder ohne die) Ausnahmen von Artikel 74*c* handele. Zudem verlangt **der Kanton GE** die Erwähnung des EDÖB.

❖ **Änderungsanträge und Anregungen zu Artikel 76**

- **Zu Absatz 1**

UniZH/UNIL NFP 77 beantragen, im französischen Text «utiles» durch «nécessaires» zu ersetzen.

- **Zu Absatz 2**

ISSS beantragt, den Text wie folgt anzupassen: «… sofern dies zum Schutz [*ihrer*] kritischen Infrastrukturen …».

- **Zu Absatz 3**

ISSS beantragt, den Text wie folgt anzupassen: «… Fernmeldedienstanbieterinnen[, *die nicht kritische Infrastrukturanbieterinnen sind*,] Adressierungselemente …».

- **Zu Absatz 4**

ISSS beantragt, den Text wie folgt anzupassen: «… Fernmeldedienstanbieterinnen[, *die nicht kritische Infrastrukturanbieterinnen sind,*] können dem NCSC Adressierungselemente …».

Nach **UniZH/UNIL NFP 77** sollte der Text eher vorsehen, dass die Fernmeldedienstanbieterinnen dem NCSC Personendaten, einschliesslich Adressierungselementen, bekanntgeben könnten.

3.3.2.20 Artikel 76*a* Unterstützung für Behörden

[1] Das NCSC unterstützt den NDB beim frühzeitigen Erkennen und Verhindern von Bedrohungen der inneren oder äusseren Sicherheit, bei der Beurteilung der Bedrohungslage und bei der nachrichtendienstlichen Frühwarnung zum Schutz von kritischen Infrastrukturen nach Artikel 6 Absätze 1 Buchstabe a, 2 und 5 NDG6 mit Auswertungen zu Anzahl, Art und Ausmass von Cyberangriffen sowie technischen Analysen von Cyberrisiken.

[2] Es gewährt dem NDB Zugriff auf Informationen im Abrufverfahren, die Aufschluss über die Identität und die Vorgehensweise der Verursacherinnen und Verursacher von Cyberangriffen geben.

[3] Es gewährt den Strafverfolgungsbehörden Zugriff auf Informationen im Abrufverfahren, die Aufschluss über die Identität und die Vorgehensweise der Verursacherinnen und Verursacher von Cyberangriffen geben.

[4] Es kann den kantonalen Stellen, die für die Cybersicherheit zuständig sind, Zugriff auf Informationen im Abrufverfahren gewähren, die für den Schutz kantonaler Behörden und kantonaler kritischer Infrastrukturen vor Cyberrisiken erforderlich sind.

7 Vernehmlassungsteilnehmende haben sich zur Unterstützung für Behörden geäussert.

❖ Allgemeine Bemerkungen zu Artikel 76*a*

Der Kanton UR fordert, dass Informationen zur Identität und zur Vorgehensweise der Angreifenden vollumfänglich übermittelt werden dürfen.

Der Kanton NW findet, dass die mit den NDB geteilten Informationen ebenfalls allen Strafverfolgungsbehörden zur Verfügung gestellt werden müssten.

Der Kanton ZG ist der Meinung, dass der Kreis der Adressaten der Auswertungen und der technischen Analysen auf die Strafverfolgungsbehörden auszudehnen sei.

❖ Zustimmung zu Artikel 76*a*

Swiss Banking spricht sich für diese Regelung aus.

❖ Änderungsanträge und Anregungen zu Artikel 76*a*

- **Zu Absatz 2**

Der VöV beantragt, den Text wie folgt anzupassen: «… Abrufverfahren, [*die ausschliesslich*] Aufschluss ...».

6 SR **121**

- **Zu Absatz 3**

Der VöV beantragt, den Text wie folgt anzupassen: «… Abrufverfahren, [*die ausschliesslich*] Aufschluss ...».

Der Kanton BE beantragt die Streichung dieser Bestimmung, sollte Artikel 73*c* gestrichen werden.

Laut **privatim** muss der Zugang im Abrufverfahren zu den Informationen, die das NCSC im Rahmen der Meldepflicht erhält, für den NDB (Art. 76*a* Abs. 2 ISG), für die Strafverfolgungsbehörden (Art. 76*a* Abs. 3 ISG) und für die kantonalen Stellen für Cybersicherheit (Art. 76*a* Abs. 3 ISG) eingeschränkt oder mithilfe eines «Push»-Verfahrens realisiert werden.

- **Zu Absatz 4**

Der Kanton BE beantragt die Streichung dieses Absatzes, sollte Artikel 73*c* gestrichen werden.

3.3.2.21 Artikel 77 Internationale Zusammenarbeit

[1] Das NCSC kann mit ausländischen und internationalen Stellen, die für die Cybersicherheit zuständig sind, Informationen austauschen, wenn sie diese zur Erfüllung von Aufgaben benötigen, die denjenigen des NCSC entsprechen. Umfasst der Informationsaustausch auch Personendaten nach Artikel 75, ist Artikel 6 DSG[7] zu beachten.
[2] Der Informationsaustausch nach Absatz 1 ist nur dann zulässig, wenn die ausländischen und internationalen Stellen die bestimmungsgemässe Verwendung gewährleisten.
[3] Werden die Informationen für ein rechtliches Verfahren im Ausland benötigt, so gelten die Bestimmungen über die Amts- und Rechtshilfe.

7 Vernehmlassungsteilnehmende haben sich zur Frage der internationalen Zusammenarbeit geäussert. Niemand hat diese Bestimmung abgelehnt.

❖ Allgemeine Bemerkungen zu Artikel 77

Swiss Banking unterstützt Artikel 77, wenn die Informationen für die Bekämpfung von Cyberrisiken und insbesondere für die Zwecke dieses Gesetzes nötig sind (eine in Art. 77 Abs. 1 erster Satz ausdrücklich vorgesehene und begrüssenswerte Einschränkung). Wenn Personendaten im Sinne von Artikel 75 involviert seien, sei bei deren Übermittlung ins Ausland Artikel 6 DSG zu beachten.

Scienceindustries steht der Weitergabe von vertraulichen Daten, insbesondere von Personendaten, kritisch gegenüber. Es wäre sinnvoll, hier zumindest mit Gültigkeit für die Absätze 1, 2 und 3 einschränkend vorzusehen, dass die Weitergabe solcher Informationen nicht ohne die Zustimmung des Dateninhabers erfolgen dürfe.

VUD fordert, dass der Informationsaustausch mit ausländischen Behörden gemäss Artikel 77 ISG streng anonym erfolgt.

Laut **BA** sollte sich dieser Gesetzestext in den Rahmen der bereits bestehenden Bestimmungen zur internationalen Zusammenarbeit einfügen, insbesondere im Bereich der Rechtshilfe.

❖ Änderungsanträge und Anregungen zu Artikel 77

- **Zu Absatz 1**

Der VöV hält das Verhältnis der Bestimmungen von Artikel 77 Absatz 1 zu Artikel 73*b* Absatz 2 und Artikel 73*c* für unklar und verlangt folglich, dass der Text wie folgt angepasst wird: «… nach Art. 75, [*sind Artikel 73b Abs. 2 und 73c sowie*] Artikel 6 DSG zu beachten».

7 SR **235.1**

Privatim begrüsst diesen Absatz.

ISSS beantragt, den Text wie folgt anzupassen: «… Artikel 75, ist Artikel 6 [*und Art. 10a DSG*] zu beachten ...».

- **Zu Absatz 2**

Damit beim Informationsaustausch gewährleistet sei, dass die ausländische Schwesterbehörde die erhaltenen Informationen für den Zweck der Bekämpfung von Cyberrisiken verwende, schlägt **Swiss Banking** vor, die Regelung wie folgt zu ergänzen: «Weitergegebene Informationen sind durch die Empfängerbehörde vertraulich zu behandeln. Sie dürfen nicht weitergegeben werden, wenn dadurch die Sicherheit des betroffenen Unternehmens oder der betroffenen Personen gefährdet würde».

ISSS beantragt, den Text wie folgt anzupassen: «… bestimmungsgemässe [*datenschutzkonforme*] Verwendung …».

- **Zu Absatz 3**

Die BA verlangt, in diesem Text einen Koordinationsmechanismus einzuführen, und schlägt folgende Formulierung vor: «… Amts- und Rechtshilfe. [*Die übermittelten Informationen können zur Substantiierung eines Rechts- oder Amtshilfeersuchens verwendet werden*] …».

Im Wissen, dass das NCSC keine Strafverfolgungsbehörde sei, verlangt **privatim** Präzisierungen in Bezug auf die Bestimmungen, aus denen sich die nationalen Kompetenzen für Amts- und Rechtshilfe ableiten würden.

3.3.2.22 Artikel 79 Abs. 1 (Datenaufbewahrung und -archivierung)

[1] Das NCSC bewahrt Personendaten nur so lange auf, wie dies zur Abwehr von Gefahren oder zur Erkennung von Vorfällen zweckmässig ist, höchstens jedoch fünf Jahre ab der letzten Verwendung; bei besonders schützenswerten Personendaten beträgt die Frist zwei Jahre.

10 Vernehmlassungsteilnehmende haben sich zur Frist für die Aufbewahrung von Personendaten durch das NCSC geäussert.

❖ Allgemeine Bemerkungen zu Artikel 79 Abs. 1

CH++ beantragt, den Begriff «Verwendung» zu präzisieren, z. B. «zwingende Verwendung». Das blosse Öffnen eines Datensatzes könne selbstverständlich nicht zur Verlängerung der erlaubten Aufbewahrungsfrist führen.

VöV, Migros sowie UniZH/UNIL NFP 77 fordern eine Präzisierung des Begriffs «letzte Verwendung».

Laut **ISSS, Härting Rechtsanwälte und privatim** verlangt der Grundsatz der Verhältnismässigkeit, dass die Daten nur so lange aufbewahrt werden, wie dies für die Zweckerfüllung erforderlich ist. Aus den Personendaten könnten anonymisierte Muster generiert werden. **ISSS und Härting Rechtsanwälte** schlagen folgende Umformulierung vor: «… beträgt die Frist [*6 Monate. In anonymisierter Form sowie als erkannte Muster dürfen die aus Personendaten gewonnenen Erkenntnisse unbefristet aufbewahrt werden*]».

Die KKJPD verlangt, die Aufbewahrungsfrist für die Daten an die Artikel 97 und 109 des Schweizerischen Strafgesetzbuches anzupassen.

Der Kanton BE beantragt eine Anpassung dieser Bestimmung, damit die Daten grundsätzlich nicht vor dem Ende der Verfolgungsverjährung der in Frage kommenden Delikte gelöscht werden.

3.3.2.23 Änderungserlasse

Die nachstehenden Erlasse werden wie folgt geändert:

1. Stromversorgungsgesetz vom 23. März 2007[8]

Art. 8a Schutz vor Cyberrisiken

1 Die Netzbetreiber, die Erzeuger und die Speicherbetreiber treffen Massnahmen für einen angemessenen Schutz ihrer Anlagen vor Cyberrisiken.

2 Der Bundesrat kann diese Pflicht auf weitere Beteiligte ausdehnen.

2. Datenschutzgesetz vom 25. September 2020[9]

Art. 24 Abs. 5bis

5bis Der EDÖB kann die Meldung mit dem Einverständnis des meldepflichtigen Verantwortlichen zur Analyse des Vorfalls an das Nationale Zentrum für Cybersicherheit weiterleiten. Die Mitteilung kann Personendaten enthalten, einschliesslich besonders schützenswerter Personendaten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen betreffend den meldepflichtigen Verantwortlichen.

Nur 6 Vernehmlassungsteilnehmende haben sich zu den zwei obigen Gesetzestexten geäussert. Keine der befragten Instanzen hat die Streichung von Artikel 8*a* StromVG beantragt. **ISSS und Härting Rechtsanwälte** haben die Streichung von Artikel 24 Absatz 5bis DSG verlangt.

- **Allgemeine Bemerkungen zu Artikel 24 Abs. 5bis Datenschutzgesetz**

Der VöV beantragt, die Bestimmung wie folgt anzupassen: «Der EDÖB kann die Meldung [*ausschliesslich*] mit dem …».

Der **Kanton GE** ist der Meinung, dass die Mitteilung des NCSC an den EDÖB verpflichtend sein sollte; die Mitteilung des EDÖB sollte nicht des Einverständnisses der meldepflichtigen Person bedürfen, wenn die Bedingungen des vorliegenden Gesetzes erfüllt seien.

UniZH/UNIL NFP 77 weisen darauf hin, dass es möglich sein müsse, sämtliche besonders schützenswerten Personendaten zu übermitteln und nicht nur bestimmte.

- **Ablehnung von Artikel 24 Abs. 5bis Datenschutzgesetz**

ISSS und Härting Rechtsanwälte verlangen die Streichung dieser Bestimmung. Denn wenn eine zentrale Stelle geschaffen werde, um alle Meldungen zu registrieren, sei dieser Zusatz nicht mehr notwendig.

3.4 Weitere Anträge und Anregungen zum Vorentwurf

Swiss Banking verlangt, den Gesetzestext an die FINMA-Aufsichtsmitteilung 05/2020 betreffend die Meldepflicht von Cyber-Attacken gemäss Artikel 29 Absatz 2 FINMAG anzupassen.

Die IG eHealth verlangt, dass Bundesrat und Parlament sicherstellen, dass das NCSC ausreichende Personalressourcen erhält.

Der Kanton ZH schlägt vor, die Meldepflicht etappenweise (z. B. sektorweise) einzuführen, um so zuerst Erfahrungen zu sammeln.

Die KKPKS beantragt zu regeln, wie Strafverfolgungsbehörden mit Meldungen umgehen müssen, wenn diese an sie statt ans NCSC gelangen.

8 SR **734.7**
9 SR **235.1,** BBl 2020 7639

Asut, Swisscom und Sunrise verlangen eine gute Koordination der Vorlage mit der Revision der Fernmeldeverordnung.

3.5 Anträge und Anregungen zu Themen ausserhalb der Vorlage

CH++ und Pour Demain unterstützen die Umwandlung des NCSC in ein Bundesamt. Die **Piratenpartei** verlangt die Schaffung eines Departements für Digitalisierung.

Der Kanton FR fordert, dass neben der Einführung einer Meldepflicht auch weitere Massnahmen zum Schutz vor Cyberbedrohungen (wie z. B. die Sensibilisierung der Bevölkerung) umgesetzt werden.

Die Piratenpartei fordert, dass bei kritischen Infrastrukturen künftig nur noch Open Source Software (OSS) verwendet werden darf. Es brauche zudem einen finanziell gut ausgestatteten Fonds, aus dem Sicherheitsaudits von weit verbreiteter Software (bspw. Open Source / FOSS) finanziert würden. Die Schweiz müsse langfristig Ressourcen aufbauen, um Hard- und Software für kritische Infrastruktur selbst zu entwickeln und zu produzieren.

4 Anhang

4.1 Kantone

ZH	Staatskanzlei des Kantons Zürich	Neumühlequai 10 Postfach 8090 Zürich staatskanzlei@sk.zh.ch
BE	Staatskanzlei des Kantons Bern	Postgasse 68 3000 Bern 8 info@sta.be.ch
LU	Staatskanzlei des Kantons Luzern	Bahnhofstrasse 15 6002 Luzern staatskanzlei@lu.ch
UR	Standeskanzlei des Kantons Uri	Rathausplatz 1 6460 Altdorf ds.la@ur.ch
SZ	Staatskanzlei des Kantons Schwyz	Regierungsgebäude Bahnhofstrasse 9 Postfach 1260 6431 Schwyz stk@sz.ch
OW	Staatskanzlei des Kantons Obwalden	Rathaus 6061 Sarnen staatskanzlei@ow.ch
NW	Staatskanzlei des Kantons Nidwalden	Dorfplatz 2 Postfach 1246 6371 Stans staatskanzlei@nw.ch
GL	Staatskanzlei des Kantons Glarus	Rathaus 8750 Glarus staatskanzlei@gl.ch
ZG	Staatskanzlei des Kantons Zug	Seestrasse 2 Regierungsgebäude am Postplatz 6300 Zug info@zg.ch
FR	Staatskanzlei des Kantons Freiburg	Rue des Chanoines 17 1701 Fribourg chancellerie@fr.ch
SO	Staatskanzlei des Kantons Solothurn	Rathaus Barfüssergasse 24 4509 Solothurn kanzlei@sk.so.ch
BS	Staatskanzlei des Kantons Basel-Stadt	Marktplatz 9 4001 Basel staatskanzlei@bs.ch
BL	Landeskanzlei des Kantons Basel-Landschaft	Regierungsgebäude Rathausstrasse 2 4410 Liestal landeskanzlei@bl.ch
SH	Staatskanzlei des Kantons Schaffhausen	Beckenstube 7 8200 Schaffhausen staatskanzlei@ktsh.ch

AR	Kantonskanzlei des Kantons Appenzell Ausserrhoden	Regierungsgebäude 9102 Herisau Kantonskanzlei@ar.ch
AI	Ratskanzlei des Kantons Appenzell Innerrhoden	Marktgasse 2 9050 Appenzell info@rk.ai.ch
SG	Staatskanzlei des Kantons St. Gallen	Regierungsgebäude 9001 St. Gallen info.sk@sg.ch
GR	Standeskanzlei des Kantons Graubünden	Reichsgasse 35 7001 Chur info@gr.ch
AG	Staatskanzlei des Kantons Aargau	Regierungsgebäude 5001 Aarau staatskanzlei@ag.ch
TG	Staatskanzlei des Kantons Thurgau	Regierungsgebäude Zürcherstrasse 188 8510 Frauenfeld staatskanzlei@tg.ch
TI	Cancelleria dello Stato del Cantone Ticino	Piazza Governo 6 6501 Bellinzona can-scds@ti.ch
VD	Chancellerie d'Etat du Canton de Vaud	Place du Château 4 1014 Lausanne info.chancellerie@vd.ch
VS	Chancellerie d'Etat du Canton du Valais	Planta 3 1950 Sion Chancellerie@admin.vs.ch
NE	Chancellerie d'Etat du Canton de Neuchâtel	Le Château Rue de la Collégiale 12 2000 Neuchâtel Secretariat.chancelle-rie@ne.ch
GE	Chancellerie d'Etat du Canton de Genève	Rue de l'Hôtel-de-Ville 2 Case postale 3964 1211 Genève 3 service-adm.ce@etat.ge.ch
JU	Chancellerie d'Etat du Canton du Jura	2, rue de l'Hôpital 2800 Delémont chancellerie@jura.ch
KKJPD	KKJPD Konferenz der Kantonalen Justiz- und Polizeidirektorin-nen und -direktoren (KKJPD)	Haus der Kantone Speichergasse 6 Postfach 3001 Bern info@kkjpd.ch
GDK	GDK Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren	Haus der Kantone Speichergasse 6 Postfach 3001 Bern office@gdk-cds.ch
RK MZF	RK MZF Regierungskonferenz Militär, Zivilschutz, Feuerwehr	Haus der Kantone Speichergasse 6 Postfach 3001 Bern

KKPKS	KKPKS Konferenz der Kantonalen Polizeikommandanten der Schweiz	Haus der Kantone Speichergasse 6 Postfach 3001 Bern info@kkpks.ch
SSK	Schweizerische Staatsanwälte-Konferenz	Haus der Kantone Speichergasse 6 Postfach 3001 Bern info@ssk-cps.ch

4.2 In der Bundesversammlung vertretene politische Parteien

Die Mitte	Die Mitte	Generalsekretariat Hirschengraben 9 Postfach 3001 Bern info@die-mitte.ch
FDP	FDP. Die Liberalen	Generalsekretariat Neuengasse 20 Postfach 3001 Bern info@fdp.ch
Die Grünen	Grüne Partei der Schweiz GPS	Waisenhausplatz 21 3011 Bern gruene@gruene.ch
GLP	Grünliberale Partei Schweiz GLP	Monbijoustrasse 30 3011 Bern schweiz@grunliberale.ch
SVP	Schweizerische Volkspartei SVP	Generalsekretariat Postfach 8252 3001 Bern gs@svp.ch
SP	Sozialdemokratische Partei der Schweiz SP	Zentralsekretariat Theaterplatz 4 Postfach 3001 Bern verena.lo-embe@spschweiz.ch

4.3 Gesamtschweizerische Dachverbände der Gemeinden, Städte und Berggebiete

SSV	Schweizerischer Städteverband (SSV)	Monbijoustrasse 8 Postfach 3001 Bern info@staedteverband.ch

4.4 Gesamtschweizerische Dachverbände der Wirtschaft

econo-mie-suisse	Verband der Schweizer Unternehmen	Hegibachstrasse 47 Postfach 8032 Zürich 8032 Zürich info@economiesuisse.ch

		bern@economiesuisse.ch sandra.spieser@economiesu-isse.ch
Swiss Banking	Schweizerische Bankiervereinigung	Hotelgasse 10, 3011 Bern
SGV	Schweizerischer Gewerbeverband	Schwarztorstrasse 26 Postfach 3001 Bern info@sgv-usam.ch
SGB	Schweizerischer Gewerkschaftsbund	Monbijoustrasse 61, 3007 Bern, info@sgb.ch

4.5 Weitere interessierte Kreise – Stellungnahmen auf Einladung

eGov-Schweiz	Verein eGov-Schweiz	c/o mundi consulting ag Marktgasse 55 Postfach 3001 Bern info@eGov-Schweiz.ch
privatim	privatim, Konferenz der schweizerischen Datenschutz-beauftragten	c/o Dr. Beat Rudin, Advokat, Postfach 205 4010 Basel kommunikation@privatim.ch
Digitale Gesell-schaft	Digitale Gesellschaft	4000 Basel office@digitale-gesell-schaft.ch
eHealth	Interessengemeinschaft eHealth	Amthausgasse 18 3011 Bern info@ig-ehealth.ch
asut	Schweizerischer Verband der Telekommunikation	Hirschengraben 8 3011 Bern info@asut.ch
Inter-pension	Inter-pension Interessengemeinschaft autonomer Sammel- und Gemeinschaftseinrichtungen	Gartenstrasse 2 3063 Ittigen info@inter-pension.ch
RAILplus AG	RAILplus AG	Bahnhofstrasse 85 5001 Aarau info@railplus.ch
AEROS UISSE	Dachverband der Schweizerischen Luft- und Raumfahrt	Kapellenstrasse 14 Postfach 3001 Bern info@aerosuisse.ch

4.6 Weitere interessierte Kreise – spontane Stellungnahmen

eAHV/IV	eAHV/IV	p.a. mundi consulting ag Marktgasse 55 Postfach 3001 Bern jerome.brugger@mundicon-sulting.com
ISSS	Information Security Society Switzerland	Kochergasse 6, 3011 Bern sekretariat@isss.ch
Centre Patronal	Centre Patronal	Route du Lac 2 1094 Paudex info@centrepatronal.ch
Verein CH++	Verein CH++	marcel.sa-lathe@chplusplus.org
Ausland-banken	Verband der Auslandbanken in der Schweiz	Usteristrasse 23 8001 Zürich info@afbs.ch
BA	Bundesanwaltschaft BA	Guisanplatz 1 3003 Bern info@ba.admin.ch
Post CH AG	Post CH AG	Wankdorfallee 4 Postfach 3030 Bern regulatoryaffairs@post.ch
digital-switzer-land	digitalswitzerland	Waisenhausplatz 14 3011 Bern office@digitalswitzerland-bern.ch
FER	Fédération des Entreprises Romandes (FER)	98 rue de Saint-Jean 1211 Genève 11 yannic.forney@fer-ge.ch
Swico	Swico	Lagerstrasse 33 8004 Zürich info@Swico.ch
GEM	Groupement des Entreprises Multinationales	Rue de Saint-Jean 98 1211 Genf 3 info@gemonline.ch
Pour Demain	Pour Demain	Marktgasse 46 3011 Bern info@pourdemain.ch
santé-suisse	Branchenorganisation der Schweizer Krankenversicherer im Bereich der sozialen Krankenversicherung	Römerstrasse 20 Postfach CH-4502 Solothurn mail@santesuisse.ch
Swiss-ICT	SwissICT	Vulkanstr. 120 8048 Zürich info@swissict.ch
Swiss-mem	Verband für KMU und Grossfirmen der Schweizer Tech-Industrie	Pfingstweidstrasse 102 Postfach CH-8037 Zürich r.rudolph@swissmem.ch

swiss-universi-ties	Dachorganisation der Schweizer Hochschulen	swissuniversities Effingerstrasse 15 Case Postale 3001 Bern weiss@swissuniversities.ch
VUD	Verein Unternehmens-Datenschutz	Verein Unternehmens-Daten-schutz VUD c/o IT & Law Consulting GmbH Sternenstrasse 18, 8002 Zürich info@vud.ch
VöV	Verband öffentlicher Verkehr	Dählhölzliweg 12 CH-3000 Bern 6 info@voev.ch
VSE	Verband Schweizerischer Elektrizitätsunternehmen	Hintere Bahnhofstrasse 10 5000 Aarau info@strom.ch
ASIP	Schweizerischer Pensionskassenverband	Kreuzstrasse 26 8008 Zurich info@asip.ch
Science-indust-ries	Wirtschaftsverband Chemie Pharma Life Sciences	Nordstrasse 15 Postfach 8021 Zürich Schweiz
Suisse-digital	Verband für Kommunikationsnetze	Bollwerk 15 CH-3011 Bern info@suissedigital.ch
SVGW	Schweizerischer Verein des Gas- und Wasserfaches	Grütlistrasse 44 | Postfach | 8027 Zürich info@svgw.ch
SVV	Schweizerische Versicherungsverband	Conrad-Ferdinand-Meyer-Strasse 14 Case postale CH-8022 Zürich info@svv.ch
VAV	Vereinigung Schweizerischer Assetmanagement- und Vermögensverwaltungsbanken	
Gach-nang	Gemeinde Gachnang (TG)	Hôtel de ville de Gachnang Islikonerstrasse 7 8547 GACHNANG Schweiz
NFP 77 ETHZ UNIL	Gemeinsame Stellungnahme	
Opera-tion Libero	Bewegung	OPERATION LIBERO CH-3000 Bern futur@operation-libero.ch
AEIS	Stiftung Auffangeinrichtung BVG	Elias-Canetti-Strasse 2 Postfach 8050 Zurich urs.mueller@aeis.ch
Trust Valley	Fondation Trust Valley	Trust Valley EPFL Innovation Park, Bâti-ment C CH-1015 Lausanne

UniBE	Universität Bern	Dr. Cord-Ulrich Fündeling Leiter Informatikdienste Hochschulstrasse 6 3012 Bern cord.fuendeling@unibe.ch
UniGE Digital Law Centre	Universität Genf	Digital Law Center - Uni Mail - Bd du Pont d'Arve 40 - CH-1211 Genf 4 Schweiz digitallawcenter@unige.ch
Abraxas	Entreprise Abraxas Informatik AG	The Circle 68 | CH-8058 Zürich-Flughafen peter.gassmann@abraxas.ch
Axpo	Axpo services AG	Axpo Services AG Parkstrasse 23 | 5401 Baden | Switzerland thomas.porchet@axpo.com
Beat Lehmann		Acting Counsel Alcan Holdings Switzerland AG Kongoweg 9 (Home Office) 5034 Suhr b.lehmann-aarau@bluewin.ch
Coop	Coop Genossenschaft	Thiersteinerallee 12 Postfach 2550 4002 Basel Damian.Misteli@coop.ch
Flughafen ZH		Zürich Flughafen CH-8058 Andrew.karim@zurich-airport.ch
Flughafen GE		Aéroport international de Genève CP100 CH 1215 Genf
Härting Rechtsanwälte		Landis Gyr Strasse 1 6300 Zug office@haerting.ch
Helvetia	Helvetia Versicherungen AG	Helvetia Versicherungen Hauptsitz St. Alban-Anlage 26 4002 Basel martin.jara@helvetia.ch
Migros	Migros-Genossenschafts-Bund	
Raffeisen		cecile.kessler@raiffeisen.ch
Romande Energie		Rue de Lausanne 53 1110 Morges Oscar.parado@romande-energie.ch
Salt		Salt Mobile SA Rue du Caudray 4 CH-1020 Renens 1
SBB		
Sunrise	Sunrise UPC	Sunrise UPC GmbH Thurgauerstrasse 101B, 8152 Glattpark (Opfikon)

		Marcel.Huber@sunrise.net
Suva		Fluhmattstrasse 1 Case postale 4358 6004 Luzern Marc.epelbaum@suva.ch
Swiss		Swiss International Air Lines AG P.O. Box ZRHS/V/ABRO CH-8 ronald.abegglen@swiss.com 058 Zürich-Flughafen
Swisscom		Alte Tiefenaustrasse 6 3048 Worblaufen Lorenz.Ing-lin@swisscom.com
Swiss-grid		Bleichemattstrasse 31 Postfach 5001 Aarau info@swissgrid.ch
Switch		Werdtstrasse 2 Postfach 8021 Zürich
TPG	Transports publics genevois	Route de la Chapelle 1 -.Case postale 950 - 1212 Grand-Lancy 1 - Schweiz Meyer.G@tpg.ch
Piraten-partei Schweiz	Piratenpartei Schweiz	Piratenpartei Bern, 3000 Bern info@be.piratenpartei.ch