22.073

Informationssicherheitsgesetz. Änderung (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen)

Loi sur la sécurité de l'information. Modification (Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques)

Erstrat – Premier Conseil

CHRONOLOGIE

NATIONALRAT/CONSEIL NATIONAL 16.03.23 (ERSTRAT - PREMIER CONSEIL)

Pointet François (GL, VD), pour la commission: Le projet qui nous occupe aujourd'hui règle l'obligation de signaler les cyberattaques contre les infrastructures critiques et inscrit dans la loi les tâches du Centre national pour la cybersécurité (NCSC), créé en 2019. Il règle en particulier la fonction de guichet unique qui est attribuée au NCSC et qui consiste à réceptionner les signalements obligatoires de cyberincidents, de même que les signalements volontaires de cyberincidents et de vulnérabilités des moyens informatiques.
L'obligation de signaler est mise en place pour les cyberattaques perpétrées par des tiers non autorisés qui visent intentionnellement des infrastructures critiques. Le signalement d'une cyberattaque n'est cependant obligatoire que si l'attaque a des conséquences graves, comme la mise en péril du fonctionnement de l'infrastructure critique touchée.
Sur le fond, personne ne conteste la nécessité de cette obligation d'annonce. C'est en effet un moyen efficace d'augmenter la résilience de notre économie et de notre pays face aux dites cyberattaques: communiquer et partager les informations pour, tous ensemble, mieux résister.
La commission a surtout discuté des données collectées et traitées et de qui serait touché par ces obligations d'annonce.
Dans les faits, votre commission a ajouté, sans opposition et avec seulement une abstention, des obligations d'annonce de vulnérabilités non publiées.
C'est le changement principal que nous avons apporté au projet du Conseil fédéral. Cela permettra au NCSC de mieux remplir les tâches de signalement qui lui incombent pour les vulnérabilités inconnues du public, c'est l'article 73b alinéa 3. L'ajout de l'obligation d'annonce des vulnérabilités a provoqué certains remous. Il est en particulier reproché de mettre l'ensemble des vulnérabilités non corrigées dans un système d'information qui pourrait être attaqué, et ces informations pourraient alors être utilisées pour attaquer les infrastructures critiques. Ce scénario est un tout petit peu étriqué; il faut toutefois mettre ce risque de scénario en relation avec l'avantage de faire circuler l'information, par exemple auprès des fournisseurs de logiciels, pour permettre un correctif rapide.
Pour le reste du projet, la majorité de la commission vous propose de suivre le Conseil fédéral et de rejeter les deux minorités Zuberbühler.
La première minorité demande, à l'article 74e, d'augmenter le délai d'annonce aux 72 heures suivant la détection de la cyberattaque ou de la vulnérabilité. Il faut bien se rendre compte de la situation en cas d'attaque. Le responsable informatique à qui on annonce une attaque doit prendre immédiatement toutes les mesures pour contenir ladite attaque, toutes les équipes doivent être appelées pour régler le problème au plus vite. Une annonce rapide au NCSC permet de prendre les mesures de contrôle pour les autres infrastructures critiques et au NCSC de se préparer à soutenir l'exploitant sous attaque, c'est l'article 74. Tout va très vite, et 72 heures, c'est beaucoup trop long.

Pour ceux qui croient que faire un signalement c'est beaucoup de travail, parce qu'ils ont autre chose à faire, j'aimerais ajouter qu'en pratique le premier signalement pourrait être simplement: "Nous sommes sous attaque." La commission a rejeté cette proposition de minorité, par 16 voix contre 7.
La proposition de minorité Zuberbühler demande, à l'article 74e, de supprimer la possibilité d'amender celui qui ne respecte pas l'obligation de signalement. Tout d'abord, on ne peut pas être amendé pour ne pas avoir détecté une attaque. De plus, il est prévu que si le signalement a été oublié et que le NCSC le constate, l'entreprise reçoit tout d'abord un avertissement et que si, suite à cela, l'entreprise n'effectue pas son signalement, une décision formelle est prise. Ensuite, si l'entreprise ne fait toujours pas son travail, une amende peut être prononcée. Nous constatons que l'entreprise coupable doit avoir fait preuve de beaucoup de mauvaise volonté ou d'une extrême négligence coupable pour qu'une amende puisse être prononcée. La commission a rejeté cette proposition de minorité, par 16 voix contre 7.
Le projet, dans son ensemble, a été accepté, par 16 voix contre 1 et 6 abstentions. Votre commission vous recommande d'accepter le projet tel que sa majorité vous le propose.

Gugger Niklaus-Samuel (M-E, ZH): Geschätzter Herr Kommissionssprecher, ich habe eine Frage: Wie beurteilt die Kommission einen möglichen erfolgreichen Cyberangriff auf das NCSC mit Blick auf die Sicherheit der kritischen Infrastrukturen und letztlich die Sicherheit der Schweiz, wenn alle IT-Schwachstellen zentral im NCSC gespeichert sind? Ich hoffe, der Ständerat korrigiert das. Ich erachte dies als sehr gefährlich, da heute bekanntlich in allen Schweizer Medien darauf hingewiesen wird, dass die Schweiz gegen Cyberangriffe sehr schlecht geschützt ist.

Pointet François (GL, VD), pour la commission: Merci, cher collègue, pour cette question. La commission a considéré que la pratique du NCSC est sûre. En particulier, il est possible de faire l'annonce de manière anonyme, ce qui ne rattache pas la vulnérabilité à une infrastructure critique. Ensuite, on peut sur le plan pratique protéger les informations et ne pas les enregistrer au même endroit. Ce serait au NCSC de faire ce travail au cas où l'obligation d'annonce de vulnérabilité serait maintenue.

Andrey Gerhard (G, FR), für die Kommission: Kaum ein Lebensbereich ist heute noch digitalisierungsfrei. Die digitale Infrastruktur hilft uns hier, steuert uns da und versorgt uns dort. Man darf mit Fug und Recht behaupten, dass die Digitalisierung punkto Wichtigkeit mittlerweile auf der Ebene der Stromversorgung angelangt ist: Ohne sie läuft nichts mehr. Entsprechend wichtig werden digitale Verwundbarkeiten. Das ist ein Thema, das noch vor Kurzem fast ausschliesslich in Fachkreisen diskutiert wurde. Seit aber immer mehr gravierende Cyberattacken erfolgreich Gemeindebehörden, Bildungsinstitutionen oder Verwaltungseinheiten in die Knie zwingen, ist das Thema nun auch in der breiten Bevölkerung angekommen.
Vor bald zwei Jahrzehnten hat die Bundesverwaltung ihrerseits jedoch schon eine Sensibilität für das Thema entwickelt und über die Jahre eine gut funktionierende Plattform für

Monitoring und Hilfestellung aufgebaut. Daraus entstanden ist das heutige NCSC, das Nationale Zentrum für Cybersicherheit. Das NCSC hantiert bis heute mit freiwilligen Massnahmen. Nun ist aber der Zeitpunkt gekommen, einen Gang höher zu schalten, die Gefährdungen sind zu bedrohlich.
Deshalb beraten wir heute eine Revision des Informationssicherheitsgesetzes, das Betreiber kritischer Infrastrukturen wie Elektrizitätswerke, Spitäler oder Hochschulen verpflichtet, dem NCSC Cyberattacken innerhalb von 24 Stunden zu melden. Diese Meldungen werden helfen, die Cybersicherheit in der Schweiz insgesamt zu verbessern. Ähnlich wie man das zum Beispiel im internationalen Flugverkehr kennt, soll eine Kultur des vorbehaltlosen Aufklärens entstehen.
Kommen wir nun zur Vorlage im Detail. Der Gesetzentwurf wurde in der Sicherheitspolitischen Kommission insgesamt mit Wohlwollen beraten; die Kommission folgt weitgehend dem Bundesrat. Sie schlägt aber eine Erweiterung vor, welche die Meldepflicht auf unbekannte schwerwiegende Schwachstellen ausdehnt. Auf der Fahne sind in den Artikeln 73b und 74a bis 74f Änderungen zu finden. Alle betreffen nur diesen Aspekt. Die Kommission ist mit 21 zu 0 Stimmen bei 1 Enthaltung der Ansicht, dass diese erweiterte Meldepflicht bei Cyberangriffen einen besseren Überblick über die Situation verschafft und präventiv wirken kann. Es kommt nämlich oft vor, dass die gleichen IT-Komponenten in verschiedensten Infrastrukturen eingesetzt werden. Andere Betreiber so schnell wie möglich über erkannte Gefahren informieren zu können, ist deshalb von zentraler Bedeutung.
"So schnell wie möglich" wäre das Stichwort für die Minderheit Zuberbühler, welche beantragt, die Meldefrist von 24 auf 72 Stunden zu verlängern. Wie eben ausgeführt, ist die Zeit wesentlich. Automatisierte Attacken

können sich wie ein Lauffeuer verbreiten. Je schneller ein Angriff gemeldet wird, desto grösser ist die Chance, einen Flächenbrand zu verhindern. Das NCSC erwartet auch keine Doktorarbeit, wenn es darum geht, eine Attacke oder eine Schwachstelle zu melden. Es reicht, einen kurzen Hinweis zu deponieren, sodass sich das angegriffene Unternehmen hauptsächlich um die Abwehr kümmern kann. Der Antrag, die Meldefrist von 24 auf 72 Stunden zu verlängern, wurde entsprechend mit 16 zu 7 Stimmen abgelehnt.
Gleich verhält es sich bei der zweiten Minderheit Zuberbühler, welche die Bussen aus der Vorlage kippen möchte. Wie einleitend ausgeführt, wurde knapp zwanzig Jahre lang der Ansatz der Freiwilligkeit verfolgt. Das Verzichten auf Sanktionen – vorgesehen sind hier maximal 100 000 Franken pro Fall –, wie man sie überdies auch im Datenschutzgesetz kennt, wo die Maximalbusse sogar auf 250 000 Franken angehoben wurde, würde die gesamte Vorlage massiv schwächen. Entsprechend ist die Kommission mit 16 zu 7 Stimmen der Auffassung, dass die Bussen im Entwurf bleiben sollen.
Die Gesamtvorlage wurde schlussendlich mit 16 zu 1 Stimmen bei 6 Enthaltungen klar angenommen.
An dieser Stelle möchte ich mich im Namen der Kommission herzlich für die konstruktive Zusammenarbeit, insbesondere mit dem NCSC, bedanken, zumal die Änderungen bezüglich Schwachstellen doch einiges an Flexibilität und Hirnschmalz abverlangt haben.

Glanzmann-Hunkeler Ida (M-E, LU): Ob wir es wahrhaben wollen oder nicht: Mit Cyberangriffen müssen wir alle leben, und wir müssen mit ihnen auch richtig umgehen können. Die Augen zu verschliessen und zu denken, dass dies uns selber nie passieren werde, ist wohl die schlechteste Strategie. Wenn mir das selbst passiert, dürfte der Schaden absehbar sein. Wir beraten aber heute das Gesetz zur Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen. Ein Cyberangriff auf solche Infrastrukturen und Unternehmen ist meist mit grossen Folgen und Auswirkungen in vielen Bereichen und mit grossen Kosten verbunden.
Die Mitte-Fraktion ist sich der Wichtigkeit dieser Vorlage bewusst und begrüsst eine Meldepflicht sowie das NCSC als Meldestelle. Für uns ist eine zentrale, einfache und rasche Umsetzung bei einem Angriff wichtig. Die klare Abgrenzung zwischen kritischen Infrastrukturen und den übrigen Betrieben ist dabei sehr wichtig. Der Kreis der Betroffenen soll bei diesem Gesetz eng gefasst werden.
Die Folgen eines Cyberangriffes sind für alle Unternehmen und hier ganz besonders für kritische Infrastrukturen sehr gross. Aus diesem Grund wird eine Meldung mit diesem Gesetz verpflichtend.
Es ist auch wichtig, dass die Meldung schnell erfolgt und dass allenfalls auch Schwachstellen ausgewiesen werden. Zusammen mit der Mehrheit der Kommission unterstützen wir eine Meldepflicht innert 24 Stunden. Es ist nicht nachvollziehbar, wieso ein Unternehmen 72 Stunden warten soll, bis es einen Angriff oder eine Krisensituation an die betreffende Stelle meldet. Im Gegenteil, eine rasche Meldung führt dazu, dass allenfalls Angriffe auf andere Unternehmen rechtzeitig erkannt oder verhindert werden können. Es geht auch nicht darum, in diesen 24 Stunden eine vollständige Meldung zu machen. Es ist auch möglich, später entsprechende Daten nachzuliefern. Nachvollziehbar ist auch, dass die Schweiz hier gegenüber der EU keine Ausnahmeregelung ins Gesetz schreiben will, sondern dies so übernimmt.
Der Bundesrat beantragt, dass nach einer Mahnung mit 100 000 Franken Busse bestraft wird, wer keine Meldung macht. Die Busse scheint auf den ersten Blick sehr hoch. Die Argumentation, dass Unternehmen Vorfälle ohne Sanktionsandrohung oft nicht melden, ist aber nachvollziehbar. Da zuerst Mahnungen ausgesprochen werden, wird die Höhe dieser Busse von der Mitte-Fraktion unterstützt.
Die Digitalisierung wird in den kommenden Jahren auch bei kritischen Infrastrukturen ein Thema werden, respektive man ist daran, sie dort zu integrieren. Da werden sich neue Felder für Cyberangriffe auftun, oder die Unternehmen müssen sich sehr bewusst schützen. Das heisst, die Unternehmen werden immer wieder aufgefordert, ihre Sicherheit zu überprüfen. Es braucht viel Sensibilisierung zum Thema Cybersicherheit und auch eine gute Prävention. Das NCSC bietet beim Schutz vor Cyberangriffen einen wichtigen Knotenpunkt, können hier doch Daten ausgetauscht und somit auch Angriffe verhindert werden. Auch der internationale Austausch ist damit gewährleistet – die Cybersicherheit macht nicht an der Grenze halt.
Der Mitte-Fraktion ist die Cybersicherheit, ganz besonders jene der kritischen Infrastrukturen, sehr wichtig, daher unterstützt sie diese Vorlage und lehnt gleichzeitig auch die Minderheitsanträge ab.

Graf-Litscher Edith (S, TG): Ich spreche für die SP-Fraktion zum Eintreten und auch gleich zu den Minderheiten. Die SP begrüsst die Einführung einer Meldepflicht von Cyberangriffen auf kritische Infrastrukturen. Energie, Strom, Wasser, Verkehr und unser Gesundheitswesen sind zentral; das wissen wir nicht erst seit der Corona-Krise. Seit Jahren verlangen wir einen Ausbau der Massnahmen gegen Cyberangriffe – eine Gefahr, die mit dem Angriffskrieg Russlands gegen die Ukraine noch akuter geworden ist.

Eine Meldepflicht für Cyberangriffe auf kritische Infrastrukturen ist eine wichtige Massnahme, da sie die Datenlage in diesem Bereich verbessert und es so erst ermöglicht, darauf angemessen zu reagieren und Warnungen auszusprechen. Damit die Schweiz ihre kritischen Infrastrukturen gezielt und effizient vor Cyberangriffen schützen kann, müssen die dafür zuständigen Stellen beim Bund Kenntnis über Herkunft, Methodik und Ausmass von Cyberangriffen haben, und dazu braucht es eben eine Meldepflicht.
In der EU ist eine solche Meldepflicht mit der Richtlinie 2016/1148 bereits seit August 2016 in Kraft. Die heutige Regelung in der Schweiz, welche seit 2005 auf Freiwilligkeit basiert, ist nicht ausreichend. Insbesondere im Cyberbereich ist heute nicht klar, wie gross das tatsächliche Ausmass der Bedrohung ist, da kaum Zahlen über die versuchten Angriffe vorliegen.
In seinem Bericht vom 13. Dezember 2019 zum Postulat Graf-Litscher 17.3475, "Meldepflicht bei schwerwiegenden Sicherheitsvorfällen bei kritischen Infrastrukturen", stellt der Bundesrat fest, dass es keine Meldepflicht für Cybervorfälle bei kritischen Infrastrukturen gibt. Deshalb erteilte er dem NCSC den Auftrag, die Einführung einer Pflicht zur Meldung

von Cybervorfällen zu prüfen. Nun liegt die Gesetzesvorlage auf dem Tisch, und wir können darüber entscheiden.
Dank der Meldepflicht verfügen die zuständigen Behörden nicht mehr nur über ein Gefühl für die ungefähre Anzahl Angriffe, vielmehr haben sie eine Übersicht über aktuelle Bedrohungen und effektiv erfolgte Angriffe. Somit können diese systematisch ausgewertet und die Erkenntnisse an Betreiber von kritischen Infrastrukturen weitergeleitet werden. Ein verlässliches Lagebild und Frühwarnsystem des Bundes versetzt die Betreiberinnen und Betreiber ausserdem in die Lage, Sicherheitslücken rechtzeitig zu erkennen, ihre Widerstandsfähigkeit – die Resilienz – zu erhöhen und Abwehrmassnahmen einzuleiten.
In der Kommission wurden zwei Minderheitsanträge eingereicht. Sie betreffen die Frist der Meldung gemäss Artikel 74e Absatz 1 und die Folgen einer Missachtung der Verfügungen des NCSC gemäss Artikel 74h. Die EU definiert in ihrer neuen Richtlinie über Massnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union ebenfalls eine Frist von 24 Stunden für die Meldung von Cyberangriffen. Es macht Sinn, wenn die Schweiz hier keine andere Frist einführt. Mit der Feststellung eines offensichtlichen Vorfalles wird man meldepflichtig.
Eine Meldung zu erstatten, ist übrigens kein grosses und kompliziertes bürokratisches Unterfangen. Sie ist einfach abzusetzen, und es muss auch keine Analyse mitgeliefert werden; man muss nur anzeigen, dass etwas passiert ist. Das NCSC wird dann entweder Hilfe anbieten oder später darauf zurückkommen.
Würde die Meldung erst nach 72 Stunden erfolgen, wie es die Minderheit Zuberbühler fordert, käme die Hilfe sehr oft zu spät. Eine Busse wird also erst fällig, wenn man trotz Kenntnis eines Vorfalles nicht innerhalb von 24 Stunden reagiert. Keine Busse wird fällig, wenn man eine Meldung erstattet, mit dem Inhalt, dass zwar etwas passiert sei, dass man aber die konkreten Umstände noch nicht genau kenne.
Ich komme zum Schluss: Die EU sieht eine Bussenpraxis vor, die effektiv, angemessen und abschreckend sein soll. Der Entwurf des Bundesrates entspricht diesen Vorgaben. Die SP-Fraktion wird deshalb der Mehrheit der Kommission folgen und warnt vor einem Verzicht auf Bussen. Damit würde die Meldepflicht zu einem Papiertiger, und wir würden uns eine grosse Chance für ein wirkungsvolles Frühwarnsystem gegen Cyberangriffe vergeben.

Fiala Doris (RL, ZH): Sie wissen es, die FDP-Fraktion ist grundsätzlich vom Leitgedanken "Privat vor Staat" geführt. Grosse Risiken sind jedoch global, so auch die Cyberkriminalität, und Sicherheit ist erste Staatsaufgabe. Die ins Auge gefasste Lösung ist deshalb massvoll. Die Meldepflicht ist richtig und wichtig, von der Bundesversammlung über die Armee bis hin zur Schweizer Nationalbank, so, wie es aufgelistet wurde.
Natürlich müssen wir auch im Bildungsbereich investieren, gerade auch in der Schweiz. In der Schweiz ist die Bildung bekanntlich bei den Kantonen angesiedelt. Lediglich die Berufsbildung und die ETH unterstehen dem Bund. Sicherheit ist jedoch erste Staatsaufgabe. Diese Besonderheit mag mit ein Grund dafür sein, dass wir punkto Cybersecurity immer noch nur im internationalen Mittelfeld mitspielen. Frankreich und Italien beispielsweise liegen deutlich vor uns.
Wir agieren politisch traditionell nicht top-down. Handlungsbedarf ist für mich und die FDP-Fraktion jedoch unbestritten. Ich danke dem Bundesrat für die neue Verpflichtung im Informationssicherheitsgesetz. Es ist für uns zwingend, dass auch das VBS weiterhin professionelle Unterstützung leistet. Ich bin stolz auf die Departementsvorsteherin, Bundesrätin Viola Amherd, und ihr Team. Dank ihr werden etwa Cyberrekruten ausgebildet, was mich begeistert und was einen äusserst wertvollen Beitrag leistet.

Das Miteinander von Staat und privatem Bereich entspricht unserem System. Wir kämpfen gemeinsam, gerade auch in der Cybersecurity. Aber die Meldepflicht trägt dazu bei, dass Cyberkriminalität wirklich nun auch ahndbar ist und dass Erpressern eher das Handwerk gelegt werden kann. Es ist gerade deshalb nicht schön, dass sich die Schweiz international gemäss dem Cyber Risk Index auf Platz 42 positioniert; hinter uns liegt Ghana. Gemäss dem Global Risk Report 2022, Chapter 3, müssen wir leider zur Kenntnis nehmen, dass Ransomware im Jahr 2022 international um 435 Prozent zugenommen hat. Demgegenüber fehlen national und international Cybersecurity-Expertinnen und -Experten. Man geht weltweit von einem Mangel von 3 Millionen Fachkräften aus. Erschreckend ist, dass insbesondere auch der professionelle Fachkräftemangel eine grosse Dramatik im Cybersicherheitsbereich darstellt. 95 Prozent der Cyberkriminalität sind auf menschliche Fehler zurückzuführen.
Nun, was tun? Eine Meldepflicht für Cyberangriffe, wie sie der Bundesrat will, eine Meldepflicht für kritische Infrastrukturen, ist nicht übertrieben, sondern zwingend. Wenn wir uns vergegenwärtigen, wie gross das Wachstum bei der Digitalisierung ist – Experten gehen von einem Wachstumswert von rund 800 Milliarden Dollar per 2024 aus –, erkennen wir rasch, wie riesig der Bedarf an Cybersecurity weltweit ist und dass die Verletzlichkeit steigt und dadurch die Meldepflicht umso wichtiger wird. Auf Seite 3 der Fahne zum Informationssicherheitsgesetz sind in Artikel 2 einleuchtend die Infrastrukturen aufgelistet, welche effektiv neu zu einer Meldepflicht verpflichtet werden. Vertrauen setzt Verantwortung voraus.
Sagen auch Sie Ja zur Meldepflicht; ich danke Ihnen allerbestens.

Fivaz Fabien (G, NE): Le rôle du Centre national pour la cybersécurité, le NCSC, doit être très étendu. Il doit être capable d'identifier les faiblesses et les risques de manière active. Il doit soutenir la population, l'économie et les collectivités pour prendre toutes les mesures nécessaires afin de se protéger contre les cyberattaques et de réagir en cas d'incident. Dans ce sens, il est important qu'un maximum de failles et d'attaques soient signalées. Il est essentiel aussi que ces informations soient divulguées et transmises le plus rapidement possible si aucun intérêt public prépondérant ne s'y oppose. Elles doivent servir, en définitive, à protéger toutes les infrastructures informatiques de notre pays.
Dans ce sens, l'obligation de signaler les cyberincidents graves pour les infrastructures critiques est importante. Elle complète parfaitement le système actuel, qui permet déjà de signaler volontairement des incidents. Ces informations profiteront à l'ensemble des acteurs. Des signalements pourront être transmis publiquement et sous forme anonymisée. Cette obligation permet aussi de renforcer la sécurité de l'ensemble du domaine cyber en Suisse.
En définitive, le NCSC doit aussi pouvoir fixer des délais pour la mise en conformité lorsqu'il constate des failles persistantes. Elle est accompagnée de mesures de soutien de la part du NCSC. Le service fournira en contrepartie de cette obligation une évaluation technique et un soutien subsidiaire dans la gestion de l'attaque. C'est une obligation: si un responsable d'infrastructure critique devait ne pas remplir cette obligation, il se verrait alors infliger une amende, dont le montant pourrait être important – 100 000 francs, d'autres l'ont dit.
Quant aux propositions de minorité, le groupe des Verts vous propose de suivre la majorité pour l'ensemble de ces propositions.
Il s'agit notamment de l'article 74e alinéa 1, où nous suivrons la majorité et le Conseil fédéral. Le signalement doit être effectué le plus rapidement possible pour que l'information profite au NCSC et à l'ensemble des infrastructures. Les premières heures sont, en ce sens, cruciales.
A l'article 74h, nous suivrons également la majorité et le Conseil fédéral. Cet aspect a fait l'objet d'importantes discussions dans le cadre de la consultation. Sans amende, l'obligation perd tout son sens; pire, elle permettrait sans doute à des infrastructures d'être les passagers clandestins du système: ne rien signaler et profiter du signalement des autres. A noter encore que le système est incitatif, je l'ai déjà dit. Le NCSC soutient en retour les infrastructures qui sont touchées.
Au vote sur l'ensemble, le groupe des Verts acceptera les modifications de la loi, et vous propose de faire de même.

AB 2023 N 553 / BO 2023 N 553

Zuberbühler David (V, AR): Aktuell fehlt eine Übersicht darüber, welche Cyberangriffe wo stattgefunden haben, da Cyberangriffe heute dem NCSC auf freiwilliger Basis gemeldet werden. Der Bundesrat ist der Ansicht, dass Freiwilligkeit bei der Meldung zu einem unvollständigen Lagebild führen könnte. Da Cyberrisiken zu den wichtigsten Bedrohungen der Sicherheit und der Wirtschaft unseres Landes gehören, will er eine Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen einführen und dadurch zur Frühwarnung beitragen.

Microsoft hat erst kürzlich den Digital Defense Report 2022 veröffentlicht. Mit diesem Report fasst Microsoft die wichtigsten Erkenntnisse seiner Sicherheitsexperten zusammen. Der Bericht zeigt, dass Cyberangriffe auf kritische Infrastrukturen eine immer grössere Rolle spielen. Wir teilen deshalb die Einschätzung des Bundesrates, dass aufgrund der rasant wachsenden Zahl von Cyberangriffen auf Schweizer Unternehmen und Institutionen in geeignete Schutzmassnahmen investiert werden muss. Dies gilt besonders bei den kritischen Infrastrukturen, die eine wichtige gesellschaftliche und wirtschaftliche Funktion erfüllen. Ihre Störung, ihr Ausfall oder ihre Zerstörung hätten gravierende Auswirkungen auf das Funktionieren der Gesellschaft, der Wirtschaft und des Staates. Sie müssen deshalb auch im Zuge eines Cyberangriffes möglichst gut funktionieren.
Betreiber kritischer Infrastrukturen müssen sich im Ernstfall möglichst rasch mit den Behörden austauschen können. Die Kooperation kann dabei für beide Seiten einen Mehrwert darstellen. Die betroffenen Unternehmen profitieren von Unterstützungsleistungen der Behörden, und die Behörden erhalten wichtige Informationen für ein umfassendes Lagebild.
Die SVP-Fraktion hat gegen eine Meldepflicht keine grundsätzlichen Einwände, solange die administrativen und finanziellen Auswirkungen auf die Wirtschaft gering bleiben. Wir sind aber der Ansicht, dass die Meldepflicht in erster Linie im Rahmen einer Service-Mentalität erfolgen und nicht als Kontrollinstrument ausgelegt werden soll. Staat und Unternehmen haben bei Cyberangriffen schliesslich von Anfang an das gleiche Interesse, nämlich die Sicherheit und Funktionsfähigkeit betroffener Systeme und Daten zu gewährleisten.
Die SVP-Fraktion erkennt deshalb wenig Sinn darin, die neue Meldepflicht mit hohen Bussen durchzusetzen, die überdies ein Klima des Misstrauens schaffen. Zudem erachten wir eine persönliche Strafbarkeit von natürlichen Personen als kontraproduktiv, da es Personen abschreckt, im Bereich der Cybersicherheit Verantwortung zu übernehmen. Unsere Fraktion vertritt deshalb die Ansicht, dass es statt eines staatlichen Zwangs ein gutes Angebot des Staates braucht, das für die betroffenen Betreiber kritischer Infrastrukturen höchst attraktiv ist und die Zusammenarbeit eben ohne Zwänge fördert. Der Bundesrat will eigentlich das Gleiche. In seiner Botschaft zum vorliegenden Gesetz schreibt er schliesslich, dass die über den Informationsaustausch entwickelte Kultur der Zusammenarbeit und des gegenseitigen Vertrauens weitergeführt werden soll und es dabei entscheidend sei, dass den Unternehmen und Organisationen aus der Einführung der Meldepflicht eben auch ein Mehrwert entstehe.
Die SVP-Fraktion lehnt die Möglichkeit einer Sanktionierung grundsätzlich ab, weil sie der Ansicht ist, dass die Meldepflicht nicht über Bussen, sondern über Anreize durchgesetzt werden muss und dass Bestrafungen dem Ziel eines möglichst guten Informationsaustausches zwischen Bund und Privaten zuwiderlaufen. Letztlich kann es ja nicht sein, dass diejenigen gebüsst werden, die angegriffen werden und von denen schliesslich keine kriminelle Energie ausgeht. Die Meldepflicht muss dem Bund, den betroffenen Unternehmen und der Gesamtwirtschaft einen messbaren Mehrwert bringen.
Dass Cyberangriffe oder noch nicht öffentlich bekannte Schwachstellen gemeldet werden, muss mit Anreizen sichergestellt werden – ganz bestimmt nicht durch das Androhen einer Busse. Die Strafbestimmung in Artikel 74h ist deshalb letztlich das Killerkriterium, das darüber entscheidet, ob unsere Fraktion der Änderung des Informationssicherheitsgesetzes zustimmen wird oder nicht. Sollte die Strafbestimmung im Rahmen der Detailberatung nicht ersatzlos gestrichen werden, wird unsere Fraktion dem vorliegenden Entwurf nicht zustimmen.

Mettler Melanie (GL, BE): Das Informationssicherheitsgesetz dient dazu, dass wir in der Schweiz besser vor Cyberangriffen geschützt werden und diesbezüglich stärker sensibilisiert und besser unterstützt werden. Man denkt es vielleicht kaum – wir denken von uns selber ja immer, wir seien Weltmeister in allem, aber die Schweiz ist eben nicht in allem Weltmeisterin -: Gerade bei den digitalen Kompetenzen sind wir relativ schlecht; wir haben tiefe Werte bei der digitalen Kompetenz, der sogenannten "digital literacy". Gekoppelt mit dem Föderalismus heisst das dann auch, dass wir in sehr kleinen Strukturen arbeiten, die vielleicht nicht überall dieselbe Professionalität aufweisen. Kleine Strukturen können ein Vorteil sein, gerade im Bereich der Cybersicherheit, aber es ist damit halt auch schwierig, die Übersicht zu behalten und sich ein Bild davon zu machen, wo Bedrohungen eigentlich wirklich anfallen. Es ist deshalb richtig, dass wir hier eine Meldepflicht einführen.
Das NCSC unterstützt die Betreiberinnen von kritischen Infrastrukturen beim Schutz vor Cyberbedrohung; das ist seine Hauptaufgabe. Um diese Aufgabe durchführen zu können, muss das NCSC auch wissen, wo Bedrohungen anfallen, wie sie anfallen und wie die Entwicklungen sind, wie sich die Bedrohungslage mit Blick auf innere und äussere Sicherheit entwickelt, um entsprechende Empfehlungen, Sensibilisierungsmassnahmen und Unterstützungsangebote entwickeln zu können.
Worum geht es hier? Was heisst eigentlich "kritische Infrastrukturen"? Das geht eben sehr weit, das sieht man, wenn man sich das mal vor Augen führt: Es sind die Hochschulen, die Bundes-, Kantons- und Gemein-

debehörden, Einrichtungen der Trinkwasserversorgung und andere Infrastrukturen, das ist klar; es sind aber auch Unternehmen aus den Bereichen Energie, Bauwesen, Gesundheit, Information, Verkehr. Das ist alles vulnerabel.
Die GLP-Fraktion ist überzeugt, dass hier eine pragmatische Umsetzung zu machen ist, ohne grossen administrativen Aufwand zu kreieren, ohne eine neue Datenkrake zu bauen. Deshalb unterstützen wir hier bei allen Artikeln die Mehrheit und werden dem Gesetz zustimmen.

Amherd Viola, Bundesrätin: Cyberangriffe sind eine zentrale Bedrohung für Wirtschaft, Staat und Gesellschaft. In enger Zusammenarbeit mit der Privatwirtschaft, den Kantonen und den Hochschulen tritt der Bund gegen diese Bedrohung an. Eine grosse Herausforderung dabei ist, dass Angreifer ihre Methoden ständig ändern. Entscheidend für die rechtzeitige Warnung und Abwehr von Cyberangriffen ist daher, dass neue Angriffsmethoden rasch erkannt werden. Aus diesem Grund sind Meldungen zu Cyberangriffen an das NCSC sehr wichtig.
Das NCSC führt heute schon eine Meldestelle, an welche Cyberangriffe gemeldet werden können. Über eine geschlossene Plattform pflegt es zudem den Informationsaustausch mit kritischen Infrastrukturen. Dieser freiwillige Informationsaustausch stösst aber an Grenzen. Während einige Unternehmen sich aktiv daran beteiligen, profitieren andere von den Warnungen, ohne selber zum Informationsaustausch beizutragen. Dies ist vor allem dann störend, wenn es sich bei den Unternehmen um kritische Infrastrukturen handelt, deren Funktionieren für uns alle von grosser Bedeutung ist.
Der Bundesrat hat sich deshalb dafür entschieden, dem Parlament die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen vorzuschlagen, wie sie bereits in vielen Ländern existiert und in der EU 2018 eingeführt wurde. Verfolgt wird damit das Ziel, den Informationsaustausch zu stärken und dem NCSC fundierte Einschätzungen zu Cyberbedrohungen in der Schweiz zu ermöglichen.
Der Meldepflicht unterstellt werden kritische Infrastrukturen sowie Organisationen, bei denen ein Cyberangriff direkte Auswirkungen auf kritische Infrastrukturen hat. Diese müssen schwerwiegende Cyberangriffe innerhalb von 24 Stunden über ein elektronisches Meldeformular dem NCSC melden. Erfüllen Organisationen die Meldepflicht nicht, werden sie vom NCSC auf die Meldepflicht hingewiesen. Erst wenn weiterhin keine Reaktion erfolgt, ist das NCSC befugt, die Meldung über eine Verfügung einzufordern.

AB 2023 N 554 / BO 2023 N 554

Neben der Meldepflicht legt die Vorlage auch fest, welche Aufgaben der Bund in der Cybersicherheit übernimmt. Insbesondere wird das NCSC verpflichtet, den kritischen Infrastrukturen subsidiäre erste Hilfe bei der Bewältigung von Cyberangriffen anzubieten.
Schliesslich berücksichtigt die Vorlage auch den Schutz der Meldenden. Das NCSC leitet ohne Einverständnis keine Angaben über die Meldenden an andere Stellen weiter. Ausnahmen sind nur für die Weiterleitung an den Nachrichtendienst bei Bedrohungen der nationalen Sicherheit und für Weiterleitungen an die Strafverfolgungsbehörden bei Fällen von schwerer Kriminalität möglich.
Zusammenfassend kann gesagt werden, dass die Einführung der Meldepflicht weder zu einer finanziellen noch zu einer administrativen Belastung für die Unternehmen führt. Sie stärkt vielmehr die Zusammenarbeit zwischen Bund und Privatwirtschaft. Dafür sind folgende Gründe ausschlaggebend:
1. Die Meldepflicht kann ohne grösseren Aufwand über ein Meldeformular erfüllt werden.
2. Die Informationen werden vom NCSC vertraulich behandelt.
3. Die Meldung führt zu einem Anspruch auf subsidiäre Unterstützung durch das NCSC.
4. Sanktionen sind bei Nichterfüllung der Meldepflicht erst als letztes Mittel möglich.

In der Vernehmlassung wurde die Meldepflicht überwiegend begrüsst. 89 von 99 Teilnehmenden, darunter alle Kantone, unterstützten die Einführung einer Meldepflicht, nur 7 haben sich dagegen ausgesprochen. Umstritten war die Einführung einer Sanktion bei Nichteinhaltung der Meldepflicht. 24 Teilnehmende lehnten eine Sanktionierung ab. Wir haben beschlossen, daran festzuhalten, da es wenig sinnvoll ist, eine Pflicht einzuführen, wenn sie nicht durchgesetzt werden kann. Weil das NCSC die Unternehmen vor der allfälligen Verfügung einer Sanktion aber darauf hinweisen muss, dass die Meldepflicht nicht erfüllt wurde, gehen wir davon aus, dass es kaum zu Sanktionen kommen wird.
Ansonsten gab es in der Vernehmlassung Präzisierungsvorschläge, die wir grösstenteils übernehmen konnten. Die Vorlage findet insgesamt also breite Zustimmung. Sie legt das rechtliche Fundament für die bereits gut etablierte Zusammenarbeit zwischen Wirtschaft und Staat.
Ihre Kommission beurteilt das gleich und empfiehlt Ihnen, wie gehört, auf die Vorlage einzutreten. Sie will dabei sogar noch etwas weiter gehen als der Bundesrat. Sie will die Unternehmen dazu verpflichten, nicht nur

Cyberangriffe, sondern auch neu entdeckte Schwachstellen in den verwendeten Informatikmitteln zu melden. Die Kommission beantragt entsprechend, Artikel 74d mit einem zweiten Absatz zu ergänzen, der festlegt, dass bisher unbekannte Schwachstellen in betriebskritischen Informatikmitteln gemeldet werden müssen.
Der Antrag der Kommission stärkt den präventiven Charakter der Vorlage. Die Meldepflicht setzt nicht erst ein, wenn bereits ein Angriff passiert ist, sondern bereits, wenn ein solcher möglich ist. Gleichzeitig muss man sich bewusst sein, dass jede Ausweitung der Meldepflicht zu einem Mehraufwand bei den betroffenen Unternehmen führen kann. Es gilt also beim Änderungsantrag der Kommission, ebenso wie bei der Beurteilung der gesamten Vorlage, zwischen dem Aufwand für die Unternehmen und der Stärkung der Cybersicherheit abzuwägen. Ich bin überzeugt, dass der Nutzen dieser Vorlage für die Cybersicherheit den Aufwand für die betroffenen Unternehmen deutlich übersteigt.
Ich bitte Sie deshalb, Ihrer Kommission zu folgen und auf die Vorlage einzutreten und ihr dann auch zuzustimmen.

Tuena Mauro (V, ZH): Frau Bundesrätin, Sie sprechen in dieser Vorlage von "kritischen Infrastrukturen". In dieser Vorlage sind Seilbahnen erwähnt. Gemäss Personenbeförderungsgesetz fallen zum Beispiel auch Sessellifte usw. unter den Begriff "Seilbahnen". Können Sie mir erklären, warum zum Beispiel ein Sessellift eine kritische Infrastruktur sein soll, die dann gemäss dem vorliegenden Gesetz einen Cyberangriff melden muss?

Amherd Viola, Bundesrätin: Es kommt darauf an, welche Funktion diese Bahn hat. Wenn sie beispielsweise eine Erschliessungsfunktion zu einem Gebiet hat, das nicht anderweitig zugänglich ist, kann es natürlich sehr wichtig sein, dass diese Funktion garantiert ist.

Dobler Marcel (RL, SG): Sehr geehrte Frau Bundesrätin, in Artikel 74b ist ja sehr genau definiert, welche Kreise oder welche Firmen von dieser Meldepflicht betroffen sind. Meine Angst ist jetzt, dass dieser Kreis viel zu stark geöffnet wird, ohne dass man weiss, wie viele Firmen genau betroffen sind. Die Zermatt Bergbahnen AG z. B. ist dann ja eben auch meldepflichtig. Können Sie mir genau sagen, mit wie vielen Firmen Sie rechnen, die dieser Meldepflicht unterstellt sind?

Amherd Viola, Bundesrätin: Das kann ich Ihnen im Moment nicht sagen. Es wurden aber diesbezüglich Erhebungen vom NCSC gemacht. Ich werde Ihnen das gerne bilateral noch mitteilen.

Eintreten wird ohne Gegenantrag beschlossen
L'entrée en matière est décidée sans opposition

Bundesgesetz über die Informationssicherheit beim Bund
Loi fédérale sur la sécurité de l'information au sein de la Confédération

Detailberatung – Discussion par article

Titel und Ingress; Ziff. I Einleitung; Titel; Art. 1 Abs. 1; 2 Abs. 5; 4 Abs. 1, 1bis; 5 Einleitung, Bst. d-g; 10a; 23 Abs. 3; 44 Abs. 2; Gliederungstitel nach Art. 73; Art. 73a
Antrag der Kommission
Zustimmung zum Entwurf des Bundesrates

Titre et préambule; ch. I introduction; titre; art. 1 al. 1; 2 al. 5; 4 al. 1, 1bis; 5 introduction, let. d-g; 10a; 23 al. 3; 44 al. 2; titre suivant l'art. 73; art. 73a
Proposition de la commission
Adhérer au projet du Conseil fédéral

Angenommen – Adopté

Art. 73b
Antrag der Kommission
Abs. 1, 2
Zustimmung zum Entwurf des Bundesrates

Abs. 3
Erhält das NCSC Kenntnis von einer Schwachstelle, die nicht öffentlich bekannt ist, so informiert es umgehend ...

Art. 73b
Proposition de la commission
Al. 1, 2
Adhérer au projet du Conseil fédéral
Al. 3
Si le NCSC prend connaissance d'une vulnérabilité inconnue du public, il en informe immédiatement ...

Angenommen – Adopté

Art. 73c, 73d, 74
Antrag der Kommission
Zustimmung zum Entwurf des Bundesrates
Proposition de la commission
Adhérer au projet du Conseil fédéral

Angenommen – Adopté

Gliederungstitel nach Art. 74
Antrag der Kommission
... Cyberangriffen und Schwachstellen

AB 2023 N 555 / BO 2023 N 555

Titre suivant l'art. 74
Proposition de la commission
... cyberattaques et les vulnérabilités

Angenommen – Adopté

Art. 74a
Antrag der Kommission
Abs. 1
Behörden und Organisationen nach Artikel 74b müssen dafür sorgen, dass dem NCSC Cyberangriffe und Schwachstellen, welche ihre Informatikmittel betreffen, gemeldet werden.
Abs. 2
Zustimmung zum Entwurf des Bundesrates
Abs. 3
Durch die Meldung haben die meldepflichtigen ...
Abs. 4
Die Meldepflicht dient ausschliesslich dazu, dass das NCSC Cyberbedrohungen frühzeitig erkennen ...

Art. 74a
Proposition de la commission
Al. 1
Les autorités et les organisations énumérées à l'artcile 74b veillent à ce que les cyberattaques et les vulnérabilités concernant leurs moyens informatiques soient signalées au NCSC.
Al. 2
Adhérer au projet du Conseil fédéral
Al. 3
Lorsqu'elles signalent une cyberattaque ou une vulnérabilité, les autorités ...

Al. 4
... utilisés lors des cybermenaces et, ainsi, d'avertir ...

Angenommen – Adopté

Art. 74b
Antrag der Kommission
Abs. 1
...
d. ... auf eine Kernanlage erfolgt oder deren Informatikmittel eine Schwachstelle aufweisen;
...
Abs. 2
... für Cyberangriffe und Schwachstellen, die ausschliesslich diese Tätigkeiten betreffen.
Abs. 3
... gilt für Cyberangriffe und Schwachstellen, die sich in der ...

Art. 74b
Proposition de la commission
Al. 1
...
d. ... une installation nucléaire ou si ses moyens informatiques présentent une vulnérabilité;
...
Al. 2
... signaler les cyberattaques et les vulnérabilités qui concernent uniquement ces activités.
Al. 3
... s'applique aux cyberattaques et aux vulnérabilités qui ont un effet en ...

Angenommen – Adopté

Art. 74c
Antrag der Kommission
... durch Cyberangriffe oder Schwachstellen ausgelöste Funktionsstörungen ...

Art. 74c
Proposition de la commission
... par les cyberattaques ou les vulnérabilités n'ont qu'un effet limité ...

Angenommen – Adopté

Art. 74d
Antrag der Kommission
Titel
Zu meldende Cyberangriffe und Schwachstellen
Abs. 1
Zustimmung zum Entwurf des Bundesrates
Abs. 2
Eine Schwachstelle muss gemeldet werden, wenn sie betriebskritische Informatikmittel betrifft und sie noch nicht öffentlich bekannt ist.

Art. 74d
Proposition de la commission
Titre
Cyberattaques et vulnérabilités à signaler
Al. 1
Adhérer au projet du Conseil fédéral

Al. 2
Une vulnérabilité doit être signalée lorsqu'elle concerne des moyens informatiques essentiels pour l'exploitation et qu'elle est encore inconnue du public.

Angenommen – Adopté

Art. 74e
Antrag der Mehrheit
Abs. 1
Die Meldung muss innert 24 Stunden nach der Entdeckung des Cyberangriffs oder der Schwachstelle erfolgen.
Abs. 2
Sie muss Informationen zur meldepflichtigen Behörde oder Organisation, zur Art des Cyberangriffs oder der Schwachstelle, zu den Auswirkungen, zu ...
Abs. 3, 4
Zustimmung zum Entwurf des Bundesrates

Antrag der Minderheit
(Zuberbühler, Addor, Heimgartner, Hess Erich, Hurter Thomas, Tuena, Walliser)
Abs. 1
Die Meldung muss innert 72 Stunden nach der Entdeckung des Cyberangriffs oder der Schwachstelle erfolgen.

Art. 74e
Proposition de la majorité
Al. 1
Le signalement doit être fait dans les 24 heures suivant la détection de la cyberattaque ou de la vulnérabilité.
Al. 2
... la cyberattaque ou de la vulnérabilité, sur les effets, sur les mesures ...
Al. 3, 4
Adhérer au projet du Conseil fédéral

Proposition de la minorité
(Zuberbühler, Addor, Heimgartner, Hess Erich, Hurter Thomas, Tuena, Walliser)
Al. 1
Le signalement doit être fait dans les 72 heures suivant la détection de la cyberattaque ou de la vulnérabilité.

Zuberbühler David (V, AR): Bei Artikel 74e Absatz 1 spreche ich im Sinne der Effizienz für meine Minderheit sowie für die SVP-Fraktion.
Gemäss dem Entwurf des Bundesrates und dem Antrag der Kommissionsmehrheit bei Artikel 74e ist der Meldepflicht innert 24 Stunden nach dem Entdecken eines Cybervorfalls oder einer Schwachstelle nachzukommen. Die Pflicht bezieht sich dabei auf Betreiber kritischer Infrastrukturen gemäss

Artikel 74 Absatz 1 mit dem Ziel, Unterstützung durch das NCSC gemäss Artikel 74a Absatz 3 zu bieten sowie dieses in die Lage zu versetzen, Angriffsmuster zu erkennen, mögliche Betroffene zu warnen sowie Präventionsmassnahmen einzuleiten.
Wie sieht das denn heute in der Praxis aus? Kritische Infrastrukturen umfassen all die Einrichtungen und Systeme, die ein Gemeinwesen braucht, um zu funktionieren. Fallen sie aus, kann das zu Problemen bei der Versorgung und der öffentlichen Sicherheit führen. Ich habe nicht zuletzt deshalb in meinem Eintretensvotum darauf hingewiesen, dass Cyberangriffe auf kritische Infrastrukturen eine immer grössere Rolle spielen. So kommt es nicht von ungefähr, dass Betreiber kritischer Infrastrukturen eben nicht täglich oder wöchentlich Cyberangriffe erleben, sondern buchstäblich im Sekundentakt. Dafür haben Betreiber kritischer Infrastrukturen im Rahmen der Selbstregulierung in den letzten Jahren und Jahrzehnten entsprechende Strukturen aufgebaut und sich mit entsprechenden Partnern zusammengetan. Für all diese Teams sind Cyberangriffe buchstäblich das tägliche Brot. Um einen solchen Angriff heutzutage mit einigem Erfolg zu lancieren, braucht es auf der Seite der Angreifer eine ebenso langwierige wie gross angelegte Vorbereitung, entsprechende Mittel und Ressourcen, vor allem aber viel Zeit und Know-how.

Es ist zwar ein hehres Ziel des Informationssicherheitsgesetzes, das NCSC in die Lage zu versetzen, bei einem Angriff auf eine kritische Infrastruktur die angegriffene Organisation zu unterstützen und bei vergleichbaren Organisationen präventiv wirken zu können. Ob es angesichts der beschriebenen Vorkehrungen allerdings ein realistisches Ziel ist, darf zumindest infrage gestellt werden.
Bei dieser alles andere als einfachen Ausgangslage ist eine enge zeitliche Limite nicht zielführend, denn entweder erfolgt ein Massenangriff – dann sind 24 Stunden viel zu lang – oder der Angriff ist gezielt und über Wochen vorbereitet worden, womit 24 Stunden eben auch nicht weiterhelfen. Hinzu kommt, dass Betreiber kritischer Infrastrukturen, die aufgrund ihrer Organisationsgrösse im Bereich der Cybersicherheit vielleicht nicht so gut aufgestellt sind, Wichtigeres zu tun haben, als innerhalb von 24 Stunden Meldung an das NCSC zu erstatten. Einerseits müssen die betroffenen Unternehmen zuerst das Ausmass der Cyberattacke feststellen, andererseits liegt ihr Fokus ab dem Zeitpunkt des Cyberangriffes klar auf der Cyberabwehr. Diese Unternehmen sollten zuerst die Möglichkeit haben, selbst die Auswirkungen und Lücken im System zu identifizieren, bevor sie dem NCSC Meldung erstatten.
Last, but not least: Wahrscheinlich würde bei einer sofortigen Meldung unweigerlich eine Vielzahl von unnötigen Meldungen abgesetzt werden, weil Cybervorfälle zum Stichzeitpunkt noch gar nicht richtig beurteilt werden können. Die 24-Stunden-Regel, die bei einer Verletzung zusätzlich eine Busse nach sich ziehen würde, ist deshalb zu eng gefasst und stellt ein grundsätzliches Problem der ISG-Änderung dar. In diesem Sinne bitte ich Sie, einer praxistauglichen Umsetzung zuzustimmen und die Meldefrist auf 72 Stunden zu verlängern.

Amherd Viola, Bundesrätin: Sie haben es gehört: Die Minderheit beantragt, die Meldefrist von 24 auf 72 Stunden zu erhöhen. 24 Stunden sind bei einem Cyberangriff bereits relativ lang. Wenn Angriffe auf weitere Betroffene verhindert werden sollen, ist es wichtig, rasch Kenntnis über den Angriff zu haben. Für den Zweck der Frühwarnung ist deshalb eine kurze Frist wichtig. International hat sich zudem eine Frist von 24 Stunden durchgesetzt. Auch die EU definiert in der neuen Richtlinie zur Netzwerk- und Informationssicherheit eine Frist von 24 Stunden für die Meldung von Cyberangriffen. Die Frist ist zudem nicht so streng, wie sie vielleicht auf den ersten Blick erscheint. Im entsprechenden Artikel wird nämlich relativiert, dass Angaben, die innert 24 Stunden nicht gemacht werden können, später nachgeliefert werden dürfen. Für die Nachlieferung wurde bewusst auf eine Frist verzichtet, um die Unternehmen, die bei einem Angriff bereits unter Stress stehen, nicht zusätzlichem Druck auszusetzen. Dies scheint uns wichtiger als eine Fristverlängerung für die Erstmeldung.
Ich bitte Sie, den Minderheitsantrag abzulehnen und damit die Kommissionsmehrheit zu unterstützen.

Abstimmung – Vote
(namentlich – nominatif; 22.073/26464)
Für den Antrag der Mehrheit ... 129 Stimmen
Für den Antrag der Minderheit ... 52 Stimmen
(0 Enthaltungen)

Art. 74f
Antrag der Kommission
Abs. 1
Für die elektronische Meldung stellt das NCSC ...
Abs. 2
... ermöglichen, die Meldung gesamthaft oder ...
Abs. 3
Zustimmung zum Entwurf des Bundesrates

Art. 74f
Proposition de la commission
Al. 1
... le signalement par voie électronique.
Al. 2
... d'autres autorités tout ou partie du signalement.
Al. 3
Adhérer au projet du Conseil fédéral

Angenommen – Adopté

Art. 74g
Antrag der Kommission
Zustimmung zum Entwurf des Bundesrates
Proposition de la commission
Adhérer au projet du Conseil fédéral

Angenommen – Adopté

Art. 74h
Antrag der Mehrheit
Zustimmung zum Entwurf des Bundesrates

Antrag der Minderheit
(Zuberbühler, Addor, Heimgartner, Hess Erich, Hurter Thomas, Tuena, Walliser)
Streichen

Art. 74h
Proposition de la majorité
Adhérer au projet du Conseil fédéral

Proposition de la minorité
(Zuberbühler, Addor, Heimgartner, Hess Erich, Hurter Thomas, Tuena, Walliser)
Biffer

Zuberbühler David (V, AR): Auch bei Artikel 74h spreche ich im Sinne der Effizienz für meine Minderheit und auch für die SVP-Fraktion.
Auch hier sind der Bundesrat und die Kommissionsmehrheit der Meinung, dass die Einführung einer obligatorischen Meldepflicht der Weiterführung des freiwilligen Informationsaustauschs vorgezogen werden soll. Dennoch soll gemäss Bundesrat – und das immer wieder, wohlverstanden, unter Strafandrohung – die über den Informationsaustausch entwickelte Kultur der Zusammenarbeit und des gegenseitigen Vertrauens weitergeführt werden. Für den Bundesrat ist es gemäss der Botschaft zur ISG-Änderung entscheidend, dass den Unternehmen und Organisationen über die Einführung der Meldepflicht auch ein Mehrwert entsteht.
Ich unterstütze diese magistrale Haltung vollumfänglich, kann aber beim besten Willen nicht nachvollziehen, weshalb der Bundesrat Bussen als letzte Konsequenz in Betracht ziehen möchte. Ich habe bereits im Rahmen der Eintretensdebatte darauf hingewiesen, dass unsere Fraktion der Ansicht ist, dass es statt eines staatlichen Zwangs ein sehr

gutes Angebot des Staates braucht, welches für die betroffenen Betreiber kritischer Infrastruktur höchst attraktiv ist und die Zusammenarbeit mit dem Bund auf freiwilliger Basis ohne jegliche Zwänge fördert. Die Meldepflicht soll deshalb nicht über Bussen, sondern über positive Anreize durchgesetzt werden. Bestrafungen würden, davon sind wir überzeugt, dem Ziel eines möglichst guten Informationsaustauschs zwischen Bund und Privaten zuwiderlaufen. Der negative Anreiz in Form einer Busse steht dem Ansatz einer kooperativen Zusammenarbeit entgegen. Ausserdem ist die für eine Verletzung der Melde- und Auskunftspflichten vorgesehene Busse von 100 000 Schweizerfranken unverhältnismässig.
Die Busse ist letztlich auch nicht begründbar, da von den betroffenen Unternehmen – ich wiederhole es noch einmal – schliesslich gar keine kriminelle Energie ausgeht. Bei den betroffenen Unternehmen handelt es sich nicht um die Verursacher der Cyberangriffe, sondern um von Cyberangriffen betroffene Betreiber kritischer Infrastruktur. Der beantragte Bussenrahmen kann ausserdem die Bereitschaft der zuständigen Personen reduzieren, in Sachen Cybersecurity Verantwortung zu übernehmen.
Abschliessend weise ich darauf hin, dass es im Ermessen des NCSC liegt, ob es einen der vielen täglichen Angriffe als kritisch für das ordnungsgemässe Funktionieren der angegriffenen kritischen Infrastruktur einschätzt. In der Praxis könnte es aufgrund unterschiedlicher Auffassungen durchaus vorkommen, dass sich das NCSC und der Betreiber oder die Betreiberin einer kritischen Infrastruktur über die Qualität des Angriffs uneinig sind. Der Effekt der Bussenregelung könnte deshalb zu einer Vielzahl unnötiger Meldungen führen und damit den

Personalbedarf des NCSC unnötig aufblähen. Spätestens dann würde dieses ISG-Bürokratiemonster noch weiter aufgebläht und der Finanzhaushalt des Bundes noch weiter strapaziert werden.
In diesem Sinn bitte ich Sie, der Streichung von Artikel 74h zuzustimmen, weil damit der Verbotscharakter dieser Vorlage entfallen würde.

Amherd Viola, Bundesrätin: Die Minderheit Zuberbühler beantragt die Streichung der Möglichkeit von Sanktionierungen bei Nichtbefolgen der Meldepflicht. Ohne Sanktionierungsmöglichkeit ist die Meldepflicht nur theoretischer Natur. Es geht aber keinesfalls darum, möglichst viele Unternehmen zu bestrafen. Artikel 74g legt fest, dass das Unternehmen vor einer Verfügung durch das NCSC auf die Meldepflicht aufmerksam gemacht werden muss. Das Unternehmen wird also zuerst vorgewarnt, erhält dann eine Verfügung, und erst wenn es immer noch nicht meldet, kommt eine Busse infrage. Bussen werden also nur dann ausgesprochen, wenn sich die verantwortliche Person einer kritischen Infrastruktur aktiv weigert, über die Meldung eines Angriffs zur Frühwarnung und zur besseren Einschätzung der Bedrohungslage beizutragen.
Ich bitte Sie, die Minderheit Zuberbühler abzulehnen und der Kommissionsmehrheit zuzustimmen.

Präsident (Candinas Martin, Präsident): Bevor wir über Artikel 74h abstimmen, möchte ich unseren drei Kollegen Jean-Pierre Grin, Pierre-Yves Maillard und Michael Töngi zum Geburtstag gratulieren. Cordiala gratulaziun! *(Applaus)*

Abstimmung – Vote
(namentlich – nominatif; 22.073/26465)
Für den Antrag der Mehrheit ... 130 Stimmen
Für den Antrag der Minderheit ... 55 Stimmen
(1 Enthaltung)

Gliederungstitel vor Art. 75; Art. 75; 76; 76a; 77; 78; 79 Abs. 1; 80; Ziff. II Einleitung, Ziff. 1, 2
Antrag der Kommission
Zustimmung zum Entwurf des Bundesrates

Titre précédant l'art. 75; art. 75; 76; 76a; 77; 78; 79 al. 1; 80; ch. II introduction, ch. 1, 2
Proposition de la commission
Adhérer au projet du Conseil fédéral

Angenommen – Adopté

Ziff. II Ziff. 3 Art. 102 Abs. 2
Antrag der Kommission
... auf eine Kernanlage oder zu einer Schwachstelle in deren Informatikmitteln, welche die Voraussetzungen von ...

Ch. II ch. 3 art. 102 al. 2
Proposition de la commission
... une installation nucléaire ou concernant une vulnérabilité dans ses moyens informatiques et remplissant les conditions visées ...

Angenommen – Adopté

Ziff. II Ziff. 4, 5; Ziff. III
Antrag der Kommission
Zustimmung zum Entwurf des Bundesrates

Ch. II ch. 4, 5; ch. III
Proposition de la commission
Adhérer au projet du Conseil fédéral

Angenommen – Adopté

Gesamtabstimmung – Vote sur l'ensemble
(namentlich – nominatif; 22.073/26466)
Für Annahme des Entwurfes ... 132 Stimmen
Dagegen ... 55 Stimmen
(0 Enthaltungen)

Präsident (Candinas Martin, Präsident): Das Geschäft geht an den Ständerat.