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)

Zweitrat – Deuxième Conseil

CHRONOLOGIE

NATIONALRAT/CONSEIL NATIONAL 16.03.23 (ERSTRAT - PREMIER CONSEIL)
STÄNDERAT/CONSEIL DES ETATS 01.06.23 (ZWEITRAT - DEUXIÈME CONSEIL)

Präsidentin (Häberli-Koller Brigitte, Präsidentin): Ich eröffne die heutige Sitzung und begrüsse herzlich die Vizepräsidentin des Bundesrates, Frau Amherd.

Gmür-Schönenberger Andrea (M-E, LU), für die Kommission: Die Einführung einer Meldepflicht bei schwerwiegenden Sicherheitsvorfällen, also bei Cyberangriffen, bei kritischen Infrastrukturen wie Spitälern, Elektrizitätswerken oder Hochschulen beschäftigt das Parlament seit mehreren Jahren. Der Bundesrat hat die vorliegende Botschaft am 2. Dezember 2022 verabschiedet. Die Vorlage will die gesetzlichen Grundlagen zu einer Meldepflicht für Betreiberinnen und Betreiber kritischer Infrastrukturen schaffen und die Aufgaben des Nationalen Zentrums für Cybersicherheit (NCSC) definieren, welches als zentrale Meldestelle für Cyberangriffe vorgesehen ist. Das NCSC führt heute schon eine Meldestelle, an welche Cyberangriffe freiwillig gemeldet werden können.
Die Einführung einer Meldepflicht und die Verankerung des NCSC als nationale Meldestelle bedeuten nun wichtige Schritte zur Verbesserung der Cybersicherheit in der Schweiz. Cyberangriffe sind klar eine zentrale Bedrohung für Wirtschaft, Staat und Gesellschaft. Diese Bedrohungen sollen in enger Zusammenarbeit mit der Privatwirtschaft, den Kantonen und auch den Hochschulen bekämpft werden. Eine grosse Herausforderung dabei ist, dass Angreifer ihre Methoden ständig ändern. Entscheidend für die rechtzeitige Warnung vor und die Abwehr von Cyberangriffen ist, dass neue Angriffsmethoden rasch erkannt werden und dass rasch reagiert wird.
Unser Rat ist Zweitrat. Der Nationalrat hat die Vorlage am 16. März dieses Jahres beraten und ihr mit 132 zu 55 Stimmen zugestimmt. Umstritten war im Schwesterrat die Einführung einer Sanktion bei Nichteinhaltung der Meldepflicht. Eine Pflicht macht aber nur dann Sinn, wenn sie auch durchgesetzt werden kann. Zudem sollen Sanktionen erst als letztes Mittel eingesetzt werden. Erst bei einer klaren Weigerung eines säumigen meldepflichtigen Unternehmens wird überhaupt eine Busse gesprochen.
Für Ihre SiK ist zentral, dass die Meldepflicht ohne grossen Aufwand erfüllt werden kann und dass die Informationen durch das NCSC stets vertraulich behandelt werden. Die Zahl der Unternehmen, die von der Meldepflicht betroffen sind, konnte nicht genau angegeben werden. Allerdings beschränkt sich die Pflicht auf die Betreiber kritischer Infrastrukturen und diejenigen Unternehmen, die für deren Funktionieren relevant sind. Eine Sesselbahn z. B. gehört nur dann zu den kritischen Infrastrukturen, wenn sie die Erschliessung eines bewohnten Gebietes gewährleistet, das ansonsten nicht zugänglich wäre.
Schwerwiegende Cyberangriffe müssen innerhalb von 24 Stunden dem NCSC gemeldet werden. Dies ist eine gängige Frist. Die Meldung führt dann zu einem Anspruch auf subsidiäre Unterstützung durch das NCSC.
Der Nationalrat hat eine Änderung vorgenommen, die auch die Mehrheit Ihrer SiK unterstützt. Er will, dass die Betreiber von kritischen Infrastrukturen dem NCSC nicht nur Cyberangriffe, sondern auch nicht öffentlich

bekannte Schwachstellen melden müssen. Es handelt sich dabei um eine Änderung von Artikel 73b, Artikel 74a bis 74f und Ziffer II Artikel 102. Alle Änderungen betreffen nur diesen einen Aspekt. Weitere Ausführungen dazu werde ich in der Detailberatung machen.
Unsere Kommission ist auf die Vorlage oppositionslos eingetreten. Zur Verordnung wird sie sich konsultieren lassen. In der Gesamtabstimmung hat Ihre Kommission zur Änderung des Informationssicherheitsgesetzes einstimmig Ja gesagt.
Ich bitte Sie, Ihrer SiK zu folgen.

Amherd Viola, Bundesrätin: Ich sage gerne zwei, drei Worte zum Eintreten, obwohl die Kommissionssprecherin das bereits sehr gut dargelegt hat.
Cyberangriffe sind eine zentrale Bedrohung für Wirtschaft, Staat und Gesellschaft. In enger Zusammenarbeit mit der Privatwirtschaft, den Kantonen und den Hochschulen tritt der Bund diesen Bedrohungen entgegen. Eine grosse Herausforderung dabei ist, dass Angreifer ihre Methoden ständig ändern. Entscheidend für die rechtzeitige Warnung und Abwehr von Cyberangriffen ist darum, 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. Dort können Cyberangriffe freiwillig gemeldet werden. Über eine geschlossene Plattform pflegt das NCSC zudem den Informationsaustausch mit Betreiberinnen kritischer 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 grösster Bedeutung ist. Der Bundesrat hat deshalb entschieden, dem Parlament die Einführung einer Meldepflicht bei Cyberangriffen auf kritische Infrastrukturen vorzuschlagen, wie sie in vielen anderen Ländern bereits existiert und in der EU seit 2018 eingeführt ist.
Das Ziel ist, 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.
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 Strafverfolgung bei Fällen von schwerer Kriminalität möglich.
Zusammenfassend halte ich fest, 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 grossen Aufwand über ein Meldeformular erfüllt werden.
2. Die Informationen werden durch das NCSC vertraulich behandelt.
3. Die Meldung führt zu einem Anspruch auf subsidiäre Unterstützung durch das NCSC.
4. Sanktionen bei Nichterfüllung der Meldepflicht sind erst als letztes Mittel möglich.

In der Vernehmlassung wurde die Meldepflicht überwiegend begrüsst: 89 von 99 Teilnehmenden, darunter alle Kantone, unterstützen die Einführung einer Meldepflicht; nur 7 Teilnehmende haben sich dagegen ausgesprochen. Die Vorlage findet eine breite Zustimmung. Sie legt das rechtliche Fundament für die bereits gut etablierte Zusammenarbeit zwischen Wirtschaft und Staat.
Der Nationalrat hat dies gleich beurteilt und der Vorlage mit 132 zu 55 Stimmen deutlich zugestimmt. Er will dabei sogar noch etwas weiter gehen als der Bundesrat und die Unternehmen verpflichten, nicht nur Cyberangriffe, sondern auch neu entdeckte Schwachstellen bei den neu verwendeten Informatikmitteln zu melden. Zu diesem Zweck hat der Nationalrat Artikel 74d mit einem zweiten Absatz ergänzt, welcher festlegt, dass bisher unbekannte Schwachstellen bei betriebskritischen Informatikmitteln gemeldet werden müssen. Der Beschluss des Nationalrates stärkt den präventiven Charakter der Vorlage. Die Meldepflicht setzt nicht erst dann ein,

wenn bereits ein Angriff passiert ist, sondern schon dann, wenn ein solcher möglich ist. Gleichzeitig muss man sich bewusst sein, dass diese Änderung dazu führt, dass Unternehmen häufiger Meldungen machen müssen. Es gilt also bei der Beurteilung der Änderung des Nationalrates zwischen dem Aufwand für die Unternehmen und der Stärkung der Cybersicherheit abzuwägen.
Ihre Kommission hat diese Frage intensiv diskutiert und empfiehlt Ihnen, der Änderung des Nationalrates zu folgen. Sie hat zudem einstimmig beschlossen, die Vorlage zur Annahme zu empfehlen.
Je suis convaincue que les avantages de cette loi pour la cybersécurité dépassent largement le surcroît de travail pour les entreprises concernées.
Je vous demande donc de suivre votre commission et le Conseil national et d'entrer en matière sur le projet de loi, puis de l'approuver.

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 Beschluss des Nationalrates

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 à la décision du Conseil national

Angenommen – Adopté

Präsidentin (Häberli-Koller Brigitte, Präsidentin): Über Artikel 73b befinden wir beim 2. Abschnitt.

Art. 73c, 73d, 74
Antrag der Kommission
Zustimmung zum Beschluss des Nationalrates
Proposition de la commission
Adhérer à la décision du Conseil national

Angenommen – Adopté

Gliederungstitel nach Art. 74
Antrag der Mehrheit
Zustimmung zum Beschluss des Nationalrates

Antrag der Minderheit
(Wicki, Bauer, Burkart, Français, Minder)
Zustimmung zum Entwurf des Bundesrates

Titre suivant l'art. 74
Proposition de la majorité
Adhérer à la décision du Conseil national

Proposition de la minorité
(Wicki, Bauer, Burkart, Français, Minder)
Adhérer au projet du Conseil fédéral

Gmür-Schönenberger Andrea (M-E, LU), für die Kommission: Die Minderheit beantragt hier, auf die Erweiterung der Meldepflicht auf nicht öffentliche Schwachstellen zu verzichten. Sie bemängelt auch, dass der Begriff der Schwachstelle nicht ausreichend definiert sei. Bei diesem Wortlaut würde die Anzahl der Meldungen vermuteter Schwachstellen massiv erhöht, ohne dass dabei ein Mehrwert entstünde.
Die Kommission unterstützt die Fassung des Nationalrates mit 5 zu 5 Stimmen mit Stichentscheid des Präsidenten. Der Begriff der Schwachstelle wird in Artikel 5 Buchstabe g definiert als eine "Cyberbedrohung, die auf Schwächen oder Fehler in Informatikmitteln zurückzuführen ist". Überhaupt ist der Begriff der Schwachstelle in der Informatikbranche nichts Neues, sondern absolut gängig.
Die Meldung solcher Schwachstellen erzeugt einen Mehrwert. Alle potenziell Betroffenen werden nämlich informiert. Zudem kann bei den Herstellern darauf gedrängt werden, dass diese Mängel möglichst rasch behoben werden. Meist können solche Schwachstellen ohnehin nur vom Hersteller repariert werden. Es ist also sinnvoll, dass nicht jeder Betreiber einer kritischen Infrastruktur selber beim Hersteller vorstellig wird, sondern dass die Behebung national gebündelt eingefordert werden kann.
Die Entdeckung von Schwachstellen kann auch bereits beim Testen von Systemen erfolgen. Stellen zum Beispiel die SBB beim Erproben einer neuen Software fest, dass sie Schwachstellen aufweist, ist es mehr als sinnvoll, solche Infos weiterzugeben, damit eben andere Unternehmen mit der gleichen Software gewarnt sind. Bei der Integration von neuen Systemen und solchen, die erst noch eingeführt werden, ist daher die Meldung von Schwachstellen absolut zentral.
Diese erweiterte Meldepflicht bei Cyberangriffen verschafft einen besseren Überblick über die Situation und wirkt präventiv. 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 nicht zu unterschätzender Bedeutung. Es gilt ganz klar: je früher, desto besser. Zudem sind nur jene Schwachstellen zu melden,

die bislang unbekannt waren und bei betriebskritischen Systemen auftreten. Oft wird ja eben Software eingekauft. Der Hersteller weist häufig auch auf allfällig auftretende Probleme hin und erarbeitet entsprechende Lösungen, die per Update die Schwachstelle beheben können. Der Schutzgrad kann so signifikant erhöht werden.
Aus all diesen Gründen bitte ich Sie, der Mehrheit Ihrer Kommission zu folgen. Die nationalrätliche Kommission hatte dem Antrag mit 21 zu 0 Stimmen zugestimmt, und damit gab es auch keine Minderheit im Plenum.

Wicki Hans (RL, NW): Wie Kollegin Gmür-Schönenberger festgestellt hat, haben wir hier eine erste Differenz. Es betrifft eben nicht nur die SBB, wenn sie ein neues System einführen und dieses vor der Einführung testen, sondern auch alle KMU und Unternehmungen, die Systeme am Laufen haben und von deren Schwachstellen gar nichts wissen. Um unseren Antrag an dieser Stelle nachvollziehen zu können, braucht es eine detaillierte Grundsatzdefinition des Begriffs der nicht öffentlich bekannten Schwachstelle. Dieser Begriff beruht letztendlich auf der vom Nationalrat neu eingeführten Meldepflicht für unbekannte Schwachstellen überhaupt. Auf den ersten Blick mag die Einfügung des Nationalrates nachvollziehbar erscheinen. Mit Blick auf die Umsetzung wirft sie allerdings einige Probleme auf.
Zum einen ist der Begriff "Schwachstelle" nicht genau bestimmt, denn die Definition in Artikel 5 Buchstabe g, wonach eine Schwachstelle eine Cyberbedrohung ist, die auf Schwächen oder Fehler in Informatikmitteln zurückzuführen sei, ist nur bedingt hilfreich. Sie enthält sogar einen formallogischen Widerspruch, denn sie suggeriert, dass bereits eine Cyberbedrohung eingetreten sein muss, deren Ursache auf den erwähnten Schwächen oder Fehlern basiert. Die Ergänzungen des Nationalrates zielen demgegenüber aber auf einen vermeintlich präventiven Effekt. Mit den Zusätzen des Nationalrates würden wir also eine Mehrdeutigkeit bei der Auslegung schaffen.
Zum andern weist dieser weite Auslegungsspielraum auf eine weitere Problematik hin: die Frage, ab welcher Schwelle eine Meldung erfolgen muss. Damit entsteht ein unbestimmt grosser Aufwand für eine erhebliche Anzahl von Unternehmen. Es kann kaum unser Ziel sein, diesen Unternehmen weitere administrative Aufgaben aufzubürden, selbst wenn es sich, wie die Bundesrätin ausgeführt hat, um ein vermeintlich einfaches Online-Formular handelt, das sie auszufüllen haben. Für die Unternehmen wird ein unbestimmter Mehrauf-

wand entstehen. Auch wenn es sich einfach anhört, ein Online-Formular auszufüllen, ist das hoffentlich kein repetitiver Arbeitsgang, und bei allem, was nicht repetitiv ist, ist man im ersten Moment immer etwas unsicher, wodurch ein Mehraufwand entsteht.
Überdies führt es zu einer weiteren Problematik: Es generiert Aufwand für das NCSC. Denn wie die Mehrheitssprecherin bereits ausgeführt hat, hat das NCSC bei einer Meldung ebenfalls die Pflicht, dem meldenden Unternehmen zu helfen. Mit der Ergänzung der Meldepflicht bei nicht öffentlich bekannten Schwachstellen ist davon auszugehen, dass relativ viele Meldungen eingehen werden, dies gerade aufgrund des unbestimmten Umfanges des Begriffes und der Meldeschwelle. Das führt letztendlich auch für das NCSC zu einer erheblichen Mehrbelastung, und die Beantragung von zusätzlichen Stellen kann hier bereits prognostiziert werden.
Sie sehen also die Problematik der nationalrätlichen Ergänzungen betreffend die Schwachstellen. Sie mögen gut gemeint sein, schaffen aber eine Unsicherheit und einen Mehraufwand. Dies widerspiegelt sich auch im vorliegenden Artikel. Das heisst, "nicht öffentlich bekannt" mag an diesem Punkt an und für sich harmlos erscheinen, referiert aber auf die Zusätze in den späteren Artikeln.
Ich bitte Sie im Namen der Minderheit, zum Entwurf des Bundesrates zurückzukehren und dieses System entsprechend zu genehmigen.

Zopfi Mathias (G, GL): Ich fasse mich kurz: Ich bitte Sie hier, der Mehrheit zuzustimmen.
Der Sprecher der Minderheit hat jetzt meiner Meinung nach selbst ein bisschen kompliziert erklärt, wieso diese Meldepflicht bei Schwachstellen eben kompliziert sein soll. Meiner Meinung nach ist sie das gerade nicht. Erstens einmal: Eine Schwachstelle, die Ihnen nicht bekannt ist, die können Sie nicht melden; das wird auch nicht verlangt. Verlangt wird, dass Sie eine Schwachstelle melden, wenn Sie sie sehen. Zweitens ist es eigentlich ganz banal und einfach. Wir haben es hier mit einer riesigen Bedrohung zu tun, solche Cybervorfälle können gewaltige Folgen haben. Die Idee hinter der Meldepflicht ist doch ganz einfach: Sie entdecken, dass Sie bei sich, in Ihrem System eine Schwachstelle haben – Sie müssen nicht danach suchen, Sie entdecken sie –, und Sie gehen davon aus, dass diese Schwachstelle auch andere betreffen könnte. Das heisst, andere könnten diese Schwachstelle auch haben, sie haben sie selber aber noch nicht gefunden. Da ist es doch das Nachvollziehbarste, Einfachste und für die Sicherheit dieser Unternehmen, gerade für KMU, das Allerbeste, wenn Sie diese Schwachstelle melden und andere aufgrund dieser Meldung den Schwachstellen in ihrem eigenen System nachgehen können.
Ich verstehe den Widerstand nicht. Ich gehe davon aus, dass es nicht so viele Meldungen geben wird, weil nicht so viele Unternehmen systematisch nach solchen Schwachstellen suchen können und suchen werden. Aber gerade die grösseren Unternehmen, wie vielleicht die SBB, werden solche Schwachstellen erkennen und dann mit ihrer Meldung vielen KMU Ärger ersparen. Die Meldepflicht schafft also effektiv mehr Sicherheit und kaum einen Mehraufwand. Entschuldigen Sie, aber wenn Sie eine Cyberschwachstelle entdecken, dann sollte es drinliegen – auch wenn es kein repetitiver Vorgang ist –, einmal ein Online-Formular auszufüllen, um andere Unternehmen damit zu schützen.
Ich danke für die Zustimmung zur Mehrheit.

Salzmann Werner (V, BE): Wie Sie gehört haben, ist die Abstimmung in der Kommission sehr eng ausgefallen; ich habe der Mehrheit zugestimmt. In der Zwischenzeit haben wir sehr viele Zuschriften erhalten. Die Verunsicherung bei den Betroffenen ist relativ gross. Ich bin nach wie vor klar der Meinung, dass Schwachstellen gemeldet werden müssen. Da aber die Verunsicherung gross ist, könnten wir als Kompromiss der Minderheit Wicki zustimmen. Die Schwesterkommission könnte dann noch einmal genau anschauen – die Formulierung scheint nicht allen ganz klar zu sein –, was genau gemeldet und wie es genau erfasst werden muss.
Aus diesem Grund empfehle ich Ihnen, der Minderheit zuzustimmen.

Français Olivier (RL, VD): C'est un article important parce que c'est la définition de la mission. Nous nous achoppons sur un seul terme: "vulnérabilité". La majorité de la commission veut élaborer la loi de façon à croire que la vulnérabilité sera très clairement définie quoi qu'il arrive. Alors, dans ce cas, franchement, il ne faut pas faire de loi! Si on fait une loi pour signaler une cyberattaque et que l'infrastructure critique attaquée est vulnérable, le Centre national pour la cybersécurité (NCSC) fera son travail. Il est impossible que les autorités puissent assurer la sécurité d'un système informatique, et on ne peut pas rédiger le texte de manière à faire croire qu'elles en sont capables.
C'est pour cela que le texte du Conseil fédéral est cohérent. S'il y a des problèmes en cas de cyberattaque et que l'on constate que le système informatique est vulnérable, alors il faut intervenir. Il ne faut pas inverser le fardeau de la preuve, bien au contraire. A mon avis, on ferait une très grosse erreur. On donnerait une responsabilité, mais le système informatique est de toute façon incontrôlable.

Je pense que la version du Conseil national, soutenue par la majorité de la commission, est inapplicable. Je ne peux que vous recommander d'accepter la version du Conseil fédéral, qui me paraît nettement plus cohérente par rapport à l'action à mener. On ne peut pas faire d'un système informatique un coffre-fort. La majorité de la commission donne l'impression qu'on peut faire d'un système informatique un coffre-fort. Ce n'est pas possible! Comme je l'ai dit: si on avait la certitude

qu'on peut faire d'un système informatique un coffre-fort, on ne ferait même pas de loi. Or, si on fait une loi, c'est parce que justement ce coffre-fort est vulnérable et que c'est parce qu'il est vulnérable qu'il faut donner la garantie au NCSC d'aller au coeur du système informatique.
Deux ou trois phrases sont un peu contraignantes. Il est dit que les organes publics et parapublics sont soumis à l'obligation de signaler les cyberattaques contre leur système informatique.
Dieu merci. Mais on parle de la connaissance du grand public. Or, la cyberattaque n'est pas le fait du grand public. La cyberattaque est composée de systèmes terriblement pervers qui ne sont pas à la portée du grand public – peut-être de milieux spécialisés, mais pas du grand public. Beaucoup d'erreurs, à mon avis, se trouvent dans le texte du Conseil national. J'ai de la peine à comprendre comment on peut suivre cette proposition.
Je ne peux que vous recommander de suivre le projet du Conseil fédéral et de la minorité de la commission.

Wicki Hans (RL, NW): Kollege Zopfi hat mich jetzt schon etwas herausgefordert. Er verniedlicht das Problem natürlich ungemein. Es ist eben nicht so, dass alles klar und alles klar geregelt ist. Die Verunsicherung ist enorm hoch. Es steht eben nirgends im Gesetz, dass nur grosse Unternehmungen wie die SBB Schwachstellen suchen müssen, wenn sie ein System einführen; es steht dort eben gerade nichts dazu. Im Gesetz steht lediglich, dass Schwachstellen, die nicht einmal bekannt sind, gemeldet werden müssen. Jetzt frage ich Sie: Wo im Gesetz steht denn, dass nach Schwachstellen nur gesucht werden muss, wenn man ein System einführen will? Ihre Argumentation tönt völlig gut und absolut nachvollziehbar, das ist alles klar – aber das steht so nicht im Gesetz. Schwachstellen müssen gemeldet werden, auch wenn sie nicht öffentlich bekannt sind. Wenn man das nicht macht, unterliegt man dem Risiko, dass man eine Busse erhält; das steht weiter unten.
Ich frage mich schon, was die Unternehmungen da alles auf sich nehmen müssen, damit sie diese möglichen Schwachstellen, die noch gar nicht bekannt sind, erkennen und dann auch melden können. Das ist das Problem. Ich möchte nur sicherstellen, dass nicht alle Unternehmungen jetzt beginnen, ihre IT-Abteilung zwangsweise auszubauen und nach möglichen Schwachstellen zu suchen, die nicht bekannt sind. Sie haben mit dem normalen Unterhalt ihrer Systeme schon genug zu tun. Auf dieser Basis, muss ich Ihnen sagen, ist das Gesetz zu schwammig, zu problematisch, und es gibt grosse Verunsicherung.
Darum bitte ich Sie, den Minderheitsantrag zu unterstützen.

Gmür-Schönenberger Andrea (M-E, LU), für die Kommission: Es geht nicht darum, die Unternehmen ohne Not administrativ zu belasten. Das will absolut niemand. Wie gesagt: Ein Problem, das man nicht erkennt, kann man definitiv nicht melden. Aber es gibt immer wieder Situationen, wo man beim Gebrauch eines Systems eben merkt, dass es Mängel hat. Um diese geht es und darum, für die betroffenen Unternehmen dann einen Mehrwert zu schaffen.
Ich bitte Sie also, dem Antrag der Mehrheit zuzustimmen.

Amherd Viola, Bundesrätin: Sie haben es gehört: Ihre Kommissionsmehrheit wie auch der Nationalrat beantragen die Ausweitung der Meldepflicht auf Schwachstellen.
Insgesamt beurteilen wir inhaltliche Erweiterungen der Meldepflicht skeptisch. Wir müssen uns bewusst sein, dass jede Erweiterung der Meldepflicht für die Unternehmen bedeutet, dass sie häufiger eine Meldung erfassen müssen. Wir haben bei der Erarbeitung der Vorlage grossen Wert darauf gelegt, die Meldepflicht auf das Notwendigste zu beschränken. Zugleich teilen wir aber die Ansicht, dass es sehr wichtig ist, Schwachstellen in kritischen Systemen möglichst früh zu erkennen. Eine Meldepflicht für Schwachstellen ist dann gerechtfertigt, wenn sie bisher noch nicht bekannte Schwachstellen in kritischen Systemen betrifft. In einem solchen Fall ist es entscheidend, dass der Bund alle kritischen Infrastrukturen, welche von der Schwachstelle betroffen sein könnten, rasch warnen kann. Deshalb ist eine Meldung von Schwachstellen sinnvoll.
Ihre Kommissionsmehrheit und der Nationalrat beantragen, in Artikel 74d Absatz 2 ISG die Meldepflicht auf Schwachstellen auszuweiten, die bisher noch nicht bekannt sind und die betriebskritische Systeme betreffen. Damit entfällt die Meldepflicht bei Schwachstellen, welche durch den Hersteller selber oder durch Sicherheitsforscher bereits öffentlich gemacht worden sind. Diese stellen die überwiegende Mehrheit der Schwachstellen dar. Es ist auch nicht so, dass man mit diesem zusätzlichen Artikel Schwachstellen suchen muss. Es ist keine

Pflicht, Schwachstellen zu suchen. Wenn man aber eine Schwachstelle entdeckt, dann soll man sie melden, das ist die Idee hinter dem Mehrheitsantrag und dem Entscheid des Nationalrates.
Wenn wenig kritische Schwachstellen erkannt werden, welche die Funktionsfähigkeit der betroffenen Unternehmen nicht gefährden – zum Beispiel solche bei öffentlichen Websites –, müssen diese nicht gemeldet werden, weil sie eben öffentlich bekannt sind. Dank diesen Einschränkungen führt der Antrag lediglich zu einer moderaten Ausweitung der Meldepflicht. Gleichzeitig ergänzt er die Meldepflicht um einen wichtigen Aspekt, und zwar um die Frühwarnung vor Schwachstellen. Unter dieser Voraussetzung und zumal es nur um die Betreiberinnen und Betreiber kritischer Infrastrukturen geht und eben nicht um alle KMU, können wir mit der Ergänzung gemäss Nationalrat und Kommissionsmehrheit leben.

Abstimmung – Vote
(namentlich – nominatif; 22.073/5808)
Für den Antrag der Minderheit ... 31 Stimmen
Für den Antrag der Mehrheit ... 13 Stimmen
(0 Enthaltungen)

Art. 73b
Antrag der Mehrheit
Zustimmung zum Beschluss des Nationalrates

Antrag der Minderheit
(Wicki, Bauer, Burkart, Français, Minder)
Abs. 3
Zustimmung zum Entwurf des Bundesrates

Art. 73b
Proposition de la majorité
Adhérer à la décision du Conseil national

Proposition de la minorité
(Wicki, Bauer, Burkart, Français, Minder)
Al. 3
Adhérer au projet du Conseil fédéral

Abs. 3 – Al. 3
Angenommen gemäss Antrag der Minderheit
Adopté selon la proposition de la minorité

Übrige Bestimmungen angenommen
Les autres dispositions sont adoptées

Art. 74a
Antrag der Mehrheit
Zustimmung zum Beschluss des Nationalrates

Antrag der Minderheit
(Wicki, Bauer, Burkart, Français, Minder)
Abs. 1, 3, 4
Zustimmung zum Entwurf des Bundesrates

Art. 74a
Proposition de la majorité
Adhérer à la décision du Conseil national

Proposition de la minorité
(Wicki, Bauer, Burkart, Français, Minder)
Al. 1, 3, 4
Adhérer au projet du Conseil fédéral

Abs. 1, 3, 4 – Al. 1, 3, 4
Angenommen gemäss Antrag der Minderheit
Adopté selon la proposition de la minorité

Übrige Bestimmungen angenommen
Les autres dispositions sont adoptées

Art. 74b
Antrag der Mehrheit
Zustimmung zum Beschluss des Nationalrates

Antrag der Minderheit
(Wicki, Bauer, Burkart, Français, Minder)
Abs. 1 Bst. d, 2, 3
Zustimmung zum Entwurf des Bundesrates

Art. 74b
Proposition de la majorité
Adhérer à la décision du Conseil national

Proposition de la minorité
(Wicki, Bauer, Burkart, Français, Minder)
Al. 1 let. d, 2, 3
Adhérer au projet du Conseil fédéral

Abs. 1 Bst. d, 2, 3 – Al. 1 let. d, 2, 3
Angenommen gemäss Antrag der Minderheit
Adopté selon la proposition de la minorité

Übrige Bestimmungen angenommen
Les autres dispositions sont adoptées

Art. 74c
Antrag der Mehrheit
Zustimmung zum Beschluss des Nationalrates

Antrag der Minderheit
(Wicki, Bauer, Burkart, Français, Minder)
Zustimmung zum Entwurf des Bundesrates

Art. 74c
Proposition de la majorité
Adhérer à la décision du Conseil national

Proposition de la minorité
(Wicki, Bauer, Burkart, Français, Minder)
Adhérer au projet du Conseil fédéral

Angenommen gemäss Antrag der Minderheit
Adopté selon la proposition de la minorité

Art. 74d
Antrag der Mehrheit
Zustimmung zum Beschluss des Nationalrates

Antrag der Minderheit
(Wicki, Bauer, Burkart, Français, Minder)
Titel, Abs. 2
Zustimmung zum Entwurf des Bundesrates

Art. 74d
Proposition de la majorité
Adhérer à la décision du Conseil national

Proposition de la minorité
(Wicki, Bauer, Burkart, Français, Minder)
Titre, al. 2
Adhérer au projet du Conseil fédéral

Titel, Abs. 2 – Titre, al. 2
Angenommen gemäss Antrag der Minderheit
Adopté selon la proposition de la minorité

Übrige Bestimmungen angenommen
Les autres dispositions sont adoptées

Art. 74e
Antrag der Mehrheit
Zustimmung zum Beschluss des Nationalrates

Antrag der Minderheit
(Wicki, Bauer, Burkart, Français, Minder)
Abs. 1, 2
Zustimmung zum Entwurf des Bundesrates

Art. 74e
Proposition de la majorité
Adhérer à la décision du Conseil national

Proposition de la minorité
(Wicki, Bauer, Burkart, Français, Minder)
Al. 1, 2
Adhérer au projet du Conseil fédéral

Abs. 1, 2 – Al. 1, 2
Angenommen gemäss Antrag der Minderheit
Adopté selon la proposition de la minorité

Übrige Bestimmungen angenommen
Les autres dispositions sont adoptées

Art. 74f
Antrag der Mehrheit
Zustimmung zum Beschluss des Nationalrates

Antrag der Minderheit
(Wicki, Bauer, Burkart, Français, Minder)
Abs. 1, 2
Zustimmung zum Entwurf des Bundesrates

Art. 74f
Proposition de la majorité
Adhérer à la décision du Conseil national

Proposition de la minorité
(Wicki, Bauer, Burkart, Français, Minder)
Al. 1, 2
Adhérer au projet du Conseil fédéral

Abs. 1, 2 – Al. 1, 2
Angenommen gemäss Antrag der Minderheit
Adopté selon la proposition de la minorité

Übrige Bestimmungen angenommen
Les autres dispositions sont adoptées

Art. 74g; 74h; 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 Beschluss des Nationalrates

Art. 74g; 74h; 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 à la décision du Conseil national

Angenommen – Adopté

AB 2023 S 390 / BO 2023 E 390

Ziff. II Ziff. 3
Antrag der Mehrheit
Zustimmung zum Beschluss des Nationalrates

Antrag der Minderheit
(Wicki, Bauer, Burkart, Français, Minder)
Zustimmung zum Entwurf des Bundesrates

Ch. II ch. 3
Proposition de la majorité
Adhérer à la décision du Conseil national

Proposition de la minorité
(Wicki, Bauer, Burkart, Français, Minder)
Adhérer au projet du Conseil fédéral

Angenommen gemäss Antrag der Minderheit
Adopté selon la proposition de la minorité

Ziff. II Ziff. 4, 5; Ziff. III
Antrag der Kommission
Zustimmung zum Beschluss des Nationalrates

Ch. II ch. 4, 5; ch. III
Proposition de la commission
Adhérer à la décision du Conseil national

Angenommen – Adopté

Gesamtabstimmung – Vote sur l'ensemble
(namentlich – nominatif; 22.073/5809)
Für Annahme des Entwurfes ... 42 Stimmen
(Einstimmigkeit)
(0 Enthaltungen)

Präsidentin (Häberli-Koller Brigitte, Präsidentin): Das Geschäft geht an den Nationalrat.