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)

*Differenzen – Divergences*

---

CHRONOLOGIE

NATIONALRAT/CONSEIL NATIONAL 16.03.23 (ERSTRAT - PREMIER CONSEIL)
STÄNDERAT/CONSEIL DES ETATS 01.06.23 (ZWEITRAT - DEUXIÈME CONSEIL)
NATIONALRAT/CONSEIL NATIONAL 11.09.23 (DIFFERENZEN - DIVERGENCES)
STÄNDERAT/CONSEIL DES ETATS 19.09.23 (DIFFERENZEN - DIVERGENCES)
NATIONALRAT/CONSEIL NATIONAL 21.09.23 (DIFFERENZEN - DIVERGENCES)
NATIONALRAT/CONSEIL NATIONAL 29.09.23 (SCHLUSSABSTIMMUNG - VOTE FINAL)
STÄNDERAT/CONSEIL DES ETATS 29.09.23 (SCHLUSSABSTIMMUNG - VOTE FINAL)

---

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

**Art. 73b Abs. 3; Gliederungstitel nach Art. 74; Art. 74a Abs. 1, 3, 4; 74b Abs. 1 Bst. d, 2, 3; 74c**
*Antrag der Mehrheit*
Festhalten

*Antrag der Minderheit*
(Zopfi, Jositsch, Juillard, Vara)
Zustimmung zum Beschluss des Nationalrates

**Art. 73b al. 3; titre suivant l'art. 74; art. 74a al. 1, 3, 4; 74b al. 1 let. d, 2, 3; 74c**
*Proposition de la majorité*
Maintenir

*Proposition de la minorité*
(Zopfi, Jositsch, Juillard, Vara)
Adhérer à la décision du Conseil national

**Art. 74d**
*Antrag der Mehrheit*
*Titel, Abs. 2*
Festhalten

*Antrag der Minderheit*
(Zopfi, Jositsch, Juillard, Vara)
*Titel*
Zustimmung zum Beschluss des Nationalrates
*Abs. 2*
Gemäss Nationalrat, aber:
...
a0. Einen kritischen Schweregrad aufweist;
...
c. Nicht durch eigene Entwicklungen der Betroffenen oder durch Entwicklungen Dritter, die im Auftrag der Betroffenen ausgeführt wurden, entstanden sind.

**Art. 74d**
*Proposition de la majorité*
*Titre, al. 2*
Maintenir

*Proposition de la minorité*
(Zopfi, Jositsch, Juillard, Vara)
*Titre*
Adhérer à la décision du Conseil national
*Al. 2*
Selon Conseil national, mais:
...
a0. présente un degré de gravité critique;
...
c. elle ne résulte pas de développements internes de l'entreprise concernée ni de développements réalisés par des tiers pour le compte l'entreprise concernée.

**Art. 74e**
*Antrag der Mehrheit*
*Abs. 1, 2*
Festhalten

*Antrag der Minderheit*
(Zopfi, Jositsch, Juillard, Vara)
*Abs. 1*
Die Meldung muss innert 24 Stunden nach der Entdeckung des Cyberangriffs und innert 7 Tagen nach der Entdeckung der Schwachstelle erfolgen.
*Abs. 2*
Meldungen zu Cyberangriffen müssen Informationen zur meldepflichtigen Behörde oder Organisation, zur Art und Ausführung des Cyberangriffs, zu seinen Auswirkungen, zu ergriffenen Massnahmen und, soweit bekannt, zum geplanten weiteren Vorgehen enthalten.
*Abs. 2bis*
Meldungen zu Schwachstellen können anonym erfolgen. Sie müssen Informationen zu den betroffenen Informatikmitteln und eine technische Beschreibung der Schwachstelle enthalten.

**Art. 74e**
*Proposition de la majorité*
*Al. 1, 2*
Maintenir

*Proposition de la minorité*
(Zopfi, Jositsch, Juillard, Vara)
*Al. 1*
Le signalement doit être fait dans les 24 heures suivant la détection de la cyberattaque et dans les 7 jours

suivant la découverte de la vulnérabilité.
*Al. 2*
Les signalements concernant les cyberattaques doivent contenir des informations sur l'autorité ou l'organisation assujetties à l'obligation de signaler, sur le type et l'exécution de la cyberattaque, sur ses effets, sur les mesures prises et, si elles sont connues, sur les mesures prévues.
*Al. 2bis*
Le signalement de vulnérabilités peut être anonymes. Il doit contenir des informations sur les moyens informatiques concernés et une description technique de la vulnérabilité.

**Art. 74f**
*Antrag der Mehrheit*
*Abs. 1, 2*
Festhalten

AB 2023 S 792 / BO 2023 E 792

*Antrag der Minderheit*
(Zopfi, Jositsch, Juillard, Vara)
*Abs. 1, 2*
Zustimmung zum Beschluss des Nationalrates
*Abs. 1bis*
Das NCSC speichert und bearbeitet die Meldungen nur auf sicheren Systemen.

**Art. 74f**
*Proposition de la majorité*
*Al. 1, 2*
Maintenir

*Proposition de la minorité*
(Zopfi, Jositsch, Juillard, Vara)
*Al. 1, 2*
Adhérer à la décision du Conseil national
*Al. 1bis*
Le NCSC n'enregistre et ne traite les signalements que sur des systèmes sécurisés.

**Ziff. II Ziff. 3 Art. 102 Abs. 2**
*Antrag der Mehrheit*
Festhalten

*Antrag der Minderheit*
(Zopfi, Jositsch, Juillard, Vara)
Zustimmung zum Beschluss des Nationalrates

**Ch. II ch. 3 art. 102 al. 2**
*Proposition de la majorité*
Maintenir

*Proposition de la minorité*
(Zopfi, Jositsch, Juillard, Vara)
Adhérer à la décision du Conseil national

**Präsidentin** (Häberli-Koller Brigitte, Präsidentin): Bei der verbleibenden Differenz handelt es sich um ein Konzept, das wir entsprechend beraten.

**Gmür-Schönenberger** Andrea (M-E, LU), für die Kommission: Beim Informationssicherheitsgesetz geht es um die Meldepflicht für Cyberangriffe auf kritische Infrastrukturen. Bei der einen Differenz geht es darum, dass

unser Schwesterrat nicht nur eine Meldepflicht für Cyberattacken, sondern auch eine Meldepflicht für Schwachstellen fordert. Der Nationalrat hat dies in der Frühjahrssession mit 126 zu 52 Stimmen beschlossen. Unser Rat hat die Meldepflicht für Schwachstellen in der Sommersession mit 31 zu 13 Stimmen wieder abgelehnt. Der Nationalrat hat dann in der neuen Formulierung von Artikel 74d Absatz 2 präzisiert, dass eine Schwachstelle gemeldet werden muss, wenn sie nicht durch Eigenentwicklungen der betroffenen Unternehmen entstanden ist. Eine weitere Präzisierung, ebenfalls von Artikel 74d Absatz 2, hat die Minderheit der SiK-S vorgenommen. So sollen Schwachstellen nur dann gemeldet werden, wenn sie einen kritischen Schweregrad aufweisen.
Ihre SiK hält mit 9 zu 4 Stimmen an der Fassung des Bundesrates fest und lehnt eine Ausdehnung der Meldepflicht auf Schwachstellen ab. Warum?
1. Aufgrund der unterschiedlichen IT-Systeme können Schwachstellen unter den Betreibern kritischer Infrastrukturen kaum verglichen werden. Es drohen unzählige Meldungen, dies, weil kaum die gleichen Systeme und die gleiche Software eingesetzt werden. Ein Energiebetreiber, der für die Steuerung der Stromproduktion zuständig ist, verfügt über eine andere IT-Infrastruktur und andere IT-Lösungen als beispielsweise Banken – da geht es ums Zahlungssystem – oder Flughäfen, wo die aviatische Infrastruktur gemanagt werden muss. Auch innerhalb der einzelnen Branchen sind die IT-Systeme zum Teil so unterschiedlich und vielfältig, dass ein Abgleich und Vergleich von Schwachstellen kaum möglich und sinnvoll ist. Ob die zentrale Erfassung der Schwachstellen einen systemischen Mehrwert ergibt, ist fragwürdig.
2. Die Sammlung von Schwachstellen an einer zentralen Stelle ist auch gefährlich. Die Gefahr ist gross, dass die Meldepflicht für IT-Schwachstellen die Sicherheit der Systeme nicht stärkt, sondern potenziell schwächt. Eine Meldung von Schwachstellen und die damit verbundene Sammlung an zentraler staatlicher Stelle setzen voraus, dass das Sicherheitssystem dieser Behörde absolut geschützt ist. Mögliche Lecks müssen auf staatlicher Seite zu jeder Zeit komplett ausgeschlossen sein und, sollten sie dennoch vorkommen, jederzeit und unverzüglich geschlossen werden können. Diese Anforderung war bis anhin leider nicht erfüllt. Das Sicherheitsrisiko soll aber reduziert und nicht erhöht werden.
3. Die Meldung von potenziellen Schwachstellen – was auch immer als solche erkannt wird – führt zu einer administrativen Mehrbelastung für Unternehmen und Staat, die auch von echten Cyberangriffen ablenken kann. Es drohen Rechtsunsicherheit, mehr Aufwand und mehr Risiken. Für diese kontinuierlichen Meldungen müssten in allen Unternehmen allenfalls sogar zusätzliche Stellen geschaffen werden. Dies gilt auch für den Staat selbst, soll er alle potenziellen Daten- und Referenzpunkte auswerten können. Dies birgt das Risiko der bürokratischen Überforderung und kann auch dazu führen, dass Ressourcen für die Bekämpfung von ernsten Cyberangriffen nicht zur Verfügung stehen respektive die Erhöhung der Cyberresilienz nicht gewährleistet ist.
4. Schlussendlich ist das Gesetz widersprüchlich, wenn es um die Meldung geht. Schauen Sie sich Artikel 74e Absatz 1 an. Dieser fordert einerseits, dass die Schwachstelle innert sieben Tagen gemeldet werden muss. Ansonsten droht ja auch Busse. Andererseits heisst es, dass die Meldungen zu Schwachstellen anonym erfolgen können, dies bei Artikel 74e Absatz 2bis. Wie soll das überhaupt kontrolliert werden, ob die Schwachstelle innert sieben Tagen gemeldet wurde? Da wird mit ungleichen Ellen gemessen. Eine anonyme Meldung kann nie kontrolliert werden. Nur schon der Gesetzestext, wie er jetzt vorliegt, ist komplett widersprüchlich.
Die Erweiterung der Meldepflicht auf IT-Schwachstellen, die vom Nationalrat eingebracht wurde, wurde komplett ohne Vernehmlassung eingebracht. Niemand wurde dazu angehört. Die betroffenen Gesetzesadressaten, die kritischen Infrastrukturen, konnten sich dazu nicht äussern. Auch das ist ein weiterer Mangelpunkt.
Aus all diesen Gründen bitte ich Sie namens der Mehrheit der SiK, auf die Verankerung einer Meldepflicht betreffend IT-Schwachstellen für Betreiber kritischer Infrastrukturen zu verzichten.

**Zopfi** Mathias (G, GL): Der Minderheit geht es um mehr Cybersicherheit. Wir stärken in diesem Gesetz die Cybersicherheit ja grundsätzlich. Die Minderheit möchte sie jedoch noch weiter verstärken – notabene so, wie es die Mehrheit der Kommission in der ersten Runde auch wollte – und eben ab einer gewissen Grenze eine Meldepflicht für Schwachstellen einführen.
Die Cyberschwachstelle von heute ist der Cyberangriff von morgen. Das gilt nicht für bekannte und behobene Schwachstellen. Es gilt für unbekannte und nicht kommunizierte Schwachstellen. Es ist schon klar, dass eine solche Meldepflicht eine zusätzliche Auflage für Unternehmen in diesem Land darstellt. Das ist an sich bedauerlich, weil sie einen gewissen Mehraufwand bei den betroffenen kritischen Infrastrukturen verursacht; da stimme ich der Berichterstatterin zu. Die Frage muss aber sein: Ist eine solche Meldepflicht notwendig? Sicherheit ist nie gratis. Sicherheit ist ein Aufwand, und wir haben es hier mit einem Bereich zu tun, der für die Cybersicherheit in unserem Land elementar und relevant ist.
Nach der Argumentation der Mehrheit müsste man sagen, dass eine Meldepflicht nie etwas bringe: Es ist nicht bestimmt, was gemeldet werden muss, es ist nicht bestimmt, wie gemeldet werden muss usw.

Lassen Sie mich zwei Beispiele aus anderen sensiblen Bereichen nennen. Im Bundesgesetz über die Luftfahrt steht in Artikel 20, dass es für besondere Ereignisse in der Luftfahrt ein Meldesystem gibt. Wenn also irgendein Problem bei einem Luftfahrzeug vorkommt, müssen die Unternehmen das



melden, damit andere von diesem Wissen profitieren können. Das schafft bei einem vertretbaren Aufwand mehr Sicherheit.
Ein anderes Beispiel ist Artikel 24 Absatz 1 des Seilbahngesetzes: "Besondere Vorkommnisse während des Baus oder Betriebes einer Seilbahn müssen der Aufsichtsbehörde umgehend gemeldet werden." Auch das schafft Sicherheit: Wenn an einer Seilbahn in der Schweiz ein Defekt festgestellt wird und man merkt, dass das bei vielen anderen Seilbahnen in der Schweiz ebenfalls der Fall sein könnte, dann ist es Sinn und Zweck dieses Gesetzesartikels, das zu melden, damit andere Vorkehrungen treffen können.
Und jetzt stellen Sie sich das einmal konkret im Cyberbereich vor. Nehmen wir die SBB als Betreiber einer kritischen Infrastruktur: Was ist, wenn die Informatikerinnen und Informatiker der SBB eine sicherheitsrelevante kritische Schwachstelle entdecken? Das Logischste ist, andere, die dieselbe Software einsetzen, vor dieser Schwachstelle zu warnen. Und das geht eben nur über eine Meldung der Schwachstelle und nicht irgendwie anders. Wenn das nicht geschieht, dann ist es möglich, dass die SBB die Schwachstelle zwar beheben und dieses Einfallstor schliessen werden, andere Unternehmen mit kritischer Infrastruktur das aber nicht können, weil ihnen die Schwachstelle, die die SBB vielleicht sogar zufällig entdeckt haben, nicht bekannt ist.
Und nochmals: Es geht nur um die Betreiberinnen und Betreiber kritischer Infrastrukturen. Es wurde zum Teil fast so getan, auch in der ersten Runde hier im Rat, als ob jedes Schweizer KMU davon betroffen wäre. Das ist nicht der Fall, es geht eben nur, aber immerhin um die Betreiber kritischer Infrastrukturen. Ja, sie werden einen gewissen Mehraufwand haben, aber auch einen enormen Nutzen, weil Schwachstellen allen Betreibern solcher Infrastrukturen, welche relevant sind für unser Land – sonst wären sie nicht kritisch –, bekannt gemacht werden.
Deshalb hat die Mehrheit der Kommission in der ersten Runde im Rat die Meldepflicht bei Schwachstellen befürwortet. Und deshalb wurde auch von jenen, die das letzte Mal dagegen gestimmt haben, vermehrt Sympathie für eine Meldepflicht bei Schwachstellen geäussert. Sie haben einfach gesagt, dass man das doch ein bisschen anwenderfreundlicher und ein bisschen weniger aufwandgenerierend ausgestalten soll.
Jetzt schauen wir uns einmal an, was die Minderheit konkret vorschlägt. Sie sehen, dass der Nationalrat die Meldepflicht bereits stark modifiziert hat. Die Minderheit beantragt eine Meldepflicht nicht einfach überall, bei jeder Schwachstelle und unabhängig davon, ob sie relevant ist oder nicht, sondern nur ab einem kritischen Schweregrad. Man könnte jetzt fragen, was ein kritischer Schweregrad ist. Dazu kann ich Ihnen sagen, dass das definiert ist. Es gibt einen internationalen Standard dafür, was ein kritischer Schweregrad ist. Im sogenannten Common Vulnerability Scoring System (CVSS) wird das international definiert. Das ist ein System, das aus Amerika kommt und das für Schwachstellen Scores bzw. Noten verteilt, woraus man ersehen kann, welche Grösse bzw. welchen Schweregrad die Schwachstellen haben. Gemeldet werden muss nur die Schwachstelle, die einen kritischen Schweregrad aufweist.
Wir müssen das mit diesen Scores nicht verstehen, aber die Expertinnen und Experten wissen genau, was gemeint ist. Die Informatikerinnen und Informatiker in den Unternehmen sind nicht die Juristen wie ich, die das melden müssen. Die Leute in den Unternehmen wissen, was mit "kritischem Schweregrad" gemeint ist.
Die Berichterstatterin hat gesagt, es werden überall verschiedene Systeme eingesetzt. Ebenfalls nicht gemeldet werden müssen Schwachstellen von Systemen, die nur in Ihrem System eingesetzt werden, weil es sich um eine Eigenentwicklung handelt, die Sie entweder selbst gemacht haben oder die Sie für sich in Auftrag gegeben haben und die von einem Unternehmen für Sie entwickelt wurde. Wenn also nur Sie eine Software einsetzen, dann kann die Schwachstelle auch nur Sie betreffen, und das müssen Sie ebenfalls nicht melden. Auch damit ist die Flut von Meldungen gebannt.
Das Letzte: Die Minderheit beantragt Ihnen in der modifizierten Version des Nationalrates, dass innert sieben Tagen gemeldet werden muss. Auch das nimmt die Kritik auf, dass 24 Stunden, wie es bei Cyberangriffen gilt, eine sehr kurze Frist ist. Es muss innerhalb von sieben Tagen gemeldet werden, und die Meldung kann anonym erfolgen.
Jetzt sagt die Berichterstatterin, das sei ein Widerspruch, denn "anonym" und "sieben Tage" könne man nicht kontrollieren. Natürlich können Sie das! Wenn Sie im Cybersicherheitsaudit in Ihrem Unternehmen feststellen, dass Sie eine Schwachstelle haben, dann werden Sie die melden, möglicherweise anonym. Aber Sie selbst sind für sich ja nicht anonym – ich kenne mich selbst normalerweise. Also kann ich die Meldung machen und erhalte dann eine Bestätigung, dass ich eine Meldung erstattet habe. Es geht hier um die Sicherheit, nicht um

Strafen. Sollte es nachher fraglich sein, ob diese Schwachstelle je gemeldet worden ist, kann ich mit diesem Dokument beweisen, dass ich diese Schwachstelle innert sieben Tagen gemeldet habe. Beim Empfänger ist sie anonym angekommen, weil es nicht ums Strafen oder ums Büssen geht, sondern um die Entdeckung und Aufdeckung der Schwachstelle. Das reicht auch. Man muss die Schwachstelle kennen, man muss nicht unbedingt wissen, wo sie gewesen ist.
Das ist eine Konzession an die Betreiberinnen und Betreiber kritischer Infrastrukturen; dass man diese Meldung nicht anonym machen kann, war ein Punkt, den sie kritisiert haben. Es irritiert mich nun ein bisschen, dass man diese Konzession nun in einen Widerspruch verkehrt, um dagegen zu argumentieren.
Letztlich geht es darum, mehr Sicherheit zu schaffen. Sicherheit ist nie gratis. Sicherheit im Cyberbereich ist extrem relevant. Wir haben Vorfälle, und – ich sage es Ihnen nochmals – die Schwachstelle von heute ist der Cyberangriff von morgen. Ich bin überzeugt, dass wir gut daran tun, das hier in dieser moderaten Form einzuführen.
Ein letztes Wort: Die USA führen in dieser Branche. Sie werden bei diesen Systemen wahrscheinlich – nicht wahrscheinlich: höchstwahrscheinlich – in den nächsten Jahren eine solche Meldepflicht einführen. Dann wird sie automatisch indirekt wegen Branchenstandards auch für unsere Unternehmen gelten. Nur ist es dann die Meldepflicht, die Amerika eingeführt hat, das sicher nicht Rücksicht auf die Schweizer KMU nehmen wird. Hier hätten wir mit der Minderheit die Möglichkeit, eine moderate Meldepflicht betreffend Cyberschwachstellen einzuführen, die für alle umsetzbar ist und deutlich mehr Sicherheit schafft.
Ich danke Ihnen für die Unterstützung der Minderheit.

**Wicki** Hans (RL, NW): Ich danke dem Sprecher der Minderheit, dass er die Seilbahnen angesprochen hat. Es ist natürlich schon so: Auch Seilbahnen bergen Risiken. Korrekt ist hier, dass ein Schaden gemeldet werden muss, wenn er erkannt wird. Ich muss nicht suchen, sondern ein Schaden muss gemeldet werden, wenn er erkannt wird. Das Gleiche gilt bei Cyberangriffen: Wenn ich erkenne, dass ich angegriffen worden bin, dann melde ich das selbstverständlich. Aber ich muss nicht unter Strafandrohung verpflichtet werden, dauernd nach Schäden zu suchen und diese dann zu melden. Das ist der kleine, aber feine Unterschied.
Übrigens: Das gibt es auch bei den Autos, nicht nur bei den Seilbahnen. Wenn bei Autos ein Schaden erkannt wird, gibt es eine Rückrufaktion. Das ist heute schon so. Aber es ist nicht so, dass jeder Garagist einen Schaden suchen muss, den er noch gar nicht kennt. Und wir wehren uns ja nur gegen solche Aktivitäten.
Es gibt heute international schon zwanzig, dreissig Meldungen pro Tag, und man ist verpflichtet, diese in seinem System zu implementieren, sonst läuft man Gefahr, dass man von Cyberangriffen attackiert wird. Das ist der vernünftige Weg. Es gibt ein weltweit umspannendes Netz, dort gibt es viele Informationen, und diese Informationen müssen gebündelt werden. Das ist aber die Aufgabe des Nationalen Zentrums für Cybersicherheit.
Stellen wir uns vor, eine Velokurierfirma mit einem gut ausgebildeten IT-System müsste jeden Tag die Schwachstellen, die Fehler suchen. Das ist einfach unverhältnismässig. Wenn der Schaden erkannt wird, da sind wir uns einig, dann



melden wir den. Das ist wie bei den Seilbahnen. Das machen wir dort auch und bringen so die ganze Seilbahnbranche auf ein sicheres Niveau. Aber es kann nicht sein, dass mir Busse angedroht wird, wenn ich etwas nicht melde, was ich gar nicht gewusst habe. Das ist hier der Fall.
Deshalb bitte ich Sie, die Mehrheit zu unterstützen.

**Juillard** Charles (M-E, JU): Je suis, sur cette question, la proposition de minorité et je vous en expliquerai la raison.
Le porte-parole de la minorité l'a dit, les vulnérabilités d'aujourd'hui sont les cyberattaques de demain; il est extrêmement important d'avoir cela en tête, parce que les vulnérabilités sont constatées avant que la cyberattaque ait eu lieu. Certes, nous sommes dans des domaines sensibles – il ne vaut pas la peine de le répéter –, compliqués, en constante et rapide évolution, et, certes, la sécurité absolue n'existe pas. Or, signaler les cyberattaques revient à agir après coup.
Bien sûr que l'on peut en tirer des enseignements, comme vient de l'expliquer notre collègue Wicki; mais comparer un incident sur une voiture à un incident sur une centrale nucléaire a ses limites, et les effets pourraient être sensiblement différents. Signaler les cyberattaques, c'est bien, mais, quand même, si l'on pouvait anticiper au lieu de courir après, ce serait mieux. Signaler les vulnérabilités revient à faire de la prévention et faire de la prévention revient à anticiper. Lorsque l'on voit les dégâts causés par les cyberattaques, il y a un inté-

rêt évident, certain, à agir avant que les cyberattaques ne soient lancées pour essayer de les prévenir. C'est aussi un acte de solidarité que de signaler les vulnérabilités, solidarité avec les installations qui ne se seraient pas encore rendu compte qu'elles sont aussi sujettes à des attaques, parce que de telles vulnérabilités se trouvent dans leurs systèmes. Aussi, je crois que nous avons un intérêt certain à soutenir cette annonce de vulnérabilité, parce que cela revient à rendre service aux autres, à lutter préventivement contre ces attaques qui peuvent déstabiliser complètement notre système, qu'il soit de santé, énergétique ou étatique en général. Je vous invite à soutenir la proposition de la minorité de la commission.

**Zopfi** Mathias (G, GL): Wie schon in der ersten Runde kann ich das, was Kollege Wicki als Seilbahnspezialist, aber vielleicht weniger als Cyberspezialist gesagt hat, hier einfach nicht so stehenlassen.
Erstens, Kollege Wicki, sind Velokuriere keine kritische Infrastruktur. Zweitens: Wenn Sie mir zeigen, wo in diesem Gesetz steht, dass man nach Schwachstellen suchen muss, dann gebe ich Ihnen nicht nur eine Flasche Wein, dann können Sie einen Sechserkarton mit einem goldenen "Mäscheli" daran und noch eine Uhr dazu haben. Wissen Sie, warum ich das versprechen kann? Weil Sie das nicht finden werden. Es gibt keine Pflicht für die kritischen Infrastrukturen, nach Schwachstellen zu suchen. Es gibt nur die Pflicht, und nur darum geht es, eine Schwachstelle zu melden, die bekannt ist, der kritischen Infrastruktur selbst, nicht aber der Öffentlichkeit. Es steht explizit im Gesetz: "nicht öffentlich bekannt". Ob Sie die Schwachstelle zufällig gefunden haben, ob Sie sie gefunden haben, weil Sie danach gesucht haben, ob Sie sie im Rahmen eines Cybersicherheitsaudits gefunden haben, spielt keine Rolle. Sie muss Ihnen bekannt sein, dann können Sie sie melden. Was nicht bekannt ist, kann nicht gemeldet werden und muss auch nicht gemeldet werden. Das ist üblich, das ist auch an anderen Orten, in anderen Gesetzen so.
Ich bitte Sie hier, die Sachen nicht allzu sehr zu verdrehen.

**Wicki** Hans (RL, NW): Diese Replik nehme ich natürlich gerne auf. Kollege Zopfi, wenn Sie mir garantieren und bestätigen, dass die Gerichte das dann in der Zukunft nicht so auslegen, dann werfe ich noch eine Flasche nach, fülle die Kiste und schicke sie Ihnen – hundertprozentig, darauf können Sie wetten. Aber ich garantiere Ihnen, in fünf Jahren werden die Gerichte eben nicht nur sagen: "Du hättest das, was du gesehen hast, melden müssen", sondern dass du es eben immer suchen musst und dass du immer für die Allgemeinheit das Beste machen musst. Aus diesem Grund wird sich das so weit entwickeln, dass man das suchen muss. Aus diesem Grund: Die Wette gilt, Kollege Zopfi, Sie können darauf wetten. Sie müssen dann aber auch geradestehen, wenn die Gerichte das so interpretieren. Dann erwarte ich die Flasche, aber nur eine Flasche mit Masche.

**Amherd** Viola, Bundesrätin: Ausser Protokoll möchte ich doch sagen: Wenn die Flaschen dann geöffnet werden, wäre ich auch gerne dabei. *(Heiterkeit)* Spass beiseite!
Der Nationalrat hat an seiner Sitzung vom 11. September 2023 beschlossen, an der Differenz zum Ständerat festzuhalten. Er befürwortet weiterhin die Ausweitung der Meldepflicht auf Schwachstellen. Er hat dabei einem Kompromissvorschlag zugestimmt, der die Meldepflicht auf Schwachstellen bei eingekauften Software- und Hardwareprodukten beschränkt.
Ihre Sicherheitspolitische Kommission – das wurde von der Kommissionssprecherin dargelegt – hat den Beschluss des Nationalrates geprüft. Dabei hat sie auch den Antrag Zopfi behandelt, der die Meldepflicht für Schwachstellen weiter einschränken will und die Möglichkeit von anonymen Meldungen vorsieht. Ihre Kommission hat den Kompromissbeschluss des Nationalrates wie auch den Antrag Zopfi abgelehnt. Sie hat sich erneut gegen die Ausweitung der Meldepflicht auf Schwachstellen ausgesprochen und hält an der ursprünglichen Fassung des Ständerates und dem Entwurf des Bundesrates fest.
Der Bundesrat teilt die Einschätzung Ihrer Kommission. Die im Vorfeld geäusserten Bedenken der Wirtschaft zeigen, dass es einen grossen Unterschied zwischen Meldungen von Cyberangriffen und Meldungen von Schwachstellen gibt. Das NCSC nimmt seit vielen Jahren Meldungen von Cyberangriffen entgegen. Der Informationsaustausch ist gut etabliert, und es besteht ein hohes Vertrauen seitens der Wirtschaft, dass mit diesen Meldungen korrekt umgegangen wird. Bei Meldungen von Schwachstellen ist diese Zusammenarbeit noch nicht gleich stark ausgeprägt. Das NCSC hat seine Kapazitäten für die Analysen von Schwachstellen erst in den letzten Jahren aufgebaut. Es besteht deshalb noch kein regelmässiger Austausch zu Schwachstellen.
Nous plaidons pour que cet échange sur les vulnérabilités soit d'abord établi sur une base volontaire, avant d'introduire une obligation de notification. La confiance nécessaire entre l'Etat et l'économie pour l'échange d'informations sur les vulnérabilités peut être mieux renforcée sur la base d'une annonce volontaire que par l'introduction d'une obligation de déclaration.
Je vous demande donc de maintenir votre décision et de suivre le Conseil fédéral et votre commission.

*Abstimmung – Vote*
(namentlich – nominatif; 22.073/5990)
Für den Antrag der Mehrheit ... 32 Stimmen
Für den Antrag der Minderheit ... 12 Stimmen
(0 Enthaltungen)

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

AB 2023 S 795 / BO 2023 E 795