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
(Zuberbühler, Addor, Cattaneo, Heimgartner, Hess Erich, Hurter Thomas, Riniker, Tuena, Walliser)
Zustimmung zum Beschluss des Ständerates

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
(Zuberbühler, Addor, Cattaneo, Heimgartner, Hess Erich, Hurter Thomas, Riniker, Tuena, Walliser)
Adhérer à la décision du Conseil des Etats

AB 2023 N 1478 / BO 2023 N 1478

Art. 74d
Antrag der Mehrheit
Titel
Festhalten
Abs. 2
Eine Schwachstelle muss gemeldet werden, wenn sie:

a. Betriebskritische Informatikmittel betrifft;
b. Noch nicht öffentlich bekannt ist;
c. Nicht durch Eigenentwicklungen der betroffenen Unternehmen entstanden ist.

Antrag der Minderheit
(Zuberbühler, Addor, Cattaneo, Heimgartner, Hess Erich, Hurter Thomas, Riniker, Tuena, Walliser)
Titel, Abs. 2
Zustimmung zum Beschluss des Ständerates

Art. 74d
Proposition de la majorité
Titre
Maintenir
Al. 2
Une vulnérabilité doit être signalée lorsque:
a. elle concerne des moyens informatiques essentiels pour l'exploitation;
b. elle est encore inconnue du public;
c. elle ne résulte pas de développements internes de l'entreprise concernée.

Proposition de la minorité
(Zuberbühler, Addor, Cattaneo, Heimgartner, Hess Erich, Hurter Thomas, Riniker, Tuena, Walliser)
Titre, al. 2
Adhérer à la décision du Conseil des Etats

Art. 74e Abs. 1, 2; 74f Abs. 1, 2; Ziff. II Ziff. 3 Art. 102 Abs. 2
Antrag der Mehrheit
Festhalten

Antrag der Minderheit
(Zuberbühler, Addor, Cattaneo, Heimgartner, Hess Erich, Hurter Thomas, Riniker, Tuena, Walliser)
Zustimmung zum Beschluss des Ständerates

Art. 74e al. 1, 2; 74f al. 1, 2; ch. II ch. 3 art. 102 al. 2
Proposition de la majorité
Maintenir

Proposition de la minorité
(Zuberbühler, Addor, Cattaneo, Heimgartner, Hess Erich, Hurter Thomas, Riniker, Tuena, Walliser)
Adhérer à la décision du Conseil des Etats

Präsident (Candinas Martin, Präsident): Wir befinden uns in der ersten Runde der Differenzbereinigung, und es verbleibt noch eine Reihe von Differenzen.

Zuberbühler David (V, AR): Ich spreche zur Minderheit Zuberbühler zum 2. Abschnitt, in welchem es um die Pflicht zur Meldung von Cyberangriffen und Schwachstellen geht. Im Sinn der Effizienz spreche ich zeitgleich auch für die SVP-Fraktion.
Im Rahmen der Frühjahrssession hat unser Rat die Einführung einer Meldepflicht bei Cyberangriffen auf kritische Infrastrukturen beschlossen. Zusätzlich hat unser Rat in Abweichung zum Entwurf des Bundesrates der Einführung einer Pflicht zur Meldung von Schwachstellen zugestimmt. Während der Sommersession hat auch der Ständerat als Zweitrat das Geschäft beraten. Dabei hat er, wohl auch deshalb, weil selbst der Bundesrat den inhaltlichen Erweiterungen der Meldepflicht skeptisch gegenübersteht, die Ausweitung der Meldepflicht auf IT-Schwachstellen ziemlich deutlich verworfen.
Ausschlaggebend dafür war aber wohl nicht nur die skeptische Haltung des Bundesrates, sondern auch die kritische bzw. ablehnende Haltung der vielen Verbände und Unternehmen, die von dieser Erweiterung betroffen wären. Diese Verbände und Unternehmen haben ja einerseits Angst vor einer administrativen Mehrbelastung für die Unternehmen und den Staat. Andererseits haben sie Angst, dass die Sammlung von Informationen zu

Schwachstellen bei einer zentralen staatlichen Stelle die kritischen Infrastrukturen mehr gefährdet, als sie diese schützt. Informationen zu allfälligen Schwachstellen, die zu melden wären, könnten möglicherweise problemlos in die Hände von Hackern gelangen, was unter Umständen zu grossen Problemen führen könnte. Wenn eine Schwachstellenmeldung von Hackern entdeckt wird, kann dies verschiedene Herausforderungen und Risiken mit sich bringen. In solchen Fällen besteht das Risiko, dass die Schwachstelle von Hackern ausgenutzt wird, bevor entsprechende Massnahmen ergriffen werden können, um sie zu beheben. Dies kann zu potenziellen Angriffen, Datenverlusten oder anderen Sicherheitsverletzungen führen.
Ja, die Bedenken der Verbände und der betroffenen Betreiberinnen kritischer Infrastrukturen sind nicht unberechtigt. Hacker haben ja erst im Juni mehrere Millionen Datensätze des Bundesamtes für Polizei (Fedpol) und des Bundesamtes für Zoll und Grenzsicherheit (BAZG) im Darknet veröffentlicht; auch Daten der Militärpolizei landeten dort. Dabei nutzten die Hacker eine Schwachstelle auf den Servern eines Deutschschweizer Unternehmens, das diese potenziell heiklen Daten aufbewahrte. Der Vorfall wie auch der Umstand, dass beim Bund ganz offensichtlich ein Klumpenrisiko besteht, sind derart gravierend, dass der Bundesrat Ende Juni gar einen Krisenstab einberufen hat. Er tat das nicht zu Unrecht. Schliesslich handelte es sich beim Datenklau um einen Super-GAU, weil unter anderem Interpol-Anfragen sowie Sicherheitsdispositive für Staatsgäste und Magistraten im Netz frei zugänglich waren oder immer noch frei zugänglich sind.
Das ebenfalls betroffene BAZG schränkte zwar die Tragweite des Cyberangriffes ein, weil Daten des Bundesamtes selbst nicht betroffen waren. Das BAZG räumte aber dennoch ein, dass Daten aus der Korrespondenz mit Kunden betroffen waren – und wenn wir von "Korrespondenz mit Kunden" hören, dann schrillen bei uns natürlich die Alarmen.
Die Schwachstellen, die der Ständerat aus dem Informationssicherheitsgesetz streichen möchte, müssen ja auch in irgendeiner Form gemeldet werden. Wie die Vergangenheit gezeigt hat, ist es nicht ausgeschlossen, dass solche Daten eben in die Hände von Hackern gelangen. Das ist brandgefährlich. Gefährlich ist es auch deshalb, weil Hacker immer einen Schritt voraus sind und weil die von einem Cyberangriff betroffenen Kreise erst dann reagieren können, wenn der Cybervorfall bereits passiert ist.
Meine Minderheit und die SVP-Fraktion sind heute der Meinung, dass der Fokus auf die Bewältigung von Cyberangriffen gelegt werden sollte. Eine Ausweitung auf Schwachstellen könnte den Bogen überspannen, insbesondere auch deshalb, weil dazu gar keine Vernehmlassung durchgeführt wurde und weil die Gefahr einfach zu gross ist, dass hochsensible Daten in die Hände von Kriminellen gelangen könnten. Die Folgen könnten sein: gezielte Angriffe auf betroffene Systeme, Datenklau, unautorisierter Zugriff, Verkauf dieser Schwachstellenmeldungen auf dem Schwarzmarkt, Weitergabe an staatliche Akteure zwecks Durchführung von gezielten Cyberoperationen oder Spionageaktivitäten, Einschleusung von Schadsoftware oder die Durchführung von anderen schädlichen Aktivitäten.
Die SVP-Fraktion möchte die einzige Differenz mit dem Ständerat ausräumen. Ich mache Ihnen deshalb beliebt, die Minderheit Zuberbühler zu unterstützen und dem Ständerat zu folgen.

Marti Min Li (S, ZH): Grundsätzlich ist unbestritten, dass Cybersicherheit ein wichtiges Anliegen ist und dass kritische Infrastruktur bestmöglich geschützt werden soll. Die Einführung der Meldepflicht für Cyberangriffe ist daher eine wichtige Errungenschaft, die wir als SP-Fraktion seit Längerem gefordert haben und die wir ausdrücklich begrüssen.
Die Differenz zum Ständerat besteht darin, dass gemäss dem Beschluss des Nationalrates auch eine Meldepflicht für

kritische Schwachstellen eingeführt werden soll. Dagegen wehrt sich insbesondere die Wirtschaft, die darin einen erhöhten Aufwand sieht, die Definition von "Schwachstelle" als zu wenig klar erachtet und bezweifelt, dass damit mehr Sicherheit geschaffen würde.
Es kann durchaus sein, dass in der Version des Nationalrates noch einige – um es so zu sagen – Schwachstellen vorhanden sind. Aber deswegen ganz auf die Meldung der Schwachstellen zu verzichten, scheint uns zum jetzigen Zeitpunkt als verfrüht. Wir wissen, das wurde bereits in den vergangenen Debatten gesagt, dass die Schweiz in Sachen Cybersicherheit nicht an vorderster Front rangiert. Wir wissen auch, dass andere Länder weit mehr für den Schutz von kritischen Infrastrukturen tun, gerade auch, wenn es um die Meldung von Schwachstellen geht.
Wenn der Nationalrat hier jetzt also festhält, dann hat der Ständerat die Möglichkeit, den Artikel noch einmal anzuschauen, gegebenenfalls auch abzuändern, um den Bedenken etwas mehr Rechnung zu tragen. Wenn der Nationalrat aber dem Minderheitsantrag Zuberbühler zustimmt, dann ist das Thema vom Tisch. Man muss

dazu sagen, dass die Diskussion in der ständerätlichen Kommission überhaupt nicht klar war: Eine Mehrheit der Kommission war für diese Meldepflicht.
Ein Verzicht scheint uns zum jetzigen Zeitpunkt wirklich nicht sinnvoll zu sein, gerade weil wir diese Probleme mit der Cybersicherheit haben.
Aus diesem Grund bitte ich Sie im Namen der SP-Fraktion, der Mehrheit Ihrer Sicherheitspolitischen Kommission zu folgen und an dieser Meldepflicht festzuhalten.

Fivaz Fabien (G, NE): La sécurité informatique est l'affaire de toutes et tous. C'est ensemble que nous pourrons détecter et corriger les vulnérabilités à temps. C'est particulièrement le cas pour les infrastructures critiques. Une obligation d'annonce des failles de vulnérabilité est, en ce sens, extrêmement importante. Ce ne sera pas un monstre bureaucratique, et cela ne doit pas engendrer un climat de méfiance qui nuirait à la coopération. Si nous pouvons comprendre que cette nouveauté n'ait, en soi, pas fait l'objet d'une consultation et que certains cantons ou groupes d'intérêt souhaiteraient en faire un objet séparé, il nous semble à l'inverse qu'elle s'inscrit parfaitement dans le cadre du projet qui a été dessiné par le Conseil fédéral.
Un récent sondage a montré que presque la moitié des grandes entreprises suisses ont été touchées par une cyberattaque; c'est donc aussi dans leur intérêt. Nous sommes persuadés qu'une solution avec elles et pour elles pourra être dessinée.
Le groupe des Verts soutient donc la proposition de la majorité de la commission.
C'est un pont en direction du Conseil des Etats, qui pourra lui-même encore une fois améliorer le projet s'il le souhaite. Mais, s'il vous plaît, ne jetez pas le bébé avec l'eau du bain; en effet, si nous acceptons aujourd'hui la proposition de minorité Zuberbühler, il n'existera plus de divergences avec la version du Conseil des Etats, et cette proposition, qui a été acceptée assez largement par notre conseil au mois de mars, sera totalement abandonnée.
Merci de soutenir la majorité.

Glanzmann-Hunkeler Ida (M-E, LU): Beim Informationssicherheitsgesetz diskutieren wir heute über die Grundsatzfrage, ob Schwachstellen gemeldet werden müssen oder nicht. Wir von der Mitte-Fraktion sind nach wie vor der Meinung, dass erstens eine rasche Meldung eines Cyberangriffes erfolgen soll und dass zweitens danach auch Schwachstellen gemeldet werden sollen.
Die Kritik der Verbände erfolgte nach unserer ersten Beratung, mit der Begründung, dass ein administrativer Mehraufwand für Unternehmen und Staat geschaffen würde. Die Frage ist, ob wir noch eine gute Lösung, allenfalls eine Kompromisslösung finden können, in deren Rahmen Schwachstellen trotzdem gemeldet werden müssen, oder ob es allenfalls in eine Kann-Formulierung geändert werden kann. Die Frage, ob ein Mehraufwand bei besserer Sicherheit nicht doch gerechtfertigt wäre, ist wohl berechtigt.
Wir müssen uns hier bewusst sein, dass es bei diesem Gesetz um kritische Infrastrukturen geht und nicht um kleine Firmen. Wenn wir jetzt ein neues Gesetz erarbeiten und nach einem halben Jahr genau diese Formulierung im Gesetz fehlt, würden wir von der Mitte-Fraktion das kaum verstehen. Die Mitte-Fraktion wird deshalb an der Differenz zum Ständerat festhalten, das heisst mit der Mehrheit stimmen, damit der Ständerat allenfalls noch einen Kompromiss ausarbeiten kann. Besten Dank, dass Sie dieses Vorgehen ebenfalls unterstützen.

Mettler Melanie (GL, BE): Es ist für die Grünliberalen unbestritten, dass die Sicherheitsbehörden eine wichtige Rolle bei der Gewährleistung der Cybersecurity spielen. Cyberangriffe auf kritische Infrastrukturen sind bereits Teil der aktuellen "Kriegsführung"; wir sind solchen Angriffen bereits ausgesetzt. Um ihre Rolle zur Gewährleistung der Sicherheit wahrnehmen zu können, müssen die Sicherheitsbehörden natürlich auch über die notwendigen Informationen verfügen. Der Staat ist hier der einzige denkbare Akteur, der diese Position mit einer Gesamtsicht der Bedrohungssituation einnehmen kann bzw. muss.
Die Abläufe werden ja auch nicht auf der grünen Wiese gestaltet, sondern sind international bereits gut etabliert. Das NCSC unterstützt die Betreiberinnen von kritischen Infrastrukturen beim Schutz vor Cyberbedrohung; das ist seine Hauptaufgabe. Um diese Aufgabe durchführen zu können, muss es eben wissen, wo Bedrohungen anfallen, wie sie anfallen, wie die Entwicklungen sind, wie sich die Bedrohungslage mit Blick auf die innere und äussere Sicherheit entwickelt, um eben auch Empfehlungen machen zu können sowie Sensibilisierungsmassnahmen und Unterstützungsangebote entwickeln zu können. *(Glocke und Zwischenruf des Präsidenten: Frau Mettler, Sie können weiterfahren.)* Ich bin vielleicht selber schuld, wenn ich etwas sage, was alle schon wissen. – Die Meldung beim NCSC führt zu einem subsidiären Unterstützungsangebot.
Bezüglich der Ausgestaltung der Meldepflicht in den konkreten administrativen Prozessen – darum ging es ja bei den Lobbyingschreiben, die viele von uns erhalten haben – sind die Grünliberalen neutral. Natürlich muss der Informationsfluss einfach und effizient und eben sicher sein. Es ist auch klar, dass die grösseren

Organisationen bereits heute professionelle Abläufe haben, eine hohe "digital literacy" aufweisen und entsprechend professionell aufgestellt sind. Wichtig für die Cybersecurity in der Schweiz sind aber auch sehr kleine Unternehmen und Organisationseinheiten mit heute noch tiefer "digital literacy". Das können Gemeindeverwaltungen, kleine Energieversorger, Unternehmen im Bauwesen, Logistikunternehmen, Bildungsinstitutionen usw. sein.
Hier im Nationalrat wurde die Vorlage mit 132 zu 55 Stimmen unterstützt. Jetzt hat der Ständerat die Verbindlichkeit offenbar reduziert. Er stört sich auch daran, dass bei Nichterfüllen der Meldepflicht als letzte Eskalationsstufe Sanktionsmöglichkeiten vorgesehen sind. Die Grünliberalen sind aber der Ansicht, dass es gerade bei kleineren Organisationen – dort liegen ja die Risiken – einen Anreiz braucht, die Unterstützungsangebote zu nutzen. Konkrete Vorschläge bezüglich effizienterer Prozesse begrüssen die Grünliberalen natürlich, denn es geht hier um die Sicherheit in der Schweiz und nicht darum, eine administrative Datenkrake zu schaffen.
Wir werden überall der Mehrheit folgen.

Fiala Doris (RL, ZH): Zuerst möchte ich meine Interessenbindung nochmals offenlegen: Ich bin Präsidentin der Swiss Cybersecurity Days und kämpfe in dieser Funktion seit Jahren für ein besseres Verständnis und für mehr Resilienz im Bereich der Cyberkriminalität.
Das Inventar der kritischen Infrastrukturen zeigt auf, welche wichtigen Bauten und Anlagen strategisch von grosser Bedeutung sind. Das sogenannte SKI-Inventar ist nicht öffentlich zugänglich, jedoch für das Risikomanagement auf allen Stufen – Bund, Kantone, Gemeinden – von grosser Bedeutung. Die sogenannte Digitalisierung in

allen Bereichen steht nicht nur für Fortschritt, sondern auch für grosse Verletzlichkeit. Flughäfen, öffentlicher Verkehr, Stromversorgungs-, Telekommunikations-, Wasserversorgungsinfrastruktur und vieles mehr: Die Liste kritischer Infrastrukturen ist lang. Längst nicht alles untersteht dem Bund. Sicherheit bleibt aber erste Staatsaufgabe – neben der Eigenverantwortung der Unternehmen.
Punkto Cybersicherheit lag die Schweiz im ITU-Ranking 2022 international leider noch nicht auf einem Topplatz. Wir sollten allerdings nicht das Kind mit dem Bade ausschütten: Die Meldepflicht für IT-Schwachstellen bei nicht bereits erfolgter Cyberkriminalität ginge der FDP-Liberalen Fraktion zu weit. Wir bitten Sie daher, dem Beschluss des Ständerates und somit der Minderheit Zuberbühler zu folgen. Die Gründe hierfür sind zahlreich. Die Meldungen von IT-Schwachstellen würden mit Sicherheit zu hohen administrativen Mehrbelastungen führen; vermutlich wäre auch das neu geschaffene NCSC unter der Leitung von Florian Schütz überfordert. Die Eigenverantwortung der Unternehmer wäre beschnitten, und der Bund hätte darüber hinaus wohl auch Mühe, alles zu bewältigen. Das ist verständlich.
Last, but not least: Kryptowährungen sind nicht der Grund für Cyberkriminalität. Wer in der unternehmerischen Verzweiflung nach einer Cyberattacke glaubt, sich mit Erpressergeldern unbemerkt von Verletzlichkeiten und Cyberkriminalität freikaufen zu können, schadet letztlich nicht nur seinem Unternehmen, sondern auch der Sicherheit unseres Landes. Cyberkriminalität ist, wie die Swiss Blockchain Federation richtigerweise sagt, ein Problem, das in internationaler Zusammenarbeit und ganzheitlich angegangen werden muss. Private Lösungen oder Insellösungen sind einfach zu umgehen und deshalb abzulehnen. Wer sich erpressen lässt, trägt dazu bei, dass Erpressungen unsere Wirtschaft vermehrt lahmlegen – ein Teufelskreis. Es ist fatal, dass Cyberrisiken bereits heute fast nicht mehr zu versichern sind. Die laufende öffentliche Debatte rund um das Informationssicherheitsgesetz trägt dazu bei, dass Schamgefühle betroffener Unternehmen abgebaut und ihre Vorkehrungen im Kampf gegen Cyberkriminalität hoffentlich gestärkt werden. Resilienz muss das Ziel sein, und das auf eine Art und Weise, die uns trotz der vielen Bäume noch den Wald sehen lässt.
Ich bitte Sie daher, umsichtig zu handeln und den Gefahrenschutz dort anzusiedeln, wo er hingehört, damit die Sicherheit bestmöglich gewährleistet wird.

Amherd Viola, Bundesrätin: Der Ständerat lehnt die vom Nationalrat beschlossene Ausweitung der Meldepflicht auf Schwachstellen in kritischen Systemen ab. Er folgt damit dem Entwurf des Bundesrates und trägt den Bedenken der Wirtschaft Rechnung. Seitens der Wirtschaft wird befürchtet, dass die Ausweitung zu einer Vielzahl von Meldungen führen könnte, weil nicht klar genug definiert wird, was eine Schwachstelle ist und ab wann sie meldepflichtig sein soll.
Ihre Sicherheitspolitische Kommission hat einen Kompromissantrag angenommen. Es sind damit nur noch Schwachstellen meldepflichtig, die bei eingekaufter Soft- und Hardware entdeckt werden. Einzelfehler bei Eigenentwicklungen der betroffenen Unternehmen werden von der Meldepflicht ausgeschlossen. Auch diesem

Kompromissantrag stehen Exponenten der Wirtschaft kritisch gegenüber; sie sind skeptisch bezüglich einer Ausweitung der Meldepflicht. Einerseits wird befürchtet, dass der Bund eine zentrale Datenbank mit gemeldeten Schwachstellen unterhalten müsste, die zum Ziel von Hackerangriffen werden könnte. Andererseits wird infrage gestellt, ob die Meldepflicht für Schwachstellen bei betriebskritischen Systemen wirklich zu einer massgeblichen Verbesserung der präventiven Frühwarnung führen kann.
Beim Entscheid, ob eine Meldepflicht für Schwachstellen eingeführt werden soll, gilt es grundsätzlich abzuwägen, ob die Stärkung der Frühwarnung vor unbekannten Schwachstellen den Mehraufwand einer Meldepflicht rechtfertigt. Der Bundesrat ist der Ansicht, dass der Meldeaufwand im Vergleich zum erwarteten Mehrwert zu gross ist und dass die Meldung von Schwachstellen weiterhin freiwillig erfolgen soll. Auf dieser Basis kann das für den Informationsaustausch zu Schwachstellen nötige Vertrauen zwischen Staat und Wirtschaft weiter ausgebaut werden.
Ich bitte Sie, dem Antrag des Bundesrates und des Ständerates zu folgen und die Ausweitung der Meldepflicht auf Schwachstellen abzulehnen.

Andrey Gerhard (G, FR), für die Kommission: Wir haben es gehört: Es bestehen in diesem Geschäft noch Differenzen zum Ständerat, und zwar in Bezug auf die Schwachstellen. Ich möchte aber zuerst noch einmal festhalten, dass eine Mehrheit der Sicherheitspolitischen Kommission die Einführung einer Meldepflicht für Cyberattacken als sehr wichtigen Schritt erachtet, um den immer bedrohlicheren Vorfällen entgegenzutreten. Wir haben das im Nationalrat ja auch so beschlossen.
Künftig sollen es kritische Infrastrukturen möglichst rasch dem heutigen NCSC bzw. dem zukünftigen Bundesamt für Cybersicherheit melden, wenn ihre Betriebstüchtigkeit durch einen Cyberangriff bedroht ist. Damit kann das NCSC einerseits andere Infrastrukturen informieren und andererseits die betroffenen Betreiberinnen unterstützen.
In der gleichen Logik beantragt die Mehrheit Ihrer Kommission eine Meldepflicht auch in Bezug auf Schwachstellen. Nicht öffentlich bekannte Sicherheitslücken, welche die Betriebsfähigkeit der kritischen Infrastrukturen beeinträchtigen können, sollen dem NCSC ebenfalls gemeldet werden; dies mit dem Ziel, dass andere Infrastrukturen, welche in ihrem Betrieb ebenfalls solche Lücken haben, so rasch wie möglich gewarnt werden und dass damit potenzielle Angriffsmöglichkeiten für Cyberkriminelle eliminiert werden können.
Es wird moniert, dass das zu einem gewissen administrativen Aufwand führen kann. Das ist sicherlich nicht komplett zu verneinen, hingegen ist auch nicht ausser Acht zu lassen, dass die Unternehmen mit der Begleitung, die angeboten wird, ja durchaus auch von einer Dienstleistung des NCSC profitieren.
Der Ständerat ist dem Anliegen seiner Sicherheitspolitischen Kommission, der nationalrätlichen Erweiterung zuzustimmen, nicht gefolgt. Daraufhin hat die SiK-N anlässlich der Beratung im Juni die Meldepflicht für Schwachstellen eingegrenzt. Wir haben es soeben von Bundesrätin Amherd gehört: So sollen Schwachstellen nur dann gemeldet werden müssen, wenn sie allgemein verfügbare Softwarekomponenten betreffen, also wenn sie keine Eigenentwicklungen sind. Es ist dies, wie Sie der Fahne entnehmen können, eine marginale Änderung bei Artikel 74d. Damit sollen unnötige Meldungen und administrativer Aufwand für die Unternehmen vermieden werden, zumal spezifische Eigenentwicklungen nicht von anderen Betreibern eingesetzt werden und deshalb der Nutzen einer Meldung an das NCSC nicht gegeben ist. Dieser neue Antrag wurde von Ihrer Kommission mit 14 zu 9 Stimmen bei 1 Enthaltung verabschiedet. Eine Minderheit Zuberbühler lehnt hingegen die Einführung einer Meldepflicht für Schwachstellen generell ab und beantragt, dem Beschluss des Ständerates zu folgen bzw. am Entwurf des Bundesrates festzuhalten.
Im Namen der SiK-N bitte ich Sie, dem Kompromissantrag bezüglich der Meldepflicht für Schwachstellen zu folgen.

Pointet François (GL, VD), pour la commission: Le projet qui nous occupe aujourd'hui établit l'obligation de signaler les cyberattaques contre les infrastructures critiques. Nous sommes au niveau des divergences. Il nous en reste encore une avec le Conseil des Etats, qui concerne une obligation d'annoncer les vulnérabilités inconnues du public.
Cette proposition d'ajouter cette obligation a été suivie en première lecture par une majorité forte de votre commission, et acceptée en plénum. Depuis, le Conseil des Etats a refusé sèchement la proposition, mais en indiquant qu'il était ouvert à la recherche d'un compromis.
La commission a donc reconsidéré sa position lors de sa séance du 19 juin et vous propose justement un compromis. L'obligation d'annonce a été allégée, en ce sens qu'elle ne concerne plus les systèmes développés en interne de l'entreprise concernée. Autrement dit, l'obligation d'annonce des vulnérabilités reste, dans la proposition que nous vous

faisons aujourd'hui, lorsqu'il est fort probable qu'elle existe pour une autre infrastructure critique ou une organisation qui ne la connaîtrait pas encore. Cela fait donc sens, aux yeux de la majorité de la commission, pour augmenter la sécurité face aux cyberattaques en comblant au plus vite les vulnérabilités non connues du public.
La commission a pris connaissance des griefs annoncés par les milieux économiques. Ces arguments sont essentiellement les suivants: la crainte que les informations fournies au Centre national pour la cybersécurité (NCSC) puissent être piratées et utilisées à des fins d'attaques, et une augmentation inconsidérée des tâches administratives.
Ces arguments ont convaincu la minorité de la commission, mais la majorité reste d'avis que le compromis proposé permettrait d'augmenter la cybersécurité de nos infrastructures critiques et ne conduirait pas à une augmentation inconsidérée des coûts. En effet, les infrastructures critiques doivent de toute manière gérer et corriger les vulnérabilités qu'elles constatent. Communiquer au Centre national pour la cybersécurité (NCSC) les vulnérabilités non publiées hors des systèmes développés en interne ne constituerait pas une tâche coûteuse ou inconsidérée du point de vue des efforts. Pour ce qui est de la crainte que les informations collectées par le NCSC soient volées, il est bon de rappeler que le NCSC gère déjà des annonces de vulnérabilité non publiées.
La commission vous propose de soutenir le compromis par 14 voix contre 9 et 1 abstention.

Abstimmung – Vote
(namentlich – nominatif; 22.073/27207)
Für den Antrag der Mehrheit ... 102 Stimmen
Für den Antrag der Minderheit ... 80 Stimmen
(0 Enthaltungen)

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