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
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Fivaz Fabien, Andrey, Barrile, Mettler, Molina, Pointet, Roth Franziska, Schlatter, Seiler Graf)
Festhalten

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
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Fivaz Fabien, Andrey, Barrile, Mettler, Molina, Pointet, Roth Franziska, Schlatter, Seiler Graf)
Maintenir

Art. 74d
Antrag der Mehrheit
Titel, Abs. 2
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Fivaz Fabien, Andrey, Barrile, Mettler, Molina, Pointet, Roth Franziska, Schlatter, Seiler Graf)
Titel
Festhalten
Abs. 2
Festhalten, 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
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Fivaz Fabien, Andrey, Barrile, Mettler, Molina, Pointet, Roth Franziska, Schlatter, Seiler Graf)
Titre
Maintenir
Al. 2
Maintenir, 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
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Fivaz Fabien, Andrey, Barrile, Mettler, Molina, Pointet, Roth Franziska, Schlatter, Seiler Graf)
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
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Fivaz Fabien, Andrey, Barrile, Mettler, Molina, Pointet, Roth Franziska, Schlatter, Seiler Graf)
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 con cernés et une description technique de la vulnérabilité.

AB 2023 N 1832 / BO 2023 N 1832

Art. 74f
Antrag der Mehrheit
Abs. 1, 2
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Fivaz Fabien, Andrey, Barrile, Mettler, Molina, Pointet, Roth Franziska, Schlatter, Seiler Graf)
Abs. 1, 2
Festhalten
Abs. 1bis
Das NCSC speichert und bearbeitet die Meldungen nur auf sicheren Systemen.

Art. 74f
Proposition de la majorité
Al. 1, 2
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Fivaz Fabien, Andrey, Barrile, Mettler, Molina, Pointet, Roth Franziska, Schlatter, Seiler Graf)
Al. 1, 2
Maintenir
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
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Fivaz Fabien, Andrey, Barrile, Mettler, Molina, Pointet, Roth Franziska, Schlatter, Seiler Graf)
Festhalten

Ch. II ch. 3 art. 102 al. 2
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Fivaz Fabien, Andrey, Barrile, Mettler, Molina, Pointet, Roth Franziska, Schlatter, Seiler Graf)
Maintenir

Präsident (Candinas Martin, Präsident): Wir befinden uns in der zweiten Runde der Differenzbereinigung.

Fivaz Fabien (G, NE): Je vous présente la proposition de minorité sur la question des vulnérabilités et de leur signalement. J'aimerais rappeler l'objectif de la proposition, qui était soutenu par la majorité, ici au conseil, et jusqu'à mardi en commission: l'idée est d'obliger les infrastructures critiques à signaler non seulement les cyberattaques – c'est dans le projet, à la base, du Conseil fédéral –, mais également les vulnérabilités qui

auraient été détectées dans leurs systèmes. Ces vulnérabilités sont au coeur du problème: ce sont les failles de sécurité qui, si elles ne sont pas corrigées, sont simplement des portes ouvertes à des cyberattaques et qui peuvent être exploitées. Dans ce sens, il est logique et nécessaire qu'elles soient communiquées et connues pour être corrigées rapidement, et cela dans un cercle relativement large.
La proposition de compromis que nous faisons est un peu le compromis du compromis. Selon cette nouvelle proposition, seules les vulnérabilités critiques devraient être signalées lorsqu'elles concernent des moyens qui sont essentiels pour l'exploitation de l'infrastructure. Il faut également que cette vulnérabilité soit jusque-là inconnue du public – c'est essentiel – et qu'elle ne résulte pas de développements internes à l'entreprise.
Le délai de signalement a, quant à lui, été prolongé. A la base, on prévoyait vingt-quatre heures – c'est ce qui est prévu pour les cyberattaques – mais il a été prolongé à sept jours, ce qui permettra, entre autres, de corriger le problème avant de le signaler.
Afin de rassurer celles et ceux qui craignent que les vulnérabilités puissent être communiquées si elles sont publiques, et donc utilisées, la proposition contient également, à l'article 74f, une obligation, pour le Centre national pour la cybersécurité, de traiter ces signalements sur des systèmes qui sont eux-mêmes sécurisés.
J'aimerais dire quand même que nous attendons des infrastructures critiques qu'elles corrigent dans les plus brefs délais l'ensemble des vulnérabilités qu'elles détectent, afin de limiter le risque d'exploitation et le risque systémique où finalement une vulnérabilité détectée dans un système se propage à l'ensemble et rend possible des cyberattaques à très large échelle.
Je vous propose donc de suivre ma minorité et vous en remercie.

Zuberbühler David (V, AR): Sie erinnern sich: Unser Rat hatte in der Frühjahrssession mit 126 zu 52 Stimmen beschlossen, eine Meldepflicht für Schwachstellen einzuführen. Der Ständerat lehnte die Bestimmung in der Sommersession mit 31 zu 13 Stimmen ab. Auf Antrag Ihrer Sicherheitspolitischen Kommission haben Sie Anfang Session mit 102 zu 80 Stimmen eine Neuformulierung von Artikel 74d Absatz 2 beschlossen. Die Neuformulierung sah vor, dass eine Schwachstelle nicht hätte gemeldet werden müssen, wenn es sich dabei um eine Eigenentwicklung eines betroffenen Unternehmens gehandelt hätte. Der Ständerat hat am letzten Dienstag sehr deutlich bzw. noch deutlicher als zuvor, nämlich mit 32 zu 12 Stimmen bei 0 Enthaltungen, entschieden, die Schwachstellenmeldung definitiv aus dem Informationssicherheitsgesetz (ISG) zu streichen.
Im Namen der SVP-Fraktion mache ich Ihnen deshalb beliebt, die letzte Differenz zum Ständerat auszuräumen, damit das Geschäft nicht noch in die Einigungskonferenz gehen muss, wo es unter Umständen Schiffbruch erleiden könnte. Die SVP-Fraktion ist nach wie vor der Ansicht, dass der Fokus auf die Bewältigung von Cyberangriffen gelegt werden sollte. Eine Ausweitung auf die Schwachstellen geht zu weit – zu weit, weil dazu keine Vernehmlassung durchgeführt wurde und sich die Betreiber kritischer Infrastrukturen dazu gar nicht äussern konnten; zu weit, weil die Meldung von Schwachstellen zu einer grossen Mehrbelastung für die Unternehmen und den Staat führen würde; und zu weit, weil die Gefahr einfach zu gross ist, dass hochsensible Daten, die an einer zentralen Stelle beim Bund gesammelt werden, in die Hände von Hackern gelangen könnten.
Ich erinnere daran, was ich bereits am ersten Montag dieser Session gesagt habe: Wie die Vergangenheit gezeigt hat, ist es nicht ausgeschlossen, dass hochsensible Daten in die Hände von Hackern gelangen könnten. Der Super-GAU bzw. Datenklau bei der Firma Xplain, bei der Kriminelle mehrere Millionen Dateien erbeuteten, lässt grüssen!
Das ist gefährlich – gefährlich deshalb, weil Hacker immer einen Schritt voraus sind und die von einem Cyberangriff betroffenen Kreise erst dann reagieren können, wenn der Cybervorfall bereits passiert ist. Stellen Sie sich vor: Sie spielen morgen als Fussballprofi einen WM-Final und wissen, dass Ihr Knöchel oder Fuss angeschlagen ist. Werden Sie Ihre körperliche Schwachstelle melden, auf die Gefahr hin, dass Ihr Gegner davon Wind bekommt? Und was passiert dann? Die Wahrscheinlichkeit ist gross, dass Ihr Gegner absichtlich auf Ihren Fuss oder Knöchel steht und dass Sie so verletzt werden, dass Sie ausgewechselt werden müssen. Auch im Hockey gibt es einen Grund, weshalb in den Playoffs keine medizinischen Bulletins ausgegeben werden. Informationen gibt es in der Regel keine, die Clubs halten die medizinischen Bulletins aus praktischen Gründen unter Verschluss. Es könnte ja noch einer auf die Idee kommen und da draufhauen, wo es sowieso schon zwickt. Die Clubs kennen die Blessuren und Schlimmeres ihrer Spieler. Sie kennen folglich die Schwachstellen und schützen sie, wollen aber nicht, dass der Gegner sie kennt.
Genauso verhält es sich mit den IT-Schwachstellen: Die Betreiber kritischer Infrastrukturen kennen ihre Schwachstellen oder finden neue, sie wollen aber nicht, dass ein krimineller Dritter an diese Informationen kommt und die kritische

Infrastruktur aufgrund dieses Wissens lahmlegt. Die freiwillige Meldung von Schwachstellen ist heute schon möglich. Die Einführung eines Obligatoriums geht aber definitiv zu weit, weil das NCSC dafür noch gar nicht bereit ist bzw. erst seit wenigen Jahren ein Schwachstellenmanagement betreibt.
Deshalb bitte ich Sie, der Mehrheit der Kommission und damit dem Bundesrat zu folgen.

Amherd Viola, Bundesrätin: Es wurde vom Präsidenten einleitend gesagt: Wir befinden uns in der zweiten Runde der Differenzbereinigung. Sie sind also inhaltlich mit dem Geschäft vertraut.
Der Ständerat hat an seiner Sitzung vom 19. September die Ausweitung der Meldepflicht auf Schwachstellen erneut abgelehnt. Ihre Sicherheitspolitische Kommission empfiehlt, die Differenz zu bereinigen. Sie hat mit 15 zu 9 Stimmen entschieden, dem Ständerat zu folgen. Wir teilen die Ansicht Ihrer Kommission, dass die Einführung einer Meldepflicht gegen den Widerstand der betroffenen Betreiber von kritischen Infrastrukturen nicht zielführend ist. Wir wollen weiterhin gemeinsam mit der Wirtschaft gegen Cyberbedrohungen vorgehen. Für diese Zusammenarbeit braucht es ein hohes gegenseitiges Vertrauen. Eine Meldepflicht bei Schwachstellen würde diese Zusammenarbeit erschweren.
Ich bitte Sie, dem Entscheid Ihrer Kommission zu folgen und damit die letzte verbliebene Differenz auszuräumen.

Pointet François (GL, VD), pour la commission: Le projet qui nous occupe une nouvelle fois aujourd'hui établit l'obligation de signaler les cyberattaques contre les infrastructures critiques; nous sommes dans la deuxième ronde d'élimination des divergences. Il nous reste une divergence avec le Conseil des Etats qui concerne l'obligation d'annoncer les vulnérabilités inconnues du public, obligation que votre commission voulait introduire dans la loi.
La majorité de votre commission a décidé de s'aligner sur le Conseil des Etats et d'abandonner l'idée de mettre en place une telle obligation pour les infrastructures critiques. Il a été considéré qu'il était trop tôt pour passer à une telle obligation et qu'une période d'observation était nécessaire. Nous resterons donc sur un système volontaire, en espérant que le NCSC développe efficacement le principe de telles annonces pour notre sécurité et incite les infrastructures critiques à faire de telles annonces, malgré l'absence d'obligation.
La proposition de minorité Fivaz Fabien vise à maintenir la divergence. Elle contient un allègement supplémentaire par rapport à la version d'obligation d'annonce des vulnérabilités discutées lundi en début de session. Cet allègement consiste en un allongement du délai d'annonce à sept jours.
Votre commission vous propose de rejeter la proposition de minorité Fivaz Fabien, par 15 voix contre 9 et 0 abstention, et de suivre ainsi le Conseil des Etats.

Andrey Gerhard (G, FR), für die Kommission: Wir befinden uns nun, wie mehrfach genannt, in der Differenzbereinigung, in den letzten Zügen der Änderung des Informationssicherheitsgesetzes. Sie erinnern sich, die Vorlage in ihrer ursprünglichen Form war weitgehend unbestritten. Zu grösseren Diskussionen und damit zu dieser Differenz, die wir nun das zweite Mal beraten, hat die vom Nationalrat hinzugefügte Meldepflicht auch für gravierende Schwachstellen geführt.
Der Ständerat hat am Dienstag das zweite Mal, mit 32 zu 12 Stimmen, an der bundesrätlichen Fassung festgehalten und ist damit dem Kompromissvorschlag der SiK-N, welchen wir vergangene Woche hier im Plenum mit 102 zu 80 Stimmen beschlossen hatten, nicht gefolgt. Dieser Kompromiss hätte die Meldepflicht für Schwachstellen in Eigenentwicklungen ausgenommen. Der Antrag Zopfi aus dem Ständerat wurde mit dem Minderheitsantrag Fivaz Fabien deckungsgleich in die SiK-N getragen; er erstreckt sich auf der Fahne über mehrere Artikel.
Der Antrag der Minderheit adressiert die Vorbehalte, welche von betroffenen Unternehmen und Verbänden vorgebracht wurden, so z. B. die Möglichkeit, Meldungen auch anonym zu machen, die Frist zur Meldung auszudehnen oder das NCSC zu verpflichten, Meldungen nur auf sicheren Systemen zu transportieren und zu bearbeiten. Nach Aussagen der Verwaltung respektive des NCSC wäre dieser zweite Kompromissvorschlag praktikabel, umsetzbar und im Grundsatz nicht unerwünscht. Die Behörde sei auf Informationsaustausch angewiesen, denn aus Mangel an Ressourcen könne sie nicht selber nach Schwachstellen in kritischer Software suchen.
Die Frage der Schwachstellenmeldung wurde jedoch nicht vernehmlasst, und die betroffenen Stakeholder konnten sich nicht dazu äussern. Deshalb zieht es das NCSC vor, nun zuerst freiwillige Meldungen zu kultivieren, bevor eine Pflicht eingeführt werden soll; also ähnlich, wie dies bei den Cyberattacken praktiziert wurde, die nach einer Phase der Freiwilligkeit mit dem Inkrafttreten der Gesetzesänderung neu meldepflichtig werden.

Ihre Sicherheitspolitische Kommission ist dieser Argumentation gefolgt und empfiehlt Ihnen mit 15 zu 9 Stimmen, der ursprünglichen und damit auch der ständerätlichen Fassung zu folgen, den Minderheitsantrag Fivaz Fabien abzulehnen und somit die Differenz auszuräumen.

Abstimmung – Vote
(namentlich – nominatif; 22.073/27520)
Für den Antrag der Mehrheit ... 98 Stimmen
Für den Antrag der Minderheit ... 59 Stimmen
(1 Enthaltung)

Präsident (Candinas Martin, Präsident): Das Geschäft ist bereit für die Schlussabstimmung.