GRÜNE Schweiz
Waisenhausplatz 21
3011 Bern

rahel.estermann@gruene.ch
031 326 66 15

Eidgenössisches Finanzdepartement,
Herr Bundesrat Ueli Maurer
3003 Bern

per E-Mail an:
ncsc@gs-efd.admin.ch

Bern, 13. April 2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe (Revision Informationssicherheitsgesetz ISG): Vernehmlassung

Sehr geehrter Herr Bundesrat, sehr geehrte Damen und Herren

Sie haben die GRÜNEN eingeladen, sich zum Entwurf zur Änderung des Informationssicherheitsgesetzes (Meldepflicht für Cyberangriffe auf kritische Infrastrukturen) zu äussern. Wir danken Ihnen dafür und nehmen gerne Stellung.

Die GRÜNEN begrüssen die Revision des Gesetzes in der vorgesehenen Richtung. Dies ist ein wichtiger Schritt, der die gesteigerte Bedeutung der Datensicherheit im digitalen Zeitalter aufnimmt und auf eine neue Kultur der gemeinsamen Verantwortung für Cyber-Security verweist. Aus unserer Sicht sollte der Bereich Cyber-Security sogar durch ein eigenes Bundesamt oder ein Staatssekretariat (Vorstoss 21.4389) verankert sein. Bis dahin plädieren wir im Rahmen dieser Gesetzesrevision dafür, die Kompetenzen und Ressourcen des National Cyber Security Centers (NCSC) auszubauen. Wichtig ist, dessen Sensibilisierungsaufgabe umfassend auszulegen: Unsere Gesellschaft ist darauf angewiesen, dass Behörden wie auch Unternehmen und Privatpersonen Massnahmen für die Datensicherheit ernst nehmen. Im Gesetz muss zudem der Begriff der «kritischen Infrastrukturen» erweitert werden, beispielsweise durch kritische Komponenten oder den Bereich der Demokratie. Zudem soll das Gesetz nicht nur die Meldung von Cyberangriffen, sondern von Cybervorfällen verpflichtend machen. Die Anreize für möglichst viele Meldungen (auch freiwillige) müssen hoch, die Hürden dafür tief gesetzt sein. Die Gesetzesrevision soll der Anfang einer neuen gemeinsamen Verantwortungskultur sein, so wie sie beispielsweise im Bereich der Flug- oder Nuklearsicherheit bereits etabliert ist.
Zu den einzelnen Artikeln nehmen wir wie folgt Stellung:

Grundsätzliche Überlegungen und Art. 73a

Wir begrüssen die weitreichende Ausgestaltung der Aufgaben des NCSC in Art. 73a, insbesondere die Sensibilisierung der Öffentlichkeit in lit. a. Der Schutz von Cyber-Risiken ist nur so stark wie sein schwächstes Glied – das heisst, dass eine Gesellschaft darauf angewiesen ist, dass alle Akteurinnen – von Behörden über Unternehmen bis hin zu Privatpersonen –

Massnahmen zur Cyber-Security ernst nehmen. Der Bund schreibt selbst treffend in den Erläuterungen (Seite 28): «Eine erhöhte Cyberkompetenz der Bevölkerung ist eine wichtige Voraussetzung für die erfolgreiche Digitalisierung der Gesellschaft.»

Gerade deshalb ist es nötig, dass das NCSC eine aktivere Rolle einnehmen kann. Es muss Schwachstellen und Bedrohungen aktiv erkennen – einerseits durch die Überwachung der globalen Geschehnisse im Bereich Cybersicherheit; andererseits durch das aktive Überwachen der Bedrohungslage durch Scans nach Sicherheitslücken in sämtlichen Informatikmitteln im Geltungsbereich des Gesetzes. Die so erlangten Erkenntnisse sind sodann analog zu passiv erhaltenen Meldungen zu verarbeiten.

Art. 73a lit. a (Sensibilisierung der Öffentlichkeit) muss aus Sicht der GRÜNEN weit ausgelegt und konsequent umgesetzt werden – Information und damit Opfer-Prävention ist auch in diesem Bereich genauso wichtig wie das Beheben von Problemen und Schäden. Der Bund bzw. das NCSC sollen auf Basis der Gesetzes Sensibilisierungskampagnen durchführen und Anreize setzen, damit Cyber-Security-Massnahmen und die Meldung von Vorfällen zur üblichen Praxis werden für alle Organisationen und Personen. Auch wenn es sich dabei nicht nur um (aus gesellschaftlicher Sicht) kritische Infrastrukturen handelt, kann der Missbrauch von persönlichen Daten (beispielsweise Gesundheitsdaten) für Einzelne genauso gravierende Folgen haben. Auch kleinere Firmen ohne gut bestückte IT-Abteilung, die oftmals wichtige Glieder im Wirtschaftsgeschehen sind, müssen spezifisch sensibilisiert und unterstützt werden. Die enge Vernetzung verschiedenster Akteure im wirtschaftlichen und gesellschaftlichen Leben verlangt es, dass wir Cyber-Security umfassend und nicht auf kritische Infrastrukturen beschränkt verstehen.

Die «Unterstützung von Betreiberinnen von kritischen Infrastrukturen» (Art. 73a lit. f) muss ebenfalls breiter gedacht werden, als die Erläuterungen und Definitionen das bisher vorsehen. Denn einzelne Komponenten oder Teile von Software können ebenfalls kritisch sein. Entdeckte Sicherheitslücken in weit verbreiteten Einzelkomponenten (beispielsweise Heartbleed 2014 oder Log4j 2021) zeigen, dass dadurch schnell eine grosse Anzahl an kritischen Einfallstoren entstehen. Art.74 lit. s erwähnt genau solche «Hard- und Software, deren Produkte von kritischen Infrastrukturen genutzt werden» als Bereiche der Meldepflicht und anerkennt deren Bedeutung. Im Sinne der Vorbeugung sollte der Bund die Sicherung und Verbesserung solcher Komponenten aktiv unterstützen, beispielsweise durch ein Public-Private-Partnership für einen Fonds für die Wartung solcher Komponenten.

Im Sinne der Prävention von Cyber-Security-Vorfällen regen wir zudem an, dass der Bund verbindliche Mindeststandards schaffen muss, welche sich an den anerkannten Regeln der Technik orientieren sowie messbare und überprüfbare Massnahmen und damit «best practices» definieren. Dies würde es auch erleichtern, Haftungsfragen zu klären und somit die Rechte von Nutzer*innen und Abnehmer*innen von Software zu stärken. Wir verweisen an dieser Stelle auf die detaillierten Ausführungen der Vernehmlassungsantwort der Digitalen Gesellschaft.

Art. 73b – Meldungen zu Cybervorfällen und Schwachstellen

Für die Sensibilisierung für Cyber-Risiken und eine Erhöhung des Sicherheitsniveaus insgesamt ist es aus Sicht der GRÜNEN zentral, dass möglichst viele Vorfälle und deren Details öffentlich sind. Deshalb verlangen wir eine Umkehrung der Vorzeichen bezüglich Veröffentlichung (Art. 73 Abs. 2 und Abs. 3): Sprechen nicht gewichtige Gründe dagegen, soll das NCSC gemeldete Vorfälle und Schwachstellen veröffentlichen. Dies unter der Einhaltung des

Schutzes von persönlichen oder sonst sensiblen Daten und natürlich unter der Berücksichtigung, dass damit Angreiferinnen keine zusätzlichen, nützlichen Informationen zur Verfügung stehen. Zudem erscheint es zweckmässig, dass das NCSC kontinuierlich und in aggregierter Form über Vorfälle und Schwachstellen berichtet und damit ein breiteres Publikum erreicht. So ist es möglich, dass die Öffentlichkeit sich einen aktuellen Überblick über die Sicherheitslage im Cyber-Bereich verschaffen kann und weiss, welche Angriffsarten und Schwachstellen besonders verbreitet sind.

Für eine tragfähige Lagebeurteilung ist es zentral, dass möglichst viele Ereignisse (also Vorfälle und Schwachstellen) gemeldet werden. Die Meldepflicht bzw. der Begriff der kritischen Infrastrukturen (Art. 74b) müssen grosszügig ausgelegt sowie die Anreize für eine Meldung hoch und die Hürden dafür tief gelegt werden (siehe auch Überlegungen zu Art. 73a lit. a oben).

Zudem muss das NCSC grössere Kompetenzen erhalten bei gravierenden Vorfällen. Es soll dann Weisungen und Fristen gegenüber Hersteller- und Betreiberorganisationen erlassen dürfen, welche diese verpflichten, Schwachstellen schnell zu beheben und Schäden zu mindern. Wichtig ist hier insbesondere, dass Abs. 3 auch auf Betreiberorganisationen ausgedehnt wird – Sicherheitsupdates beispielsweise nützen nur dann, wenn sie auch wirklich eingespielt werden.

Das NCSC soll die Fristen und Weisungen dabei gemäss einem risikobasierten Ansatz gestalten: Je kritischer eine Infrastruktur bzw. grösser der potenzielle Schaden, desto kürzer die Fristen.

Wird dem NCSC eine Sicherheitslücke bekannt, die ein Drittprodukt betrifft und bei der nicht davon auszugehen ist, dass sie der Herstellerin bereits bekannt ist, muss die Sicherheitslücke vom NCSC umgehend im Rahmen eines «responsible disclosure»-Verfahrens der betroffenen Herstellerin gemeldet werden. Zusätzlich sollten dem NCSC Mittel an die Hand gegeben werden, um bei meldenden Organisationen auf der Behebung einer Sicherheitslücke zu bestehen.

Der Grundsatz, entdeckte (aber noch nicht bekannte) Sicherheitslücken («Zero Day Exploits») im Rahmen eines «responsible-disclosure»-Verfahrens zu veröffentlichen, sollte neben dem NCSC für alle Bundesstellen gelten, auch für den Nachrichtendienst. Alle Bundesstellen sollen auf den Einsatz von Informatikmitteln verzichten, welche diese Lücken ausnutzen – denn mit solchen «Staatstrojanern» wird das Geschäft mit Sicherheitslücken und damit Unsicherheit vorangetrieben.

Art 73c (insbesondere Abs. 3) – Strafverfahren

Wir begrüssen, dass der verantwortungsvolle Umgang mit Sicherheitsrisiken («responsible disclosure» beispielsweise) vor der Strafverfolgung geschützt ist.

Art. 74 – Unterstützung durch das NCSC

Die GRÜNEN begrüssen es sehr, dass das NCSC die Betreiberinnen bezüglich Cyber-Risiken unterstützt.

Art. 74a – Meldepflicht

Die Revision sieht im eigentlichen Kernpunkt, Art. 74a, eine Meldepflicht von kritischen Infrastrukturen nur für Cyberangriffe vor (definiert in Art. 5 als «Cybervorfall, der von Unbefugten absichtlich ausgelöst wurde»). Dies geht zu wenig weit. Die Meldepflicht von kritischen Infrastrukturen sollte allgemeine Cybervorfälle einschliessen, definiert in Art. 5 als «Ereignis beim Betrieb von Informatikmitteln, das dazu führen kann, dass die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist.» Mit Blick auf das Schadenspotential ist es unerheblich, ob ein Ereignis absichtlich von Unbefugten («Cyberangriff») oder unabsichtlich, von Befugten oder von Informatikmitteln («Cybervorfall») ausgelöst wurde. Die Definition von Cybervorfällen umfasst zudem algorithmische Entscheidungssysteme (Künstliche Intelligenz, KI) und entsprechende Fehlfunktionen. Es ist essenziell, dass auch KI unter die Meldepflicht fällt, da diese Systeme über zunehmende Leistungsfähigkeit verfügen und in immer mehr kritischen Infrastrukturen eingesetzt werden. Zudem ist es etwa in der Flug- oder Nuklearsicherheit etablierte Praxis, dass nicht nur schwere Unfälle oder Angriffe, sondern auch sonstige Zwischenfälle rapportiert und aufgearbeitet werden. Eine solche moderne Sicherheitskultur sollte auch im Cyber- und KI-Bereich Einzug finden.

Dies ist auch deshalb sinnvoll, weil sich die Tragweite und Ursache eines Vorfalls zu Beginn des Ereignisses oft gar nicht abschätzen lassen. Um den möglichen Sicherheitsrisiken, die davon ausgehen, trotzdem Rechnung zu tragen, ist eine unmittelbare Meldung von allen Vorfällen nötig, möglichst innerhalb von 24 Stunden.

Art. 74b – Bereiche der Meldepflicht

Der Artikel legt fest, für welche Bereiche die Meldepflicht gilt. Die GRÜNEN regen an, dass die Bereiche der in lit. c genannten Organisationen mit öffentlich-rechtlichen Aufgaben erweitert werden um den Bereich der Demokratie. Dies würde insbesondere Parteien in Parlamenten und Politiker*innen in relevanten Ämtern umfassen. Diese nehmen gewichtige öffentlich-rechtliche Aufgaben wahr und ein Cyberangriff auf sie hat potenziell grosse Auswirkungen auf die Demokratie. Während in der Schweiz bisher wenig über Cyber-Angriffe auf die Demokratie bekannt ist, ist dies in anderen Ländern bereits gängige Praxis. Die Schweiz hat sich in diesem Thema bisher erstaunlich sorglos gezeigt, obwohl die schweizerische direkte Demokratie so viele politische Prozesse in der Öffentlichkeit bewirkt wie kaum in einem anderen Land. Es erscheint wenig plausibel, wenn Organisationen der Postdienste, der Rheinschifffahrt oder Nachrichtenagenturen der Meldepflicht unterliegen – nicht aber im nationalen Parlament vertretene Parteien.

Zudem soll der Bereich von lit. f sich nicht auf die Anzahl Nutzende beziehen, da dies nichts darüber aussagt, ob es sich um ein für einen Cyberangriff lohnendes Ziel handelt. Ausserdem soll an derselben Stelle von «Wirtschaft» die Rede sein, nicht von «digitaler Wirtschaft».

Art. 74c – Ausnahmen der Meldepflicht

Die GRÜNEN beantragen die gesamte Streichung des Ausnahmen-Artikels. Der erste Teil (lit. a) – eine geringe Abhängigkeit von Informatikmitteln – erscheint im 21. Jahrhundert zunehmend unwahrscheinlich. Der zweite Teil (lit. b) scheint schwer abschätzbar und ermöglicht deshalb zahlreiche Schlupflöcher, der Meldepflicht zu entgehen – was erhöhte Risiken für die Cyber-Sicherheit der Gesellschaft bedeutet.

Art. 74e und Art. 74f – Inhalt und Übermittlung der Meldungen

Der Artikel 74e ist aus Sicht der GRÜNEN so zu überarbeiten, dass die Automatisierung von Meldungen möglich und wünschenswert werden. Mit den zur Verfügung stehenden technischen Möglichkeiten ist die Auswertung eines grossen Volumens von Meldungen möglich, auch wenn diese eher Anhaltspunkte denn kompletten Meldungen entsprechen. Dies ist insbesondere wichtig, weil mit der Meldung von Cybervorfällen (siehe oben, Ausführungen zu Art. 74a) eine erhöhte Anzahl Interaktionen zu erwarten ist. Die Anforderungen an die Meldungen müssen dementsprechend je nach Art des Ereignisses (Angriff oder Vorfall) abgestuft sein. Dies ist wichtig, um die Schwelle für eine Kontaktaufnahme zu senken.

Neben manuellen Meldungen soll eine IT-Schnittstelle (API) auch automatisierte Meldungen an das NCSC erlauben. So können Cyber-Überwachungssysteme von kritischen Infrastrukturen etwa automatisch verdächtige Signale an das Zentrum weiterleiten. Die Datengrundlage des NCSC wird damit umfassender und zeitnaher als bei rein manuellen Eingaben nach grösseren Vorfällen.

In jedem Fall sollte in der Umsetzung nach Möglichkeit sichergestellt werden, dass sich überschneidende Meldepflichten (DSG, Finma, etc.) durch einen einzigen Meldevorgang erfüllt werden können.

Art. 74i – Widerhandlungen und Verantwortlichkeit

Der Artikel-Text muss expliziter machen, dass die vorgesehenen Sanktionen auf der Leitungsebene der Organisationen greifen, und nicht auf der Ebene der Fachspezialist*innen (allenfalls sind Organe zu nennen). Dies ist wichtig, um die Verantwortlichkeiten für Cyber-Security in den Leitungsgremien zu verankern.

Die GRÜNEN regen zudem an, den höchsten Führungsorganen Verantwortung für die Cyber-Governance zuzuordnen, wie dies beispielsweise bereits bei Verwaltungsräten von Aktiengesellschaften für die Ausgestaltung des Rechnungswesens und die Finanzplanung und -kontrolle der Fall ist. Im digitalen Zeitalter gebührt der Ausgestaltung einer Daten-Governance in Unternehmen das gleiche Gewicht wie den Finanzen. Eine solche Verantwortung müsste der Bund im Aktienrecht verankern.

Wir danken Ihnen, Herr Bundesrat, sehr geehrte Damen und Herren, für die Berücksichtigung unserer Vorschläge in der Revision des Gesetzes.

Freundliche Grüsse

Balthasar Glättli
Präsident

Rahel Estermann
stv. Generalsekretärin, Leiterin Politik