Eidgenössisches Finanzdepartement EFD
Herr Bundesrat
Ueli Maurer
Bundesgasse 3, 3003 Bern

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

Zürich, 14. April 2022

Vernehmlassung zur Revision des Informationssicherheitsgesetzes (ISG)

Stellungnahme von swissICT zur laufenden Vernehmlassung

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

swissICT bedankt sich für die Möglichkeit, an der Vernehmlassung der Regelungen zur Einführung einer Meldepflicht für Cybersecurity-Vorfälle im Rahmen der Revision des Informationssicherheitsgesetzes (ISG) teilnehmen und eine entsprechende Stellungnahme einreichen zu können.

swissICT

swissICT ist mit über 2'500 Mitgliedern der grösste Fachverband des ICT Werkplatzes Schweiz und verbindet als einziger Verband ICT-Anbieter, Anwender und Fachkräfte in der Schweiz. Der Verband sorgt sich um das Image der Schweizer ICT-Branche, setzt sich für gute Rahmenbedingungen ein und fördert den Austausch und das Fach-Know-how seiner Mitglieder.

Generelle Bemerkungen

swissICT begrüsst generell die Revision und die darin eingeschlagene Stossrichtung zur Einführung einer Meldepflicht von Cyberangriffen für Betreiber kritischer Infrastrukturen. Wir vertreten jedoch die Auffassung, dass der Vorentwurf in verschiedener Hinsicht über das Ziel hinausschiesst und für die betroffenen Unternehmen zusätzliche administrative Bürden ohne erkennbaren Nutzen schafft. Im Wesentlichen richtet sich unsere Kritik auf folgende Punkte:

- Der Kreis meldepflichtiger Betreiber kritischer Infrastrukturen wird nach unserem Dafürhalten zu weit gefasst. Einzelne Kategorien sollten weggelassen oder zumindest herabgestuft werden.
- Die im Gesetz vorgesehene Einschränkung meldepflichtiger Angriffe wird in der Praxis kaum je zum Tragen kommen. Faktisch sind nahezu alle Angriffe zu melden, was kritisch hinterfragt werden sollte.

- Die Modalitäten der Meldepflicht sind mit bestehenden Normen (z.B. Datenschutzgesetzgebung, Meldepflichten für Finanzinstitute) abzustimmen, um Widersprüche (z.B. hinsichtlich Meldefristen) zu vermeiden.
- Die umfassenden und fortdauernden Meldepflichten nehmen erhebliche Ressourcen in Anspruch, die bei einem Cyberangriff nicht für dessen zielgerichtete Abwehr eingesetzt werden können.
- Der Entwurf der Bestimmungen über die Meldepflicht enthält keine konkrete Pflicht des NCSC, Erkenntnisse der Analysen mit Betroffenen zu teilen. Dies ist im Gesetz zu ergänzen.

Spezifische Bemerkungen zu einzelnen Bestimmungen

1.1. Art. 73a E-ISG

Diese Grundsatzbestimmung zu den Aufgaben des nationalen Zentrums für Cybersicherheit (NCSC) ist ausreichend breit gefasst.

1.2. Art. 73b E-ISG

Keine Anmerkungen.

1.3. Art. 73c E-ISG

Zentral ist hier Abs. 3, wonach Informationen, die von einer Person im Rahmen einer Meldung dem NCSC bekanntgegeben wurden, in einem Strafverfahren gegen diese Person nur mit deren Einverständnis verwendet werden dürfen. Wie auch in anderen Gesetzen sind möglicherweise zur persönlichen Strafbarkeit der Verantwortlichen führende Strafbestimmungen zu vermeiden, denn sie schaden der Compliance der Unternehmen mehr, als dass sie ihr helfen würden: IT-Sicherheit ist ein Gebiet, in dem immer wieder mal Fehler passieren. Wer bei einer Meldung trotz sorgsamer Vorkehrungen in der IT-Sicherheit mit einer Strafe für Verfehlungen rechnen muss, wird meist auf eine Meldung verzichten. Obwohl der aktuelle Wortlaut des Entwurfs von Art. 73c E-ISG diesem Dilemma bereits Rechnung trägt, erscheint die folgende Präzisierung im Licht des Selbstbelastungszwangsverbots bei Cybervorfällen angebracht: *"Soweit eine Person im Rahmen einer Meldung dem NCSC möglicherweise die Person belastende Informationen mitteilt, können diese Informationen in einem Strafverfahren gegen die Person nur mit deren Einverständnis verwendet werden."*

1.4. Art. 74 E-ISG

Bemerkenswert ist hier Abs. 4, wonach das NCSC zur Analyse eines Cybervorfalls mit dem Einverständnis der betroffenen Betreiberin auf deren Informationen und Informatikmittel zugreifen kann. Das Einverständnis kann unabhängig von allfälligen Geheimhaltungspflichten gewährt werden.

Da die vorgesehene Meldepflicht offenbar sehr breit sein soll und fast die ganze Palette von Branchen im schweizerischen Wirtschaftsleben umfasst (siehe die Ausführungen unten zu Art. 74b E-ISG), ist dafür zu sorgen, dass bei einer Meldung keine Rechte Dritter gefährdet oder gar verletzt werden, d.h. das NCSC muss die Geheimhaltungsbedürfnisse Dritter schützen und entsprechende Geheimhaltungspflichten beachten.

1.5. Art. 74a E-ISG

Keine Anmerkungen.

1.6. Art. 74b E-ISG

Hier werden zahlreiche Branchen genannt – ein wesentlicher Teil des schweizerischen Wirtschaftslebens. Nicht ganz klar scheint, ob die – sehr umfangreiche – Liste der Betreiberinnen kritischer Infrastrukturen abschliessend ist

oder nicht. Der Umfang der Liste reflektiert jedenfalls die arbeitsteiligen Abläufe in der heutigen Wirtschaft. Die Meldepflicht wird zurecht auf die ganzen (Zu-)Lieferketten ausgedehnt, was in der unternehmerischen Praxis jedoch oft auf eine organisatorisch bzw. administrative Herausforderung hinauslaufen wird. Beim Anblick der Liste fragt man sich jedenfalls unweigerlich, ob bei insgesamt 19 (!) Kategorien kritischer Infrastrukturen angesichts der damit verbundenen und durchaus auch belastenden Auflagen im Bereich der Meldepflicht nicht zumindest diskutiert werden müsste, ob man eine qualitative Gewichtung in z.B. "hochkritisch" bzw. "kritisch" vornehmen und die 19 Kategorien dann in folgende zwei Gruppen einteilen könnte: "Kritische Infrastruktur der Kategorie 1" und "Kritische Infrastruktur der Kategorie 2". Die "hochkritischen" Infrastrukturen hätten dann strengere Auflagen im Zusammenhang mit der Meldepflicht zu erfüllen, als die bloss "kritischen" Infrastrukturen. In beiden Kategorien ist klar zu kommunizieren, wer wem was wie wann zu melden hat. Weiter könnte man eine Kategorisierung nach Art und Gefährdungspotential des jeweiligen Vorfalls vorsehen. Auf diese Weise liesse sich verhindern, dass weite Teile der Wirtschaft mit neuen organisatorisch-administrativen Auflagen belastet würden – insbesondere für KMU wäre dies eine willkommene Entlastung.

Was die 19 Kategorien angeht, so ist vorab lit. s bemerkenswert: Cyberangreifer manipulieren oft die Hard- und Software bereits vor der Auslieferung an die Endkunden, damit sie später Zugriff auf die Systeme erhalten. Besonders relevant sind Cyberangriffe auf Hersteller von Software, wenn diese über Fernwartungszugänge verfügen. Angreifer können versuchen, über solche legitimen Zugänge direkt in die Systeme der kritischen Infrastrukturen einzudringen. Neben dem Kriterium des Fernwartungszugangs sind Hersteller von Hard- und Software dann meldepflichtig, wenn ihre Produkte in besonders heiklen Bereichen zum Einsatz kommen. Zurecht zählt der Entwurf in diesem Zusammenhang vier relevante Gruppen auf. Es wird aber leider versäumt klarzustellen, dass die Anbieterinnen von Software as a Service (SaaS) keine kritischen Infrastrukturen betreiben, da bei diesen Dienstleistungen den Endkunden keine Software überlassen wird; vielmehr erhalten die Endkunden bloss Zugang zu den Funktionalitäten der Software.

Lit. f schliesslich definiert drei alternative Bedingungen, bei denen Anbieterinnen von Online-Marktplätzen, Cloudcomputing und weiteren digitalen Diensten unter die Meldepflicht fallen, nämlich (i) eine grosse Zahl von Nutzern, (ii) eine hohe Bedeutung für die digitale Wirtschaft, und (iii) das Anbieten von Sicherheits- und Vertrauensdiensten. Alle Bedingungen sind unklar und lassen übermässig viel Spielraum für individuelle Interpretationen. Es wäre wünschenswert, wenn entweder das Gesetz oder dann aber die Verordnung klare Definitionen aufwiesen.

1.7. Art. 74c E-ISG

Keine Anmerkungen.

1.8. Art. 74d E-ISG

Art. 74d E-ISG legt fest, welche Cyberangriffe auf kritische Infrastrukturen dem NCSC zu melden sind. Hierbei werden im ersten Absatz vier alternative Fallgruppen definiert, welche die Meldepflicht auslösen. Für den Eintritt der Meldepflicht muss sich keine dieser Fallgruppen bereits verwirklicht haben; vielmehr greift die Meldepflicht schon dann, wenn Anzeichen für das Bestehen einer dieser Fallgruppen existieren, was die Meldepflicht in ein frühes Stadium vorverlagert.

Von den vier Fallgruppen wird insbesondere die dritte Kategorie (Anzeichen, dass ein Cyberangriff "zu einem Abfluss oder zur Manipulation von Informationen geführt hat oder führen könnte") in der Praxis sehr häufig erfüllt sein, weil sich ein solcher Abfluss bzw. eine solche Manipulation innerhalb der Meldefrist ("so rasch als möglich"; vgl. Art. 74a E-ISG) kaum je mit hinreichender Sicherheit ausschliessen lässt. In Kombination mit den weiteren Fallgruppen gemäss Absatz 1 sind kaum Fälle denkbar, wo die Meldepflicht nicht zum Tragen kommt.

Sollten die Voraussetzungen von Absatz 1 im Einzelfall ausnahmsweise dennoch nicht erfüllt sein, kann eine Meldepflicht immer noch aufgrund des zweiten Absatzes bestehen, nämlich wenn der Cyberangriff "mit Erpressung, Drohung oder Nötigung gegenüber der Betreiberin einer kritischen Infrastruktur oder ihren

Mitarbeitenden verbunden ist." Erfasst werden hier also beispielsweise die klassischen und in der Realität überaus häufigen Ransomware-Attacken, bei denen ein Lösegeld für die Entschlüsselung von Daten gefordert und/oder mit der Offenlegung von Daten gedroht wird.

Im Ergebnis bleiben aufgrund der vielfältigen und offenen Kriterien für meldepflichtige Cyberangriffe eigentlich nur harmlose, nicht von einem fremden Staat ausgeführte oder veranlasste, innerhalb von längstens 30 Tagen entdeckte Angriffe ohne Abfluss oder Manipulation von Informationen und ohne erpresserische, drohende oder nötigende Elemente übrig. Solche Cyberangriffe (nicht Cybervorfälle) sind in der Realität kaum vorstellbar. Zu melden ist somit praktisch jeder Cyberangriff. Dies mag aus Sicht des mit der Meldepflicht verfolgten Zwecks (Früherkennung, Warnung, Empfehlung geeigneter Präventions- und Abwehrmassnahmen; vgl. Art. 74a E-ISG) gewollt sein, macht jedoch die vermeintliche Eingrenzung meldepflichtiger Cyberangriffe in Art. 74d E-ISG weitgehend obsolet. Auf die Bestimmung kann schmerzfrei verzichtet werden. Dies wäre auch im Einklang mit der EU NIS-Richtlinie, die ebenfalls keine solche Regelung kennt.

1.9. Art. 74e E-ISG

Gemäss Art. 74e E-ISG hat die Betreiberin einer kritischen Infrastruktur Cyberangriffe zu melden und mit der Meldung bestimmte Informationen mitzuliefern. Wie diese Informationen jedoch genau aussehen und inwiefern sie mit Anforderungen an die Angaben anderer Behörden übereinstimmen, ist (noch) nicht ersichtlich. Es ist für die betroffenen Unternehmen, Behörden oder Anstalten jedoch von hoher Bedeutung, die Anstrengungen im Bereich Cybersecurity zu bündeln und die Informationen nicht in unterschiedlicher Tiefe und Breite an verschiedene Behörden (gleichzeitig) herausgeben zu müssen. Die in Art. 74e E-ISG geforderten Informationen sollten deshalb präziser beschrieben und mit anderen Behörden (z.B. FINMA) abgestimmt werden. Betrachtet man gleichzeitig die gesetzten Fristen für die Meldepflicht (24 Stunden Meldepflicht gegenüber FINMA, so rasch als möglich Meldung gegenüber NCSC), so sollte dies harmonisiert und die Inhalte abgestimmt werden.

Die weiterzugebende Information bezüglich der nächsten Schritte kann höchstens im Sinne von «best efforts» weitergegeben werden, was im Gesetzestext aufgenommen werden sollte. Zum Zeitpunkt eines Angriffs haben die Verantwortlichen meist sehr viel zu tun und sind kaum in der Lage, vertiefte Informationen an Behörden aufzubereiten und weiterzuleiten.

1.10. Art. 74f E-ISG

Die in Art. 74f E-ISG statuierte Schnittstellenthematik zur Weiterleitung der Information nebst dem NCSC an weitere Behörden ist eine Pflicht für die Behörden, nicht die Unternehmen. Die Kompatibilität ist auf alle Fälle zu gewährleisten resp. die einfache Handhabung.

1.11. Art. 74g E-ISG

Die festgelegten Mitwirkungspflichten machen im operativen Bereich zwar Sinn, dürfen die Unternehmen und Anstalten, Behörden und Gemeinden aber in einer schwierigen Zeit noch mehr belasten. Es ist deshalb wichtig zu ergänzen, dass diese Informationen nur dann während der Krise eingeholt werden dürfen, wenn dies zwingend notwendig ist für die Sicherheit der jeweiligen Versorgung.

1.12. Art. 74i E-ISG

Art. 74i Abs. 3 sieht eine Obergrenze des voraussichtlichen Bussenbetrags vor, der es erlaubt, anstelle einer natürlichen Person den Geschäftsbetrieb zu belasten. Dieser Betrag sollte von CHF 20’000 auf CHF 50’000 erhöht werden. Der höhere Betrag erlaubt zum einen besser, unverhältnismässigen Untersuchungsaufwand in Bagatellfällen zu vermeiden. Zum anderen entsteht dadurch ein Gleichlauf mit Art. 64 Abs. 2 des revidierten Datenschutzgesetzes (revDSG). Dieser Gleichlauf erleichtert die Orientierung und ist sachlich gerechtfertigt, weil kein Grund für eine Abweichung besteht.

Ergänzend zu unseren detaillierten Rückmeldungen unterstützen wir auch die Rückmeldungen von asut, digitalswitzerland und ISSS.

Wir danken Ihnen im Namen unserer Mitglieder im Voraus dafür, dass Sie unsere Anregungen in geeigneter Weise bei der weiteren Umsetzung berücksichtigen.

Gerne stehen wir Ihnen für Rückfragen und weitere Diskussionen zur Verfügung.

Freundliche Grüsse

Kathy Riklin
Vorstand swissICT
Alt-Nationalrätin
Leiterin swissICT Politikkommission

Christian Hunziker
Geschäftsführer swissICT
Delegierter des Verwaltungsrates 3L Informatik AG