Swico
Lagerstrasse 33
CH-8004 Zürich

Tel. +41 44 446 90 94
www.swico.ch
info@swicorecycling.ch

Herr Bundesrat Ueli Maurer
Eidgenössisches Finanzdepartement EFD
Geschäftsstelle Nationales Zentrum für
Cybersicherheit NCSC

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

Zürich, 13. April 2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrter Herr Bundesrat Maurer
Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit, zu oben genanntem Geschäft Stellung zu beziehen und nehmen diese gerne innerhalb der angesetzten Frist wahr.

Swico ist der Wirtschaftsverband der Digitalisierer und vertritt die Interessen etablierter Unternehmen sowie auch Start-ups in Politik, Wirtschaft und Gesellschaft. Swico zählt über 700 Mitglieder aus der ICT- und Online-Branche. Diese Unternehmen beschäftigen 56'000 Mitarbeitende und erwirtschaften jährlich einen Umsatz von 40 Milliarden Franken. Neben Interessenvertretung betreibt Swico das nationale Rücknahmesystem «Swico Recycling» für Elektronik-Altgeräte. Mit unserer Interessengruppe Information Security verfügen wir über ein Fachgremium mit besonders einschlägigen Kenntnissen, das wir vorliegend einbezogen haben.

Aus Sicht von Swico ist eine Meldepflicht im Kontext der kritischen Infrastruktur grundsätzlich zu begrüssen, sofern sie gewisse Voraussetzungen erfüllt. So soll diese mit Augenmass umgesetzt werden und für die betroffenen Unternehmen einen deutlichen Mehrwert bringen. Besonders wichtig sind eine klare Definition des Betroffenenkreises, sowie die Berücksichtigung von bereits bestehenden Meldepflichten.

1 Übergeordnete Bemerkungen

1.1 Definition des Betroffenenkreises

Die im Gesetzesentwurf erwähnten Branchen und Bereiche lassen auf einen sehr umfassenden Geltungsbereich schliessen. Das führt zu einer grossen Verunsicherung im Kreis unserer Mitglieder, ob sie von der Meldepflicht erfasst sind. Es braucht Klarheit darüber,

welche Akteure unter die Meldepflicht fallen. Für detaillierte Bemerkungen hierzu verweisen wir gerne auf die Ausführungen in Art. 74b E-ISG weiter hinten.

1.2 Kosten-Nutzen Verhältnis

Die Meldepflicht muss den betroffenen Unternehmen und der Gesamtwirtschaft einen messbaren Mehrwert bringen. Die Meldepflicht ist deshalb mit Augenmass umzusetzen und soll sich auf schwerwiegende Cybervorfälle fokussieren. Sie muss einen risikobasierten Ansatz verfolgen, der administrative und finanzielle Aufwände auf ein Minimum reduziert.

1.3 Andere, bestehende Meldepflichten

Es bestehen bereits zahlreiche Meldepflichten im Bereich Cybersicherheit oder weiteren Bereichen. Es erscheint uns deshalb wichtig, etablierte Instrumente nicht zu schwächen, sondern eine Angleichung anzustreben. In den nachfolgenden Ausführungen werden diese Meldepflichten und deren Verhältnis zum E-ISG an spezifischen Stellen vermerkt, weshalb wir für detaillierte Ausführungen gerne darauf verweisen (s. Art. 74a, 74b, 74e, 74f und 76 E-ISG).

2 Detailbemerkungen

- *Art. 1 Abs. 1 lit. b E-ISG, Zweck*

Im neuen lit. b wird als Zweck des Gesetzes die Erhöhung der Widerstandsfähigkeit der Schweiz gegenüber Cyberrisiken festgehalten. Wie bereits einleitend genannt, fehlt es jedoch vielfach an definitorischen Rahmenbedingungen. So ist auch an dieser Stelle unklar, was die offizielle Definition von «Cyber» und «Cyberrisko» ist. Wir befürworten deshalb eine Anlehnung dieser Begrifflichkeiten an die Verordnung über den Schutz vor Cyberrisiken der Bundesverwaltung (CyRV).

- *Art. 5 lit. d-e E-ISG, Begriffe*

In lit. e wird der Begriff «Cyberangriff» definiert als Cybervorfall, der von Unbefugten absichtlich ausgelöst wurde. Dabei muss präzisiert werden, ob es sich bei den «Unbefugten» um Interne, Externe oder beides handelt.

Die im Art. 5 E-ISG vorgenommene Differenzierung zwischen Schwachstelle, Cybervorfall (lit. d) und Cyberangriff (lit. e) ist sinnvoll, da dies die Motivation für Meldepflichtige erhöhen könnte, indem nicht jeder Vorfall absolut gemeldet werden muss, sondern nur der Cyberangriff auf kritische Infrastrukturen meldepflichtig ist (während Cybervorfälle und Schwachstellen freiwillig von jeder Person gemeldet werden können). Diese Klarstellung ist wichtig, da im Gegensatz hierzu gemäss CyRV Bundes-intern Schwachstellen und Cybervorfälle gemeldet werden müssen.

Jedoch ist die vorgeschlagene Definition von «Cybervorfall» in der bestehenden Form kaum anwendbar, weil sie mit der blossen – auch theoretischen – Möglichkeit der Beeinträchtigung der Schutzziele operiert. Eine blosse Möglichkeit kann in der Praxis nicht ausgeschlossen werden. Eine Lösungsoption ist, den Begriff an Art. 4 Ziff. 7 NIS-Richtlinie anzulehnen. Diese definiert einen Sicherheitsvorfall als «alle Ereignisse, die tatsächlich eine nachteilige Auswirkung auf die Sicherheit von Netz- und Informationssystemen haben». Die Anpassung könnte vorliegend somit lauten:

Art. 5 lit. d E-ISG

«Cybervorfall: Ereignis beim Betrieb von Informatikmitteln, das tatsächlich dazu führt, dass…»

- *5. Kapitel: Massnahmen des Bundes zum Schutz der Schweiz vor Cyberrisiken (Änderung Gliederungstitel)*

Eine Regelung der Aufgaben des NCSC auf Stufe Gesetz ist zu begrüssen, insbesondere mit ausgebauten Fähigkeiten im Bereich Schwachstellenmanagement (Anerkennung als «CVE Numbering Authority» durch MITRE).

- *73b E-ISG, Bearbeitung von Meldungen zu Cybervorfällen und Schwachstellen*

Diese Bestimmung präzisiert, dass das NCSC als Anlaufstelle für Cyberrisiken (gemäss Art. 12 Abs. 1 lit. a CyRV) neben Meldungen zu Cybervorfällen auch solche zu Schwachstellen entgegennimmt. Abs. 3 dieses Artikels hält fest, dass das NCSC bei Meldung einer Schwachstelle umgehend den Hersteller informiert und ihm eine angemessene Frist zwecks Behebung setzt. Behebt der Hersteller die Schwachstelle nicht innert dieser Frist, so kann das NCSC die Schwachstelle unter Angabe der betroffenen Soft- oder Hardware veröffentlichen, sofern dies zielführend ist. Gemäss vorgeschlagenem Gesetzeswortlaut könnten unter den Begriff «Hersteller von Hard- und Software» auch Anbieter von SaaS- und Cloud-Lösungen fallen. Dies ist jedoch systematisch und inhaltlich unrichtig, weil die Meldepflicht der Cloudbetreiber in Art. 74b lit. f E-ISG richtigerweise separat geregelt wird. Der Klarheit halber sollte deshalb ausdrücklich festgehalten werden, dass der Begriff «Hersteller von Hard- und Software» im ISG jeweils nur Hersteller umfasst, deren Produkte der Kunde auf eigener Infrastruktur betreibt. Dafür bieten sich die Erläuterungen oder auch der Vernehmlassungsbericht an.

- *Art. 73c E-ISG, Weiterleitung von Informationen (neu)*

Dieser Artikel definiert in Abs. 1 und 2 die Voraussetzungen, unter welchen es dem NCSC erlaubt ist, gewisse Informationen, die in einer Meldung enthalten sind, an den NDB oder die Strafverfolgungsbehörden weiterzuleiten. Diese neu vorgesehene Möglichkeit dürfte zu Widerstand und Kritik auf Betroffenenseite führen, weshalb ein besonderes Augenmerk auf die künftige Auslegung zu richten ist. Für die Betroffenen könnte eine solche Weitergabe namentlich öffentliche Berichterstattung, Strafverfolgung oder Monitoring durch den NDB nach sich ziehen. Aus diesem Grund sind wir der Ansicht, dass die Weitergabe der Information neutral auszugestalten ist (d.h. ohne Möglichkeit des Rückschlusses auf eine bestimmte Organisation). Ist dies nicht möglich, so sollte zwingend das Einverständnis der betroffenen Organisation eingeholt werden, sofern keine anderen, gesetzlichen Bestimmungen eine zu einer Weitergabe verpflichten. Dies gilt auch für die Voraussetzung der Weiterleitung von Informationen über strafrechtlich geschützte Geheimnisse gemäss Abs. 4 dieser Bestimmung.

- *Art. 74 E-ISG, Unterstützung von Betreiberinnen von kritischen Infrastrukturen beim Schutz vor Cyberrisiken*

Ergänzend zu seinen allgemeinen Aufgaben erbringt das NCSC gemäss dieser Bestimmung weitergehende Leistungen. Abs. 3 sieht die Unterstützung von Betreiberinnen kritischer Infrastrukturen mit technischer Beratung vor. In der Botschaft wird die Subsidiarität dieser Massnahme zu privaten IT-Dienstleistungen, die auf dem Markt sind, genannt. Zusätzlich soll diese Unterstützung durch das NCSC nur erfolgen, wenn sie zeitkritisch ist und ein erheblicher Schaden droht. Dies birgt das Risiko, dass Betreiberinnen auf Eigenleistungen verzichten und sich im Ernstfall auf das NCSC abstützen, um kostspielige Prävention einzusparen. Eine angemessene Lösung für dieses Problem könnte der Verweis durch das NCSC auf bestehende Best Practice sein, verbunden mit unverbindlichen Umsetzungsempfehlungen, die sich

wiederum auf einen bestimmten Umsetzungsgrad beziehen. Dies bringt jedoch gleichzeitig die Gefahr mit sich, dass das NCSC sich in Bezug auf den angeratenen Umsetzungsgrad haftbar macht. Deshalb erscheint schliesslich ein Verweis auf die zahlreichen, vorhandenen Best Practice mit dem Vermerk, dass diese angemessen umgesetzt werden sollen, als sachgerechte Lösung.

- *Art. 74a E-ISG, Meldepflicht (neu)*

Dieser Artikel definiert die Meldepflicht in den Grundzügen. Es wird festgehalten, dass Betreiberinnen von kritischen Infrastrukturen im Falle von Cyberangriffen der Meldepflicht unterstellt sind und dass die Meldung «so rasch als möglich» nach Entdeckung des Angriffs dem NCSC zu berichten ist. Dabei sollte eine Meldung nur als verspätet betrachtet werden, wenn der meldepflichtige Betreiber eine mögliche Meldung unbegründet und ungerechtfertigt verzögert hat. Dadurch entsteht auch ein Gleichlauf mit anderen Meldepflichten, etwa jenen nach Art. 29 Abs. 2 FINMAG oder nach Art. 24 des revidierten Datenschutzgesetzes.

Nicht definiert wird im Gesetz, wer «Betreiber oder Betreiberin» einer kritischen Infrastruktur ist. Nach der NIS-Richtlinie ist dies die Einrichtung (d.h. diejenige juristische Person), die den vom Cyberangriff betroffenen Dienst «bereitstellt». Dies deutet darauf hin, dass «Betreiber oder Betreiberin» ist, wer einen Dienst nach aussen anbietet und i.d.R. auch als Vertragspartnerin der Dienstbezüger auftritt. Wenn eine kritische Infrastruktur arbeitsteilig betrieben wird, haben die entsprechenden juristischen Personen aber einen gewissen Ermessensspielraum bei der Bestimmung der rechtlichen Betreiberin. Dementsprechend hat eine Meldung durch eine von gegebenenfalls mehreren, beteiligten juristischen Personen zu genügen. Der Bund soll hierzu eine Formulierung wählen, die sicherstellt, dass beispielsweise Meldungen von Tochtergesellschaften auch der Muttergesellschaft zugerechnet werden.

Das Ereignis, welches die Meldeflicht auslöst, sollte an dieser Stelle der Klarstellung halber allenfalls nochmals explizit aufgenommen werden (gemäss Art. 5 lit. d E-ISG vorne). Andernfalls könnte der Anwendungsbereich der vorliegenden Bestimmung zu breit ausgelegt werden und zu «alarm fatigue» führen.

- *Art. 74b Bereiche (neu)*

Der erläuternde Bericht hält richtigerweise fest, dass die Definition kritischer Infrastrukturen nach Art. 5 (Begriffe) E-ISG zu breit gefasst ist. Art. 74b nimmt deshalb eine Konkretisierung vor, welche Unternehmen oder Organisationen als kritische Infrastruktur gelten und darum unter die Meldepflicht fallen. Dazu soll auf bestehende gesetzliche Grundlagen zurückgegriffen werden und – wo keine solchen bestehen – der betroffene Bereich möglichst genau bezeichnet werden. Die Konkretisierung des Begriffs ist aus Sicht von Swico unbedingt notwendig. Jedoch wird der vorliegende Versuch voraussichtlich zu Diskussionsbedarf führen, insbesondere auch für Bereiche, wo kein Verweis auf bestehende Gesetzesgrundlagen möglich ist. Es erscheint uns sinnvoll, eine Arbeitsgruppe oder ein Expertengremium einzusetzen, die sich dem Thema annehmen und eine Definition erarbeiten.

In lit. a bis lit. s werden einzelne Bereiche konkret genannt. Dabei behandelt lit. e Banken, Versicherungen und Finanzmarktinfrastrukturen. Der erläuternde Bericht hält fest, dass die bereits bestehende Meldepflicht für Cyberangriffe gegenüber der FINMA parallel bestehen bleibt und FINMA und NCSC sich so abgleichen werden, dass der Aufwand für die Meldepflichtigen so gering wie möglich ausfällt. Grundsätzlich ist dieses Bestreben zu begrüssen: Die Ausgestaltung hat so zu erfolgen, dass eine Meldung keinen übermässigen

Aufwand verursacht. Gleichzeitig darf hoher Aufwand ohne weitere Differenzierung nicht als generelle Abwehr gegen Meldungen angesehen werden.

Lit. s nennt Hersteller von Hard- und Software, deren Produkte von kritischen Infrastrukturen genutzt werden, sofern die Hard- oder Software einen Fernwartungszugang hat oder zu einem der in Ziff. 1-4 beschriebenen Zwecke eingesetzt wird. Ziff. 4 nennt als solchen Zweck «IT-Sicherheit, Verschlüsselung, Identifikation, Zugriffs- und Zutrittsberechtigung». Aus unserer Sicht kann insbesondere Ziff. 4 sehr breit ausgelegt werden. Es erscheint deshalb sinnvoll, Ziff. 1-4 ersatzlos zu streichen und stattdessen den Begriff des Fernwartungszugangs zu definieren, da eine klare, abschliessende Umschreibung des Einsatzzecks kaum möglich ist. Damit würde auch die Problematik des unklaren Einbezugs der Supply Chain in die Meldepflicht gelöst, da die KI-Betreiber selbst in der Verantwortung stehen würden, ihre Lieferanten je nach Einsatzzweck der Hard- und Software in die Pflicht zu nehmen.

Zum Begriff der Hard- und Software verweisen wir zudem auf die bereits gemachten Ausführungen im Rahmen von Art. 73b Abs. 3 E-ISG weiter vorne.

- *Art. 74c E-ISG, Ausnahmen von der Meldepflicht (neu)*

Lit. a bis c. dieser Bestimmung stellen Kriterien auf, um bestimmte Kategorien von Betreiberinnen kritischer Infrastrukturen von der Meldepflicht auszunehmen. Wir sind der Ansicht, dass die vorgeschlagenen Kriterien in der Praxis schwierig zu ermitteln sein werden. Deshalb schlagen wir vor, stärker auf den möglichen Einfluss eines Schadens als Kriterium abzustellen. Im Falle einer Organisation, deren Einfluss vernachlässigbar ist (bzw. der Schaden aus dem Ereignis), könnte entsprechend auf eine Meldung verzichtet werden.

Auf der anderen Seite fehlt bei den Kategorien, die zum Ausschluss führen, folgende Ergänzung:
«...
c. [neu] weil mitigierende Massnahmen solche Cyberangriffe unschädlich machen. »

- *Art. 74d E-ISG, zu meldende Cyberangriffe (neu)*

Diese Bestimmung zählt die Kriterien auf, unter denen ein Cyberangriff meldepflichtig ist, wobei die Erfüllung eines der Kriterien ausreichend ist. Der Artikel sieht keinen Hinweis auf das für eine Meldung minimal notwendige Schadenspotenzial vor und lässt vor allem in lit. c einen breiten Auslegungsspielraum offen. Der erläuternde Bericht hält in Bezug auf diese Bestimmung hingegen fest, dass die Meldepflicht nur für Cyberangriffe gelten soll, die ein gewisses Schadenspotenzial aufweisen.

Um die Meldung trivialer Vorfälle auszuschliessen, schlagen wir folgende Ergänzung vor:

«...
c. er zu einem Abfluss oder zur Manipulation von Informationen geführt hat oder führen könnte, die für die Funktionsfähigkeit der betroffenen kritischen Infrastruktur oder einer anderen kritischen Infrastruktur relevant sind; oder»

Wir stellen bei der Aufzählung in diesem Artikel zudem fest, dass ein starker Fokus auf Ransomware gelegt wird. Mit Blick auf die Zukunftssicherheit bei einer rasch verändernden Lage erscheint uns dies fraglich. Eine rasche Anpassungsmöglichkeit ist gemäss erläuterndem Bericht auf Verordnungsstufe möglich, was wir in diesem Zusammenhang als zweckdienlich erachten.

- *Art. 74e E-ISG, Inhalt der Meldung (neu)*

Dieser Artikel hält die wesentlichen Angaben, die für die Erfüllung der Meldepflicht notwendig sind, gesetzlich fest. Aus unserer Sicht fehlt dabei die Berücksichtigung des bereits heute gut etablierten Austausches von technischen Informationen (Threat Intelligence) zwischen GovCERT und den Betreibern von KI. Dieses bestehende Instrument sollte nicht gefährdet, sondern allenfalls als weiterer Kanal für die Meldung von Cyberangriffen etabliert werden.

- *Art. 74f E-ISG, Übermittlung der Meldung (neu)*

Mit dieser Bestimmung wird das NCSC verpflichtet, zwecks Erfüllung der Meldepflicht ein sicheres, elektronisches Meldeformular zur Verfügung zu stellen. Der erläuternde Bericht konkretisiert, dass es jedoch in jedem Fall weiterhin zulässig bleibt, das NCSC auf andere Weise (beispielsweise E-Mail, Telefon) über einen Cyberangriff in Kenntnis zu setzen. Vom Grundgedanken her ist es sehr begrüssenswert, wenn eine Meldung ausserhalb des Meldeformulars zugelassen wird, jedoch muss die Sicherheit des Meldevorgangs und –inhalts auf anderen Wegen gewährleistet sein. Insgesamt sollte der Meldemechanismus so frei wie möglich gestaltet werden, um beispielsweise automatische Meldungen durch RSS Feeds oder API zu erlauben oder auch via den bestehenden Austausch von Daten via das System MISP, das viele KI-Betreiber bereits im Einsatz haben.

Abs. 2 hält fest, dass das System der Betreiberin einer kritischen Infrastruktur ermöglichen muss, die Meldung an weitere Behördenstellen weiterzuleiten. Dabei ist vor allem die Kombination mit einer Meldung nach revDSG sinnvoll.

- *Art. 74i E-ISG, Widerhandlungen gegen Verfügungen des NCSC (neu)*

Gemäss dieser Bestimmung macht sich diejenige Person strafbar, die innerhalb der kritischen Infrastruktur hätte dafür sorgen müssen, dass der Verfügung des NCSC gemäss Art. 74i i.V.m. Art. 74h Abs. 2 Folge geleistet wird. Das Adressieren der Leitungsebene von Unternehmen wird gemäss erläuterndem Bericht dabei als Möglichkeit der sachgerechten Zuordnung angesehen. In Anbetracht der Unbestimmtheit der meldepflichtigen Ereignisse/ Vorfälle gemäss Ausführungen weiter vorne, stehen Bussenandrohungen in der vorgesehenen Höhe von CHF 100'000 jedoch dem Legalitätsprinzip entgegen. Zudem widerspricht das vorgesehene Vollzugsregime mit abschreckenden Anreizen der Tatsache, dass es sich bei Cybersecurity um eine Querschnittsaufgabe handelt: Den Gefahren kann nur mittels eines partnerschaftlichen und kooperativen Ansatzes zwischen Staat und Wirtschaft erfolgsversprechend begegnet werden. Wir beantragen deshalb die ersatzlose Streichung von Art. 74i (i.V.m. der notwendigen Anpassung in Art. 74h Abs. 2 E-ISG).

Eventualiter beantragen wir, die Bussenschwellen nach ISG und revDSG gleichzusetzen und von der Verfolgung von natürlichen Personen gänzlich abzusehen (mit Ausnahme von direktvorsätzlichen Fällen).

- *Art. 76 E-ISG, Zusammenarbeit im Inland*

Dieser Artikel bildet die gesetzliche Grundlage für den Informationsaustausch zwischen dem NCSC und den Betreiberinnen von kritischen Infrastrukturen (Abs. 1 und 2) sowie zwischen dem NCSC und den Fernmeldedienstanbieterinnen (Abs. 3 und 4). Wie bereits weiter vorne vermerkt, muss aus unserer Sicht unbedingt der bereits bestehende und gut etablierte Austausch von technischen Informationen (Threat Intelligence) zwischen NCSC, den Betreiberinnen und Betreibern von KI und weiteren Parteien berücksichtigt und nicht gefährdet werden. Insbesondere die international etablierten Protokolle zum Teilen von Informationen (TLP-Protokoll) sollten nicht untergraben, sondern rechtlich präziser umschrieben werden.

Wir bedanken uns bestens für die Berücksichtigung unserer Anliegen und stehen Ihnen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse
Swico

Ivette Djonova
Head Legal & Public Affairs

Andreas Knöpfli
Präsident