digitalswitzerland

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

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

Bern, 13. März 2022

**Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe**

# Stellungnahme zum Bundesgesetz über die Informationssicherheit beim Bund

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, uns zu den Änderungen im Bundesgesetz über die Informationssicherheit beim Bund, äussern zu können. digitalswitzerland nimmt diese Gelegenheit gerne wahr.

**Betroffenheit digitalswitzerland**
digitalswitzerland ist eine schweizweite, branchenübergreifende Initiative, welche die Schweiz als weltweit führenden digitalen Innovationsstandort stärken und verankern will. Unter dem Dach von digitalswitzerland arbeiten an diesem Ziel mehr als 240 Organisationen, bestehend aus Vereinsmitgliedern und politisch neutralen Stiftungspartnern, transversal zusammen. digitalswitzerland ist Ansprechpartner in allen Digitalisierungsfragen und engagiert sich für die Lösung vielfältiger Herausforderungen.

## 1. Begrüssung der Meldepflicht

digitalswitzerland unterstützt grundsätzlich die Einführung einer Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe. Die Mitglieder von digitalswitzerland beschäftigen sich täglich mit der Cybersicherheit ihrer eigenen Unternehmen oder betreuen IT-Systeme ihrer Kunden in diesem Bereich. Die Anzahl von Cyberangriffen nimmt rasant zu. Ein adäquater Schutz ist generell für jedes Unternehmen angezeigt. Dies gilt insbesondere für Betreiberinnen von kritischen Infrastrukturen, die eine wichtige Funktion für Wirtschaft und Gesellschaft übernehmen und auch im Falle eines Cybervorfalls oder -angriffs diese gewährleisten müssen. Deswegen begrüsst digitalswitzerland grundsätzlich eine Meldepflicht für Betreiberinnen von kritischer Infrastrukturen. Nichtdestotrotz gibt es aus Sicht von digitalswitzerland braucht Gesetzesentwurf noch Präzisierungen, damit die Regulierung für die Unternehmungen verträglich und damit zielführend für alle Beteiligten wird.

## 2. Präzisierungen der Meldepflichtigen und des Meldegegenstands

Im Zuge der Gesetzgebung darf nicht vergessen werden, dass eine Meldepflicht an die Behörden zu einer administrativen Belastung der Unternehmen führt. Es braucht daher klare Aussagen dazu, «wer» «wem» «was» unter welchen Bedingungen liefern muss.

Der Gesetzesentwurf erwähnt unter Art. 74b E-ISG eine Vielzahl von betroffenen Branchen. Insbesondere Art. 74b lit. s E-ISG nennt Betreiber von Hard- und Software, deren Produkte von kritischen Infrastrukturen genutzt werden. Damit wird der Geltungsbereich der Meldepflicht auf die Lieferketten ausgedehnt, was auf eine noch grössere Betroffenheit schliessen lässt, als die Aufzählung unter Art. 74b E-ISG zeigt. Die gewählte Formulierung lässt im derzeitigen Fall auf einen grossen Kreis an betroffenen Firmen schliessen.

**Einführung Terminologie «Meldepflichtigen»**

Um eine höhere Präzision zu erreichen und Missverständnisse zu vermeiden, wird die Einführung der Terminologie des «Meldepflichtigen» vorgeschlagen. Auch wenn im Kontext der kritischen Infrastrukturen eine klarere Definition schwierig sein dürfte, da sie sicherheitsrelevant ist, braucht es trotzdem möglichst klare Anhaltspunkte zum Geltungsbereich. Gerade die Ausdehnung auf Unternehmungen in der Lieferkette weist auf eine breite Betroffenheit der Wirtschaft hin.

Sollte der Geltungsbereich, wie von uns verstanden, grosse Teile der Wirtschaft betreffen, wird eine Regulierungfolgenabschätzung notwendig. Denkbar wäre auch ein abgestufter Regulierungsansatz, der sich an der Kritikalität der Unternehmen orientiert. Durch Definierung von Ambitionsniveaus könnten Erfahrungen mit der Meldepflicht gesammelt werden, bevor sie auf weite Teile der Wirtschaft ausgedehnt würde. Als oberste Stufe wären die Betreiberinnen von kritischen Infrastrukturen wie etwa die Energie- und Wasserversorger zu nennen. Alsdann könnte die Meldepflicht entlang von Ambitionsniveaus ausgerollt werden. Denn gerade für kleine Unternehmen und Startups sind zusätzliche Regulierungsaufwände so klein wie möglich zu halten.

**Meldegegenstand klar benennen**

Damit keine Missverständnisse beim Meldegegenstand entstehen, sollte zudem klar definiert werden, was gemeldet werden muss. Hier bleibt der Gesetzestext unscharf, da er wahlweise von Cybervorfällen, Cyberangriffen oder Schwachstellen spricht. Auch scheint die Definiton des Begriffs «Cybervorfall» kaum handhabbar, weil sie mit der blossen – auch theoretischen – Möglichkeit der Beeinträchtigung der Schutzziele operiert. Eine Möglichkeit kann oft nicht ausgeschlossen werden. Die Definition sollte daher angepasst werden. Es drängt sich auf, sich hier an Art. 4 Nr. 7 der NIS-Richtlinie anzulehnen. Sie definiert den «Sicherheitsvorfall» als «alle Ereignisse, die tatsächlich nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssystemen haben». Im Ergebnis sollte Art. 5 lit. d daher wie folgt lauten:

| |
|---|
| Änderung Art. 5 lit. d E-ISG (Änderung kursiv markiert)<br>«Cybervorfall: Ereignis beim Betrieb von Informatikmitteln, das ~~dazu führen kann~~ *dazu führt*, dass die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist.» |

**Unklare Defintion von Online-Marktplatz**

Art. 74b lit. f E-ISG definiert zwei Bedingungen bei welchen Anbieterinnen von Online-Marktplätze, Cloudcomputing und weiteren digitalen Diensten unter die Meldepflicht fallen. Das Gesetz nennt 1) «eine grosse Zahl von Nutzenden» und 2) eine «hohe Bedeutung für die digitale Wirtschaft». Diese Definitionen sind aus Sicht von digitalswitzerland sehr unklar gewählt. Sie müssten entweder bereits im Gesetzestext präziser definiert oder spätestens dann in der Verordnung geklärt werden.

Wir geben zudem grundsätzlich zu bedenken, dass die Definition von Online-Marktplätzen als «kritische Infrastruktur» zweifelhaft erscheint. So sollte sich die Definition dieses Begriffs an etablierten regulatorischen Grundsätzen orientieren und einen Gleichklang mit der Gesetzgebung innerhalb des europäischen Auslands herstellen (siehe unter anderem hier: Annex zum Entwurf einer EU-Richtlinie zum Schutz kritischer Infrastrukturen). Dies sind per definitionem Dienste, die für die Aufrechterhaltung lebenswichtiger gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten unerlässlich sind, z.B. aus den Bereichen Finanzwesen, Gesundheit, Verkehr. Es wird vorgeschlagen, den Gesetzestext in diesem Sinne zu präzisieren.

| |
|---|
| Änderung Art. 74b, Abs. f E-ISG «Bereiche» (Änderung kursiv markiert)<br>«Die Meldepflicht gilt für:<br>[…]<br>f. Anbieterinnen von ~~*Online-Marktplätzen,*~~ Cloudcomputing, Suchmaschinen und weiteren digitalen Diensten sowie Registrare von Domain-Namen und Betreiberinnen von Rechenzentren, die in der Schweiz:<br>[…] |

Durch die angestrebte Breite und Tiefe der Meldepflicht ist es aus Sicht von digitalswitzerland unabdingbar, dass die Verletzung von Rechten von Dritten im Falle einer Meldung nicht gefährdet sind. Daher wird eine Präzisierung von Art. 74 Abs. 4 E-ISG gefordert. Es sollte klarer dargelegt werden, wie das NCSC die Geheimhaltungspflichten schützt.

## 3. Überschneidungen mit anderen Meldepflichten vermeiden

Die Wirtschaft kennt bereits in anderen Bereichen Meldepflichten. Überschneidungen mit bestehenden sektoriellen Meldepflichten im Bereich Cybersicherheit sollten vermieden werden. So kennt der Finanzsektor gemäss Art. 29 Abs. 2 FINMAG bereits eine Meldepflicht von Cyber-Attacken. Entsprechend wichtig ist eine Alignierung des NCSC mit den anderen Meldeempfängern. Eine möglichst weitestgehende Standardisierung oder zumindest Interoperabilität sollte angestrebt werden. Dies betrifft auch den Inhalt der Meldung und die Meldefristen. Dies muss in der entsprechenden Verordnung festgehalten werden. Der administrative Aufwand für die Unternehmen könnte mit einem «one-stop-shop» für Meldepflichten erheblich vermindert werden. So würde eine einzige Meldung genügen, die je nach Erfüllung der relevanten Kriterien bzw. Überschreiten der relevanten Schwellen direkt von NCSC, mit dem Einverständnis des Meldepflichtigen, an weitere Meldeempfänger (z.B. FINMA) weitergeleitet würde. Aus Sicht von digitalswitzerland ist hier der Bund in der Pflicht, eine optimale Koordination sicherzustellen, damit statt der verschiedenen staatlichen Anlaufstellen und Sektorregulierungen eine einzige Ansprechstelle geschaffen wird, welche die erforderliche Koordination garantiert. Dies gilt sowohl für die Meldepflicht seitens des Unternehmens als auch für eine allfällige Reaktion seitens der Behörden. Gerade im Momenten der Bedrohung kann es nicht sein, dass Unternehmen durch unterschiedliche Meldepflichten unnötig belastet werden.

## 4. Gegenwert klar erkennbar machen

Damit die Meldepflicht die vorgesehene «Servicementalität» erhält, muss ihr ein klarer Mehrwert entspringen. Gemäss den Vernehmlassungsunterlagen ziehen die Betreiberinnen kritischer Infrastrukturen einen Mehrwert aus den technischen Einschätzungen und Unterstützung bei schwerwiegenden Cyber-Vorfällen. Die Meldepflicht soll eine verlässliche Einschätzung der Bedrohungslage und ein «Frühwarnsystem» darstellen. Diese Vorteile werden von digitalswitzerland begrüsst. Die Meldepflicht muss stets von diesem Service-Gedanken geprägt sein und darf nicht zu einem Kontrollinstrument gegenüber betroffenen Firmen werden. Es muss darum gehen, partnerschaftlich

Risiken zu identifizieren, diese zu kommunizieren und dadurch einen Beitrag zur besseren Cybersicherheit für alle zu leisten. Das gemeinsame Ziel und der Nutzen muss für die Unternehmen von Anfang an plastisch und konkret dargelegt werden. Nur so können sie Vertrauen in den Nutzen der Institution aufbauen. Der unmittelbare und übergeordnete Nutzen muss im Verhältnis zu den Pflichten klar ersichtlich sein – gerade für KMU und Startups ist die Verhältnismässigkeit der Massnahmen ein wichtiges Kriterium. Dieser wichtige Gegenwert wird in der Vorlage noch zu wenig ersichtlich und muss entsprechend besser dargelegt werden.

## 5. Keine persönliche Strafbarkeit

digitalswitzeralnd ist überzeugt, dass Cyber-Bedrohungen nur partnerschaftlich zwischen Staat und Wirtschaft effektiv eingedämmt werden können. Diesem kooperativen Geist widerlaufen Art. 74h und 74i E-ISG. Strafbestimmungen die zur persönlichen Strafbarkeit der Verantwortlichen führen können, sind gänzlich abzulehnen. Solche Bestimmungen sind für die Compliance von Unternehmen vielmehr schädlich als förderlich. Fachkräfte, die in einem inhärent fehleranfälligen Bereich wie der Cyber-Sicherheit mit Sanktionen rechnen müssen, obwohl sie alle zumutbaren Vorkehrungen getroffen haben, werden verständlicherweise zur Übernahme dieser Verantwortung weniger bereit sein. Es wird für die Unternehmen also noch schwieriger, im bereits ausgetrockneten Stellenmarkt entsprechende IT-Fachkräfte zu rekrutieren. Im schlimmsten Fall werden durch den Fokus auf die Sanktionsrisiken, die sowieso schon knappen Ressourcen noch für die Absicherung gegen Sanktionsrisiken anstelle der Cyberrisiken verwendet. Und dies in einem Bereich, in dem eigentlich gleichgerichtete Interessen bestehen.
In diesem Zusammenhang ist auch der Grundsatz des Selbstbelastungszwangsverbots bei Cyberangriffen und Cybervorfällen eminent wichtig. digitalswitzerland schlägt in diesem Zusammenhang eine Präzisierung von Art. 73c Abs. 3 vor.

| Änderung Art. 73c Abs. 3 E-ISG |
| --- |
| *Informationen, die ~~von einer Person~~ dem NCSC im Rahmen einer Meldung ~~dem NCSC~~ bekanntgegeben wurden und die meldende Person selbst belasten könnten, dürfen in einem Strafverfahren gegen diese Person nur mit ~~deren~~ Einverständnis dieser Person verwendet werden.* |

Wir danken Ihnen für die Aufmerksamkeit, die Sie unseren Anliegen entgegenbringen und stehen für weitere Auskünfte gerne zur Verfügung.

Freundliche Grüsse

Stefan Metzger
Managing Director digitalswitzerland

Andreas W. Kaelin
Senior Advisor Cyber Security digitalswitzerland

**Für weitere Auskünfte:**
Andreas Kaelin, digitalswitzerland | Geschäftsstelle Bern
Tel. +41 31 311 62 45 | andreas@digitalswitzerland.com