Swiss Banking

Eidgenössisches Finanzdepartement
Nationales Zentrum für Cybersicherheit NCSC
Schwarztorstrasse 59
CH-3003 Bern

Per Mail: ncsc@gs-efd.admin.ch

Basel, 13. April 2022

Meldepflicht von Betreiber/-innen kritischer Infrastrukturen für Cyberangriffe
Vernehmlassung – unsere Stellungnahme

Sehr geehrter Herr Bundesrat Maurer
Sehr geehrter Herr Schütz
Sehr geehrte Damen und Herren

Wir nehmen Bezug auf die vom Bundesrat am 12.01.2022 eröffnete Vernehmlassung zur Revision des Informationssicherheitsgesetzes (ISG) betr. Einführung einer Meldepflicht für Betreiber/-innen kritischer Infrastrukturen bei Cyberangriffen. Zu Ihrem Entwurf äussern wir uns wie folgt.

Zusammenfassung

Die Schweizerische Bankiervereinigung (SBVg) befürwortet die Verankerung der Aufgaben des Nationalen Zentrums für Cybersicherheit (NCSC) auf Gesetzesstufe (s. nachstehend 2.1 und 2.2); sie sollen als Dienstleistungen des Bundes die eigenverantwortlich zu treffenden Massnahmen der Unternehmen ergänzen.

Die SBVg unterstützt die Einführung einer Pflicht der Betreiberinnen kritischer Infrastrukturen, Cyberangriffe den Behörden zu melden, unter Vorbehalt nachfolgender Anliegen.

Die von der FINMA beaufsichtigten Institute sind gemäss Art. 29 Abs. 2 FINMAG bereits heute verpflichtet, der FINMA unverzüglich Vorkommnisse zu melden, die für die Aufsicht von wesentlicher Bedeutung sind. Diese umfassen auch Cyberangriffe (FINMA-Aufsichtsmitteilung 05/2020 betr. Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG).

Um zu vermeiden, dass unterschiedliche Meldungen sowohl dem NCSC als auch der FINMA erstattet werden müssen, schlagen wir vor:

- Das Meldeformular ist so zu konzipieren, dass es parallel und ohne zusätzlichen Aufwand auch weiteren Behörden (z.B. FINMA, EDÖB) geschickt werden kann.
- Rückfragen involvierter Behörden müssen über das Formular und den dafür zu schaffenden Kanal beantwortet werden können.

In jedem Fall müssen die verschiedenen Meldepflichten für die betroffenen Unternehmen konsistent ausgestaltet sein.

Die Meldepflicht muss verhältnismässig ausgestaltet sein, wie es der Entwurf zu einem guten Teil bereits vorsieht: Wo wir es als sinnvoll erachten, schlagen wir nachstehend Anpassungen und Ergänzungen vor. Wir befürworten insbesondere:

- eine Meldepflicht nur für Cyberangriffe, nicht für blosse Cybervorfälle (so bereits vorgesehen, Art. 74a);
- eine zwingende Meldepflicht nur bei Cyberangriffen mit einem gewissen Schadenspotenzial gemäss unserem Vorschlag zu Art. 74d.

Das Melderegime muss praxisfreundlich ausgestaltet sein. Zu diesem Zweck schlagen wir vor, auf Verordnungsstufe einen Beispielkatalog auszuarbeiten, und sind gerne bereit, daran mitzuwirken (s. nachstehend 2.4).

Übereinstimmend mit economiesuisse schlagen wir zudem die Streichung der Strafdrohung in Art. 74h und 74i vor (s. nachstehend 2.7), da sie sich im Blick auf die Compliance des Unternehmens kontraproduktiv auswirken könnte.

Das elektronische Meldesystem (Art. 74f) muss höchsten Sicherheitsanforderungen genügen.

Den Bestimmungen über Anpassungen beim Datenschutz und die Zusammenarbeit mit in- und ausländischen Behörden, die im Bereich der Cybersicherheit tätig sind (Art. 75–77), stimmen wir zu. Wir schlagen vor, im Gesetz explizit festzuhalten, dass bei Meldungen an das NCSC allfällige Berufsgeheimnisse zu wahren sind.

1. Allgemeines

Die Schweizerische Bankiervereinigung (SBVg) und ihre Mitglieder engagieren sich mit hoher Priorität für Massnahmen zur Stärkung der Cyberresilienz am Wirtschaftsstandort Schweiz. Ausdruck dieses Engagements war nicht zuletzt die mit dem Expertengremium Information Security & Cyber Defence erarbeitete Strategie der SBVg (parallel zur Nationalen Cyber Strategie des Bundes, NCS II). Die darin postulierten Massnahmen sind teilweise schon umgesetzt (so z.B. die Schaffung des Nationalen Zentrums für Cybersicherheit, NCSC) oder befinden sich in der Umsetzung (so z.B. die Bildung eines Swiss Financial Sector Cyber Security Centre, FS-CSC). Umsetzbar ist eine solche Strategie nur als **Public-Private Partnership (PPP) mit den Bundesbehörden, insbesondere dem NCSC**. Für die in diesem Sinne sehr erfolgreiche Zusammenarbeit möchten wir Ihnen auch an dieser Stelle danken.

Die Meldepflicht bei Cyberangriffen stellt einen **wichtigen Schritt auf dem Weg der Umsetzung dieser gemeinsamen Bemühungen** dar – einen Schritt, der notwendigerweise dem Gesetzgeber, also der staatlichen Seite der Partnership zukommt. Wir unterstützen Sie dabei und äussern uns nachstehend zu einzelnen Gesichtspunkten, insbesondere dort, wo wir noch Verbesserungsbedarf sehen.

2. Bemerkungen zu einzelnen Bestimmungen des Entwurfs

2.1 Gesetzeszweck und Begriffsumschreibungen (Art. 1 und 5)

Wir begrüssen, dass der **Gesetzeszweck** (Art. 1 Abs. 1 Bst. b) neu ausdrücklich die Erhöhung der «Widerstandsfähigkeit der Schweiz gegenüber Cyberrisiken» (Cyberresilienz) mitenthalten soll. Dadurch untermauert das Gesetz die in Art. 73a ff. festgehaltenen Aufgaben des NCSC.

Wir sind einverstanden mit der Umschreibung der **Schlüsselbegriffe**:

- *«Cybervorfall» (Art. 5 Bst. d: «Ereignis beim Betrieb von Informatikmitteln, das dazu führen kann, dass die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist») und*
- *«Cyberangriff» (Art. 5 Bst. e: «Cybervorfall, der von Unbefugten absichtlich ausgelöst wurde»).*

Der Cybervorfall ist heute in **Art. 3 Bst. b Cyberrisikenverordnung (CyRV)** so umschrieben, dass er auch den Cyberangriff abdeckt. Art. 5 Bst. d des Gesetzesentwurfs übernimmt materiell diesen Begriff, und Art. 5 Bst. e führt einen gesonderten Begriff des Cyberangriffs ein, um die Meldepflicht auf diesen zu beschränken. Das erscheint uns sinnvoll. Art. 3 CyRV wird entsprechend anzupassen sein.

2.2 Umschreibung der Aufgaben des NCSC (Art. 73a ff.)

Wir begrüssen die **gesetzliche Verankerung der Aufgaben und Zuständigkeiten des NCSC**.

Nach unserem Verständnis ist der Gesetzestext so zu verstehen, dass die «Anleitungen für präventive und reaktive Massnahmen gegen Cyberrisiken» gemäss Art. 73a Bst. c den Unternehmen als Grundlage zu

freiwilligen Massnahmen in eigener Verantwortung dienen sollen. Verbindliche Anweisungen wären u.E. nicht sinnvoll, weil das NCSC die Lage in den Unternehmen nicht detailliert selber einschätzen kann. Das gilt insbesondere auch für Art. 74 Abs. 1–3.

Wir schlagen zudem vor, in diesen Abschnitt eine **ausdrückliche Ermächtigung des NCSC zur Kooperation mit privatrechtlichen Organisationen der Wirtschaft (Art. 73bis)**, aufzunehmen. Ein Beispiel dafür ist der derzeit im Aufbau befindliche Verein Financial Swiss Sector Cyber Security Centre (Swiss FS-CSC). So lässt sich einerseits eine Selbstverständlichkeit festhalten. Andererseits werden künftige Diskussionen um die Zulässigkeit von Public-Private Partnerships dadurch vermieden. Die entsprechende Bestimmung könnte wie folgt lauten:

> *«Zusammenarbeit mit Organisationen der Privatwirtschaft*
>
> *[1] Das NCSC kann im Rahmen seiner Aufgaben gemäss diesem Abschnitt mit Organisationen der Privatwirtschaft, insbesondere Unternehmen und ihren Verbänden, zusammenarbeiten.*
> *[2] Dabei sind die Berufs- und Geschäftsgeheimnisse der betroffenen Unternehmen zu wahren.»*

2.3 Meldepflicht der Betreiberinnen von kritischen Infrastrukturen (Art. 74a ff.)

Wir begrüssen die Einführung einer Meldepflicht und deren **Begrenzung auf Cyberangriffe mit erheblichem Schadenspotenzial unter Ausklammerung blosser Vorfälle**, die aber freiwillig gemeldet werden können (Erläuternder Bericht, S. 10 oben) (s. dazu nachstehend 2.5).

Zur Vermeidung mehrfacher Meldungen in unterschiedlichen Verfahren unterbreiten wir Ihnen einen Vorschlag, der **einfache Parallelmeldungen mit dem Formular des NCSC** erlaubt (s. nachstehend 3).

Wir schlagen vor, die Meldepflicht im Sinne der **Verhältnismässigkeit** – und in Anlehnung an die FINMA-Aufsichtsmitteilung 05/2020 – auf erfolgreiche oder teilweise erfolgreiche Cyberangriffe auf kritische Funktionen von Beaufsichtigten einzuschränken, deren Ausfall oder Fehlfunktion erhebliche Auswirkungen auf die Geschäftstätigkeit hätte und diese stark beeinträchtigen würde (s. nachstehend 2.4).

Als «Betreiberinnen von kritischen Infrastrukturen» (Art. 74a) lässt der Gesetzesentwurf u.a. **sämtliche Banken, Versicherungen und Finanzmarktinfrastrukturen** unter die Meldepflicht fallen (Art. 74b Bst. e), sofern diese nicht die Kriterien für eine Ausnahme gemäss Art 74c erfüllen Wir schlagen zur Wahrung der Verhältnismässigkeit und zur Schaffung von Rechtssicherheit vor, dass die Ausnahmen von der Meldepflicht auf Verordnungsstufe weiter konkretisiert werden.

In diesem Sinn schlagen wir vor, Art. 74c zu überarbeiten. Abs. 1 kann somit wie folgt lauten:

> *«[1] Der Bundesrat legt auf Verordnungsstufe klare Kriterien fest, anhand derer die Infrastrukturen meldepflichtig werden. Sinn dieser Kriterien ist es, jene Betreiberinnen kritischer Infrastrukturen von der Meldepflicht auszunehmen, bei denen durch Cyberangriffe ausgelöste Funktionsausfälle oder Fehlfunktionen [Rest unverändert]»*

Sodann regen wir an, die vage Formulierung in Art. 74a durch einen Abs. 2 mit einer **Fristregelung** zu ergänzen. Dabei sollte die zweistufige Regelung gemäss der FINMA Aufsichtsmitteilung 05/2020 übernommen werden (innert 24 Std. erste Meldung; innert 72 Std. ergänzte, ausführlichere Meldung). Das vereinfacht nicht zuletzt auch die Vertragslage mit Lieferanten.

2.4 Kriterien für zu meldende Angriffe (Art. 74d)

Die vorgeschlagenen Kriterien sind ungeeignet, um die Meldepflicht auszulösen, denn im Zeitpunkt, da eine Meldung sinnvoll und erwünscht wäre, dürften sie in einer Vielzahl der Fälle noch nicht absehbar sein. Wir schlagen deshalb die **vollständige Ersetzung von Art. 74d durch eine Formulierung im Sinn der FINMA-Aufsichtsmitteilung 05/2020** vor, die z.B. wie folgt lauten könnte:

> *«Zu melden sind Cyberangriffe mit erheblichen Auswirkungen auf die Geschäftstätigkeit des Unternehmens, insbesondere erfolgreiche oder teilweise erfolgreiche Angriffe auf kritische Funktionen, deren Ausfall oder Störung den Schutz der Kundinnen und Kunden oder das Funktionieren der Märkte stark beeinträchtigen würde.»*

Das Ziel, eine uferlose Meldepflicht mit unscharfen Grenzen zu vermeiden, spricht für die von uns vorgeschlagene Schaffung eines **Beispielkatalogs aus der Praxis** auf Verordnungsstufe. Gerne sind wir bereit, an dessen Ausarbeitung mitzuwirken.

Entsprechend der vom Gesetzgeber bestimmten Regelung wird insbesondere auch **die FINMA-Aufsichtsmitteilung 05/2020 betr. Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG anzupassen** sein.

Es wird der Bank ohnehin freistehen, **weitergehend als vorgeschrieben** zu melden, insbesondere auch blosse Cybervorfälle (Erläuternder Bericht, ebd.). Diese Möglichkeit, freiwillig weitere Cybervorfälle und -angriffe als vorgeschrieben zu melden, erwähnt der Gesetzesentwurf nicht ausdrücklich. Im Sinn der Rechtssicherheit schlagen wir eine **Bestimmung über die Zulässigkeit freiwilliger Meldungen (Art. 74d Abs. 2)** vor, die z.B. so lauten könnte:

> *«[2] Über die Meldepflicht aufgrund von Artikel 74a ff. hinaus darf eine Betreiberin von kritischen Infrastrukturen auch Cybervorfälle und -angriffe melden, welche die Kriterien gemäss Artikel 74d nicht vollständig erfüllen.»*

Damit wird explizit ausgeschlossen, dass eine überschiessende Erfüllung der Meldepflicht als Verletzung des Berufsgeheimnisses missverstanden werden könnte, und **einer denkbaren Rechtsunsicherheit vorgebeugt.**

2.5 Inhalt der Meldung (Art. 74e)

Die **offene, knappe Formulierung** über den Inhalt der Meldung ist zu begrüssen. Es gilt zu vermeiden, dass eine zu detaillierte Umschreibung bei den meldepflichtigen Unternehmen zu unverhältnismässigem Aufwand führt. Dies wird insbesondere bei der Ausgestaltung der Verordnung durch den Bundesrat zu berücksichtigen sein.

2.6 Elektronische Übermittlung der Meldung (Art. 74f)

Wir begrüssen die Schaffung eines elektronischen Systems für die Meldung von Cyberangriffen. Art. 74f legt die **Anforderungen für das Meldesystem** fest. Es muss

- sicher sein (Art. 74f Abs. 1). Dieses Erfordernis ist durch die Erfüllung höchster Standards zu gewährleisten;
- dem meldenden Unternehmen erlauben, die erfolgte Meldung ganz oder teilweise auch weiteren Behörden zukommen zu lassen (Art. 74f Abs. 2) und
- dem meldenden Unternehmen ermöglichen, einer solchen Zweitbehörde von ihr benötigte Zusatzinformationen zu übermitteln, die das NCSC nicht benötigt (Art. 74f Abs. 3).

Das Gesetz wird aber den Unternehmen nicht verbieten, **Meldungen dem NCSC auch auf anderen Wegen, z.B. per E-Mail oder telefonisch**, zu übermitteln (Erläuternder Bericht, S. 21).

Und das Meldesystem wird auch für **freiwillige Meldungen an weitere Behörden** zur Verfügung stehen (Erläuternder Bericht, S. 21).

2.7 Verletzungen der Meldepflicht (Art. 74h und 74i)

Übereinstimmend mit economiesuisse ersuchen wir Sie um **Streichung der Strafdrohung**, da sie nach bisherigen Erfahrungen der Branche kontraproduktive Auswirkungen hinsichtlich der Compliance haben und das initiative, eigenverantwortliche Handeln der Mitarbeitenden in den betroffenen Unternehmen lähmen könnte.

3. Abgrenzung zu bestehenden Meldepflichten anderer Gesetze

Bestehende Meldepflichten aufgrund anderer Gesetze – beispielsweise Art. 29 Abs. 2 FINMAG für die Banken und Art. 24 nDSG – sollen durch die neue Meldepflicht gemäss Art. 74a ff. (s. vorstehend 2.3–2.4) *«nicht ersetzt, sondern nur ergänzt»* werden (Erläuternder Bericht, S. 5).

> *«Dabei wurde darauf geachtet, dass die gesetzlichen Grundlagen eine gleichzeitige Erfüllung verschiedener Meldepflichten erlauben. Der Aufwand für die Erfüllung der verschiedenen Meldepflichten soll so möglichst geringgehalten werden. Dies gilt vor allem, aber nicht nur für das Verhältnis zur datenschutzrechtlichen Meldepflicht nach Artikel 24 des revidierten Datenschutzgesetzes (nachfolgend: nDSG), da es in der Praxis häufig der Fall ist, dass Cyberangriffe zu Datenverlusten führen. Die*

gewählte Lösung sieht vor, dass es den Meldenden offensteht, die Meldung des Cyberangriffs gleichzeitig mit der Übermittlung an das NCSC anderen Meldestellen weiterzuleiten, um damit anderweitige Meldepflichten zu erfüllen. Umgekehrt wird das NCSC auch Meldungen zu Cyberangriffen entgegennehmen, welche in Erfüllung einer anderweitigen Meldepflicht abgegeben wurden, sofern sie die benötigten Inhalte umfasst. Damit soll verhindert werden, dass Betroffene den gleichen Vorfall unterschiedlichen Stellen über unterschiedliche Verfahren melden müssen.»

Zur Lösung dieses richtig erkannten Problems schlagen wir vor, das Meldeformular so zu konzipieren, dass es **im Sinn einer Parallelmeldung** gleichzeitig verschiedenen Behörden (z.B. FINMA, EDÖB) zugestellt werden und ohne zusätzlichen Aufwand auch für Antworten auf Rückfragen involvierter Behörden verwendet werden kann. Mit anderen Worten muss das Formular und der dafür zu schaffende Kanal die verschiedenen durch einen Cyberangriff ausgelösten Meldepflichten abdecken (also insbesondere auch die Meldepflicht gegenüber der FINMA gemäss Art. 29 Abs. 2 FINMAG).

In jedem Fall müssen die verschiedenen Meldepflichten für die betroffenen Unternehmen konsistent ausgestaltet sein.

Gern sind wir bereit, bei der **Entwicklung** dieses Meldesystems mitzuwirken.

Als Konsequenz der einen wie der anderen Variante wäre, wie schon erwähnt, insbesondere auch die **Aufsichtsmitteilung 05/2020 der FINMA betr. Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG anzupassen**.

4. Anpassungen beim Datenschutz und Informationsaustausch mit anderen Behörden (Art. 75 ff.)

4.1 Datenschutz (Art. 73b Abs.2 Satz 2, 75 und 76), Berufsgeheimnisse

Die vorgesehenen Anpassungen beim Datenschutz verdienen **Zustimmung**.

Mit dem **Erfordernis der Einwilligung der betroffenen Person** in Art. 73b Abs. 2 Satz 2 ist dem Anliegen, dass Daten nicht oder eben nur mit Zustimmung der betroffenen Person weitergegeben werden sollen, Rechnung getragen.

Wir sind zudem der Auffassung, dass bei Meldungen im Sinn der neuen Regelung allfällige **Berufsgeheimnisse zu wahren** sind. Das betrifft insbesondere auch das Bankkundengeheimnis. Wir bitten Sie, diesem Anliegen bei der Überarbeitung des Gesetzestextes Rechnung zu tragen, beispielsweise durch die Einfügung einer expliziten Regelung.

4.2 Informationsaustausch mit anderen Behörden (Art. 76a und 77)

Wir stimmen der **Regelung über die Zusammenarbeit des NCSC mit dem Nachrichtendienst des Bundes (NDB) und den inländischen Strafverfolgungsbehörden** zu (Art. 76a).

Wir sind auch mit der Regelung für den **Informationstausch zwischen dem NCSC und ausländischen Behörden gleicher Funktion** einverstanden (Art. 77), wenn die Informationen für die Bekämpfung von Cyberrisiken und insbesondere die Zwecke dieses Gesetzes nötig sind (eine in Art. 77 Abs. 1 Satz 1 ausdrücklich vorgesehene und begrüssenswerte Einschränkung).

Sind Personendaten im Sinne von Art. 75 involviert, ist bei deren **Übermittlung ins Ausland** Art. 6 DSG zu beachten.

Wichtig ist der **Spezialitätsvorbehalt** (Art. 77 Abs. 2): Beim Informationsaustausch muss gewährleistet sein, dass die ausländische Schwesterbehörde die erhaltenen Informationen nur für den Zweck der Bekämpfung von Cyberrisiken verwendet.

Wir schlagen vor, die Regelung durch einen **Art. 76 über die Vertraulichkeit der Informationen** zu ergänzen, der z.B. wie folgt lautet:

> *«Weitergegebene Informationen sind durch die Empfängerbehörde vertraulich zu behandeln. Sie dürfen nicht weitergegeben werden, wenn dadurch die Sicherheit des betroffenen Unternehmens oder der betroffenen Personen gefährdet würde.»*

Sobald es um ein *«rechtliches Verfahren»* geht (also z.B. aufsichts- oder steuerrechtlicher Natur), kommen die **Bestimmungen über die Amts- und Rechtshilfe** zur Anwendung (Art. 77 Abs. 3).

Wir bitten Sie um die wohlwollende Prüfung unserer vorstehend geschilderten Anliegen und stehen auf Ihren Wunsch für deren gesprächsweise Erläuterung gerne zur Verfügung.

Freundliche Grüsse

August Benz
Stv. CEO
Leiter Private Banking & Asset Management

Alexandra Arni
Mitglied der Direktion
Leiterin ICT