CH++

Eidgenössisches Finanzdepartement EFD
Bundesrat Ueli Maurer
Bundesgasse 3, 3003 Bern
Eingabe per Mail an: ncsc@gs-efd.admin.ch

Lausanne, 12. April 2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe
Stellungnahme zum Bundesgesetz über die Informationssicherheit beim Bund

Sehr geehrter Herr Bundesrat Maurer,
Sehr geehrter Delegierter des Bundes für Cybersicherheit Schütz,
Sehr geehrte Damen und Herren;

Mit grossem Interesse haben wir die Vernehmlassung zur Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen und die weiteren vorgesehen Änderungen im Informationssicherheitsgesetz ISG zur Kenntnis genommen. Unsere Organisation CH++ widmet sich unabhängig einer nachhaltigen, wohlhabend und handlungsfähigen Schweiz durch Wissenschaft und Technologie — und dazu gehört fraglos und immer mehr auch die Cybersicherheit. Gerne nehmen wir entsprechend hiermit von der Möglichkeit gebrauch, Ihnen unsere Vernehmlassungsantwort zukommen zu lassen, die wir in den vergangenen Monaten mit einer Reihe namhafter ExpertInnen haben ausarbeiten können.

Wir bedanken uns für Ihr Interesse und stehen Ihnen für weiteren Dialog stets gerne zur Verfügung.

Marcel Salathé, Präsidium
Hannes Gassert, Präsidium
Olga Baranova, Geschäftsleitung

CH++

Allgemeine Würdigung

CH++ begrüsst die Einführung einer Meldepflicht im ISG: Ein verlässliches Lagebild muss Grundlage sein unserer Abwehrmassnahmen, in der Verwaltung ebenso wie in der Wirtschaft.

Ebenfalls unterstützt CH++ die erhöhte Verbindlichkeit auf Gesetzesstufe, sowohl bei den Verpflichtungen des NCSC wie auch auf jenen der Betreiberorganisationen kritischer Infrastruktur, inklusive Sanktionsmöglichkeiten. Punkte wie die Definition der zu meldenden Cyberangriffe oder der Auskunftspflichten sind aus Sicht CH++ gut gelungen.

CH++ ist jedoch der Ansicht, dass verschiedentlich Schärfungen vorzunehmen sind am aktuellen Entwurf, welche wir in der Folge darlegen. Namentlich ist aus Sicht von CH++ das Mandat des NCSC robuster auszugestalten und die Meldepflicht breiter zu gestalten — und gleichzeitig sie effizienter zu gestalten.

Darüber hinaus unterstützt CH++, wie Sie der Presse haben entnehmen können[1], die bereits von Bundesrat Maurer angekündigte Überführung des NCSC in ein Staatssekretariat, um den Stellenwert des Themas, den Ressourcenbedarf und die Mitwirkungsmöglichkeiten und die internationale Verhandlungsfähigkeit der Behörde auf das aus unserer Sicht angebrachte Niveau zu heben.

[1] https://magazin.nzz.ch/meinungen/die-schweiz-muss-ihre-digitale-souveraenitaet-verteidigen-ld.1653935

CH++

Artikel 73

1. Grundsatz

Die hier aufgeführten Tätigkeiten beschreiben ein breites Aufgabengebiet, sind aber noch zu passiv ausgestaltet und weisen dem NCSC eine entsprechend zu kleine und zu wenig aktive Verantwortungsposition zu.

Hinzuzufügen ist aus Sicht CH++ die aktive Erkennung von Schwachstellen und Bedrohungen, einerseits durch die Überwachung der globalen Geschehnisse im Bereich Cybersicherheit und 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 Meldung zu verarbeiten.

2. Bearbeitung von Meldungen zu Cybervorfällen und Schwachstellen

Nach Ansicht von CH++ sind die Bedingungen für eine Veröffentlichung sowohl in den lit. 2 und 3 (“sofern ..”) umzukehren in eine grundsätzliche Verpflichtung zur Veröffentlichung, unter Vorbehalt übergeordneter Interessen. Der “Default” kann nicht “security through obscurity” sein oder aktive Zurückhaltung sicherheitsrelevanter Informationen, sondern die aktive Transparenz — mit begründeten Ausnahmen. Über diese Ausnahmen ist sodann regelmässig Bericht zu erstatten an den Bundesrat und die zuständige parlamentarische Kommission.

Die möglichen Massnahmen in der Bearbeitung von Meldungen sind aus Perspektive von CH++ zudem noch zu wenig klar zu wenig robust. In Ergänzung zu den genannten Möglichkeiten schlägt CH++ vor, dass das NCSC in besonders gravierenden Fällen Weisungen mit Fristen erlassen kann, die Hersteller und

Betreiberorganisationen dazu verpflichten, die entsprechenden Produkte oder Infrastrukturen nachweislich abzusichern.

Darüber hinaus erscheint es angebracht, lit. 3 um eine Sanktionsmöglichkeit zuzüglich zur Veröffentlichung zu ergänzen, beispielsweise durch den Ausschluss des Herstellers von jeglichen öffentlichen Beschaffungen im Bereich kritischer Infrastruktur bis zur Behebung der Schwachstelle. Ein entsprechender Absatz im Bundesgesetz über das öffentliche Beschaffungswesen erscheint angebracht.
Im Weiteren sind in einem weiteren Absatz analog zu Absatz 3 nicht nur Hersteller, sondern auch auf Betreiberorganisationen entsprechender Hard- und Software in die Pflicht zu nehmen. Das Forcieren der Bereitstellung eines Sicherheitsupdates verbessert die Sicherheitslage wenig, wenn dieses sodann nicht zügig und flächendeckend eingespielt wird.

3. Weiterleitung von Informationen

CH++ begrüsst lit. 3 klar. Der verantwortungsvolle Umgang mit Sicherheitslücken (responsible disclosure etc.) darf nicht mit dem Risiko einer Strafverfolgung belegt werden.

Artikel 74

Meldepflicht

Die Meldepflicht ist aus Sicht von CH++ schneller, automatisierter und breiter auszugestalten:

- Die Meldungen haben nicht “so schnell wie möglich”, sondern umgehend zu erfolgen, im Regelfall innert 24 Stunden.
- Lit. f ist zu präzisieren: Die Auslegung von “grossen Zahl von Nutzenden” birgt die Gefahr, dass etwas kleinere Anbieter mit weniger Sicherheits-Ressourcen,

die aber womöglich sehr lohnenswerte Ziele darstellen und deren Nutzende hohen Risiken wie etwa Identitätsdiebstahl ausgesetzt sind, von der Regulierung nicht betroffen wären. Eine konkrete, im Zweifelsfall eher niedrige Zahl ist hier spätestens auf Verordnungsstufe zu definieren. Im Weiteren ist der in Punkt 2 verwendete Begriff “digitale Wirtschaft” abzuändern zu “Wirtschaft”.

- Lit s. begrüsst CH++ explizit, die Lieferketten sind miteinzubeziehen.

Ausnahmen von der Meldepflicht

CH++ steht dem gesamten Artikel 74c kritisch gegenüber und schlägt vor, diesen zu streichen. A priori die Eintretenswahrscheinlichkeit eines Risikos und die Grösse des erwartbaren Schadens verlässlich so gut einschätzen zu können, dass solche Ausnahmen bedenkenlos für gesamte Bereiche erteilt werden können, scheint schwierig — und entsprechend riskant.

Inhalt und Art. 74f Übermittlung der Meldung

Diese Artikel sind aus Sicht CH++ so zu überarbeiten, dass die Automatisierung von Meldungen möglich und wünschenswert werden. Mit den zur Verfügung stehenden technischen Möglichkeiten ist die Auswertung auch eines grossen Volumens von Meldungen möglich, auch wenn diese eher Anhaltspunkte denn kompletten Meldungen entsprechen. Art. 74e wäre entsprechend abzuschwächen auf eine Kann-Formulierung, sodass auch Meldungen wie Signale verdächtiger Aktivität andere auffällige Muster gemeldet werden können. Damit sinkt die Schwelle zur Interaktion mit dem NCSC.

Art. 74f wäre anzupassen hin zur expliziten Nennung der Datenanlieferung via gesicherter Schnittstelle als zusätzliche Möglichkeit. Dank dieser Automatisierung sinkt potentiell die administrative Belastung seitens der Meldepflichtigen, was die Akzeptanz der neuen Pflicht erhöhen dürfte. In der Industrie ist dies ein weit

verbreiteter Ansatz, sich innerhalb einer Community mit “Threat Intelligence” gegenseitig zu unterstützen. Ein API-zentrierter Ansatz wie er zum Beispiel in den Partnernetzwerken von Meta/Facebook oder AT&T erfolgreich praktiziert wird, ist aus Sicht CH++ durch das NCSC weiter zu verfolgen, wofür nun eine entsprechende gesetzliche Grundlage zu schaffen ist.

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

Widerhandlungen gegen Verfügungen des NCSC

CH++ schlägt vor, im Text klarer zu machen, dass die Sanktionen auf der Leitungsebene der Unternehmen zu greifen haben, nicht auf Ebene der Fachspezialisten, allenfalls durch Nennung spezifisch haftbarer Organe bzw. deren Mitglieder.

Art. 79 Abs. 1

Hier schlägt CH++ vor, den Begriff Verwendung zu qualifizieren, z.B. mit “zwingende Verwendung”. Das blosse Öffnen eines Datensatzes kann selbstverständlich nicht zur Verlängerung der erlaubten Aufbewahrungsdauer führen.