digitalswitzerland

Departement für Verteidigung, Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS
Schwarztorstrasse 59
CH-3003 Bern

Einreichung per Mail an:
ncsc@ncsc.admin.ch

Zürich, 13. September 2024

Betreff: Vernehmlassungsantwort zur Cybersicherheitsverordnung CSV

Sehr geehrte Frau Bundesrätin Amherd,
Sehr geehrter Herr Suter,

Wir danken Ihnen für die Gelegenheit, uns zur Vernehmlassung zur Cybersicherheitsverordnung (CSV) äussern zu können, welche wir hiermit für digitalswitzerland wahrnehmen.

digitalswitzerland begrüsst die Konkretisierung der im neuen ISG festgehaltenen Meldevorgänge bei Cyberangriffen auf kritische Infrastrukturen. Obschon die Vorlage äusserst klar und nachvollziehbar ist, erlauben wir uns, einige konkrete Änderungsvorschläge zu machen (jeweils in Gelb):

Art. 4. CSV Steuerungsausschuss NCS

Wir unterstützen es, einen Steuerungsausschuss Nationale Cyberstrategie (StA NCS) einzusetzen, schlagen aber vor, bei der Zusammensetzung auch Vertreterinnen und Vertreter von kritischen Infrastrukturen zu berücksichtigen. Die Formulierung «Vertreter der Wirtschaft» ist diesbezüglich zu wenig klar.

Art. 4, Abs. 1: Der StA NCS setzt sich aus Vertreterinnen und Vertretern der Departemente, der Bundeskanzlei, der Kantone, der Wirtschaft, ***insbesondere der Betreiber kritischer Infrastrukturen,*** *der Gesellschaft und der Hochschulen zusammen.*

Art. 9 Koordinierte Offenlegung von Schwachstellen

Artikel 9 Absatz 1 legt fest, dass die Offenlegung von Schwachstellen nach international anerkannten Standards zu erfolgen hat, obschon es diese noch nicht in ausreichendem Masse gibt. Um diese Lücke zu schliessen, sollen auch Best Practices[1] einbezogen werden. Der Änderungsvorschlag lautet:

Art. 9, Abs. 1: Das BACS sorgt für die koordinierte Offenlegung der Schwachstellen nach international anerkannten Standards ***und Best Practices.***

[1] CERT/CC hat bspw. eine Policy und einen Guide. Weitere Beispiele sind der OWASP Vulnerability Management Guide, oder NIST SP 800-53. FIRST hat Standards für die Koordination und Offenlegung von Schwachstellen entwickelt, siehe hier, hier und hier

In der vorgeschlagenen Formulierung der CSV ist der Bereich von "Prozessen" oder Konfigurationen von digitalen Services nicht abgedeckt. Es handelt sich bei Schwachstellen in diesem Bereich nicht (direkt) um Hard- oder Software-Probleme, sondern um falsche Konfiguration oder falsche Verwendung von Services. Jüngste Beispiele solcher Vorgänge sind:

- Eine Schwachstelle bei der Authentifizierung, die es Kriminellen ermöglichte, die für die Erstellung eines Kontos auf einer cloudbasierten Arbeitsumgebung erforderliche E-Mail-Verifizierung zu umgehen
- Ein öffentlicher Docker-Container, der einen GitHub Access-Token enthält.[2]
- Hinweise auf geheime, militärische Einrichtungen durch die Verwendung von Lokalisierungsdiensten durch Angestellte.[3]

Deswegen schlagen wir folgende Änderung vor:

Art. 9, Abs. 2: Es setzt ***dem für die betroffene Hardware, Software oder Services Verantwortlichen*** *eine Frist von 90 Tagen zur Behebung der Schwachstellen.*

Art. 11 Kommunikationssystem für den sicheren Informationsaustausch

Alle Betreiber kritischer Infrastrukturen im Land, einschliesslich solcher ohne Sitz in der Schweiz, sollten die Möglichkeit haben, am Informationsaustausch teilzunehmen (Art. 74 rev. ISG). Für globale Unternehmen ist der grenzüberschreitende Austausch von zentraler Bedeutung.

Deswegen schlagen wir folgende Änderung vor:

Art. 11 Abs. 1 1 Zugang zum Kommunikationssystem des BACS für den sicheren Informationsaustausch (Artikel 74 Abs. 2 Buchstabe a ISG) haben Organisationen und Behörden ~~mit Sitz in der Schweiz ,~~ ***die entweder ihren Sitz in der Schweiz haben oder vom BACS zum Informationsaustausch zugelassen werden und die von ihm dafür festgelegten Anforderungen erfüllen.***

Art. 13 Registrierung

Die aktuelle Formulierung deutet auf eine Verantwortlichkeit der gemeldeten Person hin, dabei soll es laut Botschaft lediglich um eine Kontaktperson gehen. Daher sollte die Formulierung in «Angaben zu einer oder mehreren Kontaktpersonen» angepasst werden.

Deswegen schlagen wir folgende Änderung vor:

Art. 13 Abs. 2., Bst. b: ~~Kontaktangaben der gemeldeten Person.~~ ***Angaben zu einer oder mehreren Kontaktpersonen.***

[2] Siehe: https://www.schneier.com/blog/archives/2024/08/leaked-github-python-token.html

[3] Siehe: https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/

Art. 18 Zu Meldende Cyberangriffe

Wir regen an, den Schweregrad eines Cyberangriffs bei der Meldepflicht mitzuberücksichtigen. Dadurch könnte viel administrativer Aufwand vermieden werden. Wir möchten dadurch verhindern, dass beispielsweise kurze Systemausfälle bei einem eingeschränkten Personenkreis gemeldet werden müssen. In bereits existierenden sektorspezifischen Compliance-Regelwerken[4] wird dem Schweregrad Rechnung getragen.

Deshalb schlagen wir folgende Änderungen vor, die zur Harmonisierung/Angleichung der Verordnung mit anderen Regelwerken beitragen:

Art. 18 Abs. 1 Bst. a: «Mitarbeitende oder Dritte, ***welche den unmittelbaren Betrieb der kritischen Infrastruktur verantworten, von durch Cyberangriffen verursachten Unterbrüchen kritischer Systeme betroffen sind und dadurch der stabile Betrieb der Infrastruktur unmittelbar gefährdet ist*** *oder…»*

*Art. 18 Abs. 2 Bst. a: «****Kritische*** *geschäftsrelevante Informationen …offengelegt* ~~***werden***~~***, entwendet, zerstört, deaktiviert oder sonst wie bearbeitet werden, welche sich mittel- oder langfristig auf wesentliche Applikationen oder Systeme auswirken;***»*

Neu eingefügt als Abs. 2 Bst. b: ***«die Integrität der Geschäftsprozesse beeinträchtigt ist, oder»***

Eine Abstufung bzw. eine Definition des Schweregrades wäre auch beim Abfluss von Informationen hilfreich. Wird lediglich ein unproblematisches Dokument publiziert, wiegt dies nicht so schwer, wie wenn vertrauliche sensible Daten an die Öffentlichkeit gelangen.

Art 19 Angaben zum Verursacher:

Im Rahmen der Meldung müssen auch Angaben zum Verursacher der Cyberattacke gemacht werden. Dies bedingt aufwändige forensische Verfahren, die äusserst komplex sind und im Aufgabenbereich der Strafverfolgung, und nicht der Unternehmen, liegen.

Deswegen schlagen wir folgende Änderung vor:

Art. 19, Abs. 1, Bst. e: Angaben zum Verursacher, ***falls diese ohne aufwändige forensische Verfahren ermittelt werden können.***

Art. 20 Übermittlung der Meldung

Der Artikel scheint eine Meldung durch eine Drittperson zu betreffen, die nicht meldepflichtig ist, jedoch eine registrierte Organisation betrifft. Die vorgeschlagene Formulierung würde dazu führen, dass die meldende Person der meldepflichtigen Organisation bekannt wird, da ihre Kontaktdaten gemäss Art. 19 Abs. 4 Bst. b weitergegeben werden. Dies könnte ein Hindernis für Drittmeldungen darstellen, da nicht

[4] Bspw. FINMA 05/2020, siehe: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20200507-finma-aufsichtsmitteilung-05-2020.pdf

meldepflichtige Personen oder Organisationen möglicherweise anonym bleiben möchten, was in diesem Fall nicht möglich wäre.

Deshalb schlagen wir folgende Änderungen vor:

Art. 20: Falls ~~die~~ ***eine*** *Meldung nicht über das Kommunikationssystem des BACS erfolgt, informiert dieses das BACS die Kontaktperson nach Artikel 13 Absatz 2 Buchstabe b* ***einer registrierten und von der Meldung betroffenen Organisation*** *über den Eingang und den Inhalt der Meldung,* ***indes ohne die Kontaktangaben der meldenden Organisation oder Person, es sei denn, auch die Kontaktangaben sind zum Schutz der Cybersicherheit erforderlich.***

Weitergehende Bemerkungen

Zudem möchten wir die Gelegenheit ergreifen, aufbauend auf der Zielsetzung des ISG und der CSV, vier weitere Diskussionspunkte zu nennen, die die Digitalwirtschaft beschäftigen:

Koordination des BACS

Ziel muss sein, dass meldepflichtige Akteure jeweils nur eine Meldung an eine Behörde machen. Das BACS spielt eine zentrale, koordinative Rolle, was die Meldepflicht betrifft. Wir regen an, dass das BACS sämtliche meldepflichtigen Vorfälle entgegennimmt und diese dann mit weiteren relevanten Behördenstellen koordiniert. Eine einzige Meldestelle verhindert Mehraufwand und Doppelspurigkeiten. Alternativ können wir uns auch vorstellen, dass sich Behörden, an welche gemeldet werden muss, (FINMA, EDÖB, BACS) untereinander koordinieren.

Meldeverhalten bei Schwachstellen

Unabhängig der gesetzlichen Meldevorschriften ist für digitalswitzerland und seine Mitglieder eine proaktive, offene Meldekultur bei Cyberschwachstellen von grosser Bedeutung. Artikel 9 zur koordinierten Offenlegung von Schwachstellen gibt die richtige Richtung vor, spezifiziert aber nur die Pflichten des BACS gegenüber Herstellern von Hard - bzw. Software und anderen Behörden. Komplementär ist es aber auch notwendig, gegenüber der Wirtschaft Anreize zu setzen, die ein proaktives Meldeverhalten fördern. Massnahmen und Instrumente zur Erhöhung von freiwilligen Meldungen sollten gemeinsam mit der Wirtschaft entwickelt, kontinuierlich getestet und weiterentwickelt werden.

Priorisierung von Meldungen

Unter Art. 8, Absatz 2 wird die Priorisierung von Meldungen bei Cyberangriffen unter Berücksichtigung öffentlicher Interessen festgehalten. Eine Liste der spezifischen Kriterien bzw. eine Abstufung der konkreten Schadensszenarien, nach denen priorisiert wird, wäre für die Digitalwirtschaft eine wichtige Hilfestellung.[5] digitalswitzerland hat schon in seiner Vernehmlassungsantwort zum neuen Militärgesetz

[5] In der laufenden Diskussion um die digitale Souveränität liefert die Swiss Data Alliance hilfreiche Ansätze für eine mögliche Bewertung eines Schadensszenarios. siehe: https://www.swissdataalliance.ch/publikationen/whitepaper-digitale-souveraenitaet

(insb. Art. 95) in Bezug auf eine sog. “ausserordentliche Lage in Friedenszeiten in Bezug auf Cyberbedrohungen” eine nachvollziehbare Kategorisierung angeregt.[6]

Vertrauen durch Zuverlässigkeit

Nicht zuletzt sehen wir in der Verordnung zum Informationssicherheitsgesetz einen wichtigen Schritt hin zur Förderung **einer vertrauenswürdigen digitalen Infrastruktur** für die Schweiz. Zuverlässige, von der Wirtschaft schnell umsetzbare Meldeabläufe bei Cyberangriffen sind dafür ein Grundpfeiler. digitalswitzerland ist überzeugt, dass diese Elemente die nächsten Jahre des Erfolges der Digitalisierung der Schweiz massgeblich prägen werden und stellt sich als Dialogpartner in diesen Fragen dem Bundesamt für Cybersicherheit jederzeit zur Verfügung.

Für Ihre Kenntnisnahme und für die wohlwollende Prüfung und Berücksichtigung unserer Anliegen, sehr geehrte Frau Bundesrätin Amherd, sehr geehrter Herr Suter, danken wir Ihnen.

Freundliche Grüsse,

Stefan Metzger
Managing Director digitalswitzerland
stefan@digitalswitzerland.com

Guillaume Gabus
Public Affairs & Management
guillaume@digitalswitzerland.com

---

*Der Austausch zwischen Wirtschaft, Wissenschaft, Behördenorganisation und Politik steht im Zentrum der Arbeit von **digitalswitzerland**. Mit Impulsen und konkreten Beiträgen sollen die Möglichkeiten der digitalen Technologien genutzt werden. Darüber hinaus müssen die damit verbundenen Risiken gemanagt und das Vertrauen der Menschen in die Technologien gefördert werden, um die Schweiz in eine führende digitale Nation zu transformieren. Mit der künstlichen Intelligenz hat ein neues Kapitel in der Digitalisierung begonnen. Besondere Prioritäten sind die Bildung, eine vertrauenswürdige digitale Infrastruktur, Cybersecurity, eSustainability, Digital Health und eGovernment. Die damit verbundenen Herausforderungen geht digitalswitzerland in enger Zusammenarbeit mit den über 170 Mitgliedern, Partnern und anderen Verbänden an.*

[6] Siehe Vernehmlassungsantwort von digitalswitzerland zur Revision des Militärgesetzes (Art. 95): https://digitalswitzerland.com/wp-content/uploads/2024/03/digitalswitzerland_-Vernehmlassung_Militargesetz_DE.pdf