Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS
Direktionsstab
Schwarztorstrasse 59
3003 Bern

ncsc@ncsc.admin.ch

Bern, 12.09.2024

Vernehmlassung ISSS zur Cybersicherheitsverordnung

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, uns zur Vernehmlassung zur Cybersicherheitsverordnung (CSV) äussern zu können.

Vorstellung Taskforce Cybersicherheitsverordnung ISSS

Die Information Security Society Switzerland (ISSS) http://www.isss.ch ist der führende Fachverband in der Schweiz auf dem Gebiet der ICT-Sicherheit, welchem heute mehr als 1'100 Einzel- und Firmenmitglieder aus Wirtschaft, Verwaltung und Wissenschaft angehören. ISSS setzt sich mit den technischen, wirtschaftlichen, regulatorischen und gesellschaftspolitischen Aspekten von ICT-Sicherheit und Informationsschutz auseinander.

ISSS wurde 1993 als Verein gegründet und ist Mitglied von Digitalswitzerland sowie offizieller Security Fachpartner von SwissICT sowie ASUT. Mit unseren Mitgliedern arbeiten wir in Taskforces, um Fachexpertise gezielt abzuholen und der Öffentlichkeit zur Verfügung zu stellen. Auch vorliegende Stellungnahme wurde in einer Taskforce erarbeitet.

Taskforce Lead ISSS

Dario Walder	Vizepräsident ISSS
Andrea Michel	Geschäftsleiterin ISSS

Organisationen & Fachexperten

Fridel Rickenbacher	Swiss IT Security AG
Bettina Löw	Wirtschaftsprüferin
Christoph Pfister	atrete AG
Michael Schläpfer	Fort IT
Valmir Gashi	CyberSinn
Alexander Heuzeroth	Swiss Infosec AG
Dario Stöckli	CISO Aebi Schmidt Group
Felix Burri	Burri Consulting GmbH

Die positive Zusammenarbeit der Bundesverwaltung und besonders des BACS (früher NCSC) mit der Privatwirtschaft, auch im Kontext der Cybersicherheitsverordnung, wird von uns begrüsst. Gerne geben wir untenstehend unsere Überlegungen zum Vernehmlassungsentwurf der Cybersicherheitsverordnung bekannt:

Art. 2, Nationale Cyberstrategie
Die hier vorliegende Definition lässt unseres Erachtens die angestrebte führende Rolle in der internationalen Zusammenarbeit aussen vor. Diese Rolle hat mit 3 (von 17) Massnahmen in der aktuellen Nationalen Cybersicherheitsstrategie ein vergleichsweises hohes Gewicht, ist in der vorliegenden Verordnung jedoch nirgends festgehalten.

Art. 3, Abs f Steuerungsausschuss
Wir unterstützen es, einen Steuerungsausschuss Nationale Cyberstrategie (StA NCS) einzusetzen. Das ist aus unserer Sicht eine sinnvolle Massnahme. Wir schlagen jedoch vor, bei der Zusammensetzung dieses Steuerungsausschusses auch Vertreterinnen und Vertreter von kritischen Infrastrukturen zu berücksichtigen. Deren Einbindung ist unabdinglich. Die Formulierung «Vertreter der Wirtschaft» ist diesbezüglich zu wenig klar.

Art. 5, Abs a Aufgaben des StA NCS
Der Artikel schreibt vor, dass der Steuerungsausschuss die NCS alle 5 Jahre überprüft. In einem dynamischen und sich stets wandelnden Umfeld sollte jedoch zusätzlich risikobasiert und bei besonderen Herausforderungen eine Kurskorrektur durchgeführt werden können.

Art 6, Halterabfragen
Hier fehlt unserer Ansicht nach die Kompetenz im Nachgang zu Angriffen (zum Bsp. Art. 7 1b), Halteranfragen zu machen sowie historische Halterinformationen zu beziehen.

Art. 7, Technische Analyse von Cybervorfällen und Cyberbedrohungen
Dieser Artikel regelt unserer Ansicht nach nicht, wem das CERT zur Verfügung steht. Das ist zwar implizit geregelt, respektive andernorts beschrieben, wir empfinden es dennoch als Mangel das in der Verordnung nicht zu erwähnen.

Absatz 1a und 1b legen Wert auf den technischen Fokus der Arbeit des CERT, Absatz 1c besitzt diesen Fokus nicht und gerade Bedrohungen sind nicht notwendigerweise technischer Natur, noch ist die Technik zwingend das definierende Element einer Bedrohung. Der Artikel ist also gegebenenfalls nochmals zu überdenken.

Was in unseren Augen fehlt, ist die Vorgabe die erarbeiteten Analysen im Regelfall zu publizieren. Gegebenenfalls in gekürzter Fassung, aber Transparenz und Öffentlichkeit scheint uns bei der Positionierung als nationales CERT wichtig.

Art 8, Priorisierung der Beratung und Unterstützung bei Cyberangriffen
Es ist in der Verordnung nicht vorgesehen, dass das CERT sich bei Cyberangriffen extern verstärken kann. Eine solche Verstärkung wäre gegebenenfalls anzudenken. Überhaupt ist die Zusammenarbeit mit den kritischen Infrastrukturen und die Abgrenzung in der Verordnung kaum geregelt. Der begleitende Bericht beschreibt diese Zusammenarbeit zwar und wir würden es begrüssen, dies in der Verordnung zu regeln.

Art. 19 Inhalt der Meldung
Abs. 1, 2, 3 umschreiben den Inhalt einer Meldung. Wir sind der Meinung, dass zwischen dem Inhalt der Erstmeldung und je nach Klassifizierung des Vorfalls zwischen weiteren Inhalten unterschieden

werden sollte. Art. 21 nimmt diesen Punkt indirekt auf, es wäre jedoch einfacher zwischen einer Erstmeldung und einer umfassenden Aufarbeitung zu unterscheiden. Dadurch könnte viel administrativer Aufwand vermieden werden. Wir möchten dadurch verhindern, dass beispielsweise kurze Systemausfälle bei einem eingeschränkten Personenkreis gemeldet werden müssen.

Generell ist bezüglich Meldepflichten zu evaluieren, ob diese mit europäischen Regularien, wie z.B. NIS-2[1], DORA[2], CRA[3] harmonisiert werden könnten, um hier u. a. den Organisationen und Unternehmen mit Europabezug nicht unnötig Aufwand zu generieren.

Ziel muss sein, dass meldepflichtige Akteure jeweils nur eine Meldung an eine Behörde machen. Wir sehen das BACS in einer zentralen, koordinativen 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. Zusätzlich können wir uns auch vorstellen, dass sich Behörden, an welche gemeldet werden muss (FINMA, EDÖB, BACS) untereinander koordinieren.

Im Rahmen der Meldung müssen auch Angaben zum Verursacher der Cyberattacke gemacht werden. Dies bedingt aufwändige forensische Verfahren und ist äusserst komplex. Aus unserer Sicht sollen die Unternehmen nicht Aufgaben im Bereich der Strafverfolgung übernehmen müssen - dies müsste zumindest freiwilliger Natur sein.

Inputs zum erläuternden Bericht zur Eröffnung des Vernehmlassungsverfahrens

- Art. 9 Abs. 5 umschreibt die Bekanntgabe der Schwachstelle vor Behebung oder Veröffentlichung. In diesem Zusammenhang würde uns interessieren, wie die Interessensabwägung funktioniert und was die ausschlaggebenden Faktoren sind, ab wann die Informationen weitergegeben werden.
- Art. 15 Abs 3 erläutert die Übermittlung und Nutzung der Informationen. Gibt es in diesem Zusammenhang Voraussetzungen oder Prüfungen, die ein Informationsempfänger erfüllen muss, um am Informationsaustausch teilnehmen zu dürfen?[4]

Wir hoffen, dass wir mit unserer Stellungnahme einen Beitrag zur Förderung der ICT-Sicherheit, dem Informationsschutz und dem konstruktiven Dialog in unserem Lande leisten können und danken Ihnen für die Berücksichtigung unserer Anregungen.

Mit freundlichen Grüssen

Dario Walder

ISSS Vize Präsident
Information Security Society Switzerland (ISSS)
Zentweg 13
3006 Bern
E-Mail: vicepresident@isss.ch

[1] European Union – EUR Lex - https://eur-lex.europa.eu/eli/dir/2022/2555

[2] Digital Operational Resilience Act (DORA) - https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

[3] European Commission – EU Cyber Resilience Act - https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[4] Hier möchten wir insbesondere auf die NIS-2 Richtlinie hinweisen: NIS-2 (RICHTLINIE (EU) 2022/2555) Art. 9 Abs. 5 CSV. Koordination der Offenlegung von Schwachstellen: NIS-2: Art. 12 Tätigkeit der mit der Koordination beauftragten Behörde: NIS-2: Art. 11.