Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Ausschliesslich per E-Mail an:
ncsc@ncsc.admin.ch

13. September 2024

Stellungnahme zur Vernehmlassung des Bundesrates zum Erlass der Cybersicherheitsverordnung (CSV)

Sehr geehrte Damen und Herren

Im Mai 2024 haben Sie uns eingeladen, in oben genannter Sache Stellung zu nehmen. Diese Gelegenheit der Meinungsäusserung nehmen wir gerne wahr. economiesuisse nimmt gestützt auf den Input der betroffenen Mitglieder und aus einer übergeordneten, gesamtwirtschaftlichen Sicht wie folgt Stellung:

Zusammenfassung
economiesuisse unterstützt die Einführung einer schlanken und effizienten Meldepflicht für Betreiberinnen kritischer Infrastrukturen bei Cyberangriffen. Bereits das ISG hat diesem Anspruch nicht ausreichend Rechnung getragen. Die Ausführungsbestimmungen in der Vernehmlassungsvorlage gehen nun sogar noch über das Gesetz hinaus. Folgende Anpassungen für praxistaugliche Meldeprozesse sind unverzichtbar:

- Bessere Koordination und Harmonisierung mit anderen Vorschriften und Meldeverfahren, bspw. mit dem Datenschutzrecht oder dem Finanzmarktrecht.
- Weniger Formalismus und Detailregulierung, mehr partnerschaftliches und flexible, situationsgerechte Zusammenarbeit zwischen Bundesbehörden und Betreiberinnen kritischer Infrastrukturen. Dies gilt vor allem für die genaue Gestaltung der Meldeabläufe.
- Der Willen des Gesetzgebers ist besser zu berücksichtigen, insb. in Form von praktikablen Ausnahmeregeln von den neuen Meldepflichten. Ebenso ist auf einzelne Bestimmungen zu verzichten, denen eine explizite Rechtsgrundlage im ISG fehlt.
- Einführung einer Übergangsfrist von mindestens einem Jahr.

economiesuisse teilt die Einschätzung, dass aufgrund der rasant steigenden Zahl der Cyberangriffe auf Schweizer Unternehmen und Institutionen geeignete Schutzmassnahmen vorgekehrt werden müssen. Dies gilt im Speziellen für sog. kritische Infrastrukturen, welche aus systemischer Sicht eine erhöhte Resilienz aufweisen müssen, damit sie ihre versorgungskritische Funktion für Wirtschaft und Gesellschaft auch bei einem Cybervorfall oder -angriff erfüllen können. Im Lichte dieser Überlegungen

economiesuisse
Hegibachstrasse 47
Postfach
CH-8032 Zürich
Telefon +41 44 421 35 35

Verband der Schweizer Unternehmen
Fédération des entreprises suisses
Federazione delle imprese svizzere
Swiss Business Federation
www.economiesuisse.ch

hat das Parlament im vergangenen Herbst neue Meldepflichten für Betreiberinnen kritischer Infrastrukturen beschlossen.

Bereits im Rahmen dieser Revision des Informationssicherheitsgesetzes (ISG) haben wir folgende Kernanliegen der Gesamtwirtschaft eingebracht:

- Die Meldepflicht muss den betroffenen Unternehmen und der Volkswirtschaft letztlich mehr bringen, als sie kostet.
- Sie muss einen verhältnismässigen, subsidiären, risikobasierten Ansatz verfolgen, der administrative und finanzielle Aufwände auf ein Minimum reduziert.
- Es bedarf einer kooperativen Grundeinstellung, da sowohl die Behörden als auch die Unternehmen an einem bestmöglichen Schutz vor Cyber-Angriffen interessiert sind. Dabei müsste grundsätzlich von autoritären Massnahmen wie Bussen und Audits soweit möglich Abstand genommen werden, da sie die partnerschaftliche Basis der Zusammenarbeit in Frage stellen.

Im Kontext der Vernehmlassungsvorlage stellen wir generell Folgendes fest:

- Es fehlt nach wie vor an Koordination bzw. Harmonisierung der multiplen Meldeverfahren bei Cyberangriffen. So müssen Unternehmen (z.B. im Versicherungs- und Bankenbereich und der Luftfahrt) bei Cyberangriffen nicht selten gleich mehreren Verwaltungseinheiten Meldung machen (z.B. EDÖB, FINMA, BACS, BAZL) - und dies mit jeweils unterschiedlichen Inhalten und Fristen. Im Hinblick auf die breite Betroffenheit Schweizer Unternehmen vom EU Digital Operational Resilience Act kommen nebst der nationalen auch auf internationaler Ebene zusätzliche Anforderungen. Es ist deshalb auf Lösungen für eine Harmonisierung/Koordination der einzelnen Meldeverfahren hinzuwirken. Im Übrigen plädieren wir dafür, dass man die Meldepflichten an internationalen Standards auszurichten. Beispielsweise sollten die Fristen jenen der NIS-2-Richtlinie anpassen werden (24 Stunden für eine Frühwarnung, 72 Stunden für die Meldung eines Vorfalls). Die Meldequalität sollte gegenüber der Meldegeschwindigkeit im Vordergrund stehen.

- Bei der CSV handelt es sich um eine Ausführungsverordnung, welche nicht über die Konkretisierung des Gesetzes hinausgehen darf. Zahlreiche vorgeschlagene Regelungen gehen jedoch über den Willen des Gesetzgebers hinaus oder verfügen damit über Grundlage im Gesetz. Dies betrifft insbesondere die nationale Cyberstrategie und den Steuerungsausschuss (Art. 2-5 E-CSV). Zu beidem findet sich in der gesetzlichen Grundlage weder eine Bestimmung noch eine Delegationsklausel. Es ist generell fragwürdig, wenn solche Aspekte auf Verordnungsebene geregelt werden – auch wenn sie auf historisch gewachsenen Begebenheiten basieren (siehe auch Art. 164 Abs. 1 Bundesverfassung, wonach «Wichtiges» wie die Organisation der Bundesbehörden in einem Gesetz im formellen Sinn geregelt werden muss)

- Es ist festzuhalten, dass das "Bundesamt für Cybersicherheit" (BACS) seit dem 1. Januar 2024 das Nationale Zentrum für Cybersicherheit (NCSC) abgelöst hat. Diese Änderung hat im Schlussabstimmungstext der ISG-Revision vom 29. September 2023 noch keinen Eingang gefunden. Um Missverständnisse zu vermeiden, sollte diese Änderung im ISG baldmöglichst noch nachgezogen werden und ansonsten ist darauf zu achten, dass diese Änderung genug klar kommuniziert wird, damit dies auch für die Betroffenen der neuen Meldevorschriften verständlich ist.

- Bereits bei der Revision des ISG haben wir den unklaren Geltungsbereich als kritischer Punkt hervorgehoben. Auch im aktuellen Verordnungsentwurf bleiben Unsicherheiten, bspw.

hinsichtlich Betroffenheit von Unterlieferanten, wie etwa Cloud-Computing-Dienstleistern, Anbieterinnen von Sicherheitssoftware oder Suchmaschinen. Wir sind hier klar der Meinung, dass der Einbezug solcher Lieferanten nicht regulatorisch, sondern vertraglich zwischen den Betreiberinnen kritischer Infrastrukturen und ihren Lieferanten zu regeln ist.

- Ein Inkrafttreten per 1. Januar 2025 ist zu früh. Der endgültige Wortlaut der Regelung wird erst mit der offiziellen Veröffentlichung der Verordnung feststehen, was vermutlich erst kurz vor dem 1. Januar 2025 der Fall sein wird. Viele Unternehmen werden daher bis dahin nicht wissen, ob und inwiefern sie von der Regelung betroffen sind. Auch das angekündigte Meldeformular könnte bis Ende 2024 noch nicht vollständig ausgearbeitet sein. Es bedarf deshalb eine Umsetzungsfrist von mindestens einem Jahr.

Zu folgenden Artikeln nehmen wir ausführlicher Stellung:

Art. 4 E-CSV Zusammensetzung Steuerungsausschuss Nationale Cyberstrategie
Laut einer Medienmitteilung des BACS vom 7. Juni 2024 hat das VBS bereits den Steuerungsausschuss für die Nationale Cyberstrategie eingerichtet. Die Wirtschaft wird dort durch asut, future technologies und WiseStratEdge vertreten. Es wäre sinnvoll, zusätzlich zu diesen Vertretern auch ausdrücklich die Betreiber kritischer Infrastrukturen einzubeziehen. Obwohl es sicherlich Überschneidungen mit der Wirtschaftsvertretung gibt, sollte diese besonders betroffene Gruppe gezielt berücksichtigt werden. Zudem finden wir es fragwürdig, dass die Zusammensetzung des Steuerungsausschusses bereits vor Inkrafttreten der CSV festgelegt wurde.

Art. 7 E-CSV Technische Analyse von Cybervorfällen und Cyberbedrohungen
Betreffend die technische Analyse von Cybervorfällen und Cyberbedrohungen, plädieren wir für eine gemeinsame Präzisierung der Leistungen und der Zusammenarbeit zwischen BACS und privaten CERTs, sowie von der Meldepflicht betroffenen Unternehmen der kritischen Infrastrukturen. Um dies zu besprechen, braucht es ein entsprechendes Stakeholder-Treffen, welches wir entsprechend sehr begrüssen würden.

Art. 9 E-CSV Koordinierte Offenlegung von Schwachstellen

Antrag:
Art. 9 Abs. 1 und 2 E-CSV

[1]Das BACS sorgt nach deren Behebung für die koordinierte Offenlegung der Schwachstellen nach international anerkannten Standards.
[2]Es setzt der Herstellerin der betroffenen Hard- oder Software eine angemessene Frist ~~von 90 Tagen~~ zur Behebung der Schwachstellen.

Begründung:
Koordinierte Offenlegung nach Behebung der Schwachstellen: Die Anpassung, dass die Offenlegung der Schwachstellen erst nach deren Behebung erfolgt, basiert auf den Diskussionen im Rahmen der Revision ISG. Dort hat sich das Parlament bewusst gegen eine Offenlegungspflicht von Schwachstellen (vor ihrer Behebung) ausgesprochen. Die Offenlegung einer Schwachstelle vor ihrer Behebung bringt erhebliche Risiken für die betroffenen Systeme und deren Nutzerinnen und Nutzer mit sich. Durch die vorgeschlagene Änderung wird gewährleistet, dass mögliche Angriffspunkte erst dann

publik gemacht werden, wenn die Schwachstellen bereits geschlossen sind, was die Sicherheit und den Schutz der betroffenen Systeme erhöht.
Anpassung der Frist auf "angemessen": Die Änderung der starren 90-Tage-Frist in eine flexible, „angemessene“ Frist berücksichtigt die Komplexität und Variabilität moderner Hard- und Softwarelandschaften. Die ständige Weiterentwicklung und Diversifikation der Systeme erfordert eine flexible Handhabung der Fristen zur Schwachstellenbehebung. Ein „One-Size-Fits-All“-Ansatz, bei dem pauschal 90 Tage als Frist, könnte in einigen Fällen zu einer hastigen und möglicherweise unzureichenden Behebung führen, was die Qualität der Sicherheitsmassnahmen beeinträchtigen könnte. Ein flexibleres System erlaubt es, die Frist entsprechend der Art und Schwere der Schwachstelle sowie den spezifischen Umständen der betroffenen Herstellerin anzupassen, um so eine gründliche und qualitativ hochwertige Behebung sicherzustellen.

Art. 11 E-CSV Kommunikationssystem für den sicheren Informationsaustausch

Antrag:
Art. 11 Abs. 1 E-CSV

[1]Zugang zum Kommunikationssystem des BACS für den sicheren Informationsaustausch (Artikel 74 Abs. 2 Buchstabe a ISG) haben meldepflichtige Organisationen und Behörden ~~mit Sitz in der Schweiz~~ ,

Begründung:
Basierend auf den bisherigen Erfahrungen mit dem Informationsaustausch über den Cyber Security Hub (CSH) des BACS scheint der aktuelle Formulierungsvorschlag unnötig restriktiv zu sein. Es sollten alle im Land tätigen Betreiber kritischer Infrastrukturen (Art. 74 rev. ISG) – auch jene ohne Sitz in der Schweiz – am Informationsaustausch teilnehmen dürfen. Für globale Unternehmen ist der länderübergreifende Austausch von entscheidender Bedeutung. Auf dem Finanzplatz wird dies bereits erfolgreich umgesetzt, indem auch Zweigniederlassungen ausländischer Finanzinstitute mit FINMA-Bewilligung am CSH teilnehmen können. Dieses Prinzip sollte bei der Gestaltung von Art. 11 Abs. 1 E-CSV ebenfalls berücksichtigt werden.

Art. 13 E-CSV Registrierung

Antrag:
Art. 13 Abs. 2 E-CSV

Streichen.

Eventualiter:
Art. 13 Abs. 2 lit. b E-CSV
[2] Die Registrierung muss mindestens folgende Informationen enthalten:
a. Firma, Name oder Bezeichnung und Adresse;
b. ~~Kontaktangaben der gemeldeten Person.~~ Angaben zu einer oder mehreren Kontaktpersonen.

Begründung:
Die Festlegung der Registrierungskriterien ist zu detailliert und formalistisch für eine Verordnung. Dies vor allem, da Firma und Adresse offensichtlich sind. Somit ist Art. 13 Abs. 2 streichen. Alternativ sollte Art. 13 Abs. 2 lit. b immerhin zu «Angaben zu einer oder mehreren Kontaktpersonen» geändert werden.

Die jetzige Formulierung impliziert eine Verantwortlichkeit der gemeldeten Person, dabei soll es laut Botschaft lediglich eine Kontaktperson sein.

Art. 16 E-CSV Ausnahmen von der Meldepflicht

Antrag:
Art. 16 Abs. 2 E-CSV
[2] Unternehmen nach Artikel 74b Absatz 1 Buchstaben f, g, h, l und p ISG, ~~für die Absatz 1 nicht anwendbar ist~~, sind von der Meldepflicht ausgenommen, sofern sie ~~im betroffenen Bereich weniger als 50 Personen beschäftigen und ihr Jahresumsatz beziehungsweise ihre Jahresbilanzsumme im betroffenen Bereich 10 Millionen Franken nicht übersteigt~~ jeweils am 1. Januar eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen.

Begründung:
Der Gesetzgeber hat hier bewusst eine offene Formulierung gewählt und die Konkretisierung dieser Bestimmung dem Bundesrat übertragen, um eine praxisnahe Lösung zu erwirken. Ausnahmen aufgrund der Grösse der Unternehmen festzulegen, ist grundsätzlich ein praktikabler Ansatz. Die Definition eines kleinen Unternehmens sollte jedoch mit anderen, ähnlichen Schweizer Bestimmungen kohärent sein und nicht neue Massstäbe setzen. Eine Begründung für den gewählten Ansatz in den Erläuterungen ist nicht ersichtlich. Gemäss Bundesamt für Statistik (BfS) sind in der Schweiz mindestens in statistischer Hinsicht marktwirtschaftliche Unternehmen mit weniger als 250 Beschäftigten als kleine und mittlere Unternehmen definiert. Entsprechend hat bspw. diese Grösse auch Eingang in Art. 24 DSV gefunden, welche Unternehmen, die jeweils am 1. Januar eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, von der Verzeichnisführungspflicht gemäss DSG ausgenommen hat. Somit sollte diese Definition auch in der CSV übernommen werden.

Art. 18 E-CSV Zu meldende Cyberangriffe

Antrag:
Art. 18 E-CSV Abs. 1, Abs. 2

[1] Die Funktionsfähigkeit einer kritischen Infrastruktur gilt als durch einen Cyberangriff gefährdet, wenn:
a. Gleichzeitig mehrere Mitarbeitende oder systemrelevante Dritte von absichtlich durch den Cyberangriff verursachten Systemunterbrüchen betroffen sind; oder (…).

[2] Eine Manipulation oder ein Abfluss von Informationen liegt vor, wenn:
a. geschäftsrelevante Informationen von Unbefugten verändert oder offengelegt ~~werden~~, entwendet, zerstört, deaktiviert oder sonst wie bearbeitet werden, welche sich mittel- oder langfristig auf wesentliche Applikationen oder Systeme auswirken; oder
b. eine Verletzung der Datensicherheit nach Artikel 24 des Datenschutzgesetzes vom 25. September 2020 vorliegt, welche voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt.

Begründung:
Das Informationssicherheitsgesetz verlangt die Meldung eines erfolgreichen Cyberangriffs, wenn dieser die Funktionsfähigkeit kritischer Infrastrukturen gefährdet (Art. 74d). Wichtig ist, dass nur erfolgreiche Angriffe mit funktionalen Folgen meldepflichtig sind, um unnötigen Verwaltungsaufwand zu vermeiden. Ein reiner Phishing-Angriff ohne funktionalen Schaden sollte nicht gemeldet werden müssen.

Der Bundesrat stellt klar, dass nur gezielte und absichtliche Angriffe meldepflichtig sind, wie in Art. 5 lit. e nISG definiert. Unbeabsichtigte Ausfälle, etwa durch Fehlbedienung, fallen nicht unter die Meldepflicht. Ein Angriff ist meldepflichtig, wenn er absichtlich die Vertraulichkeit, Verfügbarkeit oder Integrität beeinträchtigt.

Der Begriff „Systemunterbruch" sollte so definiert werden, dass nur Unterbrechungen mit systemrelevanten Folgen gemeldet werden müssen, nicht jedoch solche durch Wartungsarbeiten oder den Ausfall weniger kritischer Systeme. Auch „Dritte" sollten nur dann meldepflichtig sein, wenn deren Ausfall kritische Infrastrukturen betrifft. Grundsätzlich wäre es gut, wenn die Meldevorschriften internationalen Standards entsprechen.

Schliesslich sollte die Schwelle für die Meldung von Datensicherheitsverletzungen an die Anforderungen des Datenschutzgesetzes angepasst werden. Eine Meldung ist nur nötig, wenn ein hohes Risiko für die betroffene Person besteht. Ein Angriff, der gemeldet werden muss, liegt nur vor, wenn er erhebliche Auswirkungen auf Systeme hat und die Schutzziele gefährdet.

Art. 19 E-CSV Inhalt der Meldung

Antrag:
Art. 19 Abs. 3

Streichen.

Begründung:
Art. 74e nISG spricht nur von Informationen zur Art und Ausführung des Cyberangriffs, zu seinen Auswirkungen, zu ergriffenen Massnahmen und - soweit bekannt - zum geplanten Vorgehen. Art. 19 Abs. 3 E-CSV geht darüber hinaus. Ebenso sind die relevanten Informationen im Ernstfall stark kontextabhängig, weshalb eine derart detaillierte Regelung unnötig starr ist. Entsprechend sollte Art. 19 Abs. 3 m.E. gestrichen werden. Darüber hinaus begrüssen wir explizit, dass Art. 19 Abs. 4 auch Meldungen einschliesst, die nicht über das Informationssystem erflogen, denn damit kann Art. 13 CSV klar als bedingte Registrierungspflicht gelesen werden. Eine solche besteht dann nur, wenn eine meldepflichtige Organisation sich freiwillig entscheidet, über das NCSC-Kommunikationssystem zu kommunizieren.

Art. 20 E-CSV Übermittlung der Meldung

Antrag:
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.

Begründung:
Wir verstehen diesen Artikel so, dass es sich dabei um eine Meldung durch eine Drittperson handelt, welche an sich nicht meldepflichtig wäre, deren Meldung aber eine (weitere) registrierte Organisation betrifft. In diesem Falle würde die nun vorgeschlagene Formulierung bedeuten, dass die meldende Person gegenüber der meldepflichtigen Organisation bekannt wird. Denn diese muss gemäss Art. 19 Abs. 4 Bst. b deren Kontaktangaben bekannt geben, womit diese zum Inhalt der Meldung werden, welche

weitergegeben wird. Dies kann ein mögliches Hindernis für Drittmeldungen darstellen. Nicht meldepflichtige Personen/Organisationen möchten ggf. anonym bleiben, das bei dieser Vorgabe nicht möglich wäre.

Gerne verweisen wir ausserdem auf die Stellungnahmen unserer Mitglieder.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse

economiesuisse

Lukas Federer
Stv. Bereichsleiter Umwelt, Energie und Infrastruktur

Leonie Ritscher
Projektleiterin Wettbewerb & Regulatorisches