CH++

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
Bundesrätin Viola Amherd
Eingabe per Mail an: ncsc@ncsc.admin.ch

Vernehmlassungsantwort zur Cybersicherheitsverordnung (CSV)

Mit grossem Interesse haben wir die Vernehmlassung zur Cybersicherheitsverordnung zur Kenntnis genommen. Unsere Organisation CH++ widmet sich unabhängig einer nachhaltigen, wohlhabenden und handlungsfähigen Schweiz durch Wissenschaft und Technologie — und dazu gehört fraglos auch die Cybersicherheit. Gerne nehmen wir entsprechend hiermit von der Möglichkeit gebrauch, Ihnen unsere Vernehmlassungsantwort zukommen zu lassen.

CH++ begrüsst die Stossrichtung des Entwurfs und hält ihn für zweckdienlich, um die Sicherheit des Landes effektiv, kollaborativ und vertrauenswürdig zu erhöhen. Punktuell sind allerdings Schärfungen und Klärungen nötig, die wir gerne im Folgenden erläutern.

Die vorgeschlagene Cybersicherheitsverordnung stellt einen wichtigen Schritt zur Stärkung der Cybersicherheit in der Schweiz dar. Mit den von uns vorgeschlagenen Präzisierungen und Ergänzungen könnte die Wirksamkeit der Verordnung noch weiter erhöht werden. Wir danken Ihnen für die Berücksichtigung unserer Anmerkungen und stehen Ihnen für weiteren Dialog stets gerne zur Verfügung.

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

2. Abschnitt: Nationale Cyberstrategie und Steuerungsausschuss Art. 2 Nationale Cyberstrategie 1 Die Nationale Cyberstrategie (NCS) legt den strategischen Rahmen für die Prävention im Bereich der Cybersicherheit, die Früherkennung von Cyberbedrohungen, die Reaktionsmöglichkeiten und die Resilienz bei Vorfällen sowie die Bekämpfung der Cyberkriminalität fest. 2 Sie wird in Abstimmung mit den Kantonen festgelegt.	Wir begrüßen grundsätzlich die Festlegung einer Nationalen Cyberstrategie (NCS). Allerdings sehen wir mit Besorgnis, dass laut Artikel 2, Absatz 2 die NCS nur "in Abstimmung mit den Kantonen" festgelegt wird. Dies wirft die Frage auf, inwiefern zukünftig gewährleistet ist, dass die NCS nicht ausschließlich durch Teilnehmende aus Bund und Kantonen festgelegt wird.
Art. 4 Zusammensetzung des StA NCS 1 Der StA NCS setzt sich aus Vertreterinnen und Vertretern der Departemente, der Bundeskanzlei, der Kantone, der Wirtschaft, der Gesellschaft und der Hochschulen zusammen. 2 Der Bundesrat bestimmt alle fünf Jahre die Mitglieder des StA NCS, mit Ausnahme der Vertreterinnen und Vertreter der Kantone; diese werden von der Konferenz der Kantonsregierungen bestimmt. 3 Er ernennt aus dem Kreis der Vertreterinnen und Vertreter der Wirtschaft, der Gesellschaft und der Hochschulen die	Die breite Zusammensetzung des Steuerungsausschusses ist grundsätzlich zu begrüssen. Allerdings fehlen klare Kriterien für die Auswahl der Mitglieder, insbesondere aus Wirtschaft, Gesellschaft und Hochschulen. Wir schlagen vor, transparente Auswahlkriterien festzulegen, die sicherstellen, dass die Mitglieder über die notwendige Expertise im Bereich Cybersicherheit verfügen. Dabei sollte besonders darauf geachtet werden, dass ausgewiesene Sicherheitsexperten angemessen vertreten sind. Die aktuelle Zusammensetzung, bei der nur eine von drei Vertretern der Wirtschaft eine

vorsitzende Person.	ausgewiesene Sicherheitsexpertin ist, erscheint uns nicht ausgewogen.
Art. 7 Technische Analyse von Cybervorfällen und Cyberbedrohungen 1 Das BACS betreibt das nationale Einsatzteam für Computersicherheit (Computer Emergency Response Team [CERT]), das insbesondere die folgenden Aufgaben wahrnimmt: a. technische Vorfallbewältigung; b. Analyse technischer Fragestellungen; c. Identifikation und Beurteilung von Cyberbedrohungen. 2 Es betreibt für die Analyse der Cybervorfälle und Cyberbedrohungen eine resiliente Infrastruktur; diese muss unabhängig von der restlichen Bundesinformatik funktionieren	Der Begriff “CERT” ist eine urheberrechtlich geschützte Marke. Um allfälligen künftigen Komplikationen aus dem Weg zu gehen, bietet es sich an, den Begriff CSIRT (Computer Security Incident Response Team) zu nutzen. “Resilient” ist aus unserer Sicht ein nicht genügend präziser Begriff. Wir schlagen vor, mittels einer Formulierung wie der folgenden zusätzliche Klarheit zu schaffen: “Der Betrieb dieser Infrastruktur muss jederzeit und möglichst unabhängig von Dritten sichergestellt werden können.” Zudem stellt sich die Frage nach der technischen Infrastruktur für die Analysen. Es sollte präzisiert werden, ob und inwiefern Cloud-Dienste für die technischen Analysen verwendet werden dürfen. Falls ja, wie werden diese Cloud-Dienste ausgewählt? Handelt es sich um vom Bund betriebene oder kommerziell verfügbare Dienste? Wie werden wichtige Sicherheitsaspekte wie Abhängigkeit und Verfügbarkeitsgarantie geregelt?

Art. 9 Koordinierte Offenlegung von Schwachstellen 1 Das BACS sorgt für die koordinierte Offenlegung der Schwachstellen nach international anerkannten Standards. 2 Es setzt der Herstellerin der betroffenen Hard- oder Software eine Frist von 90 Tagen zur Behebung der Schwachstellen. 3 Es kann die Frist verkürzen, wenn eine Schwachstelle: a. die Funktionsfähigkeit von kritischen Infrastrukturen gefährdet; b. besonders leicht für einen Cyberangriff ausgenutzt werden kann; oder c. weit verbreitete Systeme betrifft. 4 Es kann die Frist verlängern, wenn sich die Behebung der Schwachstelle als besonders aufwendig erweist. 5 Es kann die Betreiberinnen kritischer Infrastrukturen bereits vor der Behebung oder Offenlegung über Schwachstellen informieren.	Wir schlagen vor, Punkt 4 strenger zu formulieren, um sicherzustellen, dass die Fristen nicht in zu vielen verlängert werden, bzw. um den Druck leicht zu erhöhen: Fristen dürfen nur “in begründeten Ausnahmefällen" verlängert werden. Wir schlagen vor, Punkt 5 zu schärfen. Es gilt hier sicherzustellen, dass möglichst nicht der Eindruck entstehen kann, das VBS behalte Informationen über Sicherheitslücken in riskanten Situationen zurück, um diese allenfalls selbst länger offensiv nutzen zu können. Entsprechend schlagen wir vor, die Kann-Formulierung abzuändern zu: “Es informiert grundsätzlich die Betreiberinnen kritischer Infrastrukturen bereits vor der Behebung oder Offenlegung über Schwachstellen.”

6 Auf die vom Bundesamt für Kommunikation (BAKOM) im Rahmen seiner Aufsichtskontrollen (Art. 36 ff. der Verordnung vom 25. November 20152 über Fernmeldeanlagen) entdeckten Schwachstellen sind die Absätze 1 bis 4 nicht anwendbar. Das BAKOM informiert in solchen Fällen das BACS. 7 Das BACS informiert das BAKOM umgehend über die in Fernmeldeanlagen nach Artikel 3 Buchstabe d des Fernmeldegesetzes vom 30. April 19973 entdeckten Schwachstellen.	
5. Abschnitt: Meldepflicht Art. 16 Ausnahmen von der Meldepflicht 1 Die folgenden Behörden und Organisationen sind unter den nachstehenden Voraussetzungen von der Meldepflicht ausgenommen: a. Stellen nach Artikel 74b Absatz 1 Buchstaben b und c ISG: sofern sie für weniger als 1000 Einwohnerinnen und Einwohner zuständig sind; massgeblich ist die ständige Wohnbevölkerung; b. Unternehmen nach Artikel 74b Absatz 1 Buchstabe d ISG, sofern sie:	Die Spitäler sollten unabhängig von ihrer Grösse als meldepflichtig qualifiziert werden, da sie eine kritische Rolle in der Gesundheitsversorgung spielen. Zudem fehlt eine Regelung zum Umgang mit Kumulations-Risiken. Wie wird vorgegangen, wenn viele kleine, nicht meldepflichtige Organisationen betroffen sind und dies in der Summe ein wesentliches Risiko ergibt? Dies ist besonders relevant, da durch die zunehmende Vernetzung auch größere Organisationen im Sinne einer Kaskadierung betroffen sein können. Wir schlagen vor, einen Mechanismus zur Erfassung und Bewertung solcher

1. als Netzbetreiber, Elektrizitätserzeuger, Elektrizitätsspeicherbetreiber oder Dienstleister im Elektrizitätsbereich gemäss Artikel 5a Absatz 1 und Anhang 1a der Stromversorgungsverordnung vom 14. März 20084 weder das Schutzniveau A noch das Schutzniveau B einhalten müssen, 2. als Betreiber von Gasleitungen nach Artikel 2 Absatz 3 der Rohrleitungssicherheitsverordnung vom 4. Juni 20215 im Durchschnitt der letzten fünf Jahre eine transportierte Energie von weniger als 400 GWh/Jahr aufweisen; c. Unternehmen nach Art. 74b Absatz 1 Buchstabe n ISG, sofern sie: 1. kein Information Security Management System nach den Artikeln 2 und 4 und dem Anhang II der Verordnung (EU) 2023/2036 oder nach Artikel 2 und dem Anhang II der Verordnung (EU) 2022/16457 einrichten müssen, 2. die Vorgaben nach Punkt 1.7 des Anhangs der Verordnung (EU) 2015/19988 in ihrem Security-Programm nach Artikel 2, 12, 13 oder 14 der Verordnung (EG) 300/20089 nicht umsetzen müssen; d. Eisenbahnunternehmen sowie Seilbahn-,	kumulativen Risiken in die Verordnung aufzunehmen.

Trolleybus-, Autobus- und Schifffahrtsunternehmen nach Artikel 74b Absatz 1 Buchstabe m ISG, sofern sie: 1. nicht mit Systemaufgaben (Art. 37 des Eisenbahngesetzes vom 20. Dezember 195710 [EBG]) beauftragt sind, 2. über eine Personenbeförderungskonzession nach Artikel 6 des Personenbeförderungsgesetzes vom 20. März 200911 (PBG) verfügen, aber keine durch Bund und Kantone gemeinsam bestellten Angebote erbringen (Art. 28–31c PBG), 3. sie über eine Infrastrukturkonzession nach Artikel 5 EBG verfügen, diese aber nicht erteilt wurde, weil ein öffentliches Interesse am Bau und Betrieb der Infrastruktur besteht (Art. 6 Abs. 1 Bst. a EBG); e. Anbieterinnen und Betreiberinnen nach Artikel 74b Absatz 1 Buchstabe t ISG: sofern sie einen Sitz in der Schweiz haben und ihre Leistungen weder teilweise noch vollumfänglich gegen Entgelt für Dritte erbringen. 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.	