Verordnung über die Cybersicherheit
(Cybersicherheitsverordnung, CSV)

vom XX.XX.2024

Der Schweizerische Bundesrat,
gestützt auf die Artikel 74*c* und 84 Absatz 1 des Informationssicherheitsgesetzes vom 18. Dezember 2020[1], *verordnet:*

1. Abschnitt: Gegenstand

Art. 1

Diese Verordnung regelt:

a. die Nationale Cyberstrategie und deren Steuerungsausschuss;
b. die Aufgaben des Bundesamtes für Cybersicherheit (BACS);
c. den Informationsaustausch des BACS mit Behörden und Organisationen zum Schutz vor Cybervorfällen und Cyberbedrohungen;
d. die Meldepflicht für Cyberangriffe.

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.

Art. 3 Einsetzung und Organisation des StA NCS

[1] Der Bundesrat setzt einen Steuerungsausschuss Nationale Cyberstrategie (StA NCS) ein.

[2] Der StA NCS verfügt über ein Sekretariat; das Bundesamt für Cybersicherheit (BACS) betreibt das Sekretariat.

1 SR **128**

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 vorsitzende Person.

Art. 5 Aufgaben des StA NCS

Der StA NCS hat folgende Aufgaben:

a. Er überprüft die NCS mindestens alle fünf Jahre, wirkt bei ihrer Weiterentwicklung mit und erarbeitet bei Bedarf Anpassungsvorschläge.

b. Er erarbeitet in Absprache mit den in der NCS aufgeführten Akteuren Vorschläge für die Prioritäten und Zeitpläne für die Umsetzung der Massnahmen der NCS.

c. Er beurteilt laufend die Umsetzung der Massnahmen und informiert den Bundesrat und die Kantone über Verzögerungen.

d. Er unterbreitet dem Bundesrat bei Bedarf Vorschläge für ergänzende Massnahmen.

e. Er erstattet dem Bundesrat, den Kantonen und der Öffentlichkeit jährlich Bericht über die Umsetzung der NCS.

3. Abschnitt: Aufgaben des BACS

Art. 6 Halterabfragen

Das BACS kann zur Warnung von Behörden, Organisationen und Personen bei unmittelbaren Cyberbedrohungen oder laufenden Cyberangriffen bei der Registerbetreiberin von Domain-Namen, die in die Kompetenz des Bundes fallen oder die diesen Domain-Namen untergeordnet sind, die Kontaktangaben der Halter von Domain-Namen abfragen.

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.

Art. 8 Priorisierung der Beratung und Unterstützung bei Cyberangriffen

[1] Übersteigt die Nachfrage nach Beratung und Unterstützung bei einem Cyberangriff die Kapazitäten des BACS, so kann es die Bearbeitung in Bezug auf den Zeitpunkt und den Umfang der Beratung und Unterstützung priorisieren.

[2] Es berücksichtigt dabei die öffentliche Sicherheit und Ordnung, das Wohlergehen der Bevölkerung und das Funktionieren der Wirtschaft.

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.

[6] Auf die vom Bundesamt für Kommunikation (BAKOM) im Rahmen seiner Aufsichtskontrollen (Art. 36 ff. der Verordnung vom 25. November 2015[2] über Fernmeldeanlagen) entdeckten Schwachstellen sind die Absätze 1–4 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 1997[3] entdeckten Schwachstellen.

Art. 10 Unterstützung von Behörden

Das BACS unterstützt die Behörden von Bund und Kantonen bei der Entwicklung, Umsetzung und Prüfung von Standards und Regulierungen im Bereich der Cybersicherheit.

2 SR 784.101.2
3 SR 784.10

4. Abschnitt: Informationsaustausch

Art. 11 Kommunikationssystem für den sicheren Informationsaustausch

[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.

[2] Das BACS ist für die Sicherheit des Kommunikationssystems und die Rechtmässigkeit der Bearbeitung der Daten verantwortlich.

Art. 12 Informationssysteme für den automatischen Austausch

[1]Das BACS stellt den Betreiberinnen kritischer Infrastrukturen Informationssysteme für den automatischen Austausch von technischen Informationen zu Cyberbedrohungen und Cybervorfällen zur Verfügung.

[2] Das BACS ist für die Sicherheit der Informationssysteme und die Rechtmässigkeit der Bearbeitung der Daten verantwortlich.

Art. 13 Registrierung

[1] Die Organisationen und Behörden müssen sich für die Nutzung des Kommunikationssystems registrieren. Sie müssen Änderungen von Angaben unverzüglich melden.

[2] Die Registrierung muss mindestens folgende Informationen enthalten:

a. Firma, Name oder Bezeichnung und Adresse;

b. Kontaktangaben der gemeldeten Person.

Art. 14 Dienstleister

[1] Die Betreiberinnen kritischer Infrastrukturen können dem BACS Dienstleister melden, die am Informationsaustausch teilnehmen wollen.

[2] Die Dienstleister müssen sich mit der Firma oder dem Namen sowie Kontaktangaben der gemeldeten Person registrieren.

Art. 15 Übermittlung und Nutzung der Informationen

[1] Registrierte Unternehmen und Behörden übermitteln Informationen dem BACS und bestimmen dabei, ob und an wen dieses die Informationen weitergegeben darf, soweit eine Weitergabe der Informationen nicht gesetzlich vorgesehen ist.

[2] Das BACS entscheidet über die Veröffentlichung der zur Weitergabe freigegebenen Informationen auf dem Kommunikationssystem sowie den Informationssystemen für den automatischen Austausch.

[3] Die Informationsempfänger müssen den Schutz der Informationen gewährleisten.

[4] Die Dienstleister von Betreiberinnen kritischer Infrastrukturen dürfen Informationen, die sie erhalten, ausschliesslich zum Schutz kritischer Infrastrukturen nutzen.

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 74*b* 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 74*b* Absatz 1 Buchstabe d ISG, sofern sie:

1. als Netzbetreiber, Elektrizitätserzeuger, Elektrizitätsspeicherbetreiber oder Dienstleister im Elektrizitätsbereich gemäss Artikel 5*a* Absatz 1 und Anhang 1*a* der Stromversorgungsverordnung vom 14. März 2008[4] 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 2021[5] im Durchschnitt der letzten fünf Jahre eine transportierte Energie von weniger als 400 GWh/Jahr aufweisen;

c. Unternehmen nach Art. 74*b* 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) 2023/203[6] oder nach Artikel 2 und dem Anhang II der Verordnung (EU) 2022/1645[7] einrichten müssen,

4 SR **734.71**
5 SR **756.12**
6 Durchführungsverordnung (EU) Nr. 2023/203 der Kommission vom 27. Oktober 2022 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 2018/1139 des Europäischen Parlaments und des Rates hinsichtlich der Anforderungen an das Management von Informationssicherheitsrisiken mit potenziellen Auswirkungen auf die Flugsicherheit für Organisationen, die unter die Verordnungen (EU) Nr. 1321/2014, (EU) Nr. 965/2012, (EU) Nr. 1178/2011, (EU) 2015/340 der Kommission, die Durchführungsverordnungen (EU) 2017/373 und (EU) 2021/664 der Kommission fallen, sowie für zuständige Behörden, die unter die Verordnungen (EU) Nr. 748/2012, (EU) Nr. 1321/2014, (EU) Nr. 965/2012, (EU) Nr. 1178/2011, (EU) 2015/340 und (EU) Nr. 139/2014 der Kommission und die Durchführungsverordnungen (EU) 2017/373 und (EU) 2021/664 der Kommission fallen, sowie zur Änderung der Verordnungen (EU) Nr. 1178/2011, (EU) Nr. 748/2012, (EU) Nr. 965/2012, (EU) Nr. 139/2014, (EU) Nr. 1321/2014, (EU) 2015/340 der Kommission und der Durchführungsverordnungen (EU) 2017/373 und (EU) 2021/664 der Kommission.
7 Delegierte Verordnung (EU) Nr. 2022/1645 der Kommission vom 14. Juli 2022 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates im Hinblick auf die Anforderungen an das Management von Informationssicherheitsrisiken mit potenziellen Auswirkungen auf die Flugsicherheit für Organisationen, die unter die Verordnungen (EU) Nr. 748/2012 und (EU) Nr. 139/2014 der Kommission fallen, und zur Änderung der Verordnungen (EU) Nr. 748/2012 und (EU) Nr. 139/2014 der Kommission.

2. die Vorgaben nach Punkt 1.7 des Anhangs der Verordnung (EU) 2015/1998[8] in ihrem Security-Programm nach Artikel 2, 12, 13 oder 14 der Verordnung (EG) 300/2008[9] nicht umsetzen müssen;

d. Eisenbahnunternehmen sowie Seilbahn-, Trolleybus-, Autobus- und Schifffahrtsunternehmen nach Artikel 74*b* Absatz 1 Buchstabe m ISG, sofern sie:

1. nicht mit Systemaufgaben (Art. 37 des Eisenbahngesetzes vom 20. Dezember 1957[10] [EBG]) beauftragt sind,
2. über eine Personenbeförderungskonzession nach Artikel 6 des Personenbeförderungsgesetzes vom 20. März 2009[11] (PBG) verfügen, aber keine durch Bund und Kantone gemeinsam bestellten Angebote erbringen (Art. 28–31*c* 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 74*b* 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 74*b* 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.

Art. 17 Dokumentationspflicht bei Gesuchen um Auskunft über die Unterstellung unter die Meldepflicht

Die interessierten Behörden und Organisationen müssen dem BACS alle Unterlagen zur Verfügung stellen, die dieses benötigt, um Auskunft über die Unterstellung unter die Meldepflicht zu erteilen.

Art. 18 Zu meldende Cyberangriffe

[1] Die Funktionsfähigkeit einer kritischen Infrastruktur gilt als gefährdet, wenn:

8 Durchführungsverordnung (EU) Nr. 2015/1998 der Kommission vom 5. November 2015 zur Festlegung detaillierter Maßnahmen für die Durchführung der gemeinsamen Grundstandards für die Luftsicherheit.
9 Verordnung (EG) Nr. 300/2008 des europäischen Parlaments und des Rates vom 11. März 2008 über gemeinsame Vorschriften für die Sicherheit in der Zivilluftfahrt und zur Aufhebung der Verordnung (EG) Nr. 2320/2002.
10 SR **742.101**
11 SR **745.1**

a. Mitarbeitende oder Dritte von Systemunterbrüchen betroffen sind; oder

b. die betroffene Organisation oder Behörde ihre Tätigkeiten nur noch mit Hilfe von Notfallplänen aufrechterhalten kann.

[2] Eine Manipulation oder ein Abfluss von Informationen liegt vor, wenn:

a. geschäftsrelevante Informationen von Unbefugten verändert oder offengelegt werden; oder

b. eine Verletzung der Datensicherheit nach Artikel 24 des Datenschutzgesetzes vom 25. September 2020[12] vorliegt.

[3] Ein Cyberangriff gilt als über einen längeren Zeitraum unentdeckt, wenn der Vorfall mehr als 90 Tage zurückliegt.

[4] Ein Cyberangriff gilt als mit Erpressung, Drohung oder Nötigung verbunden, wenn sich diese Handlungen gegen die meldepflichtige Behörde oder Organisation oder gegen deren Verantwortliche oder Mitarbeitende, einschliesslich ehemaliger Verantwortlicher oder Mitarbeitender, oder gegen für die meldepflichtige Behörde oder Organisation tätige Personen richten.

Art. 19 Inhalt der Meldung

[1] Die Meldung muss folgende Informationen zum Cyberangriff enthalten:

a. Datum und Uhrzeit der Feststellung des Angriffs;

b. Datum und Uhrzeit des Angriffs;

c. Art des Angriffs;

d. Angriffsmethode; und

e. Angaben zum Verursacher.

[2] Sie muss zudem die Information enthalten, ob der Angriff mit Erpressung, Drohung oder Nötigung verbunden war und ob Strafanzeige erstattet wurde.

[3] Sie muss folgende Informationen zu den Auswirkungen des Cyberangriffs enthalten:

a. betroffene Einheiten der Organisation oder Behörde;

b. Schweregrad der Beeinträchtigung der Verfügbarkeit, Integrität und Vertraulichkeit der eigenen Informationen und der Informationen von Dritten; und

c. Auswirkung des Cyberangriffs auf die Funktionsfähigkeit der betroffenen Einheiten der Organisation oder Behörde.

[4] Erfolgt die Meldung nicht über das Kommunikationssystem des BACS, so muss sie zusätzlich folgende Informationen zur meldepflichtigen Behörde oder Organisation enthalten:

a. Firma, Name oder Bezeichnung und Adresse; und

b. Kontaktangaben der meldenden Person.

12 SR **235.1**

Art. 20 Übermittlung der Meldung

Falls die Meldung nicht über das Kommunikationssystem des BACS erfolgt, informiert dieses die Kontaktperson nach Artikel 13 Absatz 2 Buchstabe b über den Eingang und den Inhalt der Meldung.

Art. 21 Frist zur Erfassung der Meldung

[1] Sind innerhalb der Meldefrist von 24 Stunden nicht alle erforderlichen Informationen bekannt, so gewährt das BACS der betreffenden Behörde oder Organisation eine Frist von 14 Tagen zur Ergänzung der Meldung.

[2] Liegen bis zum Ablauf der Frist nicht alle erforderlichen Informationen vor, so fordert das BACS die betreffende Behörde oder Organisation auf, diese umgehend zu ergänzen oder zu bestätigen, dass die Informationen nicht vorhanden sind.

6. Abschnitt: Schlussbestimmungen

Art. 22 Änderung anderer Erlasse

Die Änderung anderer Erlasse wird im Anhang geregelt.

Art. 23 Inkrafttreten

Diese Verordnung tritt am 1. Januar 2025 in Kraft.

Anhang
(Art. 22)

Änderung anderer Erlasse

Die nachstehenden Verordnungen werden wie folgt geändert:

1. Organisationsverordnung vom 7. März 2003[13] für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport

Art. 15a Abs. 2 Einleitungssatz sowie Bst. f und h

[2] Es nimmt insbesondere folgende Funktionen wahr:

f. Es betreibt das nationale Einsatzteam für Computersicherheit *(Computer Emergency Response Team [CERT])*.

h. Es vertritt die Schweiz zur technischen Analyse von Cyberbedrohungen und zur Bewältigung von Cybervorfällen in internationalen Gremien.

2. Verordnung über den Datenschutz vom 31. August 2022[14]

Art. 41 Abs. 1

Aufgehoben

13 SR **172.214.1**
14 SR **235.11**