Verordnung über die Cybersicherheit
(Cybersicherheitsverordnung, CSV)

vom 7. März 2025 (Stand am 1. April 2025)

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

1. Abschnitt: Gegenstand

Art. 1

Diese Verordnung regelt:

a. die Grundzüge und die Erarbeitung der Nationalen Cyberstrategie (NCS);
b. die Aufgaben des Bundesamts für Cybersicherheit (BACS);
c. den Informationsaustausch des BACS mit Behörden und Organisationen zum Schutz vor Cybervorfällen und Cyberbedrohungen;
d. die Meldepflicht bei Cyberangriffen.

2. Abschnitt: Nationale Cyberstrategie

Art. 2

[1] Die NCS legt Folgendes fest:

a. den strategischen Rahmen für die Prävention im Bereich der Cybersicherheit;
b. die Früherkennung von Cyberbedrohungen;
c. die Reaktionsmöglichkeiten und die Resilienz bei Vorfällen;
d. die Bekämpfung der Cyberkriminalität;
e. die internationale Zusammenarbeit.

[2] Das BACS erarbeitet die NCS gemeinsam mit Vertreterinnen und Vertretern der Kantone, der Wirtschaft, der Betreiberinnen kritischer Infrastrukturen, der Wissenschaft, der Gesellschaft, der Departemente und der Bundeskanzlei.

AS **2025** 169
1 SR **128**

3. Abschnitt: Aufgaben des BACS

Art. 3 Halterabfragen

Das BACS kann zur Warnung von betroffenen Behörden, Organisationen und Personen im Fall einer unmittelbaren Cyberbedrohung oder eines laufenden Cyberangriffs bei der Registerbetreiberin von Domain-Namen, die in die Kompetenz des Bundes fallen, die Kontaktangaben der Halter der Domain-Namen abfragen.

Art. 4 Technische Analyse von Cybervorfällen und Cyberbedrohungen

[1] Das BACS betreibt ein nationales Einsatzteam für Computersicherheit; dieses nimmt insbesondere die folgenden Aufgaben wahr:

a. Unterstützung bei der technischen Bewältigung von Cybervorfällen;

b. Analyse technischer Fragestellungen;

c. Identifikation und Beurteilung von Cyberbedrohungen.

[2] Es betreibt für die Analyse der Cybervorfälle und Cyberbedrohungen eine resiliente, von der restlichen Bundesinformatik unabhängige Infrastruktur.

Art. 5 Priorisierung der Beratung und Unterstützung bei Cyberangriffen

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

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

Art. 6 Offenlegung von Schwachstellen

[1] Das BACS sorgt dafür, dass Schwachstellen an Hard- und Software koordiniert offengelegt werden; es berücksichtigt dabei international anerkannte 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. weit verbreitete Systeme betrifft; oder

c. für einen Cyberangriff verwendet wird oder besonders leicht für einen Cyberangriff ausgenutzt werden kann.

[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 Offenlegung oder Behebung über Schwachstellen informieren.

6 Es informiert das Bundesamt für Kommunikation (BAKOM) unverzüglich über Schwachstellen in Fernmeldeanlagen nach Artikel 3 Buchstabe d des Fernmeldegesetzes vom 30. April 1997[2].

7 Die Absätze 1–4 gelten nicht für Schwachstellen, die das BAKOM im Rahmen seiner Aufsichtskontrollen (Art. 36–40 der Verordnung vom 25. November 2015[3] über Fernmeldeanlagen) feststellt und dem BACS meldet.

Art. 7 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.

4. Abschnitt: Informationsaustausch

Art. 8 Kommunikationssystem für den sicheren Informationsaustausch und Informationssysteme für den automatischen Austausch

1 Zugang zum Kommunikationssystem des BACS für den sicheren Informationsaustausch haben alle meldepflichtigen Betreiberinnen von kritischen Infrastrukturen sowie Organisationen mit Sitz in der Schweiz und Behörden.

2 Das BACS stellt den Betreiberinnen kritischer Infrastrukturen technische Informationen nach Artikel 74 Absatz 2 Buchstabe b ISG zu Cyberbedrohungen und Cybervorfällen über Informationssysteme für den automatischen Austausch zur Verfügung.

3 Das BACS ist für die Sicherheit des Kommunikations- sowie der Informationssysteme und die Rechtmässigkeit der Bearbeitung der Daten verantwortlich.

Art. 9 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 Angaben enthalten:

a. Firma, Name oder Bezeichnung und Adresse;

b. Kontaktperson.

2 SR **784.10**
3 SR **784.101.2**

Art. 10 Dienstleister

[1] Die Betreiberinnen kritischer Infrastrukturen können dem BACS Dienstleister melden, die für sie Leistungen im Bereich der Cybersicherheit erbringen und die am Informationsaustausch teilnehmen wollen.

[2] Die Dienstleister müssen sich mit der Firma oder dem Namen sowie Angaben zur Kontaktperson registrieren.

Art. 11 Übermittlung und Nutzung der Informationen

[1] Die registrierten Organisationen und Behörden legen bei der Übermittlung von Informationen fest, an wen das BACS diese im Kommunikationssystem für den sicheren Informationsaustausch weitergeben darf, es sei denn, die Weitergabe ist gesetzlich vorgesehen.

[2] Das BACS entscheidet über die Veröffentlichung von freigegebenen Informationen.

[3] Die Informationsempfängerinnen und -empfänger müssen den Schutz der Informationen gewährleisten.

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

5. Abschnitt: Meldepflicht

Art. 12 Ausnahmen von der Meldepflicht

[1] Die folgenden Behörden und Organisationen sind unter den nachstehenden Voraussetzungen von der Meldepflicht ausgenommen:

a. Hochschulen nach Artikel 74*b* Absatz 1 Buchstabe a ISG, sofern sie über weniger als 2000 Studierende verfügen;

b. Unternehmen nach Artikel 74*b* Absatz 1 Buchstabe d ISG, sofern sie:

   1. als Netzbetreiber, Elektrizitätserzeuger, Elektrizitätsspeicherbetreiber oder Dienstleister im Elektrizitätsbereich nach 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, oder

   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;

[4] SR **734.71**
[5] SR **746.12**

c. 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[6] [EBG]) beauftragt sind,
   2. über eine Personenbeförderungskonzession nach Artikel 6 des Personenbeförderungsgesetzes vom 20. März 2009[7] (PBG) verfügen, aber keine durch Bund und Kantone gemeinsam bestellten Angebote erbringen (Art. 28–31*c* PBG),
   3. 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);

d. Unternehmen nach Artikel 74*b* Absatz 1 Buchstabe n ISG, sofern sie:
   1. nach den Artikeln 2 und 4 und Anhang II der Durchführungsverordnung (EU) 2023/203[8] oder nach Artikel 2 und dem Anhang der Delegierten Verordnung (EU) 2022/1645[9] kein Information Security Management System einrichten müssen,

6 SR **742.101**
7 SR **745.1**
8 Durchführungsverordnung (EU) 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, in der für die Schweiz verbindlichen Fassung gemäss Ziffer 3 des Anhangs zum Abkommen vom 21. Juni 1999 zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über den Luftverkehr (SR **0.748.127.192.68**).
9 Delegierte Verordnung (EU) 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, in der für die Schweiz verbindlichen Fassung gemäss Ziffer 3 des Anhangs zum Abkommen vom 21. Juni 1999 zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über den Luftverkehr (SR **0.748.127.192.68**).

2. die Vorgaben nach Ziffer 1.7 des Anhangs der Durchführungsverordnung (EU) 2015/1998[10] in ihrem Security-Programm nach Artikel 2, 12, 13 oder 14 der Verordnung (EG) Nr. 300/2008[11] nicht umsetzen müssen;

e. Anbieterinnen und Betreiberinnen nach Artikel 74*b* Absatz 1 Buchstabe t ISG, sofern sie ihre Leistungen weder teilweise noch vollumfänglich gegen Entgelt für Dritte erbringen.

[2] Behörden und Organisationen nach Artikel 74*b* Absatz 1 Buchstaben g, h, l und p ISG sind von der Meldepflicht ausgenommen, sofern sie im betroffenen Bereich weniger als 50 Personen beschäftigen und ihr Jahresumsatz oder ihre Jahresbilanzsumme im betroffenen Bereich 10 Millionen Franken nicht übersteigt.

Art. 13 Einreichung von Unterlagen zur Abklärung der 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. 14 Zu meldende Cyberangriffe

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

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 eingesehen, verändert oder offengelegt werden; oder

b. eine Meldung von Verletzungen der Datensicherheit nach Artikel 24 des Datenschutzgesetzes vom 25. September 2020[12] erfolgt ist.

[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 eine meldepflichtige Behörde oder Organisation richten oder gegen Personen, die für eine solche Behörde oder Organisation tätig sind.

10 Durchführungsverordnung (EU) 2015/1998 der Kommission vom 5. November 2015 zur Festlegung detaillierter Massnahmen für die Durchführung der gemeinsamen Grundstandards für die Luftsicherheit, in der für die Schweiz verbindlichen Fassung gemäss Ziffer 4 des Anhangs zum Abkommen vom 21. Juni 1999 zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über den Luftverkehr (SR **0.748.127.192.68**).

11 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, in der für die Schweiz verbindlichen Fassung gemäss Ziffer 4 des Anhangs zum Abkommen vom 21. Juni 1999 zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über den Luftverkehr (SR **0.748.127.192.68**).

12 SR **235.1**

Art. 15 Inhalt der Meldung

[1] Die Meldung muss nebst den Angaben nach Artikel 74*e* Absatz 2 ISG folgende Informationen zum Cyberangriff enthalten:

a. Datum und Uhrzeit der Feststellung des Angriffs;

b. Datum und Uhrzeit des Angriffs; und

c. Angaben zum Angreifer.

[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. Schweregrad der Beeinträchtigung der Verfügbarkeit, Integrität und Vertraulichkeit der Informationen; und

b. Auswirkung des Cyberangriffs auf die Funktionsfähigkeit 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.

Art. 16 Frist zur Erfassung der Meldung

[1] Sind innerhalb der Meldefrist von 24 Stunden nach der Entdeckung des Cyberangriffs 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.

Art. 17 Übermittlung der Meldung

[1] Falls die Meldung nicht über das Kommunikationssystem des BACS erfolgt, informiert dieses die Kontaktperson nach Artikel 9 Absatz 2 Buchstabe b über den Eingang und den Inhalt der Meldung.

[2] Eine oder mehrere meldepflichtige Behörden oder Organisationen können beschliessen, den Meldeprozess einzeln oder gemeinsam an eine Drittorganisation auszulagern.

6. Abschnitt: Schlussbestimmungen

Art. 18 Änderung anderer Erlasse

Die Änderung anderer Erlasse wird im Anhang geregelt.

Art. 19 Inkrafttreten

Diese Verordnung tritt am 1. April 2025 in Kraft.

Anhang
(Art. 18)

Änderung anderer Erlasse

Die nachstehenden Erlasse werden wie folgt geändert:

…[13]

13 Die Änderungen können unter AS **2025** 169 konsultiert werden.