Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

The Federal Council
The portal of the Swiss government

Protection against cyber-risks: Federal Council approves ordinance and additional staff

Bern, 28.05.2020 - The Ordinance on Protecting against Cyber-Risks in the Federal Administration was adopted by the Federal Council during its meeting on 27 May 2020 and will come into force on 1 July 2020. Moreover, the Federal Council decided to allocate 20 new posts to increase staffing for the implementation of the 2020-2022 national strategy for the protection of Switzerland against cyber-risks.

To enable the Confederation to play a more active role in protecting Switzerland against cyber-risks, the Federal Council decided in January 2019 to establish a cybersecurity competence centre, headed by a Federal Cybersecurity Delegate. With the Ordinance on Protecting against Cyber-Risks in the Federal Administration, the Federal Department of Finance (FDF) is implementing the Federal Council's mandate of 30 January 2019 and creating the legal basis for the establishment and expansion of the National Cybersecurity Centre (NCSC). This ordinance and the 20 new posts in the area of cyber-risks will enable the Federal Council to meet the demands of businesses and political circles for a robust competence centre with a clear structure and greater centralisation.

Main organisational features

The ordinance adopted by the Federal Council governs the structure, tasks and powers of the authorities involved. This means that it also sets out the composition and tasks of the Cyber Core Group and the NCS Steering Committee, two bodies that enable increased interdepartmental cooperation within the Federal Administration. After consulting the services concerned, the NCSC can take the lead and order immediate measures when dealing with a cyberincident. The ordinance additionally regulates the obligation of Federal Administration service providers to report to the NCSC.

The FDF has started to establish the NCSC under the leadership of the Cybersecurity Delegate, Florian Schütz, who took up his position in August 2019. He is the Confederation's key contact person in the area of cyber-risks, and issues IT security guidelines for the Federal Administration, among other things. The NCSC currently consists of a strategic and an operational division. The strategic division is already being managed as an independent new unit in the FDF General Secretariat. The operational division includes the existing Reporting and Analysis Centre for Information Assurance (MELANI), Federal ICT Security and GovCERT.ch, which were previously part of the Federal IT Steering Unit (FITSU). These areas will also be transferred to the FDF General Secretariat, under the direct management of the Cybersecurity Delegate, once the organisational establishment work has been completed.

20 new posts for NCS implementation

The Federal Council adopted the implementation plan for the 2018-2022 national strategy for the protection of Switzerland against cyber-risks (NCS) back in May 2019 and approved 24 additional posts at that time. These resources are to be expanded further. Subject to the Federal Council's future decisions on resources in the area of personnel, another 20 posts are planned to cover the task areas in the offices responsible for protecting against cyber-risks.

Address for enquiries

Noemi Martig, Media Spokesperson
FDF Communications
Tel. +41 58 485 69 72
noemi.martig@gs-efd.admin.ch

Documents

Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (PDF, 160 kB)

Erläuterungen zur Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (PDF, 377 kB)

Publisher

The Federal Council
https://www.admin.ch/gov/en/start.html

Federal Department of Finance
https://www.efd.admin.ch/efd/en/home.html

General Secretariat DDPS

https://www.vbs.admin.ch/

Federal intelligence service
http://www.ndb.admin.ch

Armasuisse
http://www.ar.admin.ch/

Defence
http://www.vtg.admin.ch

https://www.admin.ch/content/gov/en/start/documentation/media-releases.msg-id-79275.html

Dieser Text ist ein Vorabdruck. Verbindlich ist die Version, die in der Amtlichen Sammlung des Bundesrechts veröffentlicht wird.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

[Signature]

[QR Code]

Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung

(Cyberrisikenverordnung, CyRV)

vom …

Der Schweizerische Bundesrat,

gestützt auf Artikel 30 des Bundesgesetzes vom 21. März 1997[1] über Massnahmen zur Wahrung der inneren Sicherheit
und auf die Artikel 43 Absätze 2 und 3, 47 Absatz 2 und 55 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997[2],

verordnet:

1. Kapitel: Allgemeine Bestimmungen

Art. 1 Gegenstand

Diese Verordnung regelt die Organisation der Bundesverwaltung zum Schutz vor Cyberrisiken sowie die Aufgaben und Zuständigkeiten der verschiedenen Stellen im Bereich Cybersicherheit.

Art. 2 Geltungsbereich

Diese Verordnung gilt für:

a. die Verwaltungseinheiten der zentralen Bundesverwaltung nach Artikel 7 der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998[3];

b. die Behörden und Stellen, die sich gemäss Artikel 2 Absätze 2 und 3 der Bundesinformatikverordnung vom 9. Dezember 2011[4] (BinfV) dazu verpflichten, sie einzuhalten.

SR .....
1 SR **120**
2 SR **172.010**
3 SR **172.010.1**
4 SR **172.010.58**

Art. 3 Begriffe

In dieser Verordnung bedeuten:

a. *Cybersicherheit:* anzustrebender Zustand, bei dem die Datenbearbeitung, insbesondere der Datenaustausch zwischen Personen und Organisationen, über Informations- und Kommunikationsinfrastrukturen wie beabsichtigt funktioniert;

b. *Cybervorfall:* unbeabsichtigtes oder von Unbefugten beabsichtigtes Ereignis, das dazu führt, dass die Vertraulichkeit, Integrität, Verfügbarkeit oder Nachvollziehbarkeit von Daten beeinträchtigt ist oder es zu Funktionsstörungen kommen kann;

c. *Cyberrisiko:* Gefahr eines Cybervorfalls, deren Grösse durch das Produkt der Eintrittswahrscheinlichkeit und des Schadensausmasses bestimmt ist;

d. *Resilienz:* die Fähigkeit eines Systems, einer Organisation oder einer Gesellschaft, intern oder extern verursachten Störungen zu widerstehen und das ordnungsgemässe Funktionieren zu erhalten oder dieses möglichst rasch und vollständig wiederzuerlangen;

e. *Informatiksicherheit*: der auf technische Systeme bezogene Aspekt der Cybersicherheit;

f. *Informatiksicherheitsvorgaben:* Sicherheitsanforderungen an die Organisation, die Prozesse, die Dienstleistungen und die Technik;

g. *kritische Infrastrukturen:* Prozesse, Systeme und Einrichtungen, die für das Funktionieren der Wirtschaft oder das Wohlergehen der Bevölkerung essenziell sind.

2. Kapitel: Grundsätze für den Schutz vor Cyberrisiken

Art. 4 Ziele

[1] Die Bundesverwaltung sorgt für eine angemessene Resilienz ihrer Organe und Systeme gegenüber Cyberrisiken.

[2] Sie arbeitet mit den Kantonen, den Gemeinden, der Wirtschaft, der Gesellschaft, der Wissenschaft und den internationalen Partnern zusammen, soweit dies dem Schutz der eigenen Sicherheitsinteressen dient, und fördert den Informationsaustausch.

Art. 5 Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken

Der Bundesrat legt in der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) den strategischen Rahmen für die Verbesserung der Prävention, Früherkennung, Reaktion und Resilienz zum Schutz vor Cyberrisiken fest.

Art. 6 Bereiche

Die Massnahmen zum Schutz vor Cyberrisiken sind in folgende drei Bereiche unterteilt:

a. Bereich Cybersicherheit: Gesamtheit der Massnahmen, die der Prävention, der Bewältigung von Vorfällen und der Verbesserung der Resilienz gegenüber Cyberrisiken dienen und die internationale Zusammenarbeit zu diesem Zweck stärken;

b. Bereich Cyberdefence: Gesamtheit der nachrichtendienstlichen und militärischen Massnahmen, die dem Schutz der für die Landesverteidigung kritischen Systeme, der Abwehr von Cyberangriffen, der Gewährleistung der Einsatzbereitschaft der Armee in allen Lagen und dem Aufbau von Kapazitäten und Fähigkeiten zur subsidiären Unterstützung ziviler Behörden dienen; dazu zählen auch aktive Massnahmen zur Erkennung von Bedrohungen, zur Identifikation von Angreifern und zur Störung und Unterbindung von Angriffen;

c. Bereich Cyberstrafverfolgung: Gesamtheit aller Massnahmen der Polizei und der Staatsanwaltschaft von Bund und Kantonen zur Bekämpfung der Cyberkriminalität.

3. Kapitel: Organisation und Zuständigkeiten

1. Abschnitt: Departementsübergreifende Zusammenarbeit

Art. 7 Bundesrat

Der Bundesrat nimmt folgende Funktionen wahr:

a. Er überwacht die Umsetzung der NCS anhand des strategischen Controllings und beschliesst bei Bedarf Massnahmen.

b. Er legt im Rahmen seiner Zuständigkeiten fest, in welchen Bereichen Vorgaben zum Schutz vor Cyberrisiken nötig sind oder angepasst werden sollen.

c. Er erlässt Weisungen über den Schutz der Bundesverwaltung vor Cyberrisiken.

d. Er bewilligt Abweichungen von seinen Vorgaben.

Art. 8 Kerngruppe Cyber

[1] Die Kerngruppe Cyber (KGCy) setzt sich zusammen aus:

a. der oder dem Delegierten für Cybersicherheit (Art. 6*a* der Organisationsverordnung vom 17. Febr. 2010[5] für das Eidgenössische Finanzdepartement) als Vertreterin oder Vertreter des Eidgenössischen Finanzdepartements (EFD);

5 SR **172.215.1**

b. einer Vertreterin oder einem Vertreter des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS);

c. einer Vertreterin oder einem Vertreter des Eidgenössischen Justiz- und Polizeidepartements (EJPD);

d. einer Vertreterin oder einem Vertreter der Kantone, die oder der durch die zuständige Konferenz der Kantonsregierungen bestimmt wird.

2 Die oder der Delegierte für Cybersicherheit hat den Vorsitz.

3 Die KGCy informiert Vertreterinnen und Vertreter weiterer Verwaltungseinheiten des Bundes, die im Bereich Cyberrisiken tätig sind, über die Traktanden und kann sie für einzelne Sitzungen beiziehen. Bei Belangen mit aussenpolitischem Bezug involviert sie das Eidgenössische Departement für auswärtige Angelegenheiten (EDA). Zudem kann sie Expertinnen oder Experten aus Wirtschaft und Hochschulen beiziehen.

4 Die KGCy hat namentlich folgende Aufgaben:

a. Sie beurteilt aktuelle Cyberrisiken sowie deren mögliche Entwicklung anhand von Informationen aus den Bereichen Cybersicherheit, -defence und -strafverfolgung.

b. Sie bewertet laufend die bestehenden Dispositive in den Bereichen Cybersicherheit, -defence und -strafverfolgung und prüft, ob diese der Bedrohungslage angepasst sind.

c. Sie begleitet, wenn nötig unter Einbezug weiterer Stellen, die interdepartementale Vorfallbewältigung.

d. Sie informiert die Kerngruppe Sicherheit des Bundes (KGSi) über aussen- und sicherheitspolitisch relevante Cybervorfälle und Entwicklungen.

5 Die drei in der KGCy vertretenen Departemente stellen Informationen für die gemeinsame Lagebeurteilung zur Verfügung.

6 Der Nachrichtendienst des Bundes ist für die Darstellung der gesamtheitlichen Cyberbedrohungslage zuhanden der KGCy zuständig.

Art. 9 Steuerungsausschuss Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken

1 Der Bundesrat setzt einen Steuerungsausschuss Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (StA NCS) ein.

2 Der StA NCS setzt sich zusammen aus der oder dem Delegierten für Cybersicherheit, durch die zuständige Konferenz der Kantonsregierungen bestimmte Vertretungen der Kantone, Vertretungen der Wirtschaft und der Hochschulen sowie Vertreterinnen und Vertretern der Verwaltungseinheiten, welche die federführende Verantwortung für die Umsetzung einer NCS-Massnahme gemäss dem NCS-Umsetzungsplan haben. Jedes Departement und die Bundeskanzlei stellen mindestens eine Vertreterin oder einen Vertreter im StA NCS.

3 Die oder der Delegierte für Cybersicherheit hat den Vorsitz.

4 Der StA NCS hat folgende Aufgaben:

a. Er sorgt für die strategische Kohärenz bei der Umsetzung der NCS-Massnahmen und prüft deren Fortschritt laufend mittels strategischem Controlling.

b. Er definiert bei verzögerter oder unvollständiger Umsetzung der NCS-Massnahmen Vorschläge für Sondermassnahmen.

c. Er sorgt für die laufende Weiterentwicklung der NCS; hierzu verfolgt er im Austausch mit der KGCy die Entwicklung der Bedrohungslage und erarbeitet bei Bedarf Anpassungsvorschläge für die NCS.

d. Er erstattet dem Bundesrat und der Öffentlichkeit jährlich Bericht über die Umsetzung der NCS.

e. Er sorgt für ein koordiniertes Vorgehen aller beteiligten Stellen aus Bund, Kantonen, Wirtschaft und Hochschulen bei der Umsetzung der NCS-Massnahmen.

f. Er stellt sicher, dass bei der Umsetzung der NCS-Massnahmen die Risikopolitik des Bundes, die Nationale Strategie zum Schutz kritischer Infrastrukturen sowie die Strategien des Bundesrates im Informatikbereich berücksichtigt werden.

Art. 10 Ausschuss Informatiksicherheit

1 Der Ausschuss Informatiksicherheit (A-IS) setzt sich aus einer Vertreterin oder einem Vertreter des Nationalen Zentrums für Cybersicherheit (NCSC[6]), den Informatiksicherheitsbeauftragten der Departemente und der Bundeskanzlei sowie der oder dem Informatiksicherheitsbeauftragten der Standarddienste der Informations- und Kommunikationstechnik (IKT) zusammen.

2 Fallweise können weitere Personen beratend beigezogen werden.

3 Die Vertreterin oder der Vertreter des NCSC hat den Vorsitz.

4 Der A-IS fungiert als Konsultativorgan für das NCSC betreffend Informatiksicherheitsfragen in der Bundesverwaltung.

Art. 11 Delegierte oder Delegierter für Cybersicherheit

1 Die oder der Delegierte für Cybersicherheit nimmt folgende Aufgaben wahr:

a. Sie oder er leitet das NCSC.

b. Sie oder er sorgt für eine optimale Abstimmung der überdepartementalen Arbeiten der Bereiche Cybersicherheit, -defence und -strafverfolgung.

c. Sie oder er sorgt für die Visibilität der Aktivitäten des Bundes im Bereich Cyberrisiken, trägt zu optimalen Rahmenbedingungen für eine innovative Cybersicherheitswirtschaft bei, ist die massgebende Ansprechperson des Bundes zu Cyberrisiken und vertritt diesen in den massgeblichen Kommissi-

6 National Cyber Security Centre

onen und Arbeitsgruppen; sie oder er sorgt für eine optimale Abstimmung der Arbeiten der Kantone und des Bundes zum Schutz der Schweiz vor Cyberrisiken.

d. Sie oder er vertritt das NCSC in den Krisenstäben des Bundes.

e. Sie oder er erlässt Informatiksicherheitsvorgaben.

f. Sie oder er entscheidet über Abweichungen von den von ihr oder ihm erlassenen Vorgaben; betreffen die Abweichungen auch IKT-Vorgaben des Informatiksteuerungsorgans des Bundes (ISB), so hört sie oder er vorgängig das ISB an.

[2] Sie oder er informiert das EFD zuhanden des Bundesrates regelmässig über den Stand der Informatiksicherheit in den Departementen und der Bundeskanzlei.

[3] Sie oder er kann sich an der Erarbeitung von Informatikvorgaben der Bundesverwaltung mit Bezug zur Cybersicherheit und an sicherheitsrelevanten Informatikvorhaben beteiligen. Namentlich kann sie oder er Informationen verlangen, dazu Stellung nehmen und Änderungen verlangen.

[4] Sie oder er kann nach Anhörung der Eidgenössischen Finanzkontrolle Überprüfungen der Informatiksicherheit verlangen.

2. Abschnitt: Organe des Bereichs Cybersicherheit

Art. 12 Nationales Zentrum für Cybersicherheit

[1] Das Nationale Zentrum für Cybersicherheit (NCSC) ist das Kompetenzzentrum des Bundes für Cyberrisiken und koordiniert die Arbeiten des Bundes im Bereich Cybersicherheit. Es hat folgende Aufgaben:

a. Es betreibt die nationale Anlaufstelle für Cyberrisiken; diese nimmt Meldungen aus der Bundesverwaltung, der Wirtschaft, den Kantonen und der Bevölkerung entgegen, analysiert sie und kann Empfehlungen dazu abgeben.

b. Es sorgt mit den zuständigen Kooperationspartnern in der Bundesverwaltung für die subsidiäre Unterstützung der Betreiber kritischer Infrastrukturen und fördert unter diesen den Informationsaustausch zu Cyberrisiken.

c. Es betreibt das «Computer Emergency Response Team» (GovCERT); dieses ist die nationale Fachstelle für die technische Vorfallbewältigung, die Analyse technischer Fragestellungen, die Einschätzungen der Bedrohungslage aus technischer Sicht und die technische Unterstützung der nationalen Anlaufstelle.

d. Es betreibt eine Fachstelle für die Informatiksicherheit des Bundes; diese erarbeitet Informatiksicherheitsvorgaben, berät die Verwaltungseinheiten bei deren Umsetzung und erhebt den Stand der Informatiksicherheit in den Departementen und der Bundeskanzlei.

e. Es stellt die Informatiksicherheitsbeauftragten des Bundes (ISBB).

f. Es koordiniert die Umsetzung der NCS, führt ein strategisches Controlling durch und bereitet die Sitzungen der KGCy und des StA NCS vor.

g. Es verfügt über einen Expertenpool, aus dem Expertinnen und Experten zur Unterstützung der Fachämter bei der Umsetzung von NCS-Massnahmen sowie bei der Entwicklung, Umsetzung und Prüfung von Standards und Regulierungen in Bezug auf die Cybersicherheit zur Verfügung gestellt werden.

h. Es trägt mit gezielten Informationen zur Sensibilisierung der Bundesverwaltung und der Öffentlichkeit in Bezug auf Cyberrisiken bei, informiert über die aktuelle Lage und gibt Anleitungen für präventive und reaktive Massnahmen heraus.

i. Es betreibt eine resiliente Analyse- und Kommunikationsinfrastruktur, die unabhängig von der restlichen Bundesinformatik funktionieren muss.

j. Es informiert die KGCy sowie bei aussen- und sicherheitspolitischer Bedeutung die KGSi über relevante Cybervorfälle.

[2] Es kann, sofern dies direkt oder indirekt dem Schutz der Bundesverwaltung vor Cyberrisiken dient, Daten zu Cybervorfällen und damit verbundenen Kommunikationsflüssen bearbeiten. Es kann sie staatlichen und privaten Sicherheitsteams bekanntgeben, sofern:

a. der Datenlieferant einverstanden ist; und

b. keine gesetzlichen Geheimhaltungspflichten verletzt werden.

[3] Eine Bekanntgabe von Personendaten ins Ausland ist nur zulässig, sofern die diesbezüglichen Vorgaben der Bundesgesetzgebung über den Datenschutz eingehalten werden.

[4] Besonders schützenswerte Personendaten dürfen nur bearbeitet werden, soweit für deren Bearbeitung mit Mitteln der Bundesinformatik die erforderliche gesetzliche Grundlage besteht.

[5] Das NCSC übernimmt in der Bundesverwaltung nach Rücksprache mit den betroffenen Dienststellen die Federführung bei der Bewältigung eines Cybervorfalls, wenn dieser das ordnungsgemässe Funktionieren der Bundesverwaltung gefährdet. Dabei hat es folgende Aufgaben und Kompetenzen:

a. Es kann die betroffenen Leistungserbringer und -bezüger verpflichten, ihm alle nötigen Informationen zur Verfügung zu stellen.

b. Es kann Sofortmassnahmen anordnen.

c. Es informiert die Leitung der betroffenen Verwaltungseinheiten über den Verlauf.

[6] Wurde nach einem Cybervorfall die Gefährdung der Vertraulichkeit oder der Funktionsfähigkeit der Bundesverwaltung durch die getroffenen Massnahmen genügend reduziert und sind die nötigen Folgearbeiten sowie deren Finanzierung definiert, so übergibt das NCSC die Verantwortung für die Weiterbearbeitung wieder an die betroffenen Stellen.

Art. 13 Departemente und Bundeskanzlei

[1] Die Departemente und die Bundeskanzlei berichten dem NCSC zum Jahresende über den Stand der Informatiksicherheit.

[2] Die internen Leistungserbringer nach den Artikeln 23 und 24 BinfV[7] erstatten dem NCSC regelmässig Bericht über entdeckte Schwachstellen und Cybervorfälle sowie über geplante und getroffene Massnahmen zu deren Behebung.

[3] Die Departemente und die Bundeskanzlei bestimmen je eine Informatiksicherheitsbeauftragte oder einen Informatiksicherheitsbeauftragten (ISBD).

Art. 14 Verwaltungseinheiten und ihre Leistungserbringer

[1] Die Verwaltungseinheiten bestimmen je eine Informatiksicherheitsbeauftragte oder einen Informatiksicherheitsbeauftragten (ISBO). Das ISB bestimmt zusätzlich eine Informatiksicherheitsbeauftragte oder einen Informatiksicherheitsbeauftragten für die IKT-Standarddienste.

[2] Die Verwaltungseinheiten sind für den Schutz ihrer Informatiksysteme, Anwendungen und Daten (Schutzobjekte) verantwortlich. Sie nehmen folgende Funktionen wahr:

a. Sie prüfen ihre Schutzobjekte regelmässig und ergreifen die notwendigen Sicherheitsmassnahmen; sie stellen namentlich sicher, dass diese für die einzelnen Schutzobjekte in aktueller Form dokumentiert sind.

b. Sie sind für die Einhaltung der Informatiksicherheitsvorgaben und der Beschlüsse des Bundesrates, des NCSC und der Departemente beziehungsweise der Bundeskanzlei in ihrem Zuständigkeitsbereich verantwortlich.

c. Sie sind unter Vorbehalt von Artikel 12 Absatz 5 verantwortlich für die Bewältigung von Cybervorfällen, die ihre Schutzobjekte betreffen.

d. Sie stellen sicher, dass beim Bezug von Leistungen bei einem externen Leistungserbringer die Informatiksicherheitsvorgaben Teil des Vertragsverhältnisses mit diesem sind.

e. Sie überprüfen die Einhaltung der Informatiksicherheitsvorgaben durch externe Leistungserbringer in geeigneter Weise.

[3] Die Leistungserbringer stellen sicher, dass sie über die nötigen Kapazitäten zur Bewältigung von Cybervorfällen bei sich und ihren Leistungsbezügern verfügen.

[4] Die Leistungserbringer melden den Leistungsbezügern entdeckte Schwachstellen und Sicherheitsvorfälle unverzüglich.

[5] Die Leistungsbezüger definieren in Zusammenarbeit mit den Leistungserbringern einen Prozess für die Bewältigung von Cybervorfällen. Darin werden namentlich die Entscheidkompetenzen für Sofortmassnahmen geregelt.

7 SR **172.010.58**

6 Kann ein Cybervorfall nicht im Rahmen des definierten Prozesses bewältigt werden, so informieren die Betroffenen das NCSC, um das weitere Vorgehen zu bestimmen.

7 Die Verwaltungseinheiten konsultieren das NCSC bei sicherheitsrelevanten Informatikvorgaben sowie -vorhaben.

8 Die Verwaltungseinheiten sind für die Entwicklung, Umsetzung und Prüfung von Standards und Regulierungen in Bezug auf die Cybersicherheit in ihren Sektoren verantwortlich. Das NCSC stellt ihnen im Rahmen der Möglichkeiten Expertinnen und Experten aus dem Pool nach Artikel 12 Absatz 1 Buchstabe g zur Verfügung.

4. Kapitel: Schlussbestimmungen

Art. 15 Änderung anderer Erlasse

Die Änderung anderer Erlasse ist im Anhang geregelt.

Art. 16 Übergangsbestimmung zu Artikel 2 Buchstabe b

1 Behörden und Stellen, die sich vor Inkrafttreten dieser Verordnung durch Vereinbarung mit dem ISB verpflichtet haben, die Bestimmungen der BinfV[8] einzuhalten, unterstehen bis am 31. Dezember 2021 den Verpflichtungen gemäss dieser Verordnung im Umfang der bisherigen Regelung.

2 Sie unterstehen ab dem 1. Januar 2022 dieser Verordnung, sofern die Vereinbarung nicht spätestens per 31. Dezember 2021 aufgelöst wurde.

Art. 17 Übergangsbestimmung zu Artikel 11 Absatz 1 Buchstabe e

1 Vor dem Inkrafttreten dieser Verordnung durch das ISB erlassene IKT-Sicherheitsvorgaben und bewilligte Ausnahmen gelten weiter.

2 Über Änderungen an Vorgaben und bewilligten Ausnahmen entscheidet das NCSC.

Art. 18 Inkrafttreten

Diese Verordnung tritt am 1. Juli 2020 in Kraft.

… Im Namen des Schweizerischen Bundesrates

Die Bundespräsidentin: Simonetta Sommaruga
Der Bundeskanzler: Walter Thurnherr

8 SR **172.010.58**

Anhang
(Art. 15)

Änderung anderer Erlasse

Die nachstehenden Verordnungen werden wie folgt geändert:

1. Bundesinformatikverordnung vom 9. Dezember 2011[9]

Art. 2 Abs. 3

[3] Behörden und Stellen, die sich nach Absatz 2 verpflichten, diese Verordnung und die darauf gestützten Vorgaben einzuhalten, verpflichten sich damit auch, die Cyberrisikenverordnung vom …[10] (CyRV) und die darauf gestützten Vorgaben einzuhalten.

Art. 3 Abs. 4 Bst. d und Abs. 8, 3. Kap. (Art. 10 und 11) sowie Art. 14 Bst. e

Aufgehoben

Art. 16a Nationales Zentrum für Cybersicherheit

Das Nationale Zentrum für Cybersicherheit (NCSC[11]) nach Artikel 12 der CyRV[12] wird bei der Erarbeitung von Informatikvorgaben der Bundesverwaltung mit Bezug zur Cybersicherheit und bei sicherheitsrelevanten Informatikvorhaben konsultiert.

Art. 17 Abs. 1 Bst. e–i

[1] Das ISB hat namentlich folgende Aufgaben:

e. Es entscheidet über Abweichungen von den von ihm erlassenen Vorgaben; sind diese Abweichungen sicherheitsrelevant, so hört es vorgängig den Delegierten oder die Delegierte für Cybersicherheit an.

f.–g. *Aufgehoben*

h. Es stellt einen Informatiksicherheitsbeauftragten oder eine Informatiksicherheitsbeauftragte für die Standarddienste.

i. *Aufgehoben*

9 SR **172.010.58**
10 SR …
11 National Cyber Security Centre
12 SR …

Art. 18 Abs. 1

[1] Der Informatikrat des Bundes (IRB) setzt sich zusammen aus dem oder der Delegierten für die IKT-Steuerung (Art. 20*a* Abs. 2 der Organisationsverordnung vom 17. Febr. 2010[13] für das Eidgenössische Finanzdepartement) und je einem namentlich bezeichneten Vertreter oder einer namentlich bezeichneten Vertreterin jedes Departements, der Bundeskanzlei und des NCSC. Der oder die Delegierte hat den Vorsitz.

Art. 19

Aufgehoben

2. Organisationsverordnung vom 17. Februar 2010[14] für das Eidgenössische Finanzdepartement

Art. 20a Abs. 3 Bst. c

Aufgehoben

13 SR **172.215.1**
14 SR **172.215.1**

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Generalsekretariat EFD

Erläuterungen zur Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung

27. Mai 2020

1 Allgemeine Erläuterungen

Mit der Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyberRV) werden die rechtlichen Grundlagen für die departementsübergreifende Organisation des Bundes für den Schutz vor Cyberrisiken geschaffen und die Zuständigkeiten für den Bereich der Cybersicherheit konkretisiert. Es werden insbesondere die Aufgaben und Kompetenzen der neu geschaffenen departementsübergreifenden Gremien «Kerngruppe Cyber» und «Steuerungsausschuss der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS)», der Funktion der oder des Delegierten des Bundes für Cybersicherheit und des Nationalen Zentrums für Cybersicherheit (NCSC) geregelt. Sie löst die bisher in der Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung (BinfV) festgehaltenen Kompetenzen und Zuständigkeiten im Bereich der Informatiksicherheit ab.

2 Erläuterungen zu den einzelnen Bestimmungen

1. Kapitel: Allgemeine Bestimmungen

Art. 1 Gegenstand

Die CyberRV regelt Aufgaben, Zuständigkeiten und die Organisation zum Schutz vor Cyberrisiken innerhalb der Bundesverwaltung. Dazu gehören auch die bisher in der Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung vom 9. Dezember 2011 (BinfV) enthaltenen Bestimmungen zur Informatiksicherheit.

Art. 2 Geltungsbereich

Buchstabe a hält fest, dass die CyberRV für die Verwaltungseinheiten der zentralen Bundesverwaltung nach Artikel 7 der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998[1] (RVOV) gilt. Buchstabe b definiert, welche weiteren Behörden und Stellen sich zur Einhaltung der CybeRV verpflichten. Dies betrifft Behörden und Stellen, welche die in der BinfV (Art. 2 und 3) beschriebenen Bedingungen erfüllen und Mittel der Bundesinformatik einsetzen wollen. In diesem Zusammenhang beschreibt Artikel 16 die Übergangsbestimmungen für Behörden und Stellen, welche sich bereits verpflichtet haben, die Bestimmungen der BinfV einzuhalten.

Art. 3 Begriffe

Der Artikel definiert die Grundbegriffe im Zusammenhang der Cybersicherheit der CyberRV.

a. Die Definition der Cybersicherheit entspricht der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS).
b. Die Definition entspricht ebenfalls jener der NCS. Sie schliesst Schwachstellen mit ein, da diese die Vertraulichkeit, Integrität, Verfügbarkeit oder Authentizität beeinträchtigen, auch wenn nicht festgestellt werden kann, ob sie bereits ausgenutzt worden sind.
c. Unter Cyberrisiko wird die Gefahr eines Cybervorfalls verstanden. Diese im Kontext der NCS etablierte Verwendung des Begriffs ist eine Vereinfachung der in der Fachsprache übliche Unterscheidung zwischen Gefahr (Zustand oder Vorgang aus dem ein Schaden entstehen kann) und Risiko (Messgrösse für die Gefahr).
d. Die Definition von Resilienz entspricht jener der Nationalen Strategie zum Schutz kritischer Infrastrukturen.

e. Zwischen den Begriffen Cybersicherheit und Informatiksicherheit gibt es enge Überschneidungen. In der Verordnung bezeichnet die Informatiksicherheit die technischen Aspekte der Cybersicherheit.
f. Die Definition zeigt auf, welche Art von Vorgaben mit dem Begriff Informatiksicherheitsvorgaben gemeint ist.
g. Die Definition von kritischen Infrastrukturen entspricht jener der Nationalen Strategie zum Schutz kritischer Infrastrukturen.

2. Kapitel: Grundsätze für den Schutz vor Cyberrisiken

Art. 4 Ziele
Absatz 1 formuliert den Schutz der Infrastrukturen der Bundesverwaltung vor Cyberrisiken als Ziel. Diese sollen gegenüber Cyberrisiken resilient sein, was bedeutet, dass sie Cyberangriffen möglichst gut widerstehen und bei erfolgreichen Angriffen ihre Funktionsfähigkeit möglichst lange beibehalten oder nach möglichst kurzer Zeit wiedererlangen.
Absatz 2 definiert die Zusammenarbeit mit den Kantonen, den Gemeinden, der Wirtschaft, der Gesellschaft, der Wissenschaft und den internationalen Partnern als Grundsatz beim Schutz vor Cyberrisiken. Das in Absatz 1 beschriebene Ziel lässt sich nur erreichen, wenn die verantwortlichen Stellen der Bundesverwaltung sich mit diesen Akteuren über Cybervorfälle und mögliche Schutzmassnahmen austauschen.

Art. 5 Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS)
Der Artikel verpflichtet den Bundesrat, die Ziele und Massnahmen im Bereich Schutz vor Cyberrisiken in der NCS festzulegen.

Art. 6 Bereiche
Der Artikel hält die in der NCS definierte Dreiteilung der Aufgabengebiete des Bundes in die Bereiche Cybersicherheit, Cyberdefence und Cyberstrafverfolgung fest. Die Unterteilung der Massnahmen zum Schutz vor Cyberrisiken in die drei Bereiche hilft, die sich aus den bestehenden Zuständigkeiten ergebende Teilung der Aufgaben zwischen den Akteuren der Bundesverwaltung klarer abzugrenzen. Zwischen den Bereichen gibt es verschiedenen Schnittstellen und gegenseitige Abhängigkeiten. Die Aufgabenzuteilung wird deshalb zwischen den beteiligten Verwaltungseinheiten abgesprochen und durch die Kerngruppe Cyber (Artikel 8) koordiniert.

3. Kapitel: Organisation und Zuständigkeiten

1. Abschnitt: Departementsübergreifende Zusammenarbeit

Art. 7 Bundesrat
Die Cyberrisiken entwickeln sich rasch weiter und beim Schutz vor diesen Risiken sind viele Akteure involviert. Es ist daher unabdingbar, dass der Bundesrat die Umsetzung der NCS (Buchstabe a) und die bestehenden Dispositive der Bundesverwaltung (Buchstabe b) laufend prüft und wenn nötig anpasst. Er wird dazu von der Kerngruppe Cyber (Artikel 8) und dem Steuerungsausschuss NCS (Artikel 9) beraten. Der Bundesrat erlässt zudem Weisungen über den Schutz der Bundesverwaltung vor Cyberrisiken (Buchstabe c) und bewilligt Abweichungen von den darin beschriebenen Vorgaben (Buchstabe d).

Art. 8 Kerngruppe Cyber

Der Artikel definiert die Zusammensetzung der Kerngruppe Cyber (KG-Cy) und deren Aufgaben. Die KG-Cy besteht aus Vertretungen der Departementen EFD, EJPD und VBS, welche jeweils die drei Bereiche Cybersicherheit, Cyberstrafverfolgung und Cyberdefence repräsentieren sowie einer der durch die zuständige Konferenz der Kantonsregierungen bestimmten Vertretung der Kantone. Die oder der Delegierte für Cybersicherheit hat den Vorsitz (Absatz 2).

Absatz 3 regelt das Verhältnis der KG-Cy zu den übrigen interessierten, aber nicht in der KG-Cy vertretenen Verwaltungseinheiten. Die KG-Cy ist verpflichtet, weitere Verwaltungseinheiten der Bundesverwaltung über die Traktanden zu informieren und kann diese oder verwaltungsexterne Expertinnen und Experten zu Sitzungen einladen. Bei Belangen mit aussenpolitischem Bezug involviert sie das Eidgenössische Departement für auswärtige Angelegenheiten (EDA).

Absatz 4 definiert die Aufgaben der KG-Cy. Sie beurteilt die aktuellen Cyberrisiken und deren mögliche Entwicklung basierend auf den Informationen aus allen drei Bereichen. Auf der Grundlage dieser Beurteilung prüft sie, ob die Dispositive der Bundesverwaltung den Cyberrisiken entsprechen. Stellt sie Handlungsbedarf fest, beantragt die oder der Delegierte beim Bundesrat entsprechende Massnahmen. Bei einem Cybervorfall begleitet sie die interdepartementale Vorfallbewältigung und informiert die Kerngruppe Sicherheit des Bundes (KGSi) über alle aussen- und sicherheitspolitischen Cybervorfälle und Entwicklungen.

Absatz 5 verpflichtet die in der KG-Cy vertretenen Departemente, die für Einschätzung der Cyberrisiken notwendigen Informationen der KG-Cy zur Verfügung zu stellen. Dies betrifft beispielsweise Fallzahlen und –beispiele, aktuelle technische und methodische Erkenntnisse zu Angriffsmuster.

Absatz 6 präzisiert, dass die Grundlage für die gesamtheitliche Beurteilung der Cyberrisiken durch den Nachrichtendienst des Bundes bereitgestellt wird. Dieser ist zuständig für die Aufbereitung und Darstellung der Informationen aus den verschiedenen Bereichen.

Art. 9 Steuerungsausschuss Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken

Der Artikel definiert die Zusammensetzung und Aufgaben des Steuerungsausschusses Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (StA NCS).

Der StA NCS wird durch den Bundesrat eingesetzt (Absatz 1). Die in Absatz 2 beschriebene breite Vertretung aller beteiligten Verwaltungseinheiten, aller Departemente und der BK sowie der Kantone, Hochschulen und Wirtschaft soll sicherstellen, dass alle relevanten Akteure in die Arbeiten des StA NCS einbezogen werden. Die oder der Delegierte des Bundes für Cybersicherheit hat den Vorsitz (Absatz 3).

Absatz 4 beschreibt die Aufgaben des StA NCS. Er sorgt für die Kohärenz bei der Umsetzung der NCS-Massnahmen (Buchstabe a), definiert nötigenfalls Vorschläge für Sondermassnahmen, welche über die oder den Delegierte/n für Cybersicherheit dem Bundesrat unterbreitet werden (Buchstabe b), sorgt für die laufende Weiterentwicklung der NCS, indem er prüft, ob die NCS der aktuellen Cyberbedrohungslage entspricht (Buchstabe c), erstattet jährlich Bericht über die Umsetzung der NCS (Buchstabe d), koordiniert die beteiligten Akteure (Buchstabe e) und stellt sicher, dass die Arbeiten zur Umsetzung der NCS in Abstimmung mit den Arbeiten zur Umsetzung der Risikopolitik des Bundes, der Nationalen Strategie zum Schutz kritischer Infrastrukturen sowie weiteren Strategien des Bundesrates im Informatikbereich erfolgen (Buchstabe f).

Art. 10 Ausschuss Informatiksicherheit

Der Artikel definiert den Ausschuss Informatiksicherheit (A-IS). Der A-IS setzt sich aus den Informatiksicherheitsbeauftragten der Departemente und der Bundeskanzlei sowie der/dem Informatiksicherheitsbeauftragten der IKT-Standarddienste zusammen. Fallweise können weitere Personen beratend beigezogen werden. Geleitet wird er von einer Vertreterin oder einem Vertreter des NCSC. Der A-IS ist das Konsultativorgan für das Nationale Zentrum für Cybersicherheit (NCSC) zu Informatiksicherheitsfragen in der Bundesverwaltung.

Art. 11 Delegierte oder Delegierter für Cybersicherheit

Absatz 1 beschreibt die Aufgaben der oder des Delegierten für Cybersicherheit. Sie oder er leitet das

NCSC (Buchstabe a) und vertritt dieses in den Krisenstäben des Bundes (Buchstabe d), hat darüber hinaus aber auch koordinative (Buchstabe b) und repräsentative Aufgaben (Buchstabe c) in Bezug auf alle drei in Artikel 6 beschriebenen Bereichen des Bundes zum Schutz vor Cyberrisiken. Über die bereichsübergreifenden Aufgaben nimmt sie oder er die Funktion als zentrale Ansprechperson des Bundes für Cyberrisiken wahr.
Die oder der Delegierte verantwortet die Risiken des Bundes in der Informatiksicherheit. Sie oder er kann in Absprache mit der Eidgenössischen Finanzkontrolle Überprüfungen der Informatiksicherheit verlangen (Absatz 4), sich bei sicherheitsrelevanten Informatikvorhaben beteiligen, Stellung dazu nehmen und nötigenfalls Änderungen verlangen (Absatz 3) sowie Sicherheitsvorgaben für die Informatik erlassen und Ausnahmen davon genehmigen (Absatz 1 Buchstabe e). Da Sicherheitsvorgaben häufig in engem Zusammenhang mit generellen IKT-Vorgaben stehen, arbeitet der oder die Delegierte mit dem Informatiksteuerungsorgan des Bundes (ISB) zusammen und hört sich dieses vor Entscheidungen über Abweichungen von Vorgaben an (Absatz 1 Buchstabe f). Zu den Aufgaben im Bereich Informatiksicherheit zählt auch die Information des Bundesrates über den Stand der Informatiksicherheit in den Departementen (Absatz 2).

2. Abschnitt: Organe des Bereichs Cybersicherheit

Art. 12 Nationales Zentrum für Cybersicherheit
Das Nationale Zentrum für Cybersicherheit (NCSC) ist zuständig für die Koordination der Arbeiten der verschiedenen mit Aufgaben zum Schutz vor Cyberrisiken betrauten Verwaltungseinheiten. Gleichzeitig übernimmt es selbst wesentliche Aufgaben. Dadurch funktioniert das NCSC als nationales Kompetenzzentrum für die Cybersicherheit.
Absatz 1 beschreibt die Aufgaben des NCSC.

a. Die nationale Anlaufstelle nimmt Meldungen aus der Bundesverwaltung, der Wirtschaft, den Kantonen und der Bevölkerung entgegen, bewertet und kategorisiert die eingegangenen Meldungen und beantwortet diese. Die Anlaufstelle pflegt den Austausch zu den zuständigen Stellen der Strafverfolgung und informiert diese unter Einhaltung der gesetzlichen Vorgaben bezüglich Datenschutz über die eingegangenen Meldungen.
b. Beim Schutz kritischer Infrastrukturen vor Cyberrisiken arbeitet das NCSC eng mit den für die jeweiligen kritischen Sektoren zuständigen Stellen (Verwaltungseinheiten, Kantone, Kommissionen) zusammen sowie mit dem Bundesamt für Bevölkerungsschutz und dem Bundesamt für wirtschaftliche Landesversorgung. Ziel der Arbeiten ist die subsidiäre Unterstützung der Betreiber kritischer Infrastrukturen, durch Informationen und spezifische Einschätzungen zu Cyberrisiken und möglichen Schutzmassnahmen. Subsidiär bedeutet, dass die Betreiber kritischer Infrastrukturen für den eigenen Schutz zuständig bleiben und sich die Unterstützung auf Hilfe beschränkt, welche nicht auf dem Markt beschafft werden kann.
c. Das «Computer Emergency Response Team» (GovCERT) ist die technische Fachstelle des NCSC. Es tritt als nationales CERT auf und nimmt diese Rolle gegenüber CERTs aus anderen Staaten wahr. Es arbeitet in dieser Rolle eng mit Sicherheitsteams staatlicher oder privater Organisationen zusammen und koordiniert technische Massnahmen zur Verbesserung der Cybersicherheit in der Schweiz.
d. Die Fachstelle für die Informatiksicherheit des Bundes erlässt den aktuellen Risiken entsprechend bundesweite Informatiksicherheitsvorgaben, unterstützt die Delegierte oder den Delegierten für Cybersicherheit bezüglich Entscheide über Abweichungen von diesen und überprüft deren Umsetzung. Damit strebt sie ein angemessenes und dem Cyberrisiko entsprechendes Sicherheitsniveau in der Bundesverwaltung an. Sie unterstützt dabei die Departemente und die Bundeskanzlei bei Fragen zur Cybersicherheit.
e. Das NCSC stellt die Informatiksicherheitsbeauftragten des Bundes (ISBB). Diese koordinieren die IKT-Sicherheitsaspekte innerhalb der Bundesverwaltung und übernehmen die fachliche Führung der Informatiksicherheitsbeauftragten der Departemente (Artikel 13 Absatz3). Sie übernehmen nach Artikel 12 Absatz 5 die Federführung bei der Bewältigung eines Cybervorfalls, wenn dieser das ordnungsgemässe Funktionieren der Bundesverwaltung gefährdet.

f. Für die Koordination der Umsetzung der NCS, die Durchführung des strategischen Controllings und die administrative Vor- und Nachbereitungen der Sitzungen der KG-Cy und des StA NCS führt das NCSC eine Geschäftsstelle unter der direkten Leitung der oder des Delegierten für Cybersicherheit.
g. Das NCSC führt einen Expertenpool, über welchen die an der Umsetzung der NCS beteiligten Stellen personelle Ressourcen mit spezifischer Expertise zur Cybersicherheit zur fachlichen Unterstützung ihrer Arbeiten beziehen können. Der Expertenpool bündelt so Fachwissen und personelle Ressourcen und fördert den regelmässigen Austausch innerhalb der Bundesverwaltung. Experten der Verwaltungseinheiten werden in die Arbeiten des Expertenpools einbezogen und nehmen am Austausch zwischen den Experten teil.
h. Das NCSC trägt mit gezielten Informationen und Kampagnen zur Sensibilisierung der Bundesverwaltung und der Öffentlichkeit vor Cyberrisiken bei, informiert über die aktuelle Lage und gibt Anleitungen für präventive und reaktive Massnahmen heraus und stärkt so das Bewusstsein für Cyberrisiken.
i. Das NCSC betreibt eine resiliente Analyse- und Kommunikationsinfrastruktur, insbesondere für den Betrieb der nationalen Anlaufstelle und des nationalen CERTs, die unabhängig von der Bundesinformatik funktionieren muss. Das NCSC ist damit Leistungserbringer für diese spezifische IKT-Infrastruktur und dafür verantwortlich, dass diese gegen Cyberangriffe geschützt ist und gewährleistet ist, dass Meldungen entgegengenommen und bearbeitet werden können.
j. Das NCSC informiert die Kerngruppe Cyber sowie bei aussen- und sicherheitspolitischer Bedeutung die Kerngruppe Sicherheit des Bundes (KGSi) über relevante Cybervorfälle und stellt so sicher, dass die interdepartementalen Gremien über alle nötigen Informationen für ihre Arbeit verfügen.

Die Absätze 2-4 regeln die Kompetenzen des NCSC bei der Datenbearbeitung im Zusammenhang mit Cybervorfällen. Es darf dann solche Daten bearbeiten, wenn dies direkt oder indirekt dem Schutz der Bundesverwaltung dient. Weil es bei der Vorfallbewältigung nötig sein kann, Daten an beteiligte Sicherheitsteams weiterzugeben, darf das NCSC dies tun, wenn der Datenlieferant einverstanden ist und keine Geheimhaltungspflichten verletzt werden. Für die Weitergabe von Daten ins Ausland sind die Vorgaben des Datenschutzgesetzes (insbes. Art. 6 des Bundesgesetzes über den Datenschutz) einzuhalten (Absatz 3). Absatz 4 bedeutet, dass das NCSC besonders schützenswerte Personendaten nur bearbeiten darf, soweit es für die Bearbeitung der fraglichen Daten eine genügende gesetzliche Grundlage gibt. Soweit ein Gesetz die Bearbeitung der Daten durch eine der Bundesinformatik unterstehende Behörde vorsieht, kann diese die Bearbeitung dem NCSC übertragen, wenn a. die Daten nur so bearbeitet werden, wie der Auftraggeber selbst es tun dürfte; und b. keine gesetzlichen oder vertraglichen Geheimhaltungspflichten dies verbieten (Art. 10a Abs. 1 des Datenschutzgesetzes).
Absatz 5 regelt die Zuständigkeit des NCSC bei einem Cybervorfall in der Bundesverwaltung. Es kann die Federführung für die Bewältigung eines Vorfalls übernehmen, wenn dieser das ordnungsgemässe Funktionieren der Bundesverwaltung gefährdet. In diesem Fall erhält es die Befugnis, Informationen einzufordern und Sondermassnahmen anzuordnen. Das NCSC ist verpflichtet, die betroffenen Verwaltungseinheiten über den Verlauf zu informieren und die Verantwortung für die Bewältigung des Vorfalls wieder abzugeben, wenn die Gefährdung für die Bundesverwaltung durch den Vorfall angemessen reduziert wurde und die Folgearbeiten und deren Finanzierung geklärt sind.

Art. 13 Departemente und Bundeskanzlei

Der Artikel definiert die Aufgaben der Departemente und der Bundeskanzlei und definieren deren Meldepflichten an das NCSC. Jeweils zum Jahresende erstatten die Departemente einen Bericht über ihren Stand der Informatiksicherheit (Absatz 1). Die internen Leistungserbringer der Bundesverwaltung sind zudem verpflichtet, dem NCSC regelmässig Bericht über entdeckte Schwachstellen, Vorfälle und getroffene Massnahmen zu erstatten (Absatz 2). Absatz 3 schreibt vor, dass alle Departemente und die BK je eine Informatiksicherheitsbeauftragte oder einen Informatiksicherheitsbeauftragten (ISBD) bestimmen müssen.

Art. 14 Verwaltungseinheiten

Der Artikel definiert die Verantwortlichkeiten der einzelnen Verwaltungseinheiten und ihrer Leistungserbringer beim Schutz vor Cyberrisiken. Alle Verwaltungseinheiten stellen je eine Informatiksicherheitsbeauftragte oder einen Informatiksicherheitsbeauftragten (Absatz 1). Deren Aufgaben sind in den Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung definiert.
In Absatz 2 wird festgehalten, dass sich die Verwaltungseinheiten selbst für den Schutz ihrer Informatiksysteme, Anwendungen und Daten (Schutzobjekte) verantwortlich zeigen. Daraus ergeben sich die Pflicht zur regelmässigen Prüfung der Schutzobjekte und der Definition und Dokumentation von Massnahmen zu deren Schutz (Buchstabe a); die Verantwortung zur Einhaltung der Informatiksicherheitsvorgaben (Buchstabe b); die Verantwortung zur Bewältigung von Cybervorfällen, welche ihre Schutzobjekte betreffen (Buchstabe c), sofern die Vorfällen nicht unter die in Artikel 12 Absatz 5 definierte Kategorie fallen; zur Sicherstellung der Einhaltung der Informatiksicherheitsvorgaben beim Bezug von externen Leistungen und zur Prüfung, dass diese eingehalten werden (Buchstaben d und e).
Absatz 3 und 4 definieren die Pflichten der Leistungserbringer. Diese müssen sicherstellen, dass sie über die nötigen Kapazitäten zur Bewältigung von Cybervorfällen bei sich und ihren Leistungsbezügern verfügen (Absatz 3) und melden diesen entdeckte Schwachstellen und Vorfälle unverzüglich.
Absatz 5 schreibt vor, dass die Leistungserbringer und –bezüger gemeinsam einen Prozess zur Vorfallbewältigung definieren, in welchem die die Entscheidungskompetenzen geregelt werden. Dieser Prozess ist auch massgeblich dafür, welche Kapazitäten gemäss Absatz 3 beim Leistungserbringer vorhanden sein müssen.
Absatz 6 schreibt vor, dass das NCSC zu involvieren ist, wenn der Cybervorfall nicht im Rahmen des nach Absatz 5 definierten Prozess bewältigt werden kann.
Absatz 7 bestimmt, dass das NCSC bei sicherheitsrelevanten Informatikvorgaben und –vorhaben konsultiert werden muss.
Absatz 8 hält fest, dass die Verwaltungseinheiten für ihre Sektoren auch in Bezug auf den Schutz vor Cyberrisiken zuständig bleiben. Sie können für diese Tätigkeit auf Expertinnen und Experten aus dem Pool des NCSC (nach Artikel 12 Absatz 1 Buchstabe g) zurückgreifen.

4. Kapitel: Schluss- und Übergangsbestimmungen

Art. 15 Änderung anderer Erlasse
Durch die CyberRV werden Änderungen an der BInfV nötig. Die Bestimmungen der BinfV mit Relevanz für die Informatik- und Cybersicherheit werden in der BInfV gestrichen und in die CyberRV übertragen. In der Organisationsverordnung EFD wird zudem Artikel 20a Absatz 3 Buchstabe c gestrichen, in welchem festgehalten war, dass das ISB den Betrieb kritischer Informationsinfrastrukturen in der Schweiz unterstützt.

Art. 16 Übergangsbestimmungen zu Art. 2 Bst. b
Bisher konnten sich Behörden und Stellen gemäss BinfV Art. 2 verpflichten, die Bestimmungen der BinfV einzuhalten, wenn sie Mittel der Bundesinformatik nutzen wollten. Als Übergangsbestimmung sollen diese Verpflichtungen im gleichen Umfang bis 31. Dezember 2021 gelten. Ab 1. Januar 2022 unterstehen sie dann der CyberRV, wenn sie die Vereinbarung nicht kündigen.

Art. 17 Übergangsbestimmung zu Art. 11 Abs. 1 Bst. e
Die vom ISB erlassenen und durch das ISB genehmigten Ausnahmebewilligungen zu IKT-Sicherheitsvorgaben bleiben gültig. Das NCSC entscheidet über allfällige Änderungen.

Art. 18 Inkrafttreten
Die Verordnung tritt am 1. Juli 2020 in Kraft.