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.