BUNDESGESETZBLATT
FÜR DIE REPUBLIK ÖSTERREICH

Jahrgang 2019 **Ausgegeben am 17. Juli 2019** **Teil II**

215. Verordnung: **Netz- und Informationssystemsicherheitsverordnung – NISV**

215. Verordnung des Bundesministers für EU, Kunst, Kultur und Medien zur Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren sowie zu Sicherheitsvorfällen nach dem Netz- und Informationssystemsicherheitsgesetz (Netz- und Informationssystemsicherheitsverordnung – NISV)

Auf Grund des § 4 Abs. 2 des Netz- und Informationssystemsicherheitsgesetzes (NISG), BGBl. I Nr. 111/2018, wird im Einvernehmen mit dem Bundesminister für Inneres verordnet:

Inhaltsverzeichnis

1. Abschnitt
Allgemeine Bestimmungen

Gegenstand der Verordnung

§ 1. Gegenstand dieser Verordnung ist die Festlegung

1. von Kriterien für die Parameter zu Sicherheitsvorfällen gemäß § 3 Z 6 lit. a bis d NISG;
2. näherer Regelungen zu den in § 2 NISG genannten Sektoren gemäß § 16 Abs. 2 NISG;
3. von Sicherheitsvorkehrungen nach § 17 Abs. 1 NISG;

4. von Ausnahmen von Verpflichtungen für Betreiber wesentlicher Dienste gemäß § 20 Abs. 1 NISG.

Begriffsbestimmungen zu wesentlichen Diensten

§ 2. Im Sinne dieser Verordnung bedeutet

1. „Internet-Knoten“ (IXP – Internet Exchange Point) eine Netzeinrichtung, die die Zusammenschaltung von mehr als zwei unabhängigen autonomen Systemen ermöglicht, in erster Linie zur Erleichterung des Austauschs von Internet-Datenverkehr;
2. „Domain-Namen-System“ (DNS) ein hierarchisch unterteiltes Bezeichnungssystem in einem Netz zur Beantwortung von Anfragen zu Domain-Namen;
3. „Top-Level-Domain-Name-Registry“ eine Einrichtung, die die Registrierung von Internet-Domain-Namen innerhalb einer spezifischen Top-Level-Domain (TLD) verwaltet und betreibt;
4. „DNS-Resolver“ Programme, die Informationen von DNS-Servern zur Beantwortung von Client-Anfragen abfragen (Namensauflösung) und bei Unkenntnis der Antwort die Client-Anfragen an übergeordnete DNS-Server weiterreichen;
5. „Autoritativer DNS-Server“ ein Server, der den Inhalt einer DNS-Zone kennt und somit Abfragen zu dieser Zone beantworten kann, ohne andere DNS-Server abfragen zu müssen;
6. „Verkehrssteuerungs- und Leitsysteme“ Einrichtungen zur Regelung und Sicherung des Verkehrs, deren Funktionsfähigkeit von Netz- und Informationssystemen abhängig ist;
7. „kommunaler Straßenverkehr“ der Straßenverkehr in Städten mit mehr als 88 000 Einwohnern;
8. „Krankenanstalten“
   a) öffentliche Krankenanstalten gemäß § 2 Abs. 1 Z 1 des Bundesgesetzes über Krankenanstalten- und Kuranstalten (KAKuG), BGBl. Nr. 1/1957, mit Ausnahme der Pflegeabteilungen in öffentlichen Krankenanstalten für Psychiatrie;
   b) private Krankenanstalten der im § 2 Abs. 1 Z 1 KAKuG bezeichneten Art, die gemäß § 16 KAKuG gemeinnützig geführte Krankenanstalten sind;
   c) Sonderkrankenanstalten gemäß § 2 Abs. 1 Z 2 KAKuG, die überwiegend unfallchirurgische Akutversorgung leisten und gemeinnützig geführt sind;
9. „Versorgungsregionen“ die 32 Versorgungsregionen gemäß dem Österreichischen Strukturplan Gesundheit (ÖSG);
10. „zentral gelegene Versorgungsregionen mit großem Einzugsgebiet“
    a) Versorgungsregionen mit mehr als 300 000 Einwohnern, sofern in diesen eine Landeshauptstadt gelegen ist;
    b) die Versorgungsregionen in der Bundeshauptstadt;
11. „akutambulante ärztliche Versorgung“ die ambulante ärztliche Versorgung, die rund um die Uhr oder während der Öffnungszeiten ohne Terminvereinbarung zur Verfügung steht.

Begriffsbestimmungen zu Sicherheitsvorfällen

§ 3. Im Sinne dieser Verordnung bedeutet

1. „Ausfall des betriebenen Dienstes“ die Unverfügbarkeit des Dienstes für Nutzer;
2. „Einschränkung der Verfügbarkeit des betriebenen Dienstes“ die signifikant geminderte Verfügbarkeit des Dienstes in qualitativer Dimension für Nutzer;
3. „Zahl der von dem Sicherheitsvorfall betroffenen Nutzer, insbesondere der Nutzer, die den Dienst für die Bereitstellung ihrer eigenen Dienste benötigen“ (§ 3 Z 6 lit. a NISG) die Zahl der von einem Sicherheitsvorfall betroffenen natürlichen und juristischen Personen, mit denen ein Vertrag über die Bereitstellung des Dienstes abgeschlossen wurde, oder die Zahl der betroffenen Nutzer, die den Dienst im Zeitpunkt des Sicherheitsvorfalls genutzt haben oder für die voraussichtliche Dauer des Sicherheitsvorfalls nutzen würden;
4. „Dauer des Sicherheitsvorfalls“ (§ 3 Z 6 lit. b NISG) der in Stunden angegebene Zeitraum vom Ausfall oder von der Einschränkung der Verfügbarkeit des betriebenen Dienstes bis zum Zeitpunkt der uneingeschränkten Wiederherstellung;
5. „geografische Ausbreitung in Bezug auf das von dem Sicherheitsvorfall betroffene Gebiet“ (§ 3 Z 6 lit. c NISG) eine geografische Ausbreitung, bei der der Ausfall oder die Einschränkung der Verfügbarkeit des betriebenen wesentlichen Dienstes Gebiete in einem oder mehreren Mitgliedstaaten der Europäischen Union oder der Europäischen Freihandelsassoziation betrifft;
6. „Auswirkung auf wirtschaftliche und gesellschaftliche Tätigkeiten“ (§ 3 Z 6 lit. d NISG) nachteilige Auswirkungen auf Einrichtungen und Personen, insbesondere betroffene Nutzer,

unabhängig davon, ob diese Auswirkungen materielle oder immaterielle Verluste für diese verursacht haben;

7. „Nutzerstunden“ das Produkt der Anzahl der von dem Sicherheitsvorfall betroffenen Nutzer (Z 3) mit der Dauer des Sicherheitsvorfalls (Z 4);
8. „Zählpunktstunden“ das Produkt der Anzahl der Zählpunkte mit der Dauer des Sicherheitsvorfalls (Z 4).

2. Abschnitt
Wesentliche Dienste und Sicherheitsvorfälle

Sektor Energie

§ 4. (1) Wegen ihrer Bedeutung für die Aufrechterhaltung der öffentlichen Versorgung mit Energie im Sinne des § 16 Abs. 2 NISG sind im Sektor Energie wesentliche Dienste:

1. im Teilsektor Elektrizität
   a) im Bereich der Stromerzeugung
      aa) der Betrieb einer Erzeugungsanlage, die mehr als 340 MW Engpassleistung hat;
      bb) der Betrieb von Systemen zur Steuerung von Erzeugungsanlagen, die zusammen mehr als 340 MW Engpassleistung haben;
   b) im Bereich der Stromverteilung der Betrieb eines Verteilernetzes, über das Elektrizität an mehr als 88 000 Zählpunkte transportiert wird, oder das in einer Landeshauptstadt gelegen ist;
   c) im Bereich der Stromübertragung der Betrieb eines Übertragungsnetzes durch Übertragungsnetzbetreiber;
2. im Teilsektor Erdöl
   a) im Bereich der Erdölförderung der Betrieb von Anlagen zur Förderung von Erdöl, wenn die geförderte Menge mehr als 20% Anteil am jährlichen inländischen Mineralölverbrauch ausmacht;
   b) im Bereich der Erdöllagerung der Betrieb einer Anlage, in der Pflichtnotstandsreserven in Form von Erdöl, Erdölprodukten, Biokraftstoffen oder Rohstoffen zur direkten Erzeugung von Biokraftstoffen gelagert werden, und die einen Lagerbestand von mehr als 10 000 Tonnen hat;
   c) im Bereich des Erdöltransports der Betrieb einer Erdölfernleitung, wenn die transportierte Menge vier Millionen Tonnen pro Jahr übersteigt;
   d) im Bereich der Erdölraffination der Betrieb von Anlagen zur Raffination und Aufbereitung von Erdöl, die mehr als acht Millionen Tonnen pro Jahr verarbeiten;
3. im Teilsektor Erdgas
   a) im Bereich der Gasförderung der Betrieb von Gasförderungsanlagen, wenn die geförderte Menge mehr als 20% Anteil am jährlichen Inlandgasverbrauch ausmacht;
   b) im Bereich der Gasspeicherung der Betrieb einer Speicheranlage, die mehr als 10 000 GWh Arbeitsgasvolumen pro Jahr hat;
   c) im Bereich des Gastransports der Betrieb einer Fernleitungsanlage;
   d) im Bereich der Gasverteilung der Betrieb eines Verteilernetzes, über das Erdgas an mehr als 88 000 Zählpunkte transportiert wird;
   e) im Bereich des Marktgebietsmanagements die Koordination der Netzsteuerung und des Einsatzes von Netzpufferung (Linepack) sowie der Abruf der physikalischen Ausgleichsenergie;
   f) im Bereich des Verteilergebietsmanagements
      aa) der Abruf der physikalischen Ausgleichsenergie im Verteilergebiet;
      bb) die Bereitstellung der Systemdienstleistung (Leistungs- und Druckregelung bzw. Druckhaltung) durch Vornahme des technisch-physikalischen Ausgleichs;
      cc) die Steuerung der Verteilerleitungsanlagen der Netzebene 1 durch Vorgaben an die Verteilernetzbetreiber.

(2) Im Sektor Energie liegt ein Sicherheitsvorfall im Sinne des § 3 Z 6 NISG vor, wenn

1. im Teilsektor Elektrizität
   a) im Bereich der Stromerzeugung
      aa) bei dem in Abs. 1 Z 1 lit. a sublit. aa genannten Dienst die Erzeugungsleistung einer Erzeugungsanlage in Summe um mehr als 340 MW verringert ist;

bb) bei dem in Abs. 1 Z 1 lit. a sublit. bb genannten Dienst die von den Systemen steuerbare Erzeugungsleistung aller Erzeugungsanlagen in Summe um mindestens 340 MW verringert ist;

b) im Bereich der Stromverteilung der in Abs. 1 Z 1 lit. b genannte Dienst für mehr als 1 056 000 Zählpunktstunden ausfällt oder nur eingeschränkt verfügbar ist;

c) im Bereich der Stromübertragung der in Abs. 1 Z 1 lit. c genannte Dienst für mehr als drei Stunden ausfällt oder nur eingeschränkt verfügbar ist;

2. im Teilsektor Erdöl

a) der in Abs. 1 Z 2 lit. a genannte Dienst für mehr als 24 Stunden ausfällt oder nur eingeschränkt verfügbar ist;

b) der in Abs. 1 Z 2 lit. b genannte Dienst für mehr als 24 Stunden ausfällt oder nur eingeschränkt verfügbar ist;

c) bei dem in Abs. 1 Z 2 lit. c genannten Dienst die geografische Ausbreitung in Bezug auf das von dem Sicherheitsvorfall betroffene Gebiet mehr als einen Mitgliedstaat der Europäischen Union betrifft;

d) der in Abs. 1 Z 2 lit. d genannte Dienst für mehr als 24 Stunden ausfällt oder nur eingeschränkt verfügbar ist;

3. im Teilsektor Erdgas

a) im Bereich der Gasförderung der in Abs. 1 Z 3 lit. a genannte Dienst für mehr als 24 Stunden ausfällt oder nur eingeschränkt verfügbar ist;

b) im Bereich der Gasspeicherung der in Abs. 1 Z 3 lit. b genannte Dienst für mehr als zwölf Stunden ausfällt oder nur eingeschränkt verfügbar ist;

c) im Bereich des Gastransports bei dem in Abs. 1 Z 3 lit. c genannten Dienst die geografische Ausbreitung in Bezug auf das von dem Sicherheitsvorfall betroffene Gebiet mehr als einen Mitgliedstaat der Europäischen Union betrifft;

d) im Bereich der Gasverteilung der in Abs. 1 Z 3 lit. d genannte Dienst für mehr als 1 056 000 Zählpunktstunden ausfällt oder nur eingeschränkt verfügbar ist;

e) im Bereich des Marktgebietsmanagements der in Abs. 1 Z 3 lit. e genannte Dienst für mehr als zwölf Stunden ausfällt oder nur eingeschränkt verfügbar ist;

f) im Bereich des Verteilergebietsmanagements einer der in Abs. 1 Z 3 lit. f genannten Dienste für mehr als zwöf Stunden ausfällt oder nur eingeschränkt verfügbar ist.

(3) Unbeschadet der Begriffsbestimmungen in § 2 gelten

1. im Teilsektor Elektrizität für die in Abs. 1 Z 1 verwendeten Begriffe die Begriffsbestimmungen des Elektrizitätswirtschafts- und -organisationsgesetzes 2010 (ElWOG 2010), BGBl. I Nr. 110/2010;
2. im Teilsektor Erdöl für die in Abs. 1 Z 2 lit. c verwendeten Begriffe die Begrifflichkeiten des Erdölbevorratungsgesetzes 2012 (EBG 2012), BGBl. I Nr. 78/2012;
3. im Teilsektor Erdgas für die in Abs. 1 Z 3 verwendeten Begriffe die Begriffsbestimmungen des Gaswirtschaftsgesetzes 2011 (GWG 2011), BGBl. I Nr. 107/2011.

Sektor Verkehr

§ 5. (1) Wegen ihrer Bedeutung für die Aufrechterhaltung des öffentlichen Verkehrs im Sinne des § 16 Abs. 2 NISG sind im Sektor Verkehr wesentliche Dienste:

1. im Teilsektor Luftverkehr

a) die Beförderung von Personen im gewerblichen Luftverkehr durch ein Luftverkehrsunternehmen, das mehr als 33% der jährlich abgefertigten Passagiere an einem Flughafen befördert, der jährlich mehr als zehn Millionen Passagiere abfertigt;

b) im Bereich des Betriebes eines Flughafens die Flugabwicklung, insbesondere die Fluggastabfertigung und die Gepäckabfertigung sowie der Betrieb der Sicherheitssysteme, an einem Flughafen, der jährlich mehr als zehn Millionen Passagiere abfertigt;

c) im Bereich der Flugsicherung

aa) Flugsicherungsdienste durch Einrichtungen, denen die Wahrnehmung der Flugsicherung als hoheitliche Aufgabe des Bundes nach dem Luftfahrtgesetz (LFG), BGBl. Nr. 253/1957, obliegt;

bb) Flugplatzkontrolldienste an einem Flughafen, der jährlich mehr als zehn Millionen Passagiere abfertigt;

2. im Teilsektor Schienenverkehr
   a) im Bereich der Infrastruktur
      aa) der Betrieb von Eisenbahninfrastrukturen, die mehr als 100 km Teil des Kernnetzes des transeuropäischen Verkehrsnetzes nach der Kartendarstellung 5.3 des Anhanges 1 der Verordnung (EU) Nr. 1315/2013 über Leitlinien der Union für den Aufbau eines transeuropäischen Verkehrsnetzes und zur Aufhebung des Beschlusses Nr. 661/2010/EU, ABl. Nr. L 348 vom 20.12.2013 S. 1, sind;
      bb) der Betrieb von Personenhauptbahnhöfen in Landeshauptstädten;
   b) im Bereich der Eisenbahnverkehrsdienste
      aa) die schienengebundene Personenbeförderung von mehr als 300 Millionen Passagieren im Jahr;
      bb) die schienengebundene Beförderung von mehr als 100 Millionen Tonnen Güter im Jahr;
3. im Teilsektor Straßenverkehr
   a) der Betrieb der Verkehrssteuerungs- und Leitsysteme des Bundesstraßennetzes;
   b) der Betrieb der Verkehrssteuerungs- und Leitsysteme im kommunalen Straßenverkehr;
   c) der Betrieb der Verkehrssteuerungs- und Leitsysteme in Tunneln nach dem Straßentunnel-Sicherheitsgesetz (STSG), BGBl. I Nr. 54/2006.

(2) Im Sektor Verkehr liegt ein Sicherheitsvorfall im Sinne des § 3 Z 6 NISG vor, wenn
1. im Teilsektor Luftverkehr
   a) der in Abs. 1 Z 1 lit. a genannte Dienst für mehr als drei Stunden ausfällt oder nur eingeschränkt verfügbar ist;
   b) im Bereich des Betriebes eines Flughafens innerhalb von 24 Stunden mehr als ein Drittel der Nutzer eines durchschnittlichen Tagesaufkommens, gemessen am Medianwert des vorangegangenen Kalenderjahres, von einem Ausfall oder der Einschränkung der Verfügbarkeit des in Abs. 1 Z 1 lit. b genannten Dienstes betroffen sind;
   c) im Bereich der Flugsicherung der in Abs. 1 Z 1 lit. c sublit. aa oder bb genannte Dienst für mehr als drei Stunden ausfällt oder nur eingeschränkt verfügbar ist;
2. im Teilsektor Schienenverkehr
   a) im Bereich der Infrastruktur
      aa) der in Abs. 1 Z 2 lit. a sublit. aa genannte Dienst für mehr als zwölf Stunden ausfällt oder nur eingeschränkt verfügbar ist;
      bb) der in Abs. 1 Z 2 lit. b sublit. bb genannte Dienst für mehr als zwölf Stunden ausfällt oder nur eingeschränkt verfügbar ist;
   b) im Bereich der Eisenbahnverkehrsdienste
      aa) der in Abs. 1 Z 2 lit. b sublit. aa genannte Dienst für mehr als drei Stunden ausfällt oder nur eingeschränkt verfügbar ist;
      bb) der in Abs. 1 Z 2 lit. b sublit. bb genannte Dienst für mehr als 24 Stunden ausfällt oder nur eingeschränkt verfügbar ist;
3. im Teilsektor Straßenverkehr
   a) in Folge eines Ausfalls oder der eingeschränkten Verfügbarkeit des in Abs. 1 Z 3 lit. a genannten Dienstes eine zuständige Behörde für mehr als sechs Stunden angesetzte Verkehrsverbote oder Verkehrsbeschränkungen erlassen hat;
   b) der in Abs. 1 Z 3 lit. b genannte Dienst für mehr als drei Stunden ausfällt oder nur eingeschränkt verfügbar ist;
   c) der in Abs. 1 Z 3 lit. a oder c genannte Dienst für mehr als sechs Stunden ausfällt oder nur eingeschränkt verfügbar ist.

(3) Unbeschadet der Begriffsbestimmungen in § 2 gelten
1. im Teilsektor Luftverkehr für die in Abs. 1 Z 1 lit. a und b verwendeten Begriffe die Begriffsbestimmungen des LFG und für die in Abs. 1 Z 1 lit. c sublit. aa und bb verwendeten Begriffe die Begriffsbestimmungen der Verordnung (EG) Nr. 549/2004, ABl. L 96 vom 31.3.2004 S. 1;
2. im Teilsektor Schienenverkehr für die in Abs. 1 Z 2 lit. a sublit. aa verwendeten Begriffe die Begriffsbestimmungen des Eisenbahngesetzes 1957 (EisbG), BGBl. Nr. 60/1957;
3. im Teilsektor Straßenverkehr für die in Abs. 1 Z 3 lit. a verwendeten Begriffe die Begriffsbestimmungen des Bundesstraßengesetzes 1971 (BStG 1971), BGBl. Nr. 286/1971.

Sektor Bankwesen

§ 6. (1) Wegen ihrer Bedeutung für die Aufrechterhaltung des Zahlungsverkehrs im Sinne des § 16 Abs. 2 NISG sind im Sektor Bankwesen wesentliche Dienste:

1. der Betrieb von Systemen zur Erbringung von Diensten, mit denen Bareinzahlungen auf ein Zahlungskonto ermöglicht werden;
2. der Betrieb von Systemen zur Erbringung von Diensten, mit denen Barabhebungen von einem Zahlungskonto ermöglicht werden;
3. der Betrieb von Systemen zur Ausführung von Zahlungsvorgängen einschließlich des Transfers von Geldbeträgen auf ein Zahlungskonto beim Zahlungsdienstleister des Zahlungsdienstnutzers oder bei einem anderen Zahlungsdienstleister;
4. der Betrieb von Systemen zur Ausführung von Zahlungsvorgängen, wenn die Beträge durch einen Kreditrahmen für einen Zahlungsdienstnutzer gedeckt sind.

(2) Im Sektor Bankwesen liegt ein Sicherheitsvorfall im Sinne des § 3 Z 6 NISG vor, wenn

1. der Vorfall eine mögliche finanzielle Auswirkung von mehr als fünf Millionen Euro oder 0,1% des harten Kernkapitals hat;
2. eine öffentliche Berichterstattung über den Vorfall stattfand;
3. eine Person in Leitungsfunktion über den Vorfall (§ 3 Z 7 NISG) unterrichtet wurde, sofern diese üblicherweise nicht über Risiken (§ 3 Z 8 NISG) oder Vorfälle unterrichtet wird und es sich nicht um eine regelmäßige oder routinemäßige Berichterstattung handelt;
4. das Betriebskontinuitätsmanagement, Notfallmanagement oder ein anderer interner Krisenplan auf Ebene der Gruppe angewendet wird;
5. zur Deckung finanzieller Verluste eine Cyberversicherung herangezogen wird.

(3) Im Sektor Bankwesen bestehen für Betreiber eines wesentlichen Dienstes im Sinne des Abs. 1 Z 1 bis 4 zu Sicherheitsvorkehrungen in § 85 des Zahlungsdienstegesetzes 2018 (ZaDiG 2018), BGBl. I Nr. 17/2018, und zur Meldepflicht in § 86 ZaDiG 2018 Vorschriften, die zumindest ein gleichwertiges Sicherheitsniveau für Netz- und Informationssysteme gemäß § 20 NISG gewährleisten.

(4) Als Betreiber wesentlicher Dienste im Sinne des Abs. 1 können nur CRR-Kreditinstitute, übergeordnete Kreditinstitute oder Zentralorganisationen von Kreditinstitute-Verbünden im Sinne des Bankwesengesetzes (BWG), BGBl. Nr. 532/1993, ermittelt werden, deren Gesamtwert der Aktiva 30 Milliarden Euro übersteigt. Bei übergeordneten Kreditinstituten ist der Gesamtwert der Aktiva der Kreditinstitutsgruppe gemäß § 30 BWG, bei Zentralorganisationen der Gesamtwert der Aktiva des Kreditinstitute-Verbunds gemäß § 30a BWG zu berücksichtigen.

Sektor Finanzmarktinfrastrukturen

§ 7. (1) Wegen ihrer Bedeutung für die Aufrechterhaltung des Handelsplatzes sind im Sektor Finanzmarktinfrastrukturen wesentliche Dienste im Sinne des § 16 Abs. 2 NISG:

1. im Bereich der Handelsplätze (§ 1 Z 12 des Börsegesetzes 2018 (BörseG 2018), BGBl. I Nr. 107/2017)
   a) die technische Anbindung der Handels- und Clearingteilnehmer;
   b) die Bereitstellung der elektronischen Handelsplattform;
   c) die Marktsteuerung als technischer Dienst;

wenn pro Geschäftsjahr an diesem Handelsplatz mehr als zehn Millionen Transaktionen stattgefunden haben;

2. im Bereich der Abwicklung durch zentrale Gegenparteien (Art. 2 Abs. 1 der Verordnung (EU) Nr. 648/2012, ABl. Nr. L 201 vom 27.7.2012 S. 1) das Zurverfügungstellen eines Abwicklungssystems, wenn die zentrale Gegenpartei gemäß § 9 Abs. 3 BörseG 2018 als Abwicklungsstelle von einem Handelsplatz, an dem pro Geschäftsjahr mehr als zehn Millionen Transaktionen stattgefunden haben, beauftragt wurde;
3. im Bereich der Zentralverwahrer (Art. 2 Abs. 1 Z 1 der Verordnung (EU) Nr. 909/2014, ABl. Nr. L 257 vom 28.8.2014 S. 1)
   a) das Bereitstellen und Führen von Depotkonten auf oberster Ebene nach Abschnitt A Nr. 2 des Anhangs zur Verordnung (EU) Nr. 909/2014, wenn die Anzahl der stücknotierten Wertpapiere mehr als acht Milliarden im Geschäftsjahr beträgt;
   b) der Betrieb eines Wertpapierliefer- und -abrechnungssystems nach Abschnitt A Nr. 3 des Anhangs zur Verordnung (EU) Nr. 909/2014, wenn die Anzahl der abgewickelten Transaktionen höher als eine Million im Geschäftsjahr ist.

(2) Im Sektor Finanzmarktinfrastrukturen liegt ein Sicherheitsvorfall im Sinne des § 3 Z 6 NISG vor, wenn

1. im Bereich der Handelsplätze der Handel aufgrund eines Ausfalls oder der eingeschränkten Verfügbarkeit eines in Abs. 1 Z 1 lit. a bis c genannten Dienstes unterbrochen wird;
2. im Bereich der Abwicklung durch zentrale Gegenparteien das Awicklungssystem für mehr als zwölf Stunden ausfällt oder nur eingeschränkt zur Verfügung gestellt werden kann;
3. im Bereich der Zentralverwahrer einer der in Abs. 1 Z 3 lit. a und b genannten Dienste für mehr als zwölf Stunden ausfällt oder nur eingeschränkt verfügbar ist.

(3) Im Sektor Finanzmarktinfrastrukturen bestehen für Einrichtungen, die einen wesentlichen Dienst erbringen im Sinne des

1. Abs. 1 Z 1 zu Sicherheitsvorkehrungen in § 11 Abs. 1 BörseG 2018 iVm Art. 15, 16 und 23 Abs. 1 und 2 der delegierten Verordnung (EU) 2017/584, ABl. Nr. L 87 vom 31.3.2017 S. 350;
2. Abs. 1 Z 2 zu Sicherheitsvorkehrungen in Art. 26 Abs. 1, 3 und 6 und Art. 34 der Verordnung (EU) Nr. 648/2012 iVm Art. 4 und 9 der delegierten Verordnung (EU) Nr. 153/2013, ABl. Nr. L 52 vom 23.2.2013 S. 41;
3. Abs. 1 Z 3 zu Sicherheitsvorkehrungen in Art. 45 der Verordnung (EU) Nr. 909/2014 iVm Art. 75 der delegierten Verordnung (EU) 2017/392, ABl. Nr. L 65 vom 10.3.2017 S. 48;

Vorschriften, die zumindest ein gleichwertiges Sicherheitsniveau für Netz- und Informationssysteme gemäß § 20 NISG gewährleisten.

Sektor Gesundheitswesen

§ 8. (1) Wegen ihrer Bedeutung für die Aufrechterhaltung des öffentlichen Gesundheitsdienstes im Sinne des § 16 Abs. 2 NISG sind im Sektor Gesundheitswesen wesentliche Dienste:

1. die medizinische Versorgung in den Bereichen Diagnose, Therapie und Pflege als
   a) akutstationäre Versorgung oder
   b) akutambulante ärztliche Versorgung (§ 2 Z 11) in einer Spitalsambulanz

durch Krankenanstalten gemäß Abs. 3 Z 1 bis 5, wenn sie insgesamt drei Betten je 1 000 Einwohner pro Bundesland in zentral gelegenen Versorgungsregionen mit großem Einzugsgebiet (§ 2 Z 10), oder zwei Betten je 1 000 Einwohner pro Bundesland in allen anderen Versorgungsregionen (Bettenrichtwerte) vorhalten;

2. das Betreiben einer Leitstelle, die die Durchführung von Notfallrettungstransporten unterstützt.

(2) Im Sektor Gesundheit liegt ein Sicherheitsvorfall im Sinne des § 3 Z 6 NISG vor, wenn

1. der in Abs. 1 Z 1 genannte Dienst für mehr als drei Stunden ausfällt oder nur eingeschränkt verfügbar ist;
2. der in Abs. 1 Z 2 genannte Dienste für mehr als drei Stunden ausfällt oder nur eingeschränkt verfügbar ist.

(3) Zur Sicherstellung des Ziels, durch eine regional möglichst gleichmäßige Verteilung über das Bundesgebiet einen vielfältigen Versorgungsbedarf abzudecken, können Betreiber wesentlicher Dienste gemäß Abs. 1 Z 1 nur folgende Krankenanstalten gemäß § 2 Z 8 sein:

1. Zentralkrankenanstalten gemäß § 2a Abs. 1 lit. c KAKuG,
2. Schwerpunktkrankenanstalten gemäß § 2a Abs. 1 lit. b KAKuG, nämlich
   a) jeweils eine pro Versorgungsregion,
      aa) wenn es in der Versorgungsregion keine Krankenanstalt gemäß Z 1 gibt, oder
      bb) zusätzlich zu einer Krankenanstalt gemäß Z 1, wenn in zentral gelegenen Versorgungsregionen mit großem Einzugsgebiet der Bettenrichtwert gemäß Abs. 1 Z 1 nicht erreicht wird, oder
   b) mehrere pro Versorgungsregion in zentral gelegenen Versorgungsregionen mit großem Einzugsgebiet, wenn ansonsten der Bettenrichtwert gemäß Abs. 1 Z 1 nicht erreicht wird, sowie
3. Standardkrankenanstalten gemäß § 2a Abs. 1 lit. a KAKuG, wenn es in der betreffenden Versorgungsregion keine Krankenanstalt gemäß Z 1 oder 2 gibt und die nächstgelegene Krankenanstalt gemäß Z 1 oder 2 für die mehrheitliche Bevölkerung nicht in zumutbarer Zeit erreichbar ist,

die neben Einrichtungen für Anästhesiologie und Intensivmedizin jedenfalls die Fachrichtungen Chirurgie, Innere Medizin sowie Frauenheilkunde und Geburtshilfe vorhalten, sowie

4. Krankenanstalten gemäß § 2 Z 8 lit. c, sowie

5. Krankenanstalten, die nicht von Z 1 bis 3 erfasst sind und die die Fachrichtung Neurochirurgie vorhalten, im Umfang dieser Fachrichtung.

(4) Hat eine Krankenanstalt gemäß Abs. 3 Z 1 bis 3 mehrere Standorte, werden wesentliche Dienste gemäß Abs. 1 Z 1 durch jene Standorte erbracht,

1. die zu den in Abs. 3 genannten Fachrichtungen zusätzlich die oder die höhere Anzahl an den Fachrichtungen Kinder- und Jugendheilkunde oder Unfallchirurgie oder Orthopädie und Traumatologie vorhalten, oder
2. wenn mehrere Standorte keine zusätzlichen oder gleich viele Fachrichtungen vorhalten, jene Standorte, die zur Erreichung der Bettenrichtwerte gemäß Abs. 1 mehr Betten je 1 000 Einwohner pro Bundesland vorhalten.

(5) Gibt es in einer Versorgungsregion mehr als eine Schwerpunktkrankenanstalt und sind für die Erreichung der Bettenrichtwerte gemäß Abs. 1 nicht alle erforderlich (Abs. 3 Z 2 lit. a), werden die wesentlichen Dienste gemäß Abs. 1 Z 1 nur durch jene Krankenanstalt erbracht, die für die mehrheitliche Bevölkerung dieser Versorgungsregion und gegebenenfalls für peripher gelegene Nachbarregionen am besten erreichbar ist.

Sektor Trinkwasserversorgung

§ 9. (1) Wegen ihrer Bedeutung für die Aufrechterhaltung der öffentlichen Versorgung mit Trinkwasser im Sinne des § 16 Abs. 2 NISG sind im Sektor Trinkwasserversorgung wesentliche Dienste:

1. die Wassergewinnung, wenn die gewonnene Wassermenge, die zur weiteren Versorgung bestimmt ist, 6 424 000 m^3 im Jahr übersteigt;
2. die Wasseraufbereitung, wenn die aufbereitete Wassermenge 6 424 000 m^3 im Jahr übersteigt;
3. die leitungsgebundene Wasserverteilung, wenn die verteilte Wassermenge 6 424 000 m^3 im Jahr übersteigt.

(2) Im Sektor Trinkwasserversorgung liegt ein Sicherheitsvorfall im Sinne des § 3 Z 6 NISG vor, wenn

1. bei dem in Abs. 1 Z 1 genannten Dienst um 17 600 m3 weniger als die durchschnittlich an einem Tag gewonnene Wassermenge gewonnen werden kann oder der Dienst für mehr als 2 112 000 Nutzerstunden ausfällt oder nur eingeschränkt verfügbar ist;
2. bei dem in Abs. 1 Z 2 genannten Dienst um 17 600 m3 weniger als die durchschnittlich an einem Tag aufbereitete Wassermenge aufbereitet werden kann oder der Dienst für mehr als 2 112 000 Nutzerstunden ausfällt oder nur eingeschränkt verfügbar ist;
3. der in Abs. 1 Z 3 genannte Dienst für mehr als 528 000 Nutzerstunden ausfällt oder nur eingeschränkt verfügbar ist.

Sektor Digitale Infrastruktur

§ 10. (1) Wegen ihrer Bedeutung für die Aufrechterhaltung der Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie im Sinne des § 16 Abs. 2 NISG sind im Sektor Digitale Infrastruktur wesentliche Dienste:

1. im Bereich des Betriebs eines Internet-Knotens das Zurverfügungstellen von Infrastruktur zur multilateralen Zusammenschaltung, wenn die Anzahl der zusammengeschalteten autonomen Systeme 100 übersteigt;
2. im Bereich des Betriebs von DNS-Diensten
   a) das Betreiben von DNS-Resolver (§ 2 Z 4), die im Rahmen der Bereitstellung eines Kommunikationsdienstes betrieben werden, wenn die Anzahl der Teilnehmer (§ 3 Z 19 Telekommunikationsgesetz 2003 (TKG 2003), BGBl. I Nr. 70/2003) 88 000 übersteigt;
   b) das Betreiben von autoritativen DNS-Servern, wenn die Anzahl der Domains, für die der Server autoritativ ist oder die aus der Zone delegiert werden, 50 000 übersteigt;
   c) das Betreiben eines TLD-Name-Registry, wenn die Anzahl der registrierten Domains 50 000 übersteigt.

(2) Im Sektor Digitale Infrastruktur liegt ein Sicherheitsvorfall im Sinne des § 3 Z 6 NISG vor, wenn

a) der in Abs. 1 Z 1 genannte Dienst für mehr als zwölf Stunden ausfällt oder nur eingeschränkt verfügbar ist;
b) der in Abs. 1 Z 2 lit. a genannte Dienst für mehr als zwölf Stunden ausfällt oder nur eingeschränkt verfügbar ist;
c) der in Abs. 1 Z 2 lit. b genannte Dienst für mehr als zwölf Stunden ausfällt oder nur eingeschränkt verfügbar ist;

d) der in Abs. 1 Z 2 lit. c genannte Dienst für mehr als zwölf Stunden ausfällt oder nur eingeschränkt verfügbar ist.

(3) Im Sektor Digitale Infrastruktur bestehen für Einrichtungen, die einen wesentlichen Dienst im Sinne des Abs. 1 Z 2 lit. a im Rahmen des Betriebs von Kommunikationsdiensten nach dem TKG 2003 erbringen, zu Sicherheitsvorkehrungen in § 16a Abs. 2 TKG 2003 und zur Meldepflicht in § 16a Abs. 5 TKG 2003 Vorschriften, die zumindest ein gleichwertiges Sicherheitsniveau für Netz- und Informationssysteme gemäß § 20 NISG gewährleisten.

3. Abschnitt
Sicherheitsvorkehrungen

§ 11. (1) Sicherheitsvorkehrungen gemäß § 17 Abs. 1 NISG, die geeignet sind und den Stand der Technik berücksichtigen sowie zur Gewährleistung der Netz- und Informationssystemsicherheit (§ 3 Z 2 NISG) zu treffen sind, umfassen die

1. Sicherheitsmaßnahmen zur Kategorie Governance und Risikomanagement gemäß Z 1.1 bis 1.6 der Anlage 1 zu dieser Verordnung;
2. Sicherheitsmaßnahmen zur Kategorie Umgang mit Dienstleistern, Lieferanten und Dritten gemäß Z 2.1 bis 2.2 der Anlage 1 zu dieser Verordnung;
3. Sicherheitsmaßnahmen zur Kategorie Sicherheitsarchitektur gemäß Z 3.1 bis 3.5 der Anlage 1 zu dieser Verordnung;
4. Sicherheitsmaßnahmen zur Kategorie Systemadministration gemäß Z 4.1 bis 4.2 der Anlage 1 zu dieser Verordnung;
5. Sicherheitsmaßnahmen zur Kategorie Identitäts- und Zugriffsmanagement gemäß Z 5.1 bis 5.2 der Anlage 1 zu dieser Verordnung;
6. Sicherheitsmaßnahmen zur Kategorie Systemwartung und Betrieb gemäß Z 6.1 bis 6.2 der Anlage 1 zu dieser Verordnung;
7. Sicherheitsmaßnahme zur Kategorie Physische Sicherheit gemäß Z 7.1 der Anlage 1 zu dieser Verordnung;
8. Sicherheitsmaßnahmen zur Kategorie Erkennung von Vorfällen gemäß Z 8.1 bis 8.3 der Anlage 1 zu dieser Verordnung;
9. Sicherheitsmaßnahmen zur Kategorie Bewältigung von Vorfällen gemäß Z 9.1 bis 9.3 der Anlage 1 zu dieser Verordnung;
10. Sicherheitsmaßnahmen zur Kategorie Betriebskontinuität gemäß Z 10.1 bis 10.2 der Anlage 1 zu dieser Verordnung;
11. Sicherheitsmaßnahme zur Kategorie Krisenmanagement gemäß Z 11.1 der Anlage 1 zu dieser Verordnung.

(2) Die Umsetzung jeder Sicherheitsmaßnahme hat, soweit möglich, in technischer und organisatorischer Hinsicht auf Basis der nach Z 1.1 der Anlage 1 zu dieser Verordnung durchgeführten Risikoanalyse zu erfolgen.

4. Abschnitt
Schlussbestimmungen

Personenbezogene Bezeichnungen

§ 12. Alle in dieser Verordnung verwendeten personenbezogenen Bezeichnungen gelten gleichermaßen für alle Geschlechter.

Verweisungen

§ 13. (1) Für Verweise auf Bundesgesetze in dieser Verordnung gilt Folgendes:

1. Soweit auf Bestimmungen des Bundesgesetzes über Krankenanstalten- und Kuranstalten (KAKuG), BGBl. Nr. 1/1957, verwiesen wird, ist dieses in der Fassung des Bundesgesetzes BGBl. I Nr. 13/2019 anzuwenden;
2. soweit auf Bestimmungen des Elektrizitätswirtschafts- und -organisationsgesetzes 2010 (ElWOG 2010), BGBl. I Nr. 110/2010, verwiesen wird, ist dieses in der Fassung des Bundesgesetzes BGBl. I Nr. 108/2017 anzuwenden;

3. soweit auf Bestimmungen des Erdölbevorratungsgesetzes 2012 (EBG 2012), BGBl. I Nr. 78/2012, verwiesen wird, ist dieses in der Fassung des Bundesgesetzes BGBl. I Nr. 163/2015 anzuwenden;
4. soweit auf Bestimmungen des Gaswirtschaftsgesetzes 2011 (GWG 2011), BGBl. I Nr. 107/2011, verwiesen wird, ist dieses in der Fassung des Bundesgesetzes BGBl. I Nr. 108/2017 anzuwenden;
5. soweit auf Bestimmungen des Luftfahrtgesetzes (LFG), BGBl. Nr. 253/1957, verwiesen wird, ist dieses in der Fassung des Bundesgesetzes BGBl. I Nr. 92/2017 anzuwenden;
6. soweit auf Bestimmungen des Straßentunnel-Sicherheitsgesetzes (STSG), BGBl. I Nr. 54/2006, verwiesen wird, ist dieses in der Fassung des Bundesgesetzes BGBl. I Nr. 96/2013 anzuwenden;
7. soweit auf Bestimmungen des Eisenbahngesetzes 1957 (EisbG), BGBl. Nr. 60/1957, verwiesen wird, ist dieses in der Fassung des Bundesgesetzes BGBl. I Nr. 137/2015 anzuwenden;
8. soweit auf Bestimmungen des Bundesstraßengesetzes 1971 (BStG 1971), BGBl. Nr. 286/1971, verwiesen wird, ist dieses in der Fassung des Bundesgesetzes BGBl. I Nr. 7/2017 anzuwenden;
9. soweit auf Bestimmungen des Zahlungsdienstegesetzes 2018 (ZaDiG 2018), BGBl. I Nr. 17/2018, verwiesen wird, ist dieses in der Fassung des Bundesgesetzes BGBl. I Nr. 37/2018 anzuwenden;
10. soweit auf Bestimmungen des Bankwesengesetzes (BWG), BGBl. Nr. 532/1993, verwiesen wird, ist dieses in der Fassung des Bundesgesetzes BGBl. I Nr. 112/2018 anzuwenden;
11. soweit auf Bestimmungen des Börsegesetzes 2018 (BörseG 2018), BGBl. I Nr. 107/2017, verwiesen wird, ist dieses in der Fassung des Bundesgesetzes BGBl. I Nr. 37/2018 anzuwenden;
12. soweit auf Bestimmungen des Telekommunikationsgesetzes 2003 (TKG 2003), BGBl. I Nr. 70/2003, verwiesen wird, ist dieses in der Fassung des Bundesgesetzes BGBl. I Nr. 111/2018 anzuwenden.

(2) Für Verweise auf Unionsrecht in dieser Verordnung gilt Folgendes:

1. Soweit auf Bestimmungen der Verordnung (EU) Nr. 1315/2013 verwiesen wird, so ist die Verordnung (EU) Nr. 1315/2013 über Leitlinien der Union für den Aufbau eines transeuropäischen Verkehrsnetzes und zur Aufhebung des Beschlusses Nr. 661/2010/EU, ABl. Nr. L 348 vom 20.12.2013 S. 1, zuletzt geändert durch die delegierte Verordnung (EU) Nr. 254/2019, ABl. Nr. L 43 vom 14.2.2019 S. 1, anzuwenden;
2. soweit auf Bestimmungen der Verordnung (EG) Nr. 549/2004 verwiesen wird, so ist die Verordnung (EG) Nr. 549/2004 zur Festlegung des Rahmens für die Schaffung eines einheitlichen europäischen Luftraums („Rahmenverordnung“), ABl. L 96 vom 31.3.2004 S. 1, zuletzt geändert durch die Verordnung (EU) Nr. 1070/2009, ABl. L 300 vom 14.11.2009 S. 34, anzuwenden;
3. soweit auf Bestimmungen der Verordnung (EU) Nr. 648/2012 verwiesen wird, so ist die Verordnung (EU) Nr. 648/2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister, ABl. Nr. L 201 vom 27.07.2012 S. 1, zuletzt geändert durch die Verordnung (EU) 2017/2402, ABl. Nr. L 347 vom 28.12.2017 S. 35, anzuwenden
4. soweit auf Bestimmungen der Verordnung (EU) Nr. 909/2014 verwiesen wird, so ist die Verordnung (EU) Nr. 909/2014 zur Verbesserung der Wertpapierlieferungen und -abrechnungen in der Europäischen Union und über Zentralverwahrer sowie zur Änderung der Richtlinien 98/26/EG und 2014/65/EU und der Verordnung (EU) Nr. 236/2012, ABl. Nr. L 257 vom 28.8.2014 S. 1, zuletzt geändert durch die Verordnung (EU) 2016/1033, ABl. Nr. L 175 vom 30.06.2016 S. 1, anzuwenden;
5. soweit auf Bestimmungen der delegierten Verordnung (EU) 2017/584 verwiesen wird, so ist die delegierte Verordnung (EU) 2017/584 zur Ergänzung der Richtlinie 2014/65/EU durch technische Regulierungsstandards zur Festlegung der organisatorischen Anforderungen an Handelsplätze, ABl. Nr. L 87 vom 31.3.2017 S. 350, anzuwenden;
6. soweit auf Bestimmungen der delegierten Verordnung (EU) Nr. 153/2013 verwiesen wird, so ist die delegierte Verordnung (EU) Nr. 153/2013 zur Ergänzung der Verordnung (EU) Nr. 648/2012 in Bezug auf technische Regulierungsstandards für Anforderungen an zentrale Gegenparteien Text von Bedeutung für den EWR, ABl. Nr. L 52 vom 23.2.2013 S. 41, zuletzt geändert durch die delegierte Verordnung (EU) Nr. 822/2016, ABl. 137 vom 26.5.2016 S. 1, anzuwenden;
7. soweit auf Bestimmungen der delegierten Verordnung (EU) 2017/392 verwiesen wird, so ist delegierte Verordnung (EU) 2017/392 zur Ergänzung der Verordnung (EU) Nr. 909/2014 durch technische Regulierungsstandards für die Zulassung von und für aufsichtliche und operationelle Anforderungen an Zentralverwahrer, ABl. Nr. L 65 vom 10.3.2017 S. 48, anzuwenden.

Inkrafttreten

§ 14. Diese Verordnung tritt mit Ablauf des Tages der Kundmachung in Kraft.

Schallenberg

Anlage 1

Sicherheitsmaßnahmen	
1.	**Governance und Risikomanagement**
1.1	Risikoanalyse: Eine Risikoanalyse der Netz- und Informationssysteme ist durchzuführen. Dabei sind spezifische Risiken auf Grundlage einer Analyse der betrieblichen Auswirkungen von Sicherheitsvorfällen zu ermitteln und hinsichtlich der hohen Bedeutung des Betreibers wesentlicher Dienste für das Funktionieren des Gemeinwesens zu bewerten.
1.2	Sicherheitsrichtlinie: Eine Sicherheitsrichtlinie ist zu erstellen und periodisch zu aktualisieren.
1.3	Überprüfungsplan der Netz- und Informationssysteme: Die Durchführung der periodischen Überprüfung der Netz- und Informationssystemsicherheit ist zu planen und festzulegen.
1.4	Ressourcenmanagement: Alle Ressourcen, die erforderlich sind, um die Funktionsfähigkeit der Netz- und Informationssysteme zu gewährleisten, sind im Hinblick auf kurz-, mittel- und langfristige Kapazitätsanforderungen einzuplanen und sicherzustellen.
1.5	Informationssicherheitsmanagementsystemprüfung: Die periodische Überprüfung des Informationssicherheitsmanagementsystems ist festzulegen und durchzuführen.
1.6	Personalwesen: Sicherheitsrelevante Aspekte sind in den Prozessen des Personalwesens zu berücksichtigen und umzusetzen.
2.	**Umgang mit Dienstleistern, Lieferanten und Dritten**
2.1	Beziehungen mit Dienstleistern, Lieferanten und Dritten: Anforderungen an Dienstleistern, Lieferanten und Dritte für den Betrieb von, einen sicheren Zugang zu und Zugriff auf Netz- und Informationssysteme sind festzulegen und periodisch zu überprüfen.
2.2	Leistungsvereinbarungen mit Dienstleistern und Lieferanten: Die Leistungsvereinbarungen mit Dienstleistern und Lieferanten sind periodisch zu überprüfen und zu überwachen.
3.	**Sicherheitsarchitektur**
3.1	Systemkonfiguration: Netz- und Informationssysteme sind sicher zu konfigurieren. Diese Konfiguratoin ist strukturiert zu dokumentieren. Die Dokumentation ist aktuell zu halten.
3.2	Vermögenswerte: Vermögenswerte, die im Zusammenhang mit Netz- und Informationssystemen stehen, sind strukturiert zu analysieren und zu dokumentieren.
3.3	Netzwerksegmentierung: Eine Segmentierung der Netzwerke ist innerhalb der Netz- und Informationssysteme abhängig vom Schutzbedarf vorzunehmen.
3.4	Netzwerksicherheit: Die Sicherheit innerhalb der Netzwerksegmente und der Schnittstellen zwischen den Netzwerksegmenten ist zu gewährleisten.
3.5	Kryptographie: Vertraulichkeit, Authentizität und Integrität von Informationen sind durch den angemessenen und wirksamen Einsatz kryptographischer Verfahren und Technologien sicherzustellen.
4.	**Systemadministration**
4.1	Administrative Zugangsrechte: Administrative Zugangsrechte sind eingeschränkt nach dem Minimalrechtsprinzip zuzuweisen. Diese Zuweisungen sind periodisch zu überprüfen und gegebenenfalls anzupassen.
4.2	Systeme und Anwendungen zur Systemadministration: Systeme und Anwendungen zur Systemadministration sind ausschließlich für Tätigkeiten zum Zweck der Systemadministration zu verwenden. Die Sicherheit dieser Systeme und

	Anwendungen ist zu gewährleisten.
5.	**Identitäts- und Zugriffsmanagement**
5.1	Identifikation und Authentifikation: Es sind Verfahren umzusetzen und Technologien einzusetzen, die die Identifikation und Authentifikation von Benutzern und Diensten gewährleisten.
5.2	Autorisierung: Es sind Verfahren umzusetzen und Technologien einzusetzen, die unautorisierte Zugriffe auf Netz- und Informationssysteme unterbinden.
6.	**Systemwartung und Betrieb**
6.1	Systemwartung und Betrieb: Abläufe und Vorgänge zur Gewährleistung eines sicheren Systembetriebs von Netz- und Informationssystemen sind einzuführen und periodisch zu überprüfen.
6.2	Fernzugriff: Fernzugriff ist eingeschränkt nach dem Minimalrechtsprinzip und zeitlich beschränkt zu vergeben. Die Fernzugriffsrechte sind periodisch zu überprüfen und gegebenenfalls anzupassen. Die Sicherheit des Fernzugriffs ist zu gewährleisten.
7.	**Physische Sicherheit**
7.1	Physische Sicherheit: Der physische Schutz der Netz- und Informationssysteme, insbesondere der physische Schutz vor unbefugtem Zutritt und Zugang, ist zu gewährleisten.
8.	**Erkennung von Vorfällen**
8.1	Erkennung: Mechanismen zur Erkennung und Bewertung von Vorfällen sind umzusetzen.
8.2	Protokollierung und Monitoring: Mechanismen zu Protokollierung und Monitoring, insbesondere von für die Erbringung des wesentlichen Dienstes essentiellen Tätigkeiten und Vorgängen, sind umzusetzen.
8.3	Korrelation und Analyse: Mechanismen zur Erkennung und adäquaten Bewertung von Vorfällen durch die Korrelation und Analyse der ermittelten Protokolldaten sind umzusetzen.
9.	**Bewältigung von Vorfällen**
9.1	Vorfallsreaktion: Prozesse zur Reaktion auf Vorfälle sind zu erstellen, aufrechtzuerhalten und zu erproben.
9.2	Vorfallsmeldung: Prozesse zur internen und externen Meldung von Vorfällen sind zu erstellen, aufrechtzuerhalten und zu erproben.
9.3	Vorfallsanalyse: Prozesse zur Analyse und Bewertung von Vorfällen und zur Sammlung relevanter Informationen sind zu erstellen, aufrechtzuerhalten und zu erproben, um den kontinuierlichen Verbesserungsprozess zu fördern.
10.	**Betriebskontinuität**
10.1	Betriebskontinuitätsmanagement: Die Wiederherstellung der Erbringung des wesentlichen Dienstes auf einem zuvor festgelegten Qualitätsniveau nach einem Sicherheitsvorfall ist zu gewährleisten.
10.2	Notfallmanagement: Notfallpläne sind zu erstellen, anzuwenden, regelmäßig zu bewerten und zu erproben.
11.	**Krisenmanagement**
11.1	Krisenmanagement: Rahmenbedingungen und Prozessabläufe des Krisenmanagements sind für die Aufrechterhaltung des wesentlichen Dienstes vor und während eines Sicherheitsvorfalls zu definieren, umzusetzen und zu erproben.

Unterzeichner	serialNumber=932783133,CN=Bundeskanzleramt,C=AT
Datum/Zeit	2019-07-17T15:15:35+02:00
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.bka.gv.at/verifizierung
Hinweis	Dieses Dokument wurde amtssigniert.