Liechtensteinisches Landesgesetzblatt
Jahrgang 2023 Nr. 359 ausgegeben am 6. September 2023

Cyber-Sicherheitsverordnung (CSV)

vom 4. September 2023

Aufgrund von Art. 4 Abs. 5, Art. 5 Abs. 7, Art. 9 Abs. 3, Art. 13 Abs. 3, Art. 18 Abs. 3, Art. 19 Abs. 3 und Art. 24 des Cyber-Sicherheitsgesetzes (CSG) vom 4. Mai 2023, LGBI. 2023 Nr. 269, verordnet die Regierung:

I. Allgemeine Bestimmungen

Art. 1

Gegenstand und Zweck

1) Diese Verordnung regelt in Durchführung des Cyber-Sicherheitsgesetzes das Nähere über die Massnahmen zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen, insbesondere:

a) die Ermittlung der Betreiber wesentlicher Dienste;

b) die jeweiligen Sektoren nach Art. 1 Abs. 1 Bst. a des Gesetzes;

c) die zu ergreifenden Sicherheitsmassnahmen;

d) die Meldepflicht nach Art. 5 des Gesetzes;

e) die Anforderungen an qualifizierte Dritte nach Art. 9 Abs. 2 des Gesetzes;

f) die Zusammenarbeit und den Informationsaustausch der Stabsstelle Cyber-Sicherheit mit anderen inländischen Behörden;

g) die Durchführung von Kontrollen nach Art. 18 des Gesetzes.

2) Sie dient der Umsetzung bzw. Durchführung folgender EWR-Rechtsvorschriften:

a) Richtlinie (EU) 2016/1148 über Massnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union[1];

b) Verordnung (EU) 2021/887 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren[2].

3) Die gültige Fassung der EWR-Rechtsvorschriften, auf die in dieser Verordnung Bezug genommen wird, ergibt sich aus der Kundmachung der Beschlüsse des Gemeinsamen EWR-Ausschusses im Liechtensteinischen Landesgesetzblatt nach Art. 3 Bst. k des Kundmachungsgesetzes.

Art. 2

Begriffsbestimmungen und Bezeichnungen

1) Im Sinne dieser Verordnung gelten als:

a) "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;

b) "Domain-Namen-System (DNS)": ein hierarchisch unterteiltes Bezeichnungssystem in einem Netz zur Beantwortung von Anfragen zu Domain-Namen;

c) "Top-Level-Domain-Name-Registry": eine Einrichtung, die die Registrierung von Internet-Domain-Namen innerhalb einer spezifischen Top-Level-Domain (TLD) verwaltet und betreibt.

2) Unter den in dieser Verordnung verwendeten Personenbezeichnungen sind alle Personen unabhängig ihres Geschlechts zu verstehen, sofern sich die Personenbezeichnungen nicht ausdrücklich auf ein bestimmtes Geschlecht beziehen.

---

1 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Massnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1)

2 Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren (ABl. L 202 vom 8.6.2021, S. 1)

II. Betreiber wesentlicher Dienste

A. Sektoren

Art. 3

Ermittlung der Betreiber wesentlicher Dienste

1) Die Stabsstelle Cyber-Sicherheit ermittelt für jeden Sektor nach Art. 1 Abs. 1 Bst. a des Gesetzes jene Betreiber wesentlicher Dienste mit Sitz in Liechtenstein, die einen wesentlichen Dienst erbringen.

2) Betreiber wesentlicher Dienste haben der Stabsstelle Cyber-Sicherheit auf Verlangen eine Kontaktstelle für die Kommunikation mit der Stabsstelle Cyber-Sicherheit oder dem Computer-Notfallteam (CSIRT) zu benennen. Sie haben sicherzustellen, dass sie über diese Kontaktstelle jedenfalls in jenem Zeitraum erreichbar sind, in dem sie einen wesentlichen Dienst zur Verfügung stellen. Änderungen der Kontaktstelle sind der Stabsstelle Cyber-Sicherheit unverzüglich bekanntzugeben.

Art. 4

Sektor Energie

Wegen ihrer Bedeutung für die Aufrechterhaltung der öffentlichen Versorgung mit Energie fallen unter den Sektor Energie folgende Arten von Einrichtungen, die wesentliche Dienste erbringen:

a) im Bereich Elektrizität:
   1. Elektrizitätsunternehmen, die die Funktion des Verkaufs einschliesslich des Weiterverkaufs von Elektrizität an Kunden wahrnehmen;
   2. Verteilernetzbetreiber, die die Funktion der Verteilung wahrnehmen und verantwortlich sind für:
      aa) den Betrieb, die Wartung sowie erforderlichenfalls den Ausbau des Verteilernetzes und gegebenenfalls der Verbindungsleitungen zu anderen Netzen; sowie
      bb) die Sicherstellung der langfristigen Fähigkeit des Netzes, eine angemessene Nachfrage nach Verteilung von Elektrizität zu befriedigen;

3. Übertragungsnetzbetreiber, die die Funktion der Übertragung von Elektrizität wahrnehmen und verantwortlich sind für:
   aa) den Betrieb, die Wartung sowie erforderlichenfalls den Ausbau des Übertragungsnetzes und gegebenenfalls der Verbindungsleitungen zu anderen Netzen; sowie
   bb) die Sicherstellung der langfristigen Fähigkeit des Netzes, eine angemessene Nachfrage nach Übertragung von Elektrizität zu befriedigen;

b) im Bereich Erdgas:
   1. Versorgungsunternehmen, die die Funktion der Versorgung wahrnehmen;
   2. Verteilernetzbetreiber, die die Funktion der Verteilung wahrnehmen und verantwortlich sind für:
      aa) den Betrieb, die Wartung sowie erforderlichenfalls den Ausbau des Verteilernetzes und gegebenenfalls der Verbindungsleitungen zu anderen Netzen; sowie
      bb) die Sicherstellung der langfristigen Fähigkeit des Netzes, eine angemessene Nachfrage nach Verteilung von Gas zu befriedigen;
   3. Fernleitungsnetzbetreiber, die die Funktion der Fernleitung wahrnehmen und verantwortlich sind für:
      aa) den Betrieb, die Wartung sowie erforderlichenfalls den Ausbau des Fernleitungsnetzes und gegebenenfalls der Verbindungsleitungen zu anderen Netzen; sowie
      bb) die Sicherstellung der langfristigen Fähigkeit des Netzes, eine angemessene Nachfrage nach Transport von Gas zu befriedigen;
   4. Betreiber einer Speicheranlage, die die Funktion der Speicherung wahrnehmen und für den Betrieb der Speicheranlage verantwortlich sind;
   5. Betreiber einer LNG-Anlage, die die Funktion der Verflüssigung von Erdgas oder der Einfuhr, Entladung und Wiederverdampfung von verflüssigtem Erdgas wahrnehmen und für den Betrieb einer LNG-Anlage verantwortlich sind;
   6. Erdgasunternehmen, die:
      aa) die Funktionen Gewinnung, Fernleitung, Verteilung, Lieferung, Kauf oder Speicherung von Erdgas, einschliesslich verflüssigtem Erdgas, wahrnehmen; und

bb) kommerzielle, technische und/oder wartungsbezogene Aufgaben im Zusammenhang mit diesen Funktionen erfüllen, mit Ausnahme der Endkunden.

Art. 5

Sektor Verkehr

Wegen ihrer Bedeutung für die Aufrechterhaltung des öffentlichen Verkehrs fallen unter den Sektor Verkehr folgende Arten von Einrichtungen, die wesentliche Dienste erbringen:

a) im Bereich Schienenverkehr:

1. Eisenbahninfrastrukturunternehmen, die die Funktion wahrnehmen, dem Bau und Betrieb von Eisenbahninfrastrukturen, einschliesslich deren Erhaltung und Erneuerung, zu dienen;
2. Eisenbahnverkehrsunternehmen, die die Funktion von Eisenbahnverkehrsdiensten zur Beförderung von Gütern und/oder Personen auf der Schiene erbringen und die Traktion sicherstellen sowie Unternehmen, die ausschliesslich die Traktionsleistung erbringen;

b) im Bereich Strassenverkehr:

1. das Amt für Tiefbau und Geoinformation, welches die Funktion der Planung, Überwachung und den Betrieb von Strassen wahrnimmt;
2. Betreiber intelligenter Verkehrssysteme, die die Funktion haben, Informations- und Kommunikationstechnologien im Strassenverkehr, einschliesslich seiner Infrastrukturen, Fahrzeuge und Nutzer, sowie beim Verkehrs- und Mobilitätsmanagement und für Schnittstellen zu anderen Verkehrsträgern einzusetzen.

Art. 6

Sektor Bankwesen

1) Wegen ihrer Bedeutung für die Aufrechterhaltung des Zahlungsverkehrs fallen unter den Sektor Bankwesen die folgenden wesentlichen Dienste bzw. die zu deren Betrieb genutzten Systeme:

a) der Betrieb von Systemen zur Erbringung von Diensten, mit denen Bareinzahlungen auf ein Zahlungskonto ermöglicht werden;

b) der Betrieb von Systemen zur Erbringung von Diensten, mit denen Barabhebungen von einem Zahlungskonto ermöglicht werden;

c) 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;

d) der Betrieb von Systemen zur Ausführung von Zahlungsvorgängen, wenn die Beträge durch einen Kreditrahmen für einen Zahlungsdienstnutzer gedeckt sind.

2) Als Banken, die wesentliche Dienste nach Abs. 1 erbringen, können ermittelt werden:

a) systemrelevante Institute im Sinne von Art. 3a Abs. 1 Ziff. 15 des Bankengesetzes;

b) Banken, deren Marktanteil an Zahlungsverkehrskonten im Zusammenhang mit den in Abs. 1 genannten Diensten 20 % überschreitet; oder

c) Banken, deren Anzahl Bankomaten (ATMs) zehn übersteigt.

3) Im Sektor Bankwesen bestehen für Banken, die wesentliche Dienste nach Abs. 1 erbringen, Vorschriften zu Sicherheitsanforderungen und zur Meldepflicht nach Art. 101 und 102 des Zahlungsdienstegesetzes, die zumindest ein gleichwertiges Sicherheitsniveau für Netz- und Informationssysteme nach Art. 4 Abs. 4 und Art. 5 Abs. 6 des Gesetzes gewährleisten.

Art. 7

Sektor Finanzmarktinfrastrukturen

1) Wegen ihrer Bedeutung für die Aufrechterhaltung des Handelsplatzes fallen unter den Sektor Finanzmarktinfrastrukturen folgende Arten von Einrichtungen, die wesentliche Dienste erbringen:

a) Betreiber von Handelsplätzen nach Art. 3a Abs. 1 Ziff. 5 des Bankengesetzes;

b) zentrale Gegenparteien nach Art. 2 Ziff. 1 der Verordnung (EU) Nr. 648/2012[3];

3 Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates vom 4. Juli 2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister (ABl. L 201 vom 27.7.2012, S. 1)

c) Zentralverwahrer nach Art. 2 Abs. 1 Ziff. 1 der Verordnung (EU) Nr. 909/2014[4].

2) Wesentliche Dienste nach Abs. 1 sind:

a) im Bereich der Handelsplätze nach Abs. 1 Bst. a, wenn pro Geschäftsjahr an diesem Handelsplatz mehr als zehn Millionen Transaktionen stattgefunden haben:
   1. die technische Anbindung der Handels- und Clearingteilnehmer;
   2. die Bereitstellung der elektronischen Handelsplattform;
   3. die Marktsteuerung als technischer Dienst;

b) im Bereich der Abwicklung durch zentrale Gegenparteien nach Abs. 1 Bst. b das Zurverfügungstellen eines Abwicklungssystems, wenn die zentrale Gegenpartei als Abwicklungsstelle von einem Handelsplatz, an dem pro Geschäftsjahr mehr als zehn Millionen Transaktionen stattgefunden haben, beauftragt wurde;

c) im Bereich der Zentralverwahrer nach Abs. 1 Bst. c:
   1. das Bereitstellen und Führen von Depotkonten auf oberster Ebene nach Abschnitt A Ziff. 2 des Anhangs der Verordnung (EU) Nr. 909/2014, wenn die Anzahl der stücknotierten Wertpapiere mehr als acht Milliarden im Geschäftsjahr beträgt;
   2. der Betrieb eines Wertpapierliefer- und -abrechnungssystems nach Abschnitt A Ziff. 3 des Anhangs der Verordnung (EU) Nr. 909/2014, wenn die Anzahl der abgewickelten Transaktionen höher als eine Million im Geschäftsjahr ist.

3) Im Sektor Finanzmarktinfrastrukturen bestehen Vorschriften, die zumindest ein gleichwertiges Sicherheitsniveau für Netz- und Informationssysteme nach Art. 4 Abs. 4 des Gesetzes gewährleisten, für Einrichtungen, die einen wesentlichen Dienst erbringen nach:

a) Abs. 2 Bst. a zu Sicherheitsanforderungen in Art. 30s Abs. 1 Bst. a und Abs. 3 sowie Art. 30t Abs. 1 Bst. a des Bankengesetzes iVm Art. 15, 16 und 23 Abs. 1 und 2 der Delegierten Verordnung (EU) 2017/584[5];

---

4 Verordnung (EU) Nr. 909/2014 des Europäischen Parlaments und des Rates vom 23. Juli 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. L 257 vom 28.8.2014, S. 1)

5 Delegierte Verordnung (EU) 2017/584 der Kommission vom 14. Juli 2016 zur Ergänzung der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der organisatorischen Anforderungen an Handelsplätze (ABl. L 87 vom 31.3.2017, S. 350)

b) Abs. 2 Bst. b zu Sicherheitsanforderungen in Art. 26 Abs. 1, 3 und 6 sowie Art. 34 der Verordnung (EU) Nr. 648/2012 iVm Art. 4 und 9 der Delegierten Verordnung (EU) Nr. 153/2013[6];

c) Abs. 2 Bst. c zu Sicherheitsanforderungen in Art. 45 der Verordnung (EU) Nr. 909/2014 iVm Art. 75 der Delegierten Verordnung (EU) 2017/392[7].

Art. 8

Sektor Gesundheitswesen

Wegen ihrer Bedeutung für die Aufrechterhaltung des öffentlichen Gesundheitsdienstes fallen unter den Sektor Gesundheitswesen Einrichtungen des Gesundheitswesens, die der stationären, teilstationären oder ambulanten Behandlung von akuten Krankheiten oder der Durchführung von Massnahmen der medizinischen Rehabilitation dienen, insbesondere Kliniken und Spitäler, und die dadurch einen wesentlichen Dienst erbringen.

Art. 9

Sektor Trinkwasserversorgung

1) Wegen ihrer Bedeutung für die Aufrechterhaltung der öffentlichen Versorgung mit Trinkwasser fallen unter den Sektor Trinkwasserversorgung Lieferanten von und Unternehmen der Versorgung mit Wasser im ursprünglichen Zustand oder nach Aufbereitung, das zum Trinken, zum Kochen, zur Zubereitung von Speisen oder zu anderen häuslichen Zwecken bestimmt ist, ungeachtet dessen, ob es aus einem Verteilungsnetz, in Tankfahrzeugen, in Flaschen oder anderen Behältern bereitgestellt wird und die dadurch einen wesentlichen Dienst erbringen.

---

6 Delegierte Verordnung (EU) Nr. 153/2013 der Kommission vom 19. Dezember 2012 zur Ergänzung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates in Bezug auf technische Regulierungsstandards für Anforderungen an zentrale Gegenparteien (ABl. L 52 vom 23.2.2013, S. 41)

7 Delegierte Verordnung (EU) 2017/392 der Kommission vom 11. November 2016 zur Ergänzung der Verordnung (EU) Nr. 909/2014 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für die Zulassung von und für aufsichtliche und operationelle Anforderungen an Zentralverwahrer (ABl. L 65 vom 10.3.2017, S. 48)

2) Ausgenommen sind Lieferanten, für welche die Lieferung von Wasser für den Gebrauch nach Abs. 1 nur ein Teil der allgemeinen Tätigkeit der Lieferung anderer Rohstoffe und Güter ist, die nicht als wesentliche Dienste eingestuft werden.

Art. 10

Sektor digitale Infrastruktur

Wegen ihrer Bedeutung für die Aufrechterhaltung der Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie fallen unter den Sektor digitale Infrastruktur folgende Arten von Einrichtungen, die wesentliche Dienste erbringen:

a) DNS-Diensteanbieter, die die Funktion des Anbietens von DNS-Diensten im Internet wahrnehmen;

b) TLD-Name-Registries (Top-Level-Domain-Name-Registries);

c) IXP's (Internet-Knoten);

d) das Anbieten öffentlicher elektronischer Kommunikationsnetze im Sinne der Kommunikationsgesetzgebung;

e) das Anbieten öffentlich zugänglicher elektronischer Kommunikationsdienste im Sinne der Kommunikationsgesetzgebung.

B. Sicherheitsanforderungen

Art. 11

Sicherheitsmassnahmen

1) Betreiber wesentlicher Dienste ergreifen bei der Gewährleistung des Sicherheitsniveaus der Netz- und Informationssysteme nach Art. 4 des Gesetzes die im Anhang aufgeführten Sicherheitsmassnahmen in den Bereichen:

a) Governance und Risikomanagement;

b) Benutzerberechtigungsmanagement (Identitäts- und Zugriffsmanagement);

c) Betriebsmanagement (laufender Betrieb und Wartung);

d) Projekt-, Änderungs- und Updatemanagement;

e) Umgang mit Dienstleistern, Lieferanten und Dritten;

f) physische Sicherheit;

g) Management von Sicherheitsvorfällen (Erkennung und Bewältigung);

h) Betriebskontinuität; und

i) Krisenmanagement (Notfallkonzept).

2) Sicherheitsmassnahmen in den Bereichen nach Abs. 1 sind, soweit möglich, in technischer und organisatorischer Hinsicht auf Basis einer Risikoanalyse umzusetzen, wobei die betrieblichen Auswirkungen von Sicherheitsvorfällen zu ermitteln und hinsichtlich der hohen Bedeutung des Betreibers wesentlicher Dienste für das Funktionieren des Gemeinwesens zu bewerten sind.

III. Meldepflicht

Art. 12

Meldeverfahren

1) Die Stabsstelle Cyber-Sicherheit stellt für Meldungen zu Sicherheitsvorfällen nach Art. 5 des Gesetzes ein elektronisches Formular zur Verfügung.

2) Durch die im Rahmen der Erstmeldung übermittelten Angaben zum Sicherheitsvorfall muss es dem CSIRT möglich sein, festzustellen, ob ein solcher allfällige grenzüberschreitende Auswirkungen hat.

3) Nachmeldungen umfassen eine Aktualisierung der im Rahmen der Erstmeldung übermittelten Angaben zum Sicherheitsvorfall, insbesondere über dessen Schwere, Auswirkungen sowie etwaige Kompromittierungsindikatoren (IOCs).

Art. 13

Erheblichkeit der Auswirkung eines Sicherheitsvorfalls

Bei der Beurteilung des Ausmasses eines Sicherheitsvorfalls berücksichtigen die Betreiber wesentlicher Dienste zumindest die folgenden sektorübergreifenden Faktoren:

a) die Zahl der Nutzer, die den von der jeweiligen Einrichtung angebotenen Dienst in Anspruch nehmen;

b) die Dauer des Sicherheitsvorfalls;

c) das Ausmass der Unterbrechung der Bereitstellung des Dienstes;

d) das Ausmass der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten;

e) den Marktanteil der betroffenen Einrichtung;

f) die geografische Ausbreitung des Gebiets, das von einem Sicherheitsvorfall betroffen sein könnte;

g) die Bedeutung der betroffenen Einrichtung auf die Aufrechterhaltung des Dienstes in ausreichendem Umfang, unter Berücksichtigung der Verfügbarkeit von alternativen Mitteln für die Bereitstellung des jeweiligen Dienstes.

Art. 14

Bearbeitung von Meldungen

1) Meldungen zu Sicherheitsvorfällen nach Art. 12 Abs. 1 werden durch das CSIRT unter Verwendung einer eigenen IT-Infrastruktur bearbeitet.

2) Informationen zu gemeldeten Sicherheitsvorfällen, wie insbesondere Kompromittierungsindikatoren, können vom CSIRT an externe Stellen übermittelt werden, um:

a) die Kompromittierung von Systemen festzustellen;

b) herauszufinden, welche Daten oder Systeme von einer Kompromittierung betroffen sind;

c) die Schwere von Sicherheitsvorfällen einzuschätzen;

d) Hinweise zu den von Angreifern verwendeten Angriffsvektoren und Werkzeugen zur Verfügung zu stellen, damit Bedrohungen vermindert oder beseitigt werden können;

e) Schwachstellen in Systemen zu identifizieren;

f) gezielte Gegenmassnahmen zu entwickeln, damit künftige Angriffe verhindert werden können.

IV. Organisation und Durchführung

A. Qualifizierte Dritte

Art. 15

Anforderungen

1) Qualifizierte Dritte, die mit Aufgaben der Stabsstelle Cyber-Sicherheit oder des CSIRT nach Art. 9 Abs. 2 des Gesetzes, insbesondere mit der Durchführung von Kontrollen nach Art. 18 des Gesetzes, beauftragt werden, müssen:

a) von den zu prüfenden Betreibern wesentlicher Dienste und Anbietern digitaler Dienste unabhängig sein; und

b) über die erforderlichen Kenntnisse zur Erfüllung der ihnen auferlegten Aufgaben verfügen.

2) Sie haben die erforderlichen Kenntnisse nach Abs. 1 Bst. b durch einschlägige Qualifikationen, gegebenenfalls durch entsprechende Zertifizierungen, auf Verlangen der Stabsstelle Cyber-Sicherheit nachzuweisen.

B. Zusammenarbeit und Informationsaustausch mit inländischen Behörden

Art. 16

Zusammenarbeit und Informationsaustausch mit der FMA

1) Die Stabsstelle Cyber-Sicherheit arbeitet, soweit dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist, mit der Finanzmarktaufsicht (FMA) im Hinblick auf die Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen zusammen und kann zu diesem Zweck Informationen austauschen.

2) Vom Informationsaustausch können umfasst sein:

a) bei der FMA nach Art. 101 und 102 des Zahlungsdienstegesetzes und bei der Stabsstelle Cyber-Sicherheit nach Art. 5 oder 8 des Gesetzes eingegangene Meldungen zu Sicherheitsvorfällen aus den Sektoren Bankwesen und Finanzmarktinfrastrukturen;

b) Informationen, die der FMA oder der Stabsstelle Cyber-Sicherheit im Rahmen der Erfüllung ihrer jeweiligen Aufgaben übermittelt werden;

c) Informationen über ausserordentliche Vorkommnisse im Cyberraum.

3) Die Stabsstelle Cyber-Sicherheit kann die FMA um Unterstützung bei der Überprüfung der Sicherheitsanforderungen und der Einhaltung der Meldepflichten nach Art. 4 und 5 des Gesetzes ersuchen. Die FMA kann im Rahmen ihrer Befugnisse die Überprüfungen oder Ermittlungen selbst vornehmen oder durch beauftragte Sachverständige vornehmen lassen.

Art. 17

Zusammenarbeit und Informationsaustausch mit der Landespolizei

Die Stabstelle Cyber-Sicherheit arbeitet zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen mit der Landespolizei zusammen, insbesondere in den Bereichen:

a) des Informationsaustauschs über ausserordentliche Vorkommnisse im Cyberraum;

b) der technischen Unterstützung, indem vorhandene Ressourcen bei Bedarf geteilt und gegenseitig zur Verfügung gestellt werden;

c) der Teilnahme zu Übungen und Schulungen.

Art. 18

Zusammenarbeit und Informationsaustausch mit der Staatsanwaltschaft

Die Stabsstelle Cyber-Sicherheit arbeitet zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen mit der Staatsanwaltschaft zusammen, insbesondere in den Bereichen:

a) der sicheren Übermittlung von Informationen durch die Schaffung sicherer Übermittlungskanäle;

b) des Informationsaustauschs über ausserordentliche Vorkommnisse im Cyberraum.

Art. 19

Zusammenarbeit und Informationsaustausch mit der Stabsstelle FIU

1) Die Stabsstelle Cyber-Sicherheit arbeitet zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen mit der Stabsstelle FIU zusammen, insbesondere in den Bereichen:

a) der strategischen Risikoanalyse;

b) der Durchsetzung internationaler Sanktionen sowie der Vermittlung von und den Handel mit Kriegsmaterial, nuklearen Gütern, radioaktiven Abfällen, doppelt verwendbaren Gütern und besonderen militärischen Gütern.

2) Für die Zwecke nach Abs. 1 übermitteln sich die Stabsstelle Cyber-Sicherheit und die Stabsstelle FIU die hierfür notwendigen Informationen und Unterlagen, einschliesslich personenbezogener Daten, soweit diese nicht von Art. 6 Abs. 2 des FIU-Gesetzes erfasst sind.

3) Die Stabsstelle Cyber-Sicherheit schliesst nach Rücksprache mit dem zuständigen Regierungsmitglied mit der Stabsstelle FIU eine Vereinbarung über die weiteren Modalitäten der Zusammenarbeit nach Art. 13 Abs. 2 des Gesetzes ab.

C. Kontrollen

Art. 20

Allgemeines

1) Die Stabsstelle Cyber-Sicherheit kann jederzeit Kontrollen nach Art. 18 Abs. 1 des Gesetzes durchführen oder durch qualifizierte Dritte durchführen lassen.

2) Kontrollen nach Abs. 1 sind vorgängig durch die Stabsstelle Cyber-Sicherheit anzukündigen; ausgenommen bei Vorliegen von Gefahr in Verzug.

Art. 21

Umfang und Ablauf

1) Die Stabsstelle Cyber-Sicherheit legt vor Durchführung einer Kontrolle deren Umfang in Abstimmung mit der zu kontrollierenden Stelle fest. Bei einer Kontrolle wird insbesondere festgestellt, ob:

a) geeignete und verhältnismässige technische und organisatorische Massnahmen zum Schutz der Netz- und Informationssysteme umgesetzt sind;

b) die Sicherheitsanforderungen nach dem Gesetz und dieser Verordnung eingehalten werden;

c) die Meldepflicht nach Art. 5 oder 7 des Gesetzes eingehalten wurde.

2) In begründeten Fällen kann die Stabsstelle Cyber-Sicherheit den Umfang während einer laufenden Kontrolle erweitern oder einschränken.

3) Die Stabsstelle Cyber-Sicherheit kann vertrauliche Inhalte zum Nachweis der Einhaltung von Sicherheitsanforderungen in einer sicheren und von der kontrollierten Stelle zur Verfügung gestellten Räumlichkeit prüfen.

4) Sie erstellt über die Ergebnisse der Kontrolle jeweils einen Bericht und übermittelt diesen der kontrollierten Stelle. In Absprache mit der kontrollierten Stelle sowie in begründeten Fällen kann die Stabsstelle Cyber-Sicherheit den Bericht vollständig oder auszugsweise an Dritte weitergeben.

5) Die Arbeitspapiere, Dokumente und Datenträger sind während zehn Jahren nach Abschluss der jeweiligen Kontrollen aufzubewahren; ausgenommen sind vertrauliche Inhalte nach Abs. 3.

Art. 22

Kontrollen durch qualifizierte Dritte

1) Qualifizierte Dritte haben ihre Kontrollen nach den Vorgaben der Stabsstelle Cyber-Sicherheit durchzuführen. Sie sind verpflichtet:

a) bei der Stabsstelle Cyber-Sicherheit nach Abschluss der Kontrolle einen Kontrollbericht einzureichen. Hierbei dürfen wesentliche Tatsachen nicht verschwiegen werden. Die Angaben im Kontrollbericht müssen der Wahrheit entsprechen;

b) die von der Stabsstelle Cyber-Sicherheit bestimmten Grundsätze über Kontrolltätigkeit und die Durchführung der Kontrollen einzuhalten und der Stabsstelle Cyber-Sicherheit auf Verlangen sämtliche im Rahmen der Kontrolle erstellten Arbeitspapiere zur Verfügung zu stellen;

c) der Stabsstelle Cyber-Sicherheit auf deren Verlangen jederzeit einen Zwischenbericht über den aktuellen Stand der Kontrolle abzugeben.

2) Qualifizierte Dritte unterliegen der Geheimhaltungspflicht. Vorbehalten bleiben die Berichterstattungs- und Auskunftspflicht nach Abs. 1.

3) Qualifizierte Dritte müssen bei der Durchführung einer Kontrolle von den zu kontrollierenden Stellen unabhängig sein. Sie dürfen insbesondere in den letzten 18 Monaten für die zu kontrollierende Stelle nicht beratend tätig gewesen sein.

V. Schlussbestimmung

Art. 23

Inkrafttreten

1) Diese Verordnung tritt vorbehaltlich Abs. 2 am Tag nach der Kundmachung in Kraft.

2) Art. 1 Abs. 2 Bst. a tritt gleichzeitig mit dem Beschluss des Gemeinsamen EWR-Ausschusses Nr. 21/2023 vom 3. Februar 2023 zur Änderung von Anhang XI (Elektronische Kommunikation, audiovisuelle Dienste und Informationsgesellschaft) des EWR-Abkommens in Kraft.

Fürstliche Regierung:
gez. *Dr. Daniel Risch*
Fürstlicher Regierungschef

Anhang
(Art. 11 Abs. 1)

Sicherheitsmassnahmen

1.	**Governance und Risikomanagement**
1.1	Risikoanalyse: Eine Risikoanalyse der Netz- und Informationssysteme ist periodisch 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. Regelmässig sind Schulungen im Bereich der Cybersicherheit bei den Mitarbeitenden durchzuführen.

2.	**Benutzerberechtigungsmanagement (Identitäts- und Zugriffsmanagement)**
2.1	Identifikation und Authentifikation: Es sind Verfahren umzusetzen und Technologien einzusetzen, die die Identifikation und Authentifikation von Benutzern und Diensten gewährleisten. Die Zuweisungen von Benutzerberechtigungen sind periodisch zu überprüfen und gegebenenfalls anzupassen.
2.2	Autorisierung: Es sind Verfahren umzusetzen und Technologien einzusetzen, die unautorisierte Zugriffe auf Netz- und Informationssysteme unterbinden.
2.3	Multi-Faktor-Authentifizierung: Authentifizierungsmethoden sind der Kritikalität der Netz- und Informationssysteme angemessen. Dies umfasst unter anderem eine Multi-Faktor-Authentifizierung.
3.	**Betriebsmanagement (laufender Betrieb und Wartung)**
3.1	Systemwartung und Betrieb: Abläufe und Vorgänge zur Gewährleistung eines sicheren Systembetriebs von Netz- und Informationssystemen sind einzuführen und periodisch zu überprüfen.
3.2	Systeme und Anwendungen zur Systemadministration: Systeme und Anwendungen zur Systemadministration sind ausschliesslich für Tätigkeiten zum Zweck der Systemadministration zu verwenden.
3.3	Administrative Zugangsrechte: Administrative Zugangsrechte sind eingeschränkt nach dem Minimalrechtsprinzip zuzuweisen. Diese Zuweisungen sind periodisch zu überprüfen und gegebenenfalls anzupassen.
3.4	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.

3.5	Systemkonfiguration: Netz- und Informationssysteme sind sicher zu konfigurieren. Diese Konfiguration ist zu dokumentieren. Die Dokumentation ist aktuell zu halten.
3.6	Netzwerksegmentierung: Eine Segmentierung der Netzwerke ist innerhalb der Netz- und Informationssysteme abhängig vom Schutzbedarf vorzunehmen.
3.7	Kryptographie: Vertraulichkeit, Authentizität und Integrität von Informationen sind durch den angemessenen und wirksamen Einsatz kryptographischer Verfahren und Technologien sicherzustellen.
4.	**Projekt- und Änderungsmanagement**
4.1	Projektmanagement: Die Sicherheit der Netz- und Informationssysteme ist in den Prozessen des Projektmanagements entsprechend zu berücksichtigen.
4.2	Änderungsmanagement: Die Sicherheit der Netz- und Informationssysteme ist in den Prozessen des Änderungsmanagements entsprechend zu berücksichtigen. Änderungen an den Netz- und Informationssystemen, insbesondere auch sicherheitsrelevante Konfigurationsänderungen, werden aufgezeichnet, getestet, bewertet, genehmigt, umgesetzt und überprüft.
4.3	Updatemanagement: Mögliche Datenlecks sowie öffentlich bekannte Sicherheitslücken in eingesetzter Software und Hardware sind zu identifizieren. Verfügbare Sicherheitsupdates sind zeitnah zu testen, zu bewerten und einzuspielen.
5.	**Umgang mit Dienstleistern, Lieferanten und Dritten**
5.1	Beziehungen mit Dienstleistern, Lieferanten und Dritten: Anforderungen an Dienstleister, Lieferanten und Dritte für den Betrieb von, einen sicheren Zugang zu und Zugriff auf Netz- und Informationssysteme sind festzulegen und periodisch zu überprüfen.

5.2	Schwachstellenmanagement: Spezifische Verwundbarkeiten der einzelnen Dienstleister und der Lieferanten sowie die Gesamtqualität der eingesetzten Produkte in Bezug auf die Cybersicherheit sind im laufenden Betrieb zu berücksichtigen.
5.3	Leistungsvereinbarungen mit Dienstleistern und Lieferanten: Die Leistungsvereinbarungen mit Dienstleistern und Lieferanten sind periodisch zu überprüfen und zu überwachen.
6.	**Physische Sicherheit**
	Der physische Schutz der Netz- und Informationssysteme, insbesondere der physische Schutz vor unbefugtem Zutritt und Zugang, ist zu gewährleisten.
7.	**Management von Sicherheitsvorfällen (Erkennung und Bewältigung)**
7.1	Erkennung: Mechanismen zur Erkennung und Bewertung von Sicherheitsvorfällen sind umzusetzen.
7.2	Protokollierung und Monitoring: Mechanismen zu Protokollierung und Monitoring, insbesondere von für die Erbringung des wesentlichen Dienstes essentiellen Tätigkeiten und Vorgängen, sind umzusetzen.
7.3	Korrelation und Analyse: Mechanismen zur Erkennung und adäquaten Bewertung von Sicherheitsvorfällen durch die Korrelation und Analyse der ermittelten Protokolldaten sind umzusetzen.
7.4	Sicherheitsvorfallsreaktion: Prozesse zur Reaktion auf Sicherheitsvorfälle sind zu erstellen, aufrechtzuerhalten und zu erproben.
7.5	Sicherheitsvorfallsmeldung: Prozesse zur internen und externen Meldung von Sicherheitsvorfällen sind zu erstellen, aufrechtzuerhalten und zu erproben.

7.6	Sicherheitsvorfallsanalyse: Prozesse zur Analyse und Bewertung von Sicherheitsvorfällen und zur Sammlung relevanter Informationen sind zu erstellen, aufrechtzuerhalten und zu erproben, um den kontinuierlichen Verbesserungsprozess zu fördern.
8.	**Betriebskontinuität**
8.1	Betriebskontinuitätsmanagement: Die Wiederherstellung der Erbringung des wesentlichen Dienstes auf einem zuvor festgelegten Qualitätsniveau nach einem Sicherheitsvorfall ist zu gewährleisten.
8.2	Notfallmanagement: Notfallpläne sind zu erstellen, anzuwenden, regelmässig zu bewerten und zu erproben.
9.	**Krisenmanagement (Notfallkonzept)**
	Rahmenbedingungen und Prozessabläufe des Krisenmanagements sind für die Aufrechterhaltung des wesentlichen Dienstes vor und während eines Sicherheitsvorfalls zu definieren, umzusetzen und zu erproben.