Sachstand

Schutz kritischer Infrastrukturen

Rechtslage in Deutschland, Finnland, Frankreich, Österreich und Schweden

Schutz kritischer Infrastrukturen
Rechtslage in Deutschland, Finnland, Frankreich, Österreich und Schweden

Aktenzeichen: WD 3 - 3000 - 176/22
Abschluss der Arbeit: 30.03.2023
Fachbereich: WD 3: Verfassung und Verwaltung

Inhaltsverzeichnis

1. Einleitung

Dieser Sachstand stellt die sektorübergreifenden rechtlichen Regelungen zum Schutz kritischer Infrastrukturen dar, die in den Ländern Deutschland sowie – im Wesentlichen basierend auf Angaben aus diesen Ländern – Schweden, Finnland, Österreich und Frankreich gelten. Zudem wird auf sektorübergreifende Meldepflichten eingegangen, die auf Betreiber kritischer Infrastrukturen zukommen können.

2. Deutschland

Der Begriff „kritische Infrastruktur“ ist gesetzlich nicht einheitlich definiert. Es gibt mehrere Gesetze, die als spezifischer Beitrag zum Schutz kritischer Infrastrukturen angesehen werden.[1] Diese können in sektorübergreifende und sektorspezifische Regelungen aufgeteilt werden. Die nachfolgenden Ausführungen konzentrieren sich auf die sektorübergreifenden Regelungen.

Auf **sektorübergreifender Ebene** finden sich vor allem im **IT-Sicherheitsrecht** Vorschriften für Betreiber kritischer Infrastrukturen aus unterschiedlichen Sektoren, namentlich im **Gesetz über das Bundesamt für Sicherheit in der Informationstechnik** (BSI-Gesetz – BSIG)[2], das unter anderem die EU-Richtlinie 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union vom 6. Juli 2016 **(NIS-Richtlinie)**[3] umsetzt. Dessen § 2 Abs. 10 Satz 1 lautet:

> Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die
>
> 1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung angehören und
>
> 2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Die kritischen Infrastrukturen wurden dabei gemäß § 2 Abs. 10 Satz 2 BSIG mittels der Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) genauer bestimmt. Die BSI-KritisV stellt zur **Beurteilung der Kritikalität** auf den **Versorgungsgrad** der jeweiligen Anlagen ab (§ 1 Nr. 4 BSI-KritisV).

---

1 Wischmeyer/Schumacher, in: Dietrich/Fahrner/Gazeas/von Heintschel-Heinegg, Handbuch Sicherheits- und Staatsschutzrecht, 2022, § 14 Rn. 23.

2 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 14. August 2009 (BGBl. I S. 2821), zuletzt geändert durch Art. 12 G zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien vom 23. Juni 2021 (BGBl. I S. 1982).

3 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. Juli 2016, S. 1–30.

§ 8a Abs. 1 BSIG verpflichtet die Betreiber kritischer Infrastrukturen, **angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen** der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind und sich auf dem Stand der Technik befinden.

Diese Pflicht aus § 8a Abs. 1 BSIG umfasst ab dem 1. Mai 2023 auch den **Einsatz von Systemen zur Angriffserkennung** (§ 8a Abs. 1a BSIG). Die dabei eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten sowie dem Stand der Technik entsprechen.

Nach § 8a Abs. 2 BSIG können sog. branchenspezifische Sicherheitsstandards entwickelt werden und vom BSI zertifiziert werden, wodurch die Betroffenen Rechtssicherheit über die unbestimmten Rechtsbegriffe des § 8a Abs. 1 BSIG erhalten können.

§ 8f BSIG verpflichtet Unternehmen im besonderen öffentlichen Interesse zudem, eine **Selbsterklärung** über durchgeführte Zertifizierungen, Sicherheitsaudits oder Prüfungen im Bereich der IT-Sicherheit sowie über weitere Sicherheitsvorkehrungen bezüglich des Schutzes von für das Unternehmen besonders schützenswerten informationstechnischen Systemen, Komponenten und Prozessen beim Bundesamt für Sicherheit in der Informationstechnik (BSI) abzugeben.

Neben diesen Vorschriften des BSIG finden sich weitere Regelungen zu kritischen Infrastrukturen in anderen Gesetzen. § 2 Abs. 2 Nr. 3 Satz 4 des **Raumordnungsgesetzes**[4] etwa bestimmt im Rahmen der Grundsätze des Raumordnungsrechts, dass bei der Raumordnung dem Schutz kritischer Infrastrukturen Rechnung zu tragen ist.

§ 55 der **Außenwirtschaftsverordnung** (AWV)[5] ermächtigt das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) zu prüfen, ob es die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland oder eines anderen Mitgliedstaates der Europäischen Union voraussichtlich beeinträchtigt, wenn ein Unionsfremder unmittelbar oder mittelbar ein inländisches Unternehmen oder eine Beteiligung an einem solchen erwirbt. Dabei wird durch § 55a Abs. 1 Nr. 1 AWV eine voraussichtliche Beeinträchtigung regelmäßig angenommen, wenn das Unternehmen Betreiber kritischer Infrastrukturen ist. Das BMWK kann den Erwerb dann untersagen (§ 59 AWV).

4 Raumordnungsgesetz vom 22. Dezember 2008 (BGBl. I S. 2986), zuletzt geändert durch Artikel 3 des Gesetzes vom 20. Juli 2022 (BGBl. I S. 1353).

5 Außenwirtschaftsverordnung vom 2. August 2013 (BGBl. I S. 2865; 2021 I S. 4304), zuletzt geändert durch Artikel 10 des Gesetzes vom 19. Dezember 2022 (BGBl. I S. 2632).

Am 14. Dezember 2022 wurde die **EU-Richtlinie über die Resilienz kritischer Infrastrukturen (CER-Richtlinie)**[6] verabschiedet, die weitere Regelungen zum Schutz kritischer Infrastrukturen enthält. Die Richtlinie soll in Deutschland durch das sog. KRITIS-Dachgesetz umgesetzt werden, zu dem bisher nur ein Eckpunkte-Papier[7] vorliegt.

Neben diesen allgemeinen Regelungen bestehen für die jeweiligen Sektoren spezielle Regelungen. So muss nach § 53a des Energiewirtschaftsgesetzes[8] die Versorgung von Haushaltskunden mit Erdgas gewährleistet sein, während das Erdölbevorratungsgesetz[9] zur Vorratshaltung von Erdöl und Erdölerzeugnissen verpflichtet.

Daneben bestehen zudem die Regelungen der sog. **Sicherstellungsgesetze**. Diese dienen der Sicherstellung der Versorgung der Bevölkerung mit bestimmten (lebens-)wichtigen Gütern und Leistungen wie Nahrungsmitteln, Medizinprodukten und Impfstoffen sowie deren Transport. Dazu gehören neben dem Wirtschaftssicherstellungsgesetz[10] das Verkehrssicherstellungsgesetz[11], das Ernährungssicherstellungs- und -vorsorgegesetz[12] und das Wassersicherstellungsgesetz[13], aber auch § 5 Abs. 2 Satz 1 Nr. 4 des Infektionsschutzgesetzes[14] sowie Vorschriften des Telekommunikationsgesetzes[15]. Diese Gesetze ermächtigen die Exekutive zum Erlass von Rechtsverordnungen, die erst gültig werden, wenn ein im Gesetz bestimmter Notfall oder Krisenfall eintritt, etwa wenn eine Versorgungskrise nach § 1 des Ernährungssicherstellungs- und -vorsorgegesetzes vorliegt.

---

6 Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates, PE/51/2022/REV/1, ABl. L 333, 27. Dezember 2022, S. 164–198.

7 Unterrichtung durch die Bundesregierung, Eckpunkte für das KRITIS-Dachgesetz, BT-Drs. 20/5491, abrufbar unter: https://dserver.bundestag.de/btd/20/054/2005491.pdf.

8 Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz – EnWG) vom 7. Juli 2005 (BGBl. I S. 1970, ber. S. 3621), zuletzt geändert durch Art. 3 G zu Herkunftsnachweisen für Gas, Wasserstoff, Wärme oder Kälte aus erneuerbaren Energien und zur Änd. anderer energierechtlicher Vorschriften vom 4. Januar 2023 (BGBl. I Nr. 9).

9 Gesetz über die Bevorratung mit Erdöl und Erdölerzeugnissen (Erdölbevorratungsgesetz – ErdölBevG) vom 16. Januar 2012 (BGBl. I S. 74), zuletzt geändert durch Art. 1 ÄndG vom 9. Dezember 2019 (BGBl. I S. 2101).

10 Wirtschaftssicherstellungsgesetz in der Fassung der Bekanntmachung vom 3. Oktober 1968 (BGBl. I S. 1069), zuletzt geändert durch Artikel 262 der Verordnung vom 31. August 2015 (BGBl. I S. 1474).

11 Verkehrssicherstellungsgesetz in der Fassung der Bekanntmachung vom 8. Oktober 1968 (BGBl. I S. 1082), zuletzt geändert durch Artikel 55 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1858).

12 Ernährungssicherstellungs- und -vorsorgegesetz vom 4. April 2017 (BGBl. I S. 772), zuletzt geändert durch Artikel 1 des Gesetzes vom 9. Dezember 2020 (BGBl. I S. 2863).

13 Wassersicherstellungsgesetz vom 24. August 1965 (BGBl. I S. 1225, 1817), zuletzt geändert durch Artikel 251 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328).

14 Infektionsschutzgesetz vom 20. Juli 2000 (BGBl. I S. 1045), zuletzt geändert durch Artikel 8b des Gesetzes vom 20. Dezember 2022 (BGBl. I S. 2793). Keine englische Fassung verfügbar.

15 Telekommunikationsgesetz vom 23. Juni 2021 (BGBl. I S. 1858), zuletzt geändert durch Artikel 9 des Gesetzes vom 20. Juli 2022 (BGBl. I S. 1166). Keine englische Fassung verfügbar.

§ 8b Abs. 3 BSIG sieht die **Einrichtung einer rund um die Uhr erreichbaren Kontaktstelle** vor, mittels derer die Betreiber kritischer Infrastrukturen im Fall von Störungen unverzüglich **Meldung an das BSI** zu machen haben.

3. Finnland

Derzeit gibt es in Finnland keine Gesetze, die nationale kritische Infrastrukturen, kritische Sektoren oder deren Betreiber definieren. Das finnische Parlament arbeitet derzeit an einem Gesetz zur Umsetzung der **CER-Richtlinie**, in dem die Sektoren der kritischen Infrastruktur sowie Behörden zur Überwachung der Maßnahmen zur Krisenresilienz des jeweiligen Sektors bestimmt werden sollen.

Der Schutz kritischer Infrastrukturen ist Gegenstand verschiedener gesetzlicher Regelungen. So unterstützt das **Gesetz über die Gewährleistung der Versorgungssicherheit vom 18. Dezember 1992**[16] die Krisenfestigkeit kritischer Infrastrukturen. Davon umfasst sind die Sicherung der Produktion, der Dienstleistungen und der Infrastruktur, die im Falle von schwerwiegenden Störungen und außergewöhnlichen Umständen für den Lebensunterhalt der Bevölkerung, die Wirtschaft des Landes und die Landesverteidigung notwendig sind. Die Teilnahme an Sicherungsmaßnahmen ist für private Unternehmen freiwillig, zudem werden sie nicht überwacht.

Die **Lagerung von für das Funktionieren der Gesellschaft notwendigen Produkten und Materialien** wird durch verschiedene Gesetze geregelt und erfolgt auf drei Arten. Zum einen ist die **Nationale Agentur für Notfallversorgung** für die nationale Sicherheitsbevorratung zuständig. Zum anderen sind Unternehmen und andere wichtige Akteuren verantwortlich für Pflichtbevorratung. Darüber hinaus wird die Sicherheitsbevorratung zwischen Unternehmen eines Sektors und der Nationalen Agentur für Notfallversorgung vereinbart.

Eine Konzentration der Kontinuitätsmanagement- und Überwachungsaufgaben in einer einzigen Behörde auf nationaler Ebene, wie sie die CER-Richtlinie für verschiedene Verwaltungszweige vorschreibt, fand bisher nicht statt. Dies gilt auch für die ebenfalls von der CER-Richtlinie geforderte sektorübergreifende Überwachung und die von ihr verlangten Meldepflichten. Bestimmungen über die Vorsorgeverpflichtungen der Betreiber kritischer Infrastrukturen finden sich auch in den Rechtsvorschriften verschiedener Ministerien. Manche von ihnen enthalten Aufsichts- und Berichterstattungsaufgaben, die den von der Richtlinie geforderten ähneln.

Bestimmte sektorale Rechtsvorschriften sehen Meldepflichten im Falle von Störungen vor. Mit der Umsetzung der CER-Richtlinie sollen Meldepflichten in allen Sektoren der Richtlinie eingeführt werden.

---

16 Laki huoltovarmuuden turvaamisesta 1390/1992 vom 18. Dezember 1992, auf Finnisch und Schwedisch abrufbar unter: https://www.finlex.fi/fi/laki/ajantasa/1992/19921390.

4. Frankreich

Das französische Recht kennt kritische Infrastrukturen als sog. **„points d'importance vitale"** (lebenswichtiger Aspekt, PIV). Diese werden in **Artikel L.1332-1 des Verteidigungsgesetzbuchs**[17] als „Anlagen und Strukturen, deren Nichtverfügbarkeit das Kriegspotential oder das Wirtschaftspotential, die Sicherheit oder die Überlebensfähigkeit der Nation erheblich beeinträchtigen könnte", definiert. Kapitel II des Verteidigungsgesetzbuches zum „Schutz lebenswichtiger Anlagen" (Artikel L1332-1 bis L1332-7) enthält weitere Regelungen zu den PIV. Zudem finden sich in der **Allgemeinen interministeriellen Anweisung Nr. 6600 vom 7. Januar 2014**[18] Bestimmungen zur Sicherheit von lebenswichtigen Aktivitäten.

Es werden zwölf **Sektoren von lebenswichtiger Bedeutung** unterschieden, die in vier Bereiche aufgeteilt sind. Der Bereich „humaine" beinhaltet Lebensmittel, Wasserwirtschaft und Gesundheit. Ein Komplex regelt zivile, justizielle und militärische Aktivitäten des Staates. Der Bereich Wirtschaft umfasst Energie, Finanzen und Verkehr. Der Bereich Technologie befasst sich mit elektronischer Kommunikation, audiovisuellen Medien und Information, Industrie, Raumfahrt und Forschung.

Mehrere Behörden sind für diese Bereiche zuständig. Das **Generalsekretariat für Landesverteidigung und Sicherheit (SGDSN)** sorgt im Auftrag des Premierministers für die **Steuerung und interministerielle Koordinierung des Systems**. Es legt den Rahmen für die Sicherheitspolitik der lebenswichtigen Aktivitäten fest, insbesondere in Bezug auf Methode und Doktrin, und genehmigt die **nationalen Sicherheitsrichtlinien (DNS)**. Es legt auch die von den Betreibern von Einrichtungen mit lebenswichtigen Funktionen anzuwendenden Cybersicherheitsregeln fest. Die **koordinierenden Ministerien** sind für die Ausarbeitung der DNS für jeden Sektor und Untersektor von lebenswichtigen Aktivitäten verantwortlich, wobei sie die zu berücksichtigenden Probleme, Schwachstellen und Bedrohungen angeben und die Sicherheitsziele des Sektors definieren. Die koordinierenden Ministerien sind auch die Hauptansprechpartner für die Betreiber. Das **Innenministerium** ist für die territoriale Koordinierung des Systems zuständig, um die Maßnahmen der Präfekten der Zonen und Departements zu unterstützen. Der **Zonenpräfekt** ist als regionale Stelle für die Koordinierung des Systems der Sicherheitspolitik lebenswichtiger Aktivitäten zuständig. Seine Aufgabe ist es, die Präfekturen zu koordinieren, zu unterstützen und Informationen zwischen der zentralen Ebene und den Departements zu vermitteln. Er koordiniert auch die Kontrollen der PIV in seinem Zuständigkeitsbereich. Der **Präfekt des Departements** genehmigt für jeden PIV den vom Betreiber erstellten besonderen Schutzplan. Er erstellt auch einen Plan für den Außenschutz, der die geplanten Überwachungs- und Interventionsmaßnahmen im Falle einer Bedrohung oder eines Angriffs auf diesen wichtigen Punkt enthält.

Das **SGDSN** erstellt in Zusammenarbeit mit den betroffenen Ministerien eine Liste der Betreiber von lebenswichtiger Bedeutung, bei denen es sich sehr häufig um Unternehmen handelt. Darauf finden sich derzeit 240 solcher Betreiber. Der Minister, in dessen Arbeitsfeld der jeweilige Sektor fällt, wählt sie unter den Betreibern oder Nutzern von Einrichtungen aus, die für das Leben im

---

17 Code de la défense, Stand vom 20 März 2023, auf Französisch abrufbar unter: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071307/LEGISCTA000006166900/#LEGISCTA000006166900.

18 Instruction générale interministérielle relative la sécurité des activités d'importance vitale, Secrétariat General de la Défense et de la Sécurité Nationale, 7. Januar 2014, auf Französisch abrufbar unter: https://www.legifrance.gouv.fr/download/pdf/circ?id=37828.

Land wesentlich sind. Die Auswahlkriterien und die Sicherheitsziele werden vom koordinierenden Ministerium festgelegt. Das Verfahren beruht auf einer Beratung mit potenziellen Betreibern sowie auf einer interministeriellen Beratung, die einen gleichwertigen Schutz zwischen den verschiedenen Sektoren ermöglicht. Bei der Auswahl der Betreiber von lebenswichtiger Bedeutung werden mögliche Wettbewerbsverzerrungen berücksichtigt und unangemessene Belastungen vermieden.

Die Allgemeine interministerielle Anweisung Nr. 6600 vom 7. Januar 2014 besagt, dass jeder point d'importance vitale in einem **Sicherheitsplan des Betreibers** behandelt wird. Dieser Sicherheitsplan enthält insbesondere eine Reihe von Dokumenten über die bei jeder Art von Vorfall anzuwendenden Verfahren. Der Sicherheitsplan enthält auch eine Liste von Ansprechpartnern, die jederzeit erreichbar sein müssen.

5. Österreich

In Österreich gibt es keine spezifische Gesetzgebung, die die Definition oder den Schutz kritischer Infrastrukturen zum Gegenstand hat. Allerdings gibt es mehrere Gesetze, die den Schutz kritischer Infrastrukturen zum Ziel haben.

Das **Netz- und Informationssicherheitsgesetz (NISG)**[19] setzt die **NIS-Richtlinie** um **(unter Maßgabe der EU-Durchführungsverordnung der Kommission für den Bereich der Anbieter digitaler Dienste**[20]**)**. Das Gesetz regelt Meldepflichten und Sicherheitsanforderungen für Betreiber wesentlicher Dienste, Anbieter digitaler Dienste sowie Einrichtungen der öffentlichen Verwaltung. Dabei stellt das Betreiben wesentlicher Dienste lediglich einen Teil des Begriffs „kritischer Infrastruktur" dar, wie er in § 74 Abs. 1 Ziffer 11 des österreichischen Strafgesetzbuchs[21] verwendet wird, und ist nicht mit ihm gleichzusetzen.

Des Weiteren definiert der Regierungsbeschluss **„APCIP Masterplan 2014 (Österreichisches Programm zum Schutz kritischer Infrastrukturen)**"[22] kritische Infrastruktur als eine Infrastruktur, die eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen hat und deren Störung beziehungsweise Zerstörung schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl großer Teile der Bevölkerung oder das effektive Funktionieren von staatlichen Einrichtungen haben würde.

---

19 Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG), österreichisches Bundesgesetzblatt I Nr. 111/2018, abrufbar unter https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2018_I_111/BGBLA_2018_I_111.pdfsig.

20 Durchführungsverordnung (EU) 2018/151 der Kommission vom 30. Januar 2018 über Vorschriften für die Anwendung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates hinsichtlich der weiteren Festlegung der von Anbietern digitaler Dienste beim Risikomanagement in Bezug auf die Sicherheit von Netz- und Informationssystemen zu berücksichtigenden Elemente und der Parameter für die Feststellung erheblicher Auswirkungen eines Sicherheitsvorfalls, C/2018/0471, ABl. L 26, 31.1.2018, S. 48–51.

21 Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch – StGB), österreichisches Bundesgesetzblatt Nr. 60/1974, abrufbar unter: https://www.jusline.at/gesetz/stgb.

22 APCIP Masterplan - Österreichisches Programm zum Schutz kritischer Infrastrukturen, Bundeskanzleramt Österreich, abrufbar unter: https://www.bundeskanzleramt.gv.at/themen/sicherheitspolitik/schutz-kritischer-infrastrukturen.html.

Der Schwerpunkt des APCIP liegt in der Unterstützung der als kritische Infrastruktur identifizierten Unternehmen bei der Implementierung einer umfassenden Sicherheitsarchitektur. Dazu sind diese Unternehmen verpflichtet, eigene Schwachstellen zu kennen, eine Risikoanalyse durchzuführen und Maßnahmen zu ergreifen, um diese Risiken zu vermeiden, zu mindern oder auszuräumen. Darüber hinaus müssen sie in der Lage sein, durch ihr Krisenmanagement Störungen und Notfälle besser zu bewältigen sowie ein Sicherheitsmanagement einzurichten.

Die Bundesländer Österreichs entwickeln zudem eigene Programme zum Schutz ihrer regionalen kritischen Infrastrukturen und stehen diesbezüglich mit dem Bund in regelmäßigem Austausch. Die Bundesbehörden unterstützen die Länder bei der Umsetzung der Länderprogramme nach Maßgabe der zur Verfügung stehenden Ressourcen und der aktuellen Bedrohungslage.

Der Schutz kritischer Anlagen beziehungsweise Objekte ist auch im **Sicherheitspolizeigesetz (SPG)**[23] geregelt. Gemäß § 22 Abs. 1 Ziffer 6 SPG obliegt den Sicherheitsbehörden der besondere Schutz von Einrichtungen, Anlagen, Systemen oder Teilen davon, die eine wesentliche Bedeutung für die Aufrechterhaltung der öffentlichen Sicherheit, die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie, die Verhütung oder Bekämpfung von Katastrophen, den öffentlichen Gesundheitsdienst, die öffentliche Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern oder den öffentlichen Verkehr haben (kritische Infrastrukturen). Im APCIP ist diesbezüglich auch noch geregelt, dass abhängig von der aktuellen Bedrohungslage auch Kräfte des Österreichischen Bundesheeres im Assistenzeinsatz zur Unterstützung der Sicherheitsbehörden herangezogen werden können.

Die **CER-Richtlinie** soll bis 17. Oktober 2024 in nationales Recht umgesetzt werden.

Gemäß § 19 Abs. 1 NISG haben Betreiber wesentlicher Dienste einen **Sicherheitsvorfall**, der einen von ihnen bereitgestellten wesentlichen Dienst betrifft, unverzüglich an das für sie zuständige Computer-Notfallteam **zu melden**. Diese Meldung gilt jedoch nur für jene Betreiber wesentlicher Dienste, die nach § 16 Abs. 1 i. V. m. Abs. 4 NISG vom Bundeskanzler mittels Bescheid ermittelt wurden. Die Meldung ist dann unverzüglich an das Bundesministerium für Inneres weiterzuleiten.

Zuständig für die **Entgegennahme der Meldung** ist das sektorspezifische Computer-Notfallteam, falls ein solches eingerichtet ist und der betroffene Betreiber wesentlicher Dienste dieses unterstützt, andernfalls das nationale Computer-Notfallteam, sofern ein solches eingerichtet ist; ansonsten das sog. Government Computer Emergency Response Team für die öffentliche Verwaltung in Österreich (GovCERT).

In bestimmten Sektoren sind Meldewege über sektorspezifische Regulierungsbehörden in anderen Fachgesetzen geregelt. Für die Sektoren Bankwesen und Finanzinfrastrukturen ist dies gemäß § 20 Abs. 2 NISG die Finanzmarktaufsicht (FMA), wobei auf das **Zahlungsdienstegesetz 2018 (ZaDiG**

23 Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz - SPG), österreichisches Bundesgesetzblatt Nr. 566/1991, abrufbar unter: https://www.jusline.at/gesetz/spg.

2018)[24] verwiesen wird. Im Sektor digitale Infrastruktur ist dies gemäß § 10 Abs. 3 **Netz- und Informationssystemsicherheitsverordnung (NISV)**[25] die Rundfunk und Telekom Regulierungs-GmbH (RTR), wobei auf das **Telekommunikationsgesetz 2003 (TKG 2003)**[26] verwiesen wird.

Neben den Entitäten des NISG (Betreiber wesentlicher Dienste, Anbieter digitaler Dienste, Einrichtungen der öffentlichen Verwaltung) sind den „kritischen Infrastrukturen" auch Entitäten im Sinne des § 22 Abs. 1 Ziffer 6 SPG zuzuordnen. Die Zuständigkeit für den „Schutz kritischer Infrastrukturen" liegt hierbei bei der Direktion Staatsschutz und Nachrichtendienst des Bundesministeriums des Inneren (BMI). Entsprechende Hinweise zu Meldepflichten und -wegen sind in § 4 Zeile 1 des **Staatsschutz- und Nachrichtendienst-Gesetzes (SNG)**[27] zu finden.

Nach § 23 NISG können Risiken und Vorfälle von Betreibern wesentlicher Dienste oder Anbietern digitaler Dienste auch freiwillig an das BMI gemeldet werden. Nach Abs. 2 können Risiken, Vorfälle und Sicherheitsvorfälle auch von Einrichtungen, die nicht als Betreiber wesentlicher Dienste ermittelt wurden oder keine Anbieter digitaler Dienste oder Einrichtungen der öffentlichen Verwaltung sind, an das zuständige Computer-Notfallteam gemeldet werden, das die Meldungen zusammengefasst an den Bundesminister für Inneres weiterleitet.

Zudem ist im APCIP vorgesehen, dass im BMI die Kontakt- und Meldestelle KI und ein Frühwarnsystem, das strategische Unternehmen über aktuelle Risiken und Bedrohungen informieren soll, eingerichtet wird.

Unbeschadet sonstiger gesetzlicher Melde- und Informationsverpflichtungen melden die strategischen Unternehmen Vorfälle mit schwerwiegenden Auswirkungen auf ihre Versorgungsfunktion an die Melde- und Kontaktstelle KI. Welche Vorfälle gemeldet werden sollen, wird im APCIP unter Punkt 20 geregelt. Die Sicherheitsbehörden können mit den strategischen Unternehmen Kooperationsvereinbarungen schließen. Diese Vereinbarungen sind die Grundlage einer engen operativen Zusammenarbeit einschließlich des Austauschs von Informationen. Des Weiteren können die Aufgaben der Betreiber strategischer Unternehmen sowie die diesbezügliche Unterstützung durch staatliche Stellen genauer bestimmt werden.

---

24 Bundesgesetz über die Erbringung von Zahlungsdiensten 2018, österreichisches Bundesgesetzblatt I Nr. 17/2018, abrufbar unter: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010182.

25 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, österreichisches Bundesgesetzblatt II Nr. 215/2019, abrufbar unter: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010722.

26 Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird, österreichisches Bundesgesetzblatt I Nr. 70/2003, abrufbar unter: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20002849&FassungVom=2018-05-31.

27 Bundesgesetz über die Organisation, Aufgaben und Befugnisse des Verfassungsschutzes, österreichisches BGBl. I Nr. 5/2016, abrufbar unter: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009486.

6. Schweden

Das schwedische Recht kennt keine einheitliche Definition des Begriffs „kritische Infrastruktur“. Die schwedische Katastrophenschutzbehörde (Myndigheten för samhällsskydd och beredskap, MSB) bestimmt den in Schweden gebräuchlichen Terminus **„lebenswichtige gesellschaftliche Funktionen und kritische Infrastrukturen“** als „Funktionen, Dienste oder Infrastrukturen, die gesellschaftliche Funktionen aufrechterhalten oder sichern, die für die grundlegenden Bedürfnisse, Werte oder die Sicherheit der Gesellschaft notwendig sind“.[28] Der MSB ist auf nationaler Ebene für die Koordinierung von wichtigen gesellschaftlichen Funktionen und kritischen Infrastrukturen zuständig.[29]

Gemeinden, Regionen, Landratsämter sowie zentrale und nationale Regierungsbehörden müssen innerhalb ihres geografischen und funktionalen Zuständigkeitsbereichs ermitteln, was eine **wichtige gesellschaftliche Funktion** und was eine **kritische Infrastruktur** darstellt. Diese Pflicht gilt auch für private Unternehmen und andere Organisationen innerhalb ihrer Organisation. Der MSB hat sowohl einen Leitfaden zur Identifizierung von lebenswichtigen gesellschaftlichen Funktionen und kritischen Infrastrukturen[30] als auch eine detaillierte Liste zur Unterstützung bei der Identifizierung wichtiger gesellschaftlicher Funktionen und kritischer Infrastrukturen im öffentlichen oder privaten Sektor[31] erstellt.

Am 1. August 2018 trat das **Gesetz über die Sicherheit von Informationen für lebenswichtige gesellschaftliche und digitale Dienste**[32] in Kraft. Mit dem Gesetz wurden die Bestimmungen der **NIS-Richtlinie** in schwedisches Recht umgesetzt. Abschnitt 1 statuiert, dass ein hohes Maß an Sicherheit in Netzwerken und Informationssystemen lebenswichtiger gesellschaftlicher Dienste in den Bereichen Energie, Verkehr, Bankwesen, Finanzmarktinfrastruktur, Gesundheitswesen, Trinkwasserversorgung und -verteilung und digitaler Infrastruktur sowie im Bereich digitaler Dienste erreicht werden muss.

Ein lebenswichtiger gesellschaftlicher Dienst wird als „ein Dienst, der für die Aufrechterhaltung lebenswichtiger gesellschaftlicher oder wirtschaftlicher Funktionen wichtig ist“, definiert (Abschnitt 2, Abs. 3).

---

28 Uppdaterad definition samhällsviktig verksamhet, Arbeitsübersetzung: Aktualisierte Definition von gesellschaftlich wichtigen Aktivitäten, MSB, MSB-2020-11275 vom 27. Oktober 2020, auf Schwedisch abrufbar unter: uppdaterad-definition-samhallsviktig-verksamhet.pdf (msb.se).

29 Introduktion till samhällsviktig verksamhet, MSB, Powerpoint-Präsentation von Oktober 2021, auf Schwedisch abrufbar unter: https://www.msb.se/sv/publikationer/introduktion-till-samhallsviktig-verksamhet/.

30 Identifiering av samhällsviktig verksamhet: metod, MSB, Stand vom Oktober 2021, abrufbar auf Schwedisch unter: https://rib.msb.se/filer/pdf/29799.pdf.

31 Identifiering av samhällsviktig verksamhet: metod, MSB, Stand vom Oktober 2021, abrufbar auf Schwedisch unter: https://rib.msb.se/filer/pdf/29799.pdf.

32 Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster vom 27. Juni 2018, auf Schwedisch abrufbar unter: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20181174-om-informationssakerhet-for_sfs-2018-1174.

In den Abschnitten 11-14 werden die **Pflichten für Betreiber lebenswichtiger gesellschaftlicher Dienste** geregelt. Die Betreiber müssen **systematische und risikobasierte Überprüfungen der Informationssicherheit** in Bezug auf die von ihnen genutzten Netze und Informationssysteme durchführen sowie **geeignete und verhältnismäßige technische oder organisatorische Maßnahmen** ergreifen, um Risiken zu bewältigen, die die Sicherheit dieser Systeme bedrohen. Außerdem müssen die Betreiber bei der Auswahl von Sicherheitsmaßnahmen **Risikoanalysen** durchführen und geeignete Maßnahmen ergreifen, um Vorfälle, die sich auf Netze und Informationssysteme auswirken, zu verhindern oder deren Auswirkungen zu minimieren.

Die Vorschriften des MSB zur Meldung von Vorfällen für Betreiber lebenswichtiger gesellschaftlicher Dienste[33] definieren die **Voraussetzungen**, um als **Betreiber eines lebenswichtigen gesellschaftlichen Dienstes** im Sinne der gesetzlichen Regelungen zu gelten.

Die Umsetzung der **CER-Richtlinie** sowie der **EU-Richtlinie 2022/2555 über Maßnahmen für ein hohes gemeinsames Niveau der Cybersicherheit in der Union (NIS-2-Richtlinie)**[34] ist bisher nicht erfolgt. Die schwedische Regierung wird dazu in Kürze eine Untersuchung mit dem Ziel der Umsetzung der Bestimmungen der Richtlinien in die schwedische Gesetzgebung einleiten.[35]

Gemäß § 18 des Gesetzes über die Informationssicherheit lebenswichtiger gesellschaftlicher und digitaler Dienste[36] müssen Betreiber lebenswichtiger gesellschaftlicher Dienste **Vorfälle**, die erhebliche Auswirkungen auf die Kontinuität des Dienstes haben, **unverzüglich melden**. Die Meldung hat über die Kontaktkanäle, die in Kapitel 2, Abschnitt 2 der MSB-Vorschriften zur Meldung von Vorfällen bei Betreibern lebenswichtiger gesellschaftlicher Dienste beschrieben sind, an das MSB zu erfolgen. Betreiber lebenswichtiger gesellschaftlicher Dienstleistungen müssen entweder ein spezielles Tool für die Meldung von Vorfällen (IRON) verwenden oder alternativ ein Formular einreichen, das auf der MSB-Website verfügbar ist.[37]

* * *

33 Myndigheten för samhällsskydd och beredskaps; föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster, Arbeitsübersetzung: Das schwedische Amt für Katastrophenschutz; Vorschriften über die Benachrichtigung und Identifizierung von Erbringern wesentlicher Dienstleistungen, vom 23. Oktober 2018, auf Schwedisch abrufbar unter: https://www.msb.se/siteassets/dokument/regler/rs/0264c176-6b31-43c6-9fd8-807102df3844.pdf.

34 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), PE/32/2022/REV/2, ABl. L 333 vom 27. Dezember 2022, S. 80 - 152.

35 EU och arbetet med att stärka motståndskraften i samhällsviktig verksamhet, MSB, Stand vom 24. Januar 2023, auf Schwedisch abrufbar unter: https://www.msb.se/sv/om-msb/internationella-samarbeten/eu-samarbete/eu-och-skydd-av-samhallsviktig-verksamhet/.

36 Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster vom 27. Juni 2018, auf Schwedisch abrufbar unter: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20181174-om-informationssakerhet-for_sfs-2018-1174.

37 Incidentrapportering för leverantörer av samhällsviktiga tjänster, MSB, Stand vom 29. September 2022, auf Schwedisch abrufbar unter: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/incidentrapportering-for-nis-leverantorer/incidentrapportering-for-leverantorer-av-samhallsviktiga-tjanster/.