2. Cyber-Security im Stromsektor

Arne Schönbohm, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Bonn

Die **Stromversorgung** in Deutschland und Europa funktioniert gut und ist sicher. Doch je mehr eine Gesellschaft von einer funktionierenden Technik abhängig ist, desto verletzlicher wird sie auch. Und entsprechend dramatisch sind die Folgen, wenn es beispielweise zu einem flächendeckenden Stromausfall käme. Denn aufgrund der komplexen Abhängigkeiten anderer Sektoren der Kritischen Infrastrukturen von der Energieversorgung kann der Stromausfall eine *Kettenreaktion* auslösen, die zum Ausfall der Versorgung durch andere Kritische Dienstleistungen führen kann. Der Schutz vor einem derartigen Szenario und die entsprechende Vorsorge sind eine staatliche, aber auch gesellschaftliche Aufgabe. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) spielt dabei eine wichtige Rolle.

2.1 Risikoarten und Bedrohungsszenarien

Ein Blackout im Stromsektor kann ganz unterschiedliche **Ursachen** haben: *Extremwetter*, *technisches Versagen* oder *menschliche Fehler*, *Komplexitätsüberlastung*, *Sonnenstürme* oder *Terror-Anschläge*. Aber auch *Cyber-Angriffe* sorgen für ein erhöhtes Gefährdungspotenzial. Auf einige der dieser Bedrohungen der Stromversorgung soll im Folgenden eingegangen werden.

2.1.1 Naturkatastrophen

Schwere *Gewitter*, *Überschwemmungen* und heftige *Stürme* können die Stromnetze beschädigen und Defekte auslösen, ebenso wie *gefrierender Regen*, große *Schneefälle*, *extreme Kälte* oder *Hitze*. Gleiches gilt für *Lawinenabgänge*, *Erdrutsche* oder *Felsstürze*.

Beispiel: Münsterland und Ruhrgebiet

Am 25. November 2005 verursachte ein Sturmtief ein Schneechaos. Als Folge dessen waren im Münsterland und in Teilen des Ruhrgebiets nach Medienberichten viele Orte von der Stromversorgung abgeschnitten. Mehr als 250.000 Menschen waren von diesem Blackout betroffen. Viele von ihnen hatten bis zu drei Tage keine Stromversorgung, einzelne Höfe waren bis zu fünf Tage ohne Strom. Auch der Straßen-, Schienen- und Flugverkehr brach in einigen Regionen des Landes komplett zusammen.

2.1.2 Atmosphärische Störungen

Auch durch Plasmaeruptionen entstehende Sonnenwinde stellen eine Gefahr dar. Sie können das Erdmagnetfeld deformieren und einen **geomagnetischen Sturm** auslösen. Die heftigen Schwankungen des Erdmagnetfelds induzieren Ströme in ungeschützten elektrischen Leitungen. Das kann Satelliten, Transformatoren von Hochspannungsleitungen und elektronische Geräte zerstören. Ein starker Sonnenwind würde enorme Schäden anrichten und könnte die Stromversorgung großflächig über Monate lahmlegen.

2.1.3 Technisches Versagen und menschliche Fehler

Der gestiegene Stromverbrauch und die Liberalisierung des Strommarkts haben die Belastung der Netze erheblich verschärft. Das Stromnetz arbeitet häufig an seinen **Leistungsgrenzen**. Auch die Stromüberproduktion, ausgelöst auch durch Einspeisetarife für Strom aus erneuerbaren Energien, kann ein Problem darstellen. Zudem ist Stromerzeugung aus erneuerbaren Energien oftmals erheblichen Schwankungen unterworfen. Wenn aber Stromproduktion und -verbrauch nicht übereinstimmen und diese Lücke nicht geschlossen wird, kann es zu einem Blackout kommen.

Beispiel: Türkei

Am 31. März 2015 fiel in 80 von 81 türkischen Provinzen der Strom aus, fast 80 Millionen Menschen waren betroffen. Öffentliche Verkehrsmittel standen still, Ampeln fielen aus, ein unglaubliches Verkehrschaos war die Folge. Der wirtschaftliche Gesamtschaden belief sich auf rund 700 Millionen Euro. Ursache für den Blackout waren nach Medienberichten vermutlich plötzliche, unvorhergesehene Schwankungen im türkischen Stromnetz.

Auch Mitarbeiter, die in Kraftwerken und Übertragungsleitstellen die Systeme nutzen und bedienen, können ein Risiko darstellen, wenn sie nicht in der Lage sind, ein von ihnen oder von der Technik ausgehendes Problem rechtzeitig zu lösen. Manche Störungen sind sowohl auf menschliche Fehler als auch auf technische Defekte zurückzuführen (mangelnde Wartung, mangelhafte Qualitätskontrolle, Konstruktionsfehler, ausbleibende Vor- und Nachsorge).

Beispiel: Europa

Ein Abstimmungsfehler führte am 4. November 2006 um 22:10 Uhr zu einem großräumigen Stromausfall in Europa. Auslöser war nach Analyse der Bundesnetzagentur eine mangelhaft geplante und nicht ausreichend kommunizierte Abschaltung von Hochspannungsleitungen in Niedersachsen für das Auslaufen eines Kreuzfahrtschiffs. In einer Kettenreaktion gingen daraufhin gleich mehrere Leitungen vom Netz. Etwa 15 Millionen Menschen waren in Deutschland, Frankreich, Belgien, Italien, Österreich und Spanien bis zu zwei Stunden ohne elektrische Energie.

2.1.4 Cyber-Angriffe

Bei **Cyber-Angriffen** muss zwischen verschiedenen *privaten* und *staatlich* gesteuerten Angreifergruppen, Angriffsformen und -methoden unterschieden werden. Sie unterscheiden sich allerdings weniger in den Vorgehensweisen als in den *Zielen*. Dies kann in diesem Zusammenhang nur ansatzweise dargestellt werden.

Zu *Cyber-Crime im engeren Sinn* gehören Computerbetrug und Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten (Identitätsdiebstahl), die Fälschung von Daten oder Datenveränderung, das Ausspähen und Abfangen von Daten und die Täuschung im Rechtsverkehr bei der Datenverarbeitung. *Im weiteren Sinne* zählen aber auch alle Delikte dazu, die über das Internet erfolgen. Dazu gehören: Phishing, Straftaten mit Distributed Denial of Service-Attacken, das sind Überlast-Angriffe auf IT-Infrastrukturen, digitale Erpressung sowie die Herstellung und Verbreitung von Hacker-Tools für illegale Zwecke.

Doch Angriffe auf die Cyber-Sicherheitsarchitektur oder Infrastruktur eines Staates sowie auf die IT-Systeme der Wirtschaft und Verwaltung erfolgen nicht nur aus kriminellen Motiven. Neben Cyber-Crime muss eine umfassend definierte Cyber-Abwehr auch *Cyber-Spionage*, *Cyber-Ausspähung* und *Cyber-Sabotage* im Auge behalten.

Einheitliche Definitionen dieser vier Begriffe gibt es bisher allerdings nicht. Grundsätzlich aber kann man so differenzieren:

- **Cyber-Crime** sind Verstöße gegen Eigentumsrechte nichtstaatlicher Akteure (z. B. Phishing, Identitätsdiebstahl).
- **Cyber-Spionage** umfasst Einbrüche in die IT-Infrastruktur staatlicher oder nichtstaatlicher Organisationen durch fremde Regierungsorganisationen oder private Angreifer.
- Unter **Cyber-Ausspähung** werden Versuche eines Staates verstanden, einen anderen Staat mit Hilfe des Internets nachhaltig zu schädigen.
- Und unter **Cyber-Sabotage** ist der Versuch von staatlichen oder nichtstaatlichen Einheiten zu verstehen, mit Hilfe von Internet-Technologien Angriffe auf Computersysteme zu verüben, um so Versorgungsleistungen zu stören (z. B. Energieversorgung) oder hohe wirtschaftliche Schäden zu verursachen.

Immer wieder kam es in den vergangenen Jahren in Europa zu aufsehenerregenden Cyber-Attacken auf Energieversorger.

2.1.4.1 Ransomware

Nach wie vor geht die größte Gefahr im Cyber-Raum von Schadsoftware aus. **Ransomware**-Kampagnen, besonders die gegen zahlungskräftige Unternehmen, haben sich weiterentwickelt: Sie sind mittlerweile fortschrittlich, langanhaltend und erreichen eine hohe *Komplexität*. Die Angreifer werden dabei immer *professioneller* und attackieren in letzter Zeit finanzstarke Opfer. Mittlerweile sperren sie oftmals die Daten nicht mehr nur, sondern drohen damit, sie an Interessenten zu *verkaufen* oder zu veröffentlichen. Das steigert die Bereitschaft der betroffenen Institutionen, Lösegeld zu zahlen. Dessen Höhe hängt dann von der Größe und Bedeutung des Opfers und dem vermuteten Wert der Daten ab.

Die *Zahl der Schadprogramme* ist inzwischen gigantisch. Allein im Zeitraum von Juni 2019 bis Juni 2020 kamen 117,4 Millionen neue Varianten hinzu. Insgesamt liegt die Zahl inzwischen bei mehr als einer Milliarde. Dominiert wurde die Lage dabei erneut durch das im Frühjahr 2021 schließlich zerschlagene Schadprogramm *Emotet*.

Schadprogramme gelangen in der Regel über *Anhänge* oder *Links* in E-Mails auf einen Computer. Wenn Nutzer auf einen solchen Anhang oder auf einen Link klicken, der auf eine manipulierte Webseite führt, wird ein Schadprogramm installiert. Häufig werden diese Attacken automatisiert gestartet. Die Täter suchen Sicherheits-Schwachstellen und schicken *Phishing-Mails*. Dann dringen sie in das IT-System ein und sperren Daten oder Zugänge zum ganzen System. Dadurch werden alle Daten verschlüsselt – und erst nach der Zahlung eines Lösegelds wieder freigegeben.

Beispiel: Enel Group

Der größte Energieversorger Europas, Enel Group, war laut Medienberichten im Juni 2020 von einem Ransomware-Angriff betroffen, der sich auf sein internes Netzwerk auswirkte. Der Vorfall wird auf die Ransomware-Betreiber von EKANS (SNAKE) zurückgeführt. Die Enel Group bestätigte, dass ihr internes IT-Netzwerk nach einem Ransomware-Angriff unterbrochen wurde. Dieser konnte jedoch von ihrem Antivirenprogramm abgefangen werden, bevor sich die Malware verbreiten konnte.

2.1.4.2 Sabotage

Auch die Bedrohung durch APT-Gruppierungen ist weiterhin sehr real. Unter **Advanced Persistent Threats (APT)** werden allgemein staatliche oder über Umwege von Staaten finanzierte Angreifergruppierungen verstanden. Sie unterscheiden sich von anderen Bedrohungen der IT-Sicherheit durch die *Motivation* und die *Vorgehensweise* der Angreifer. Während die meisten Schadprogramme in der Regel von finanziell motivierten Angreifern mas-

senhaft und ungezielt verteilt werden, sind APTs oft langfristig und mit großem Aufwand geplante Angriffe auf einzeln ausgewählte, herausgehobene Ziele. Sie dienen normalerweise der *Beschaffung von Informationen* über das Ziel und ggf. der *Sabotage*. Die beobachteten Kampagnen beinhalteten das massenhafte Abgreifen von Zugangsdaten der Betreiber *Kritischer Infrastrukturen*, aber auch von deren *Dienstleistern* und *Zulieferern*. Dies betraf besonders auch den Energiesektor.

Beispiel: Ukraine

Am 23. Dezember 2015 waren in der Ukraine hunderttausende Menschen in 103 Städten des Landes von einem mehrstündigen Ausfall der Stromversorgung betroffen. 27 Umspannwerke fielen aus. Im Dezember 2016 gab es einen erneuten Stromausfall in Kiew. Zwischen 100.000 und 200.000 Einwohner wurden für über eine Stunde nicht mehr mit Strom versorgt. Laut Erklärung des staatlichen Energieversorgers Ukrenergo handelte es sich in beiden Fällen um gezielte Cyber-Angriffe. Der Ausfall 2015 basiert auf dem Einsatz von Black Energy, der Ausfall 2016 nutzte die Malware Industroyer/Crashoverride. Auch 2017 wurden Kritische Infrastrukturen in der Ukraine angegriffen. Die nun eingesetzte Schadsoftware ExPetr gab vor, Daten zu verschlüsseln und diese gegen Zahlung eines Lösegelds wieder zu entschlüsseln. Sowohl technische als auch strategische Merkmale unterschieden diese Schadsoftware jedoch von anderen Ransomware-Familien. Bei der Suche nach Wegen, die Verschlüsselung auch ohne Lösegeldzahlung aufheben zu können, erkannten mehrere Sicherheitsforscher, dass die Ransomware-Funktionalität in bestimmten Teilen nicht vollständig oder grob fehlerhaft implementiert worden war. Dies könnte ein Hinweis darauf sein, dass ExPetr eher als Sabotage-Werkzeug mit strategischer Absicht in der Ukraine eingesetzt werden sollte.

2.2 Sicherheitsrelevanz des Stromsektors

Deutschland liegt inmitten eines vernetzten europäischen Stromsystems und ist aufgrund seiner zentralen geografischen Lage in Europa ein wichtiger Partner im europäischen Strommarkt und eine Drehscheibe der europäischen Stromflüsse.

Kritische Infrastrukturen

Die Energieversorgung ist eine kritische Dienstleistung der **Kritischen Infrastrukturen (KRITIS)**. Dies sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei denen nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden, wenn sie ausfielen oder beeinträchtigt wären. Wegen ihrer besonderen Bedeutung für das Funktionieren des Gemeinwesens sind im Sektor Energie *kritische*

Dienstleistungen im Sinne des § 10 Absatz 1 Satz 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik–BSI-Gesetz:

- die Versorgung der Allgemeinheit mit Elektrizität (*Stromversorgung*);
- die Versorgung der Allgemeinheit mit Gas (*Gasversorgung*);
- die Versorgung der Allgemeinheit mit Kraftstoff und Heizöl (*Kraftstoff- und Heizölversorgung*);
- die Versorgung der Allgemeinheit mit Fernwärme (*Fernwärmeversorgung*).

Die *Stromversorgung* und *Gasversorgung* werden in den Bereichen Erzeugung, Übertragung und Verteilung von Strom sowie Förderung, Transport und Verteilung von Gas, die Fernwärmeversorgung in den Bereichen Erzeugung und Verteilung von Fernwärme erbracht. Die *Kraftstoff- und Heizölversorgung* wird in den Bereichen Rohölförderung und Produktherstellung, Öltransport sowie Kraftstoff- und Heizölverteilung erbracht.

Damit zählen im Sektor Energie alle Anlagen oder Anlagenteile zu den Kritischen Infrastrukturen, die nach Maßgabe der jeweils zutreffenden und im folgenden aufgelisteten Gesetze und Verordnungen den folgenden Kategorien zuzuordnen sind und bestimmte Schwellenwerte überschreiten (Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz [BSI-Kritisverordnung – BSI-KritisV]):

- Übertragungsnetze (§ 3 Nr. 32 Energiewirtschaftsgesetz),
- Verteilernetze (§ 3 Nr. 37 Energiewirtschaftsgesetz),
- Fernleitungsnetze (§ 3 Nr. 19 Energiewirtschaftsgesetz),
- Gasverteilernetze (§ 3 Nr. 37 Energiewirtschaftsgesetz),
- Fernwärmenetze,
- Mineralölfernleitungen,
- Erzeugungsanlagen (§ 3 Nr. 18c Energiewirtschaftsgesetzes),
- Erzeugungsanlagen mit Wärmeauskopplung (§ 2 Nr. 14 Kraft-Wärme-Kopplungsgesetz),
- dezentrale Energieerzeugungsanlagen (§ 3 Nr. 11 des Energiewirtschaftsgesetz),
- Gasförderanlagen,
- Ölförderanlagen,
- Anlagen zur Erzeugung von elektrischer Energie und Nutzwärme (§ 2 Nr. 14 des Kraft-Wärme-Kopplungsgesetzes,
- Raffinerien (Gesetz über die Umweltverträglichkeitsprüfung, Anlage 1, Nr. 4.3),

- Heizwerke,
- Heizkraftwerke,
- Speicheranlagen,
- Gasspeicher (§ 3 Nr. 31 Energiewirtschaftsgesetz),
- Öl- und Produktenlager,
- zentrale Anlagen oder IT-Systeme für den Stromhandel, die den physischen, kurzfristigen Spothandel mit Energie für das deutsche Marktgebiet betreffen,
- Anlagen oder IT-Systeme zur Steuerung/Bündelung elektrischer Leistung (§ 3 Nr. 17 Erneuerbare-Energien-Gesetz),
- Anlagen zur zentralen standortübergreifenden Steuerung anderer Anlagen,
- Anlagen oder IT-Systeme von Aggregatoren zum Vertrieb von Kraftstoff und Heizöl,
- Anlagen oder IT-Systeme zur Verbindung voneinander unabhängiger Tankstellen, die der zentralen Versorgung der Tankstellen eines Tankstellennetzes mit Kraftstoff dienen, und
- Messstellen (§ 2 Nr. 11 Messstellenbetriebsgesetz).

2.3 Akteure in der Stromversorgung und deren Aufgaben

Seit der Liberalisierung des Energiemarktes in Deutschland 1998 herrscht ein gesetzlich festgelegter wettbewerblicher Rahmen, in dem die verschiedenen Akteure ihre Rollen wahrnehmen. Nach Angaben des Statistischen Bundesamtes gibt es in Deutschland **vier Übertragungsnetzbetreiber** und **874 Verteilernetzbetreiber**, die für Stromnetze im Nieder-, Mittelspannungsbereich und abschnittsweise auch im Hoch- und Höchstspannungsbereich zuständig sind. Der Bundesverband der Energie- und Wasserwirtschaft (BDEW) zählte im deutschen Energiemarkt 2019 rund *1300 Energielieferanten* und insgesamt *2200 Unternehmen*, die sich um die *Energieversorgung* kümmern.

2.3.1 Übertragungs- und Verteilnetzbetreiber

Bei den **Netzbetreibern** wird zwischen *Übertragungsnetzbetreibern* und *Verteilnetzbetreibern* unterschieden. Die Übertragungsnetzbetreiber sind für die *überregionale* Verteilung des Stroms, die Verteilnetzbetreiber für die *regionale* Verteilung verantwortlich. Als Übertragungs- und Verteilnetzbetreiber können natürliche oder juristische Personen oder rechtlich unselbständige Organisationseinheiten eines Energieversorgungsunternehmens fungieren

(§ 3 Nr. 2 und Nr. 10 EnwG). Sie sind für die Infrastruktur, die Transportwege, den Betrieb, die Wartung sowie erforderlichenfalls den Ausbau des Übertragungsnetzes und der Verteilnetze in einem bestimmten Gebiet und gegebenenfalls der Verbindungsleitungen zu anderen Netzen zuständig. Zur Netzinfrastruktur gehört auch die Infrastruktur aus Stromzählern.

Zudem verfügt das Stromnetz über verschiedene *Spannungsebenen*. Der Netzbetreiber stellt sicher, dass der Strom vom Hochspannungsnetz über das Mittelspannungsnetz in das Niederspannungsnetz der angeschlossenen Haushalte übergeben wird. Er kann dabei für eine oder mehrere Spannungsebenen zuständig sein.

Nach den Regeln der Entflechtung darf ein Netzbetreiber nicht gleichzeitig der Grundversorger sein. Besonders dann, wenn es sich um Stadtwerke handelt, werden Netzbetrieb und Belieferung daher häufig von unterschiedlichen Tochtergesellschaften wahrgenommen, um die sogenannten *Unbundling-Bestimmungen* zu erfüllen.

2.3.2 Stromerzeuger

Stromerzeuger sind dafür zuständig, elektrische Energie mithilfe technischer Einrichtungen zu produzieren. Große Stromerzeuger betreiben deshalb eigene Kraftwerke. Neben den **„Big Four“** (RWE, E.ON, Vattenfall und EnBW) gibt es in Deutschland eine Vielzahl mittelgroßer Produzenten, vor allem lokale oder regionale Stadtwerke. Die Stromerzeuger gewinnen elektrische Energie aus Braun- und Steinkohlekraftwerken, aus Mineralöl-, Erdgas-, Atomkraft- und Wasserkraftwerken. Aufgrund des Ausstiegsbeschlusses aus der Kernenergie durch das Atomgesetz (AtG) von 2002 geht der Anteil der Strommenge durch Kernenergie deutlich zurück. Seit Einführung des Erneuerbare-Energien-Gesetzes (EEG) im Jahr 2000 nimmt hingegen der Anteil erneuerbarer Energien deutlich zu. Hier ist zudem ein neuer Erzeugertyp hinzugekommen: Betreiber von Biomasse-, Windkraft- oder Photovoltaikanlagen. So kann heute auch eine Privatperson Stromerzeuger sein, wenn z. B. eine Photovoltaikanlage auf dem Dach installiert ist.

2.3.3 Stromversorger

Der **Stromversorger** ist eine Art Mittler zwischen Endverbraucher, Stromproduzent und Stromnetzbetreiber. Er beschafft die benötigten Strommengen und meldet gegenüber dem Netzbetreiber täglich den prognostizierten Stromverbrauch an. Er sorgt außerdem für einen reibungslosen Ablauf aller Prozesse im Hintergrund und übernimmt in der Regel die Abrechnung aller

Abgaben und Umlagen, die zusätzlich zu den Energiekosten anfallen. Häufig zählen Netzbetreiber und Stromversorger zu ein- und derselben Unternehmensgruppe. Allerdings fordert das Energiewirtschaftsgesetz eine deutliche Trennung zwischen diesen beiden Aufgabengebieten.

2.3.4 Stromhändler

Die Beschaffung der Strommengen erfolgt über organisierte Handelsplätze wie die Strombörse in Leipzig oder durch direkte Handelsgeschäfte zwischen Geschäftspartnern. **Stromhändler** schließen Verträge mit dem Erzeuger ab oder kaufen den Strom an der Strombörse ein. Dabei können unterschiedliche Produkte gekauft werden. Neben dem Einkauf von Strom beteiligen sich die Stromhändler gleichzeitig am Verkauf, zum Beispiel am Großhandelsmarkt sowie an der Strombörse. Stromhändler geben den Strom zur Einspeisung an die Netzbetreiber weiter.

2.4 Rechtliche Grundlagen

Die Bundesregierung hat bereits 2011 mit der *Cyber-Sicherheitsstrategie* für Deutschland den Grundstein für mehr Sicherheit im Cyber-Raum gelegt. Die dort verankerten strategischen Ziele wurden mit der im August 2014 beschlossenen *Digitalen Agenda* der Bundesregierung weiterverfolgt. Sie gibt die Leitlinien der Digitalpolitik vor und bündelt Maßnahmen auf zentralen Handlungsfeldern, um den digitalen Wandel zu begleiten und mitzugestalten. Ergänzend zur Digitalen Agenda hat das Bundeswirtschaftsministerium auf der CeBIT 2016 die *Digitale Strategie 2025* vorgestellt.

Das **IT-Sicherheitsgesetz**, das im Juli 2015 in Kraft trat, und die im August 2016 in Kraft getretene **NIS-Richtlinie** sind erste konkrete Ergebnisse der digitalen Agenda. Das IT-Sicherheitsgesetz wurde grundlegend überarbeitet. Das im Mai 2021 verabschiedete sogenannte *IT-SiG 2.0* erweitert den Ordnungsrahmen und enthält Maßnahmen zum Schutz der Gesellschaft, zur Stärkung des Staates und zum Schutz der öffentlichen Informationstechnik sowie für eine resiliente Wirtschaft.

Für den Fall der unmittelbaren Gefährdung oder Störung der Energieversorgung hat der Deutsche Bundestag zudem eine Reihe weiterer Gesetze beschlossen, auf die in diesem Zusammenhang nicht im Einzelnen eingegangen werden kann. Dazu zählen:

- das *Energiesicherungsgesetz (EnSiG)* und die hierauf beruhende Verordnung zur Sicherung der Elektrizitätsversorgung in einer Versorgungskrise (EltSV),

- das *Erdölbevorratungsgesetz (ErdölBevG*) und
- die *Verordnung über die Sicherstellung der Gasversorgung (GasLastV).*

2.4.1 IT-Sicherheitsgesetz

Das **IT-Sicherheitsgesetz** gibt den Rechtsrahmen für die Zusammenarbeit von Staat und Unternehmen für mehr Cyber-Sicherheit in den Kritischen Infrastrukturen (KRITIS) vor. Mit *verbindlichen Mindestanforderungen* nach dem „Stand der Technik" an die IT-Sicherheit, flankiert durch eine *Verpflichtung zur Meldung* erheblicher IT-Sicherheitsvorfälle, will das Gesetz den KRITIS-Schutz verbessern und die Netzsicherheit erhöhen. In diesem Zuge erhielt das BSI neue Aufgaben und Befugnisse:

- KRITIS-Betreiber müssen die Einhaltung von IT-Sicherheit nach dem Stand der Technik regelmäßig gegenüber dem BSI *nachweisen* (§ 8a des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)). Sofern Sicherheitsmängel aufgedeckt werden, darf das BSI im Einvernehmen mit den Aufsichtsbehörden deren Beseitigung anordnen.
- Das BSI wird nach § 8b BSIG die zentrale Meldestelle für die IT-Sicherheit Kritischer Infrastrukturen. Diese müssen dem BSI erhebliche Störungen ihrer IT *melden*, sofern diese Auswirkungen auf die Verfügbarkeit kritischer Dienstleistungen haben können.
- Umgekehrt hat das BSI sämtliche für Abwehr von Angriffen auf die IT-Sicherheit Kritischer Infrastrukturen relevanten *Informationen* zu sammeln, zu bewerten und an die Betreiber sowie die zuständigen (Aufsichts-)Behörden weiterzuleiten.
- Sofern bei einem KRITIS-Betreiber meldepflichtige Störungen der IT auftreten, darf das BSI erforderlichenfalls auch die *Hersteller* der entsprechenden IT-Produkte und -systeme gemäß § 8b BSIG zur *Mitwirkung* bei der Beseitigung der Störung verpflichten.
- Dem BSI wird die Befugnis eingeräumt, zur Wahrnehmung seiner Aufgaben IT-*Produkte* auf ihre Sicherheit hin zu *untersuchen*.

Hinweis

Der § 8a BSIG hat in einigen KRITIS-Bereichen keine Gültigkeit, weil hier spezialgesetzliche Regelungen gelten. Diese gelten insbesondere für die Bereiche der Energienetze und Energieanlagen. Für die genannten Bereiche hat die Bundesnetzagentur (BNetzA) Kataloge mit Sicherheitsanforderungen erstellt.

Im KRITIS-Bereich kooperiert das BSI über seine Aufgaben aus dem IT-Sicherheitsgesetz hinaus im Rahmen der öffentlich-privaten Partnerschaft **UP KRITIS** mit den KRITIS-Betreibern, deren Verbänden und den zuständigen staatlichen Stellen. Das zentrale Ziel des UP KRITIS ist es, die Versorgung mit Dienstleistungen Kritischer Infrastrukturen möglichst uneingeschränkt aufrechtzuerhalten.

Außerhalb des KRITIS-Bereichs werden die Aufgaben und Befugnisse des BSI durch das bereits 2009 verabschiedete BSI-Gesetz geregelt. Dies gilt im Energiesektor für alle Betreiber von Anlagen und IT-Systemen, die nicht unter die Kategorien und Schwellenwerte der BSI-KritisV fallen. Hiernach kann das BSI:

- als zentrale Meldestelle für IT-Sicherheit Informationen über Sicherheitslücken und neue Angriffsmuster auf die Sicherheit der Informationstechnik sammeln und auswerten (§ 4 BSIG). Hierdurch können ein verlässliches *Lagebild* erstellt, Angriffe frühzeitig erkannt und Gegenmaßnahmen ergriffen werden,
- nach § 7 BSIG Informationen und *Warnungen* vor Sicherheitslücken in informationstechnischen Produkten und Diensten sowie vor Schadprogrammen an die betroffenen Stellen und danach an die Öffentlichkeit weitergeben.

2.4.2 Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS)

Die Europäische Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) trat im August 2016 in Kraft. Sie definiert Maßnahmen, die ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der europäischen Union gewährleisten sollen. Zugleich schafft sie einen einheitlichen *Rechtsrahmen* für den EU-weiten Aufbau nationaler Kapazitäten für die Cyber-Sicherheit, für eine stärkere Zusammenarbeit der EU-Mitgliedstaaten und legt *Meldepflichten* für Kritische Infrastrukturen sowie für bestimmte Anbieter digitaler Dienste wie Cloud-Services und Online-Marktplätze fest. Mit dem am 29.06.2017 verkündeten *Umsetzungsgesetz* wurde die Richtlinie von Deutschland in nationales Recht umgesetzt. Dabei wurden die Aufsichts- und Durchsetzungsbefugnisse des BSI gegenüber KRITIS-Betreibern erweitert.

2.4.3 Energiewirtschaftsgesetz (EnWG)

Nach § 11 EnWG sind die Betreiber von Energieversorgungsnetzen verpflichtet, ein sicheres, zuverlässiges und **leistungsfähiges Energieversor-**

gungsnetz diskriminierungsfrei zu betreiben, zu warten und bedarfsgerecht zu verbessern, zu verstärken und auszubauen, soweit es wirtschaftlich zumutbar ist. Dies umfasst insbesondere auch einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und IT-Systeme, die für einen sicheren Netzbetrieb notwendig sind.

Den IT-Sicherheitspflichten aus dem EnWG unterliegen gemäß § 11 Abs. 1a und 1b EnWG Betreiber von *Energieversorgungsnetzen* im Sinne der § 3 Nr. 4, 16 EnWG sowie Betreiber von *Energieanlagen*, die mittels BSI-Kritis-Verordnung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind. Diese unterliegen als KRITIS-Betreiber grundsätzlich auch den Pflichten des BSIG, die jedoch angesichts der bereichsspezifischen Regelungen des EnWG zurücktreten.

Um die Sicherheitspflichten konkret festzulegen, erstellt die Bundesnetzagentur im Benehmen mit dem BSI einen *Katalog von Sicherheitsanforderungen* (siehe 2.6.2.1). Dabei wird zwischen den Pflichten der Betreiber von Energieversorgungsnetzen und von Energieanlagen differenziert. Im August 2015 wurde der „*IT-Sicherheitskatalog für Betreiber von Strom- und Gasnetzen*“, im Dezember 2018 der „*IT-Sicherheitskatalog für Betreiber von Energieanlagen*“ veröffentlicht. Er gilt für alle Energieanlagen, die nach der BSI-Kritis-Verordnung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind.

2.4.4 EU-Richtlinien zum Stromsektor

Auch auf europäischer Ebene gibt es eine Reihe von Verordnungen, die die Sicherheit der Stromversorgung thematisieren. Von besonderer Bedeutung ist dabei das im Juni 2019 verabschiedete sogenannte „**vierte Energiepaket**“. Es besteht aus der *Richtlinie (EU) 2019/944* über den Elektrizitätsbinnenmarkt und drei Verordnungen, nämlich der Verordnung über den Elektrizitätsbinnenmarkt (*Verordnung [EU] 2019/943*), der Verordnung über die Risikovorsorge (*Verordnung [EU] 2019/941*) und der Verordnung über die Gründung der Agentur der Europäischen Union für die Zusammenarbeit der Energieregulierungsbehörden (ACER) (*Verordnung [EU] 2019/942*).

Dabei soll mit der *Verordnung (EU) 2019/941* die Risikovorsorge gestärkt werden, indem Mitgliedsstaaten nationale Notfallpläne für den Fall von Engpässen erarbeiten. Zudem soll damit die länderübergreifende Verwaltung von Stromnetzen im Krisenfall erleichtert werden, und zwar über die neuen regionalen Betriebszentren, die mit der *Verordnung (EU) 2019/943* eingeführt wurden. Die *Verordnung (EU) 2019/942* soll dem Zusammenschluss der nationalen Regulierungsbehörden mehr Handlungsspielraum

geben und die Zusammenarbeit zwischen den Übertragungsnetzbetreibern in der EU und den Nachbarländern und der ACER fördern.

Der Verband Europäischer Übertragungsnetzbetreiber (European Network of Transmission System Operators for Electricity) wurde aufgefordert, in Zusammenarbeit mit der ACER und der Koordinierungsgruppe „Elektrizität" gemeinsame *Methoden* für die *Risikoermittlung* auszuarbeiten und vorzuschlagen, die anschließend von der ACER gebilligt werden sollen. Vier Maßnahmenpakete wurden vorgeschlagen:

1. gemeinsame Regeln für die Krisenprävention und -vorsorge, mit denen die Zusammenarbeit über Grenzen hinweg sichergestellt wird,
2. gemeinsame Regeln für die Krisenbewältigung,
3. gemeinsame Verfahren für die Bewertung von Versorgungssicherheitsrisiken und
4. ein gemeinsamer Rahmen für die bessere Bewertung und Überwachung der Sicherheit der Stromversorgung.

Diese Arbeiten an einem *europaweit harmonisierten Regelwerk* zur Cybersicherheit für Energienetze sind mittlerweile vorangeschritten. Ende 2020 wurde ein konsultierter Entwurf des Network Code on Cyber Security fertiggestellt. Der Netzkodex soll für Übertragungs- und Verteilnetzbetreiber unionsweit *verpflichtend* sein. Die Anwendung auf weitere Betreiber wesentlicher Dienste (gemäß *EU-NIS-Richtlinie 2016/1148*) wird derzeit erwogen. Der Entwurf *empfiehlt* unter anderem:

- eine Zertifizierungspflicht nach ISO 27001 für alle Netzbetreiber in der EU einzuführen, um die Einhaltung von Mindestanforderungen an die IT-Systeme unionsweit sicherzustellen,
- gemeinsame funktionelle Sicherheitsanforderungen an den Datenaustausch mit einem dreistufigen Klassifizierungssystem der Kritikalität zu formulieren, aus denen entsprechende Sicherheitsanforderungen abgeleitet werden,
- ein gemeinsames Produkttestsystem einzuführen, das Systeme und Komponenten von KRITIS-Betreibern unabhängig und nach einheitlichen Standards prüft.
- anonymisierte, technische Informationen, insbesondere zu Cybersicherheitsvorfällen, unter den europäischen Energieakteuren zu teilen,
- ein „Electricity Sector European CERT" (Computer Emergency Response Team) ins Leben zu rufen und
- Mindestsicherheitsanforderungen für Legacy Systeme zu formulieren.