Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten

nach § 109 Telekommunikationsgesetz (TKG) Version 2.0

Herausgeber:

Bundesnetzagentur

Bundesnetzagentur für Elektrizität, Gas,

Telekommunikation, Post und Eisenbahn

Stand: 29.04.2020

---

*Notifiziert gemäß der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).

Inhaltsverzeichnis

1 Systematik, Adressat, Inhalt und Verhältnismäßigkeit der Schutzmaßnahmen

Die ständig wachsende Abhängigkeit der Wirtschaft und der Gesellschaft von der Telekommunikation, insbesondere unter Berücksichtigung einer umfassenden Digitalisierung von allen Bereichen des täglichen Lebens, führt zu einem hohen Anspruch an die Sicherheit und die Verfügbarkeit von Telekommunikationsnetzen und -diensten.

Vor diesem Hintergrund definiert § 109 Telekommunikationsgesetz (TKG) bestimmte Schutzziele und Schutzpflichten. Als allgemeine Schutzziele bestimmt § 109 Abs. 1 TKG den Schutz personenbezogener Daten und den Schutz des Fernmeldegeheimnisses. Die Verfolgung dieser allgemeinen Schutzziele obliegt jedem Diensteanbieter. Die besonderen Schutzziele nach § 109 Abs. 2 TKG haben dagegen den Schutz der Telekommunikationsinfrastruktur vor Störungen und Risiken sowie die Verfügbarkeit der Telekommunikationsdienste zum Gegenstand. Die Verfolgung besonderer Schutzziele ist auf die Betreiber öffentlicher Telekommunikationsnetze und die Erbringer öffentlich zugänglicher Telekommunikationsdienste eingeschränkt.

Zur Erreichung der Schutzziele haben alle Unternehmen technische Vorkehrungen und sonstige Maßnahmen zu treffen. Zur Verfolgung der besonderen Schutzziele sind insbesondere auch Maßnahmen zum Schutz von Telekommunikations- und Datenverarbeitungssystemen gegen unerlaubte Zugriffe zu treffen, um Auswirkungen von Sicherheitsverletzungen für Nutzer oder für zusammengeschaltete Netze so gering wie möglich zu halten. Zur besseren Beherrschbarkeit der Risiken für Telekommunikationsinfrastruktur und Verfügbarkeit der Telekommunikationsdienste sieht § 109 Abs. 4 TKG die Erstellung von Sicherheitskonzepten und die Benennung von Sicherheitsbeauftragten vor.

Für staatliche Vorgaben gilt der Grundsatz der Verhältnismäßigkeit. Von den Unternehmen können daher nur geeignete, erforderliche und angemessene technische Vorkehrungen und sonstige Maßnahmen erwartet werden. Im Rahmen der Erforderlichkeit einer Vorkehrung oder Maßnahme ist der Stand der Technik zu berücksichtigen (§ 109 Abs. 1 S. 2 TKG; § 109 Abs. 2 S. 3 TKG). Angemessen ist eine Vorkehrung oder Maßnahme dann, wenn der dafür erforderliche technische und wirtschaftliche Aufwand nicht außer Verhältnis zur Bedeutung der zu schützenden Telekommunikationsnetze oder -dienste steht (§ 109 Abs. 2 S. 5 TKG).

In Erfüllung seiner telekommunikationsrechtlichen Pflichten hat das Unternehmen ergänzend die allgemeinen datenschutzrechtlichen Vorgaben des Bundesdatenschutzgesetzes (BDSG) und der Datenschutz-Grundverordnung (DSGVO) zu beachten. Werden telekommunikationsrechtliche Pflichten aus § 109 TKG im Auftrag eines Verantwortlichen durch andere Personen oder Stellen erfüllt und hierbei Daten verarbeitet, so hat der nach § 109 TKG Verantwortliche für die Einhaltung der telekommunikationsrechtlichen Vorschriften Sorge zu tragen. Unberührt hiervon bleibt die unmittelbare datenschutzrechtliche Verantwortlichkeit der beauftragten Person oder Stelle nach allgemeinem Datenschutzrecht.

2 Funktion und grundlegender Inhalt des Katalogs von Sicherheitsanforderungen

Betreiber öffentlicher Telekommunikationsnetze und Erbringer öffentlich zugänglicher Telekommunikationsdienste haben die von ihnen ergriffenen technischen und organisatorischen Schutzmaßnahmen in einem Sicherheitskonzept darzustellen gemäß § 109 Abs. 4 TKG. Grundlage für dieses Sicherheitskonzept und für die zu ergreifenden technischen Vorkehrungen und sonstigen Maßnahmen ist der „Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 TKG“, den die Bundesnetzagentur im Einvernehmen mit dem Bundesamt für die Sicherheit in der Informationstechnik und dem/der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erstellt hat.

Grundlegende Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung von personenbezogenen Daten sind in 3. Kapitel beschrieben. Die Erfüllung dieser Sicherheitsanforderungen ist für alle Unternehmen zwingend. Ein Überblick über die einschlägigen gesetzlichen Anforderungen des TKG (§§ 88 - 109) soll Kapitel 4 geben. Hinweise zur Erstellung eines Sicherheitskonzeptes finden sich in Kapitel 5. Anlage 1 beschreibt geeignete technische und organisatorische Maßnahmen zur Anforderungen an TK-Diensteerbringer mit IP-Infrastruktur. Zusätzliche Sicherheitsanforderungen enthält die Anlage 2. Die zusätzlichen Sicherheitsanforderungen richten sich an Betreiber von Telekommunikationsnetzen mit erhöhtem Gefährdungspotential.

Die Verantwortung der richtigen und ordnungsgemäßen Umsetzung von Schutzmaßnahmen obliegt stets dem Verpflichteten. Er muss dafür Sorge tragen, dass auch bei einer Aufgabenübertragung an Dritte kein Sicherheitsverlust zu erwarten ist.

Die Bundesnetzagentur kann nach § 109 Abs. 7 TKG anordnen, dass sich die Betreiber öffentlicher Telekommunikationsnetze oder die Anbieter öffentlich zugänglicher Telekommunikationsdienste einer Überprüfung durch eine qualifizierte unabhängige Stelle oder einer zuständigen nationalen Behörde unterziehen. Eine solche Überprüfung soll feststellen, ob die Anforderungen nach § 109 Abs. 1 bis 3 TKG erfüllt sind. Der Katalog für Sicherheitsanforderungen kann somit auch Grundlage für das Sicherheitsaudit einer qualifizierten unabhängigen Stelle nach § 109 Abs. 7 TKG sein.

In die Erstellung des Kataloges wurden Hersteller, Verbände der Betreiber öffentlicher Telekommunikationsnetze und Verbände der Anbieter öffentlich zugänglicher Telekommunikationsdienste eingebunden.

3 Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung von personenbezogenen Daten

Ein ganzheitliches Konzept bildet die Basis und den Ausgangspunkt zum Aufbau eines tragfähigen Sicherheitsmanagements. Informationssicherheitsmanagement, oder kurz IS-Management, ist der Teil des allgemeinen Risikomanagements, der die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, Geschäftsprozessen, Anwendungen und IT-Systemen gewährleisten soll. Informationssicherheit ist aber nicht nur eine Frage der Technik. Um ein bedarfsgerechtes Sicherheitsniveau für alle Geschäftsprozesse, Informationen und der Technik zu erreichen, sind in erheblichem Maße auch geeignete organisatorische und personelle Rahmenbedingungen zu schaffen.

Die im Folgenden aufgelisteten Sicherheitsanforderungen greifen diese Aspekte auf. Die Anforderungen gelten für alle pflichtigen Unternehmen und sind allgemeiner Natur. Sie bilden insofern die Grundlage für alle umzusetzenden Schutzmaßnahmen. Die aus den Sicherheitsanforderungen abgeleiteten Schutzmaßnahmen müssen im Weiteren angemessen in dem zu erstellenden Sicherheitskonzept berücksichtigt werden. Die Beurteilung der Angemessenheit einer sicherheitskonzeptionellen Schutzmaßnahme liegt hierbei zunächst in der Eigenverantwortung des pflichtigen Unternehmens. Dabei handelt es sich um einen kontinuierlichen Beurteilungsprozess, bei dem Strategien und Maßnahmen stetig überprüft und an veränderte Anforderungen angepasst werden. Die Bundesnetzagentur überprüft regelmäßig die Einhaltung der Vorgaben des Sicherheitskatalogs und die Umsetzung des Sicherheitskonzepts.

Auch die Sicherheitsanforderungen des vorliegenden Kataloges sind daher weder abschließend, noch zeitlich unveränderlich. Je nach Kritikalität eines bestimmten Netzes oder Dienstes bzw. Entwicklung der Technik sind im Einzelfall weitergehende Anforderungen erforderlich.

3.1 Organisation

Handelt es sich bei dem pflichtigen Unternehmen um einen Kaufmann oder eine Einpersonengesellschaft, so sind die Verantwortlichkeiten und Prozesse einfach zuzuordnen. In vielen Fällen fußt die Pflicht aus § 109 Abs. 1 bis 3 TKG jedoch auf einem arbeitsteiligen

Betrieb oder Angebot. Die Leitungsperson eines pflichtigen arbeitsteiligen Unternehmens hat daher auf eine eindeutige und festgelegte Aufbau- und Ablauforganisation zu achten. Hierzu gehört auch die Benennung des Sicherheitsbeauftragten nach § 109 Abs. 4 TKG.

3.1.1 Organisations- und Risikomanagement

Jedes Unternehmen hat sicherzustellen, dass ein verbindliches Verfahren festgelegt ist, um Risiken für Netzwerke, Dienste und die Verarbeitung personenbezogener Daten zu erkennen. Identifizierte, wesentliche Gefährdungen (Sicherheitsrisiken) für Netze, Dienste und Daten sind zu dokumentieren Erkannte Restrisiken sollen unter Berücksichtigung der Verhältnismäßigkeit kontrolliert werden.

3.1.2 Sicherheitsrollen und Verantwortlichkeiten

Für die Sicherheit von Informationen, Geschäftsprozessen, Anwendungen, Aufgaben und Regelungen ist eine personelle Verantwortlichkeit festzulegen. Es sind alle Mitarbeiter über diese Verantwortlichkeiten in geeigneter Weise zu informieren. Es soll ein Hinweis ergehen, wann und wie die für Sicherheit Zuständigen zu beteiligen sind.

- Bei der Vergabe der jeweiligen Sicherheitsrollen kann ein Ernennungsakt Klarheit, Transparenz und Öffentlichkeit verschaffen. In diesem Zusammenhang könnte auch eine Festlegung von Aufgaben und Befugnissen erfolgen.
- Benennung alleine ist nicht ausreichend. Die für Sicherheitsvorfälle zuständigen Personen müssen in der Wahrnehmung ihrer Rollen erreichbar sein. Die Schaffung einer Vertretungsregelung ist in diesem Zusammenhang eine wichtige Voraussetzung.
- Sicherheitskenntnisse altern. Es soll daher eine regelmäßige Schulung des benannten Personals durchgeführt werden.

3.1.3 Lieferantenmanagement

Die Bereitstellung von Telekommunikationsdiensten kann oft nur unter Rückgriff auf Dritte erfolgen. Lieferanten und Erfüllungsgehilfen nehmen vor diesem Hintergrund eine wichtige Rolle ein. Das pflichtige Unternehmen muss daher eine Bewertung der Zuverlässigkeit, Vertrauenswürdigkeit und Qualität des Erfüllungsgehilfen oder Lieferanten vornehmen. Es ist sicherzustellen, dass durch die Abhängigkeiten von Dritten die Sicherheit von Netzwerken oder Dienstleistungen sowie personenbezogener Daten nicht beeinträchtigt wird. In diesem Zusammenhang ist auf Folgendes zu achten:

- Eine Bewertung der Zuverlässigkeit des Dritten ist nur auf der Grundlage von geeigneten Informationen möglich. Daher gilt: Informationseinholung hat vor Beauftragung zu erfolgen.
- Dritte sind vertraglich zu binden. Es ist hierbei sicherzustellen, dass Sicherheitsanforderungen in die vertragliche Grundlage mit Anbietern einbezogen werden (z. B. beim Erwerb von IT-Produkten oder der Inanspruchnahme von IT-Services). Besondere Sorgfalt sollte in dieser Hinsicht gelten, sofern ganze Geschäftsprozesse (Helpdesks, Call Center, Netzwerkverbindungen) ausgelagert werden).
- Das datenschutzrechtlich konforme Handeln der Dritten ist sicherzustellen. Dies kann durch entsprechende vertragliche Regelungen erfolgen. Bei Auftragsverarbeitung sind die Regelungen des Art. 28 DSGVO zu beachten.
- Die Sicherheitsanforderungen sollten nicht nur festgelegt und aktualisiert, sondern auch in ihrer Einhaltung möglichst überprüft werden. Bei einer Auftragsverarbeitung muss dies grundsätzlich erfolgen. Die Überprüfungen sollten regelmäßig wiederholt werden.

3.2 Sicherheit im Personalmanagement

Mitarbeiter liefern einen wesentlichen Beitrag zur Einhaltung der eingangs erwähnten Schutzziele. Aufwendige Schutzmaßnahmen und technische Redundanzkonzepte bringen nur den gewünschten Erfolg, wenn auch die Mitarbeiter keine Sicherheitslücke im Unternehmen darstellen und der Verantwortung ihrer sicherheitsrelevanten Tätigkeit bewusst sind. Dieses Kapitel umfasst die Sicherheitsanforderungen an die Personalabteilung, die Geschäftsführung und das Personal im Unternehmen. Hierzu gehört auch Personal, welches zur Erledigung bestimmter Aufgaben extern bereitgestellt wird (z. B. von Lieferanten oder Herstellern).

Bereits vor der Einstellung und auch nach dem Verlassen des Unternehmens sind die nachfolgenden Anforderungen zu berücksichtigen.

3.2.1 Sicherheitsüberprüfung

Je nach Aufgabe und Verantwortlichkeit kann eine angemessene Sicherheitsüberprüfung erforderlich sein. Im Hinblick auf Mitarbeiter und Auftragnehmer ist es angezeigt, die Identität und die berufliche Referenz, vor allem bei Personen mit sicherheitsrelevanten Aufgaben und Verantwortlichkeiten (z. B. bei Systemadministratoren, Sicherheitsbeauftragten oder

Wachpersonal), zu validieren. Die jeweils eingesetzte Prüfungsmodalität sollte dokumentiert werden.
Zur eindeutigen Feststellung der Identität sollte das Unternehmen Mitarbeiter zur Vorlage des Personalausweises auffordern. Weitere geeignete Nachweise können beglaubigte Zeugniskopien, Personenzertifikate oder eines amtlichen Führungszeugnisses sein. Es bietet sich u.U. an, weitere zusätzliche Referenzen von früheren Arbeitgebern einzuholen.

3.2.2 Sicherheitswissen und Sensibilisierung

Das Personal muss über geeignete und relevante Sicherheitskenntnisse verfügen und ein Bewusstsein für den Umgang mit sensiblen Daten entwickeln.

Es ist daher sicherzustellen, dass das eingesetzte und beauftragte Personal geeignete und relevante Schulungen besucht hat und Material zu Sicherheitsfragen zur Verfügung gestellt wird. Der Besuch der Schulung ist zu dokumentieren.

Wissen altert. Es sollten daher regelmäßige Schulungsmaßnahmen und Sensibilisierungssitzungen für eingesetztes und beauftragtes Personal zu den betreffenden Sicherheitsthemen (z.B. Datenschutz, Fernmeldegeheimnis) abgehalten werden.

Auch Schulungsinhalte sollten regelmäßig unter Berücksichtigung von Änderungen überprüft und ggf. aktualisiert werden.

3.2.3 Personelle Veränderungen

Ein Personalwechsel ist mit Sicherheitsrisiken verbunden. Wenn Mitarbeiter den Aufgabenbereich wechseln, das Unternehmen verlassen oder neue Mitarbeiter eingearbeitet werden, muss daher das Unternehmen bestimmte Sicherheitsanforderungen beachten:

- Es sind Regelungen für die Verwaltung von Personalveränderungen oder Änderungen von Zuständigkeiten und Verantwortlichkeiten zu wahren.
- Nach einem Personal- oder Beauftragtenwechsel sind Zugriffs, Zutritts- und Zugangsrechte zu entsprechenden Systemen, Gebäuden oder Anlagen unverzüglich anzupassen bzw. zu sperren. Ausgegebene Passwörter sind nach dem Stand der Technik zu verwalten.
- Neues Personal muss über geltende Richtlinien und Verfahren informiert und sensibilisiert werden.

3.2.4 Umgang mit Verstößen

Es sollten verbindliche Regelungen festgelegt werden, wie mit Sicherheitsverletzungen aufgrund von Verstößen durch eigene Mitarbeiter umgegangen wird.

3.3 Sicherheit von Daten, Systemen und Einrichtungen

Dieses Kapitel umfasst die physische und logische Sicherheit von Daten, Netzwerk- und Informationssystemen zum Schutz der Grundwerte (Vertraulichkeit, Verfügbarkeit und Integrität).

3.3.1 Sicherer Umgang mit sensiblen Daten und Informationen

Im Bereich der Telekommunikation ist der Schutz von Bestands- und vor allem der von hoch sensiblen Daten, wie z.B. Verkehrs-, Steuer- oder Inhaltsdaten zu gewährleisten. Sie unterliegen dem Datenschutz und dem Schutz des Fernmeldegeheimnisses. Es müssen daher Regelungen zum sicheren Umgang mit solchen Daten und Informationen getroffen werden. Insbesondere gilt:

- Sensible Akten oder Dokumente müssen unter Verschluss verwahrt werden. Abschließbare Aktenschränke, verschlossene Büroräume sollten als mögliche Maßnahmen berücksichtigt werden.
- Mobile Endgeräte oder Wechseldatenträger sollten mit geeigneten Verschlüsselungstechnologien geschützt werden. Es sollte ein (MDM) Mobile Device Management genutzt werden.
- Es sollten Regelungen zur sicheren Entsorgung von Wechseldatenträgern, die nicht mehr benötigt werden oder defekt sind, getroffen werden.
- Festplatten mit sensiblen Daten müssen so entsorgt werden, dass eine Wiederherstellung der Daten nicht mehr möglich ist.

3.3.2 Physische und elementare Schutzanforderungen

Ein Sicherheitsrisiko besteht auch durch Vandalismus, Diebstahl, Feuer, Wasser, Staub oder Elementarschäden. Durch geeignete physische Schutzmaßnahmen sollten Sicherheitsrisiken dieser Art möglichst abgewehrt werden, damit die Verfügbarkeit von Netz und Dienst gewahrt bleibt. Dies beinhaltet mindestens die folgenden Maßnahmen:

- Es sind physische Sicherheitselemente festzulegen, die den unbefugten Zutritt, die Beschädigung und die Beeinträchtigung von Informationen und informationsverarbeitenden Einrichtungen verhindern (z.B. durch

Sicherheitsschlösser, Bewegungsmelder, Einbruchmeldeanlagen oder Videoüberwachung).

- Sicherheitsbereiche sollten durch eine angemessene Zutrittssteuerung geschützt werden.
- Geräte und Betriebsmittel sind in regelmäßigen oder durch den Hersteller empfohlenen Intervallen zu warten.
- Telekommunikationsverkabelung und Stromverkabelung sind vor Unterbrechung, Störung und Beschädigung angemessen zu schützen. Redundante Leitungen sind voneinander getrennt zu verlegen. Kabel sollten unterirdisch verlegt werden und durch Rohre und verschlossene Räume und Schränke geschützt werden.
- Wasserführende Leitungen sollten in Serverräumen vermieden werden.
- Maßnahmen zum Schutz vor Naturkatastrophen und Unfällen sind zu ergreifen.
- Es ist eine regelmäßige Bewertung der Wirksamkeit von physischen und umgebungsbezogenen Schutzmaßnahmen vorzunehmen.
- Der Einsatz von Feuer-, Gas- und Rauchmeldern oder Löschanlagen sollte der Größe der Räumlichkeiten angemessen vorhanden sein und regelmäßig gewartet werden.
- Die Einhaltung der Brandschutzordnung muss regelmäßig überprüft werden.

3.3.3 Versorgungssicherheit (Verfügbarkeit des Gesamtsystems)

Ein wichtiger Bestandteil im Bereich der öffentlich zugänglichen Telekommunikation ist die Gewährleistung der Versorgungssicherheit (Telekommunikation, Elektrizität, Klimatisierung, usw.). Folgende Schutzmaßnahmen sind zu ergreifen:

- Geräte und Betriebsmittel sind vor Stromausfällen und anderen Störungen zu schützen.
- Es sollten redundante Leitungen über unterschiedliche Zuleitungswege vorhanden sein.
- Eine ausreichende Dimensionierung der Klimatisierung und Stromversorgung ist festzulegen und regelmäßig zu überwachen.
- Schaltanlagen, Notstromgeneratoren, Batterien, etc. müssen regelmäßig kontrolliert und falls möglich getestet werden.
- Ein Verfahren zur Umsetzung für die Sicherheit kritischer Versorgungsgüter, Versorgungseinrichtungen und unterstützenden Einrichtungen ist zu erstellen.
- Maßnahmen zum Schutz der Lieferung und Bereitstellung der Versorgungseinrichtungen sind zu implementieren.

3.3.4 Zugriffs- und Zugangskontrolle auf Netzwerk- und Informationssystemen

Ohne geeignete Mechanismen zur Zugriffs- und Zugangskontrolle kann eine unberechtigte Nutzung von TK-Geräten und TK-Systemen nicht verhindert werden. Unbefugte können auch an vertrauliche Informationen gelangen, Manipulationen vornehmen oder Störungen verursachen. Durch geeignete Berechtigungen soll der Zugang und der Zugriff auf Informationen kontrolliert und gesteuert werden.

Mögliche Schutzmaßnahmen sind:

- Nutzer haben eindeutige Kennungen und werden authentifiziert, bevor sie auf Dienste oder Systeme zugreifen dürfen.
- Passwörter dürfen nur verschlüsselt gespeichert werden.
- Rollen, Rechte, Verantwortlichkeiten und Verfahren zum Zuweisen und Widerrufen von Zugriffsrechten sind festzulegen.
- Zugriffe auf Netzwerk- und Informationssysteme müssen protokolliert werden. Abweichungen von dieser Verfahrensweise müssen hinterlegt und protokolliert werden.
- Fernwartungszugänge müssen ausreichend gesichert werden (eigene VPN-Zugänge).
- Fremde Personen dürfen sich nur in Begleitung oder nach geeigneter Sicherheitsüberprüfung und Einweisung in gesicherten Bereichen aufhalten. Fremde Personen sind hierbei Personen von externen Firmen z.B. bei Wartungsarbeiten, Umbauten oder auch Reinigungsarbeiten.
- Die Zugangskontrollmechanismen werden regelmäßig überprüft und bei Bedarf angepasst.
- Für gesicherte technische Anlagen muss sichergestellt sein, dass nur Personen mit Befugnis Zugriff haben.

3.3.5 Integrität und Verfügbarkeit von Netzwerk- und Informationssystemen

Die Integrität und Verfügbarkeit von Netzwerk- und Informationssystemen und der Schutz vor Viren, Code-Injektionen und anderer Malware, die die Funktionalität von Systemen verändern kann, ist zu gewährleisten:

- Es ist sicherzustellen, dass Software von Netzwerk- und Informationssystemen nicht unberechtigt manipuliert oder verändert wird (z.B. durch nicht-autorisierte Änderung der Konfiguration). Änderungen sollten dokumentiert werden. Unberechtigte Zugriffe

müssen detektiert werden. Systeme und Anwendungen sollten immer die aktuellen Sicherheitsupdates erhalten.

- Es müssen geeignete Maßnahmen zur Erkennung von Schadsoftware umgesetzt werden.
- Maßnahmen zur Sensibilisierung der Mitarbeiter sollen bestehen und umgesetzt werden.
- Es ist sicherzustellen, dass sicherheitskritische Daten (wie Passwörter, gemeinsame geheime Schlüssel, private Schlüssel usw.) nicht offengelegt oder manipuliert werden.
- Die Wirksamkeit der Maßnahmen zum Schutz der Integrität von Systemen sollte überprüft und bewertet werden.
- Passwörter sollten sicher authentifiziert und bei Bedarf geändert werden.
- Mitarbeiter sollten durch Schulungsmaßnahmen befähigt sein, verdächtige E-Mails oder Links zu erkennen.

3.3.6 Vertraulichkeit der Kommunikation

Die Vertraulichkeit und die Integrität von Kommunikationsinhalten und Metadaten sind zu gewährleisten:

- Zur Sicherstellung eines angemessenen Schutzes der Vertraulichkeit von Kommunikationsinhalten und Metadaten sollten geeignete Verschlüsselungsverfahren eingesetzt werden.
- Es sind geeignete Authentifizierungsmechanismen für Kunden- und Dienstleistungsnetzwerke zu implementieren.
- Die Nutzung von Netzwerken und Diensten sollte fortwährend in geeigneter Form auf Anomalien sondiert werden.
- Es sollten standardisierte Übertragungsverfahren und -maßnahmen verwendet werden.
- Sicherheitskritische Daten von Kunden sind besonders zu schützen (z.B. Daten der SIM-Karten, IMEI-Nummer, Passwörter).
- Auch die Wirksamkeit von Methoden zum Schutz der Vertraulichkeit von Kommunikationsinhalten und -metadaten sollte stetig in geeigneter Form bewertet werden. Standortdaten wie beispielsweise Cell-IDs gehören ebenfalls zu den Metadaten und unterliegen zusätzlichen Anforderungen (siehe Abschnitt 4.2.4). Eine geeignete Bewertung kann die Ausführung einer Gegenprüfung (Cross-Checks) oder die Durchführung eines (Stress)Tests sein.

3.4 Betriebsführung

Die verantwortliche Unternehmensführung hat den ordnungsgemäßen und sicheren Betrieb zu gewährleisten. Die nachfolgenden Sicherheitsanforderungen haben das operative Betriebsverfahren, das Änderungsmanagement und den Umgang mit Unternehmenswerten zum Gegenstand.

3.4.1 Betriebsverfahren

Durch geeignete Betriebsverfahren ist sicherzustellen, dass die Informations- und Kommunikationstechnologie des jeweiligen pflichtigen Unternehmens ordnungsgemäß, sicher und kontinuierlich funktioniert.

- Um dies sicherstellen zu können, muss im Mindestmaß der Betriebsablauf festgelegt und dokumentiert werden. Ferner müssen die Verantwortlichkeiten für den Betrieb kritischer Systeme einer zuständigen Stelle zugewiesen sein.

- Verfügbare und notwendige Ressourcen müssen bekannt sein. Ressourcen in diesem Sinn umfassen u.a. das notwendige und tatsächliche Personal, Systeme, Anwendungen und Räumlichkeiten.
- Verfügbare und notwendige Ressourcen müssen stetig überprüft und ggf. in geeigneter Form gesteuert werden.

3.4.2 Änderungsmanagement

Veränderungen können Sicherheitsrisiken bergen. Sich schnell ändernde und stetig steigende Anforderungen der Benutzer führen beim pflichtigen Unternehmen zudem zu immer kürzeren Änderungsintervallen einschließlich Anpassungen von Systemkonfigurationen. Unternehmen können insofern vor der Aufgabe stehen, TK-Komponenten bedarfsgerecht und zeitnah, aber auch sicher aktualisieren zu müssen. Die Sicherheitspraxis zeigt, dass Risiken oder Betriebsstörungen häufig auf fehlerhaftes, übereiltes oder keinerlei geeignetes Änderungsmanagement zurückzuführen sind. Zur Vermeidung von Störungen oder Sicherheitsvorfällen sollten daher Änderungen an Netzwerk- und Informationssystemen, Infrastruktur, Dokumentationen, Prozessen, Verfahren und Betriebsabläufen geplant, kontrolliert, gesteuert und nach Abschluss überprüft werden.

- Änderungen an kritischen Systemen sollen auf der Grundlage von vordefinierten und in geeigneter Form dokumentierten Verfahren erfolgen.
- Es sollte eine Einschätzung aller potenziellen direkten und indirekten Auswirkungen vorgenommen werden.
- Wesentliche tatsächliche Änderungen sollten in geeigneter Form protokolliert werden.
- Die Funktionalität der TK-Systeme sollte nach Änderungen in geeigneter Form überprüft werden. Alle betroffenen Personen sollten über die erforderlichen Änderungsdetails informiert werden. Identifizierte Auffälligkeiten sollten sofort der vorher festgelegten Stelle angezeigt werden.
- Es empfehlen sich Maßnahmen der präventiven Kontrolle, z. B. das 4-Augenprinzip.

3.4.3 Asset Management

Sicherheit erfordert Kenntnis. Zumindest die wesentlichen Anlagen, Systeme und Einrichtungen, welche für den jeweiligen Netzbetrieb oder das Diensteangebot erforderlich sind, sollten eindeutig identifizierbar sein. Eine entsprechende Inventarisierung und Verwaltung von Anlagen und Systemen kann dies im Einzelfall sicherstellen. Die Verwaltung sollte auch die Konfigurationssteuerung der wesentlichen Netzwerk- und Kommunikationssysteme einschließen.

3.5 Störungen und Sicherheitsvorfälle

Behandelt werden das Erkennen, die Reaktion auf sowie die Meldung von Störungen und Sicherheitsvorfällen. Sicherheitsvorfälle können durch ein einzelnes Ereignis oder eine Verkettung verschiedener Umstände ausgelöst werden. Sicherheitsvorfälle können dazu führen, dass die Vertraulichkeit, Integrität, Verfügbarkeit oder Authentizität von Informationen und TK-Systemen beeinträchtigt werden.

3.5.1 Erkennen von Sicherheitsvorfällen und Störungen

Es muss ein Verfahren zum Erkennen von Sicherheitsvorfällen und Störungen eingerichtet und regelmäßig kontrolliert werden.
Hierzu sind z.B. vordefinierte Betriebsparameter wie Klima, Strom, Datenaufkommen im TK-Verkehr zu überwachen und im Sicherheitsvorfall oder bei Störungen zu alarmieren.
Nach Bekanntwerden von Störungen und/oder Vorfällen sollten betroffene Systeme so angepasst und/oder verbessert werden, dass zukünftig diese Problematik verhindert wird.

3.5.2 Umgang mit Sicherheitsvorfällen und Störungen

Ein Sicherheitsvorfall kann einen singulären oder multikausalen Ursprung haben. Jede Art von Sicherheitsvorfall kann dazu führen, dass die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen und TK-Systemen beeinträchtigt wird. Die pflichtigen Unternehmen haben daher ein Verfahren zur Definition und zum Umgang mit jedweder Art von Sicherheitsvorfall, einschließlich dessen Meldung an zuständige Personen und Behörden zu implementieren. Es sollte regelmäßig überprüft werden, ob das festgelegte Verfahren den aktuellen Umständen entspricht und die tatsächliche Umsetzung planungskonform erfolgt.

- Für Sicherheitsvorfälle hat geeignetes Personal verfügbar und benannt zu sein. Im Falle einer Sicherheitsverletzung kann es notwendig sein, unter Zeitdruck oder atypischen Umständen Sicherheitshandlungen durchzuführen oder sicherheitsrelevante Entscheidungen zu treffen. Das Personal sollte daher nicht nur für die Identifizierung, sondern auch für den speziellen Umgang mit Sicherheitsvorfällen geschult sein.
- Die Kritikalität der jeweiligen Störung oder Sicherheitsverletzung muss in geeigneter Form bewertet werden. Der für das Bewertungsergebnis vorgegebene Meldeweg muss sodann umgesetzt werden.
- Kritische Sicherheitsvorfälle müssen grundsätzlich untersucht werden. Untersuchung und Ergebnis muss in einem Bericht dokumentiert werden. Aus dem Bericht sollte

hervorgehen, welche Maßnahmen getroffen oder geplant sind, um gleichgelagerte Sicherheitsvorfälle und deren Auswirkungen zukünftig zu vermeiden oder das Sicherheitsrisiko zu minimieren. Die in dieser Hinsicht getroffenen oder geplanten Maßnahmen sollten begründet werden. Handelt es sich um beträchtliche Sicherheitsverletzungen gemäß § 109 Abs. 5 TKG, sind diese unverzüglich der Bundesnetzagentur und dem Bundesamt für Sicherheit in der Informationstechnik mitzuteilen.

3.5.3 Kommunikation und Meldung von Sicherheitsvorfällen

Um den Schaden bei Sicherheitsvorfällen so gering wie möglich zu halten, sollten angemessene Verfahren zur Meldung von Sicherheitsereignissen vorhanden sein.

- Ein Sicherheitsvorfall kann eine gesetzliche Meldepflicht (z. B. §§109 Abs. 5, 109a Abs. 1 TKG oder Art. 33 DSGVO) auslösen. Falls erforderlich sind daher Meldungen über aktuelle oder zurückliegende Sicherheitsereignisse an Dritte, Kunden und/ oder Behörden durchzuführen.
- Zur Sicherstellung etwaiger Meldepflichten sowie der Kommunikation und Berichterstattung von Sicherheitsvorfällen sollten geeignete Regelungen in die unternehmerischen Betriebsabläufe implementiert werden.
- Bei einem Angriff auf Passwörter sind betroffene Kunden schnellstmöglich zu informieren. Zur Sicherstellung sollte ein geeignetes Meldeverfahren festgelegt werden.

3.6 Not- oder Ausfallmanagement

Eine Störung oder ein Sicherheitsvorfall kann zum Ausfall des Dienstes oder des Netzbetriebes führen. Eine geeignete Präventionsstrategie sollte Entwicklungen dieser Art berücksichtigen und entsprechende auf den Einzelfall angepasste Abwehrkonzepte entwickeln. In diesem Zusammenhang sind nicht nur die technischen Aspekte für die Aufrechterhaltung der Dienste zu regeln. Auch organisatorische Maßnahmen sind im Vorfeld zu planen, festzulegen und fortwährend zu überprüfen. Dieses Kapitel umfasst Anforderungen zur Wiederherstellung und Aufrechterhaltung betriebsrelevanter Infrastrukturen.

3.6.1 Aufrechterhaltung von Telekommunikationsinfrastrukturen und Diensten (Business Continuity Management)

Regelungen zur Aufrechterhaltung der Infrastrukturen und Dienste haben allgemeine Handlungsanweisungen und möglichst auch konkrete, auf den Einzelfall angepasste Notallmaßnahmen zu enthalten. Relevante Kontaktinformationen sollten in einem Notfallhandbuch beschrieben und stets aktuell sein. Der Zugriff auf diese Regelungen und Informationen sollte sichergestellt sein.

- Im Vorfeld ist die Verfügbarkeit angemessener Redundanzen auf System- und Dienstebene sicherzustellen.
- Diese Redundanzen sind in regelmäßigen Abständen zu testen bzw. umzuschalten, sofern dies unterbrechungsfrei möglich ist.
- Es sind regelmäßige Backups von kritischen Systemen und Daten zu erstellen. Auf die gesetzlich vorgegebenen Lösch- und Speicherfristen ist hierbei zu achten, insbesondere sollte die Speicherdauer der Backups in einem angemessenen Verhältnis zur Speicherdauer der personenbezogenen Daten stehen.
- Es sind angepasste Notfallpläne zum Betrieb kritischer Systeme auszuarbeiten, festzulegen und zu implementieren. Es sollte regelmäßig eine Evaluierung dieser Pläne erfolgen.
- Ein geeigneter Notfallbeauftragter ist zu benennen. Dieser sollte alle Aktivitäten des Notfallmanagements kennen und steuern.

3.6.2 Wiederanlauf nach Ausfällen (Disaster Recovery Management)

Die Ausfallzeiten bis zur Wiederherstellung der Funktionsfähigkeit von Netzwerk und Kommunikationsdiensten müssen dennoch mit angemessenen Mitteln so gering wie möglich gehalten werden.

- Es sind geeignete Richtlinien und Verfahren zur schnellstmöglichen Wiederherstellung wichtiger Netzwerk- und Kommunikationsdienste zu entwickeln und festzulegen. Diese Richtlinien und Verfahren sollten in regelmäßigen Abständen evaluiert werden.
- Die wichtigsten Geschäftsprozesse für den Wiederanlauf sollten priorisiert werden.
- Im Vorfeld sollten Lieferantenverträge auf eine Ersatzbereitstellung geprüft werden.
- Eine geeignete Schutzmaßnahme kann die Vorhaltung geeigneter Ersatzgeräte für Infrastruktur und TK-Systeme sein.
- Eine geeignete Schutzmaßnahme kann im Einzelfall auch die Vorhaltung geeigneter, mobiler Netzersatzanlagen sein.

- Zur Aufrechterhaltung von Dienstleistungen kann die präventive Einrichtung von Notfallarbeitsplätzen für Mitarbeiter sinnvoll sein.

3.7 Überwachungs- und Testverfahren

Um Systeme und Prozesse möglichst sicher zu gestalten und stets zu optimieren, sollten Überwachungs- und Testverfahren eingeführt werden. Nachfolgend werden Anforderungen zur Überwachung und Protokollierung wichtiger Netzwerk- und Kommunikationssysteme beschrieben.

3.7.1 Überwachungs- und Protokollierungsmaßnahmen

Geschäfts- und sicherheitsrelevante Ereignisse sollten protokolliert werden. Protokollierungsdaten dienen der Auswertung und Überwachung bestimmter Ereignisse. Eine detailreiche und fortlaufende, möglichst automatische Protokollierung kann die Auswertungsmöglichkeiten erhöhen. Im günstigsten Fall lassen die Protokollierungsdaten auf der Grundlage einer forensischen Untersuchung eine geeignete Sicherheitsanalyse zu. Alle sicherheitsrelevanten Ereignisse sind daher zu protokollieren und in einer auswertbaren Form abzuspeichern. Werden Daten für diese Zwecke nicht mehr benötigt, so sind sie unverzüglich zu löschen.

- Es sollte ein auf den Einzelfall angepasstes Regelwerk für die Überwachung und Protokollierung betriebsrelevanter Systeme eingeführt und umgesetzt werden. Das Regelwerk sollte regelmäßig evaluiert werden.
- Durch die automatische Überwachung und Protokollierung betriebsrelevanter Systeme können im Einzelfall möglicherweise weitere, zur Auswertung geeignete Informationen gewonnen werden.
- Administrative Tätigkeiten oder Arbeiten an betriebsrelevanten Systemen sollten protokolliert werden.

3.7.2 Notfallübungen

Im Kapitel 3.6 wurden Anforderungen zur Aufrechterhaltung und zum Wiederanlauf von Infrastrukturen und Diensten nach Notfällen behandelt. Damit Notfallpläne und Verfahren unter Stresssituationen wie geplant umgesetzt werden können, sollten regelmäßig Notfallübungen durchgeführt werden. Daher sollte eine Vorgehensweise zum Testen und Üben von Notfallplänen zur Aufrechterhaltung und Wiederherstellung kritischer Dienste und

Infrastrukturen festlegt werden. Falls möglich und notwendig, sollte dies auch in Zusammenarbeit mit Dritten erfolgen.
Es sollen möglichst realistische und unterschiedliche Szenarien berücksichtigt werden. Festgestellt werden soll, ob geplante Ausfallzeiten nicht überschritten werden und ob die bestimmte Krisenleitung in der Praxis ihre Aufgaben erfüllt.

3.7.3 Testen von Netzwerk- und IT-Systemen

Änderungen oder Entwicklungsarbeiten an bestehenden Netzwerk- oder IT-Systemen sind mögliche Risikofaktoren. Es sollten daher schon im Vorfeld Regelungen zur Freigabe und zum Testen von Netzwerk- und IT-Systemen festgelegt werden.

- Netzwerk- oder IT-Systeme sollten auf gesonderten Testumgebungen getestet werden, bevor sie verwendet oder mit vorhandenen Systemen verbunden werden. Gleiches sollte auch bei Anpassungen oder z.B. nach Updates geschehen.
- Betriebsrelevante Systeme sollten regelmäßigen Sicherheitstests unterzogen werden. Dies gilt insbesondere dann, wenn neue Systeme eingeführt und Änderungen vorgenommen werden.
- Es muss sichergestellt sein, dass Tests keine Auswirkungen auf die Sicherheit von Netzwerken und Diensten haben. Die Verwendung von sensiblen Daten muss vermieden werden.

3.8 Beurteilung der Sicherheitsmaßnahmen

Alle Sicherheitsmaßnahmen müssen den Stand der Technik berücksichtigen. Die Technik entwickelt sich jedoch fortwährend weiter. Hiermit einhergehend unterliegt auch die Bedrohungslage einer ständigen Veränderung. Vor diesem Hintergrund müssen auch die getroffenen Sicherheitsmaßnahmen regelmäßig neu vom pflichtigen Unternehmen beurteilt werden. Daher sollte eine angemessene Strategie zur Beurteilung der im Einzelfall getroffenen Sicherheitsmaßnahmen erstellt werden.

- Es sollten im Mindestmaß Regelungen zur Beurteilung der getroffenen Schutzmaßnahmen erstellt werden.
- Regelmäßig durchgeführte Risikoanalysen sowie Erhebungen festgelegter Kennzahlen (z.B. Störungs- und Ausfallzeiten als Indikator) können für die Beurteilung der Sicherheitsmaßnahmen herangezogen werden.
- Durch regelmäßige und realistische Stresstests können möglicherweise neue Risikofaktoren identifiziert werden.

3.9 Einhaltung gesetzlicher Anforderungen

Die Einhaltung gesetzlicher, vertraglicher oder freiwilliger Regeln ist sicherzustellen. Hierzu sollte ein Überwachungssystem in die Betriebsabläufe implementiert werden und eine zuständige Stelle benannt werden. Auch das Recht unterliegt – ebenso wie die Technik oder die Bedrohungslage – einer fortwährenden Veränderung. Die Rechtsentwicklung sollte daher kontinuierlich und in geeigneter Form sondiert und deren Anwendung auf den Einzelfall geprüft werden. Eine Übersicht über einschlägige gesetzliche Regelungen des TKG gibt das nachfolgende Kapitel 4.

4 Rechtliche Sicherheitsanforderungen aus bereichsspezifischen Regelungen

Die zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen nach § 109 Abs. 1 und 2 TKG zielen auf den Schutz personenbezogener Daten, das Fernmeldegeheimnis und den Schutz der Telekommunikationsinfrastruktur und der Verfügbarkeit von Diensten ab. Diese Rechtsgüter sind nicht ausschließlicher Regelungsgegenstand des TKG. Insofern sind vom pflichtigen Unternehmen u. U. auch andere europäische, verfassungsrechtliche oder nationale Vorschriften zu beachten.

Die nachfolgenden Ausführungen befassen sich ausschließlich mit den bereichsspezifischen rechtlichen Anforderungen des TKG. So finden sich Regelungen zum Schutz des Fernmeldegeheimnisses bereichsspezifisch in §§ 88 ff. TKG. Dem Schutz personenbezogener Daten obliegen die §§ 91 ff. TKG. Gegenstand der §§ 100, 109 Abs. 5 TKG ist der Schutz der Telekommunikationsinfrastruktur vor Störungen und die Verfügbarkeit der Telekommunikationsdienste.

Unionsrechtliche Vorgaben, sich verändernde Sicherheitslagen und technische Entwicklungen führen zu einer fortwährenden Novellierung des TKG. Die pflichtigen Unternehmen sind zur Wahrung ihrer gesetzlichen Pflichten daher grundsätzlich gehalten, den Verlauf der einschlägigen Gesetzgebung und Rechtsprechung zu beobachten und ihre Anwendung auf den Einzelfall zu prüfen. Insofern können die nachfolgenden Hinweise lediglich einen bereichsspezifischen und momentanen Überblick über einzuhaltende Anforderungen darstellen.

4.1 Sicherheitsanforderungen zum Schutz des Fernmeldegeheimnisses (§ 88 TKG)

§ 88 TKG stellt die einfachrechtliche Ausprägung des verfassungsrechtlich verankerten Schutzes des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG dar. Das Gesetz trägt dem Umstand Rechnung, dass mit Liberalisierung des Telekommunikationsmarktes Telekommunikationsdienstleistungen durch Private erbracht werden und diese oftmals einer mittelbaren und damit nur relativen Grundrechtsbindung unterliegen. Vor diesem Hintergrund ergab sich die Notwendigkeit, den verfassungsrechtlichen Schutz aus Art. 10 Abs. 1 GG um eine Regelung auf einfachrechtlicher Ebene zu ergänzen und so die privaten Anbieter

ebenso wie die unmittelbar an Art. 10 Abs. 1 GG gebundenen staatlichen Stellen in die Pflicht zu nehmen.

Geschützt durch Art. 10 GG ist die Vertraulichkeit der Nutzung des zur Nachrichtenübermittlung eingesetzten technischen Mediums. Werden kommunikative Daten durch den Staat ohne Einwilligung zur Kenntnis genommen, aufgezeichnet, verwertet oder weitergegeben, so stellt dies ein Grundrechtseingriff dar. Wegen des Gleichklangs mit § 88 TKG verfolgt auch diese Vorschrift einen ähnlichen Inhalt. Im Unterschied zu Art. 10 GG entfaltet sich der Schutz jedoch nicht gegenüber dem Staat, sondern gegenüber den Diensteanbietern.
In Anlehnung an die verfassungsrechtliche Rechtsprechung zu Art. 10 Abs. 1 GG erfasst auch § 88 Abs. 1 TKG die näheren Umstände der Telekommunikation. Hierunter fallen alle Informationen über Zeit und Ort sowie Art und Weise des unkörperlichen Kommunikationsvorgangs, sofern diese eine Gefährdung der Vertraulichkeit des Kommunikationsvorgangs begründen können.

Im Hinblick auf die Einhaltung von Sicherheitsanforderungen zum Schutz des Fernmeldegeheimnisses soll auf folgendes hingewiesen werden:

- Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort.
- Es ist zu verhindern, dass Diensteanbieter sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation verschaffen.
- Gleichermaßen ist zu verhindern, dass sich unbefugte Dritte Kenntnisse über den Inhalt oder die näheren Umstände der Telekommunikation verschaffen.
- Zu berücksichtigen sind hierbei technische Einrichtungen zur mittelbaren und unmittelbaren Übertragung von Nachrichteninhalten, ferner auch Einrichtungen zur Erhebung, Verarbeitung und Nutzung von Verkehrsdaten (z.B. Teilnehmeranschluss, Netzabschlusspunkt, Vermittlungs- und Leitwegeinrichtungen, Verbindungsnetz sowie Billing- oder Fraud- Systeme).
- Im Bereich der Verwaltung und Verwahrung von Akten, welche dem Fernmeldegeheimnis unterliegen, sind für den Datenschutz hinreichend genügende Aufbewahrungsbehältnisse zu verwenden sowie entsprechende Räume mit Zutrittskontrolle sinnvoll einzusetzen.

- Es dürfen nur Personen Zugriff und Zugang haben, welche eine ausreichende Belehrung über die Sensibilität dieser Daten erhalten haben.
- Es muss sichergestellt werden, dass bei Nachrichtenübermittlungssystemen mit Zwischenspeicherung ausschließlich der Teilnehmer durch seine Einwilligung Inhalt, Umfang und Art der Verarbeitung bestimmt. Schutzmaßnahmen, die lediglich dem Teilnehmer selbst gestatten zu entscheiden, wer Nachrichteninhalte eingeben und darauf zugreifen darf, können durch entsprechende Zugangscodes und Kennwörter erfüllt werden. Diese werden nur dem Teilnehmer vertraulich übermittelt und sollen von diesem selbständig nach Erhalt verändert werden. Es liegt in der Einwilligungsfreiheit des Teilnehmers, an welche Person er die Zugangskennungen weitergibt.
- Schutzmaßnahme gegen eine ungerechtfertigte, entgegen dem Vertragsverhältnis vereinbarte Löschung von Nachrichteninhalten durch den Diensteanbieter kann beispielsweise das Anlegen von Backupsystemen sein.

4.2 Sicherheitsanforderungen zum Schutz der personenbezogenen Daten (§§ 91 ff. TKG)

Den bereichsspezifischen Datenschutz regelt der 2. Abschnitt des 7. Teils des TKG. Allgemeine datenschutzrechtliche Vorschriften der Datenschutz Grundverordnung (DSGVO) und die weiteren Regelungen des BDSG kommen ergänzend zur Anwendung.

Festgehalten werden kann, dass die DSGVO natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen dann keine zusätzlichen Pflichten auferlegt, wenn sie besonderen in der Richtlinie 2002/58/EG (ePrivacy-Richtlinie) festgelegten Pflichten unterliegen, welche dasselbe Ziel verfolgen (Art. 95 DSGVO). Dementsprechend kommen Vorschriften der DSGVO vorrangig zur Anwendung, außer einer entgegenstehenden Regelung des TKG erfolgt in Umsetzung der ePrivacy-Richtlinie. § 95 TKG wird daher beispielsweise weitestgehend von der DSGVO verdrängt werden: Denn die ePrivacy-Richtlinie enthält – bis auf wenige Ausnahmen – keine Regelungen zur Verarbeitung von Bestandsdaten. Hiervon ausgenommen sind lediglich § 95 Abs. 2 S. 2 und 3 TKG als Umsetzung von Art. 13 Abs. 2 ePrivacy-Richtlinie. Auf entsprechende Ausführungen wurde daher im Folgenden verzichtet.

§ 109 TKG stellt dagegen eine Umsetzung von Art. 4 Abs. 1 ePrivacy-Richtlinie sowie der Richtlinie 2002/21/EG (Rahmenrichtlinie) dar und ist insofern vorrangig anwendbar.

4.2.1 Informationspflichten (§ 93 TKG)

Die Informationspflichten sollen eine Ausübung des Rechts auf informationelle Selbstbestimmung sicherstellen, denn
„*Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.*“ (BVerfGE 1, 44)
Aus dieser Begründung des Bundesverfassungsgerichts wird auch deutlich, dass sich der verfassungsrechtliche Schutz nicht auf Eingriffe durch den Staat beschränken kann, sondern z. B. auch solche durch private Telekommunikationsunternehmen mit einbeziehen muss.

Die Erhebung, Verarbeitung und Nutzung von Bestands- und Verkehrsdaten der pflichtigen Telekommunikationsunternehmen kann u. a. in „Customer Care and Billing- Systemen“, in „Fraud- Systemen (§ 100 Abs. 3 TKG)“, in „Systemen zur Mitteilung ankommender Verbindungen (§ 101 TKG)“ oder in „Systemen zur Aufnahme in öffentliche Telefonverzeichnisse“ (§ 45m TKG) erfolgen.

Im Hinblick auf die Wahrung datenschutzrechtlicher Informationspflichten sind Art. 13 DSGVO und § 93 TKG zu beachten. In dieser Hinsicht sind auch nachfolgende Maßnahmen zu treffen:

- Es wird empfohlen, die Mitarbeiter durch geeignete Unterrichtsmaßnahmen für die Belange des Datenschutzes zu sensibilisieren. Es sollte daneben eine vertragliche Verpflichtungserklärung zur Wahrung des Datenschutzes von allen tangierten Mitarbeitern abgegeben werden.
- Den Teilnehmern sind bei Vertragsabschluss Name und Kontaktdaten des für die Verarbeitung Verantwortlichen mitzuteilen. Die Teilnehmer sind allgemein darüber zu unterrichten, welche Art von Daten zu welchen Zwecken und auf welcher Rechtsgrundlage verarbeitet werden sollen. Auch sind die Empfänger oder

Kategorien von Empfänger zu nennen, an die die personenbezogenen Daten der Teilnehmer übermittelt werden. Ist eine Übermittlung in ein Drittland, also ein Land außerhalb der EU und des Europäischen Wirtschaftsraumes, beabsichtigt, so muss dies ebenfalls gegenüber den Teilnehmern angegeben werden. Damit Betroffene wissen, wer der korrekte Ansprechpartner im Unternehmen für datenschutzbezogene Anliegen ist, müssen auch die Kontaktdaten des betrieblichen Datenschutzbeauftragten mitgeteilt werden. Ferner muss auf bestehende Betroffenenrechte – etwa das Recht auf Berichtigung oder Löschung – hingewiesen werden sowie das Recht auf Beschwerde bei der zuständigen Datenschutzbehörde. Die Teilnehmer sollten auf die zulässigen Wahl- und Gestaltungsmöglichkeiten (z. B. Verwendung der Bestandsdaten zur Beratung der Teilnehmer, zur Werbung für eigene Angebote, zur Marktforschung (§ 95 Abs. 2 TKG), Mitteilung des Einzelverbindungsnachweises (§ 99 Abs. 1 TKG), Mitteilung pauschal abgegoltener Verbindungen § 99 Abs. 1 TKG), Eintrag in Teilnehmerverzeichnisse (§ 104 TKG) und Auskunftserteilung (§ 105 TKG) hingewiesen werden.
- Die Teilnehmer sind über die ggf. besonderen Risiken der Verletzung der Netzsicherheit aufzuklären und ggf. auch über mögliche Abhilfen zu informieren.

4.2.2 Verkehrsdaten (§ 96 TKG)

Verkehrsdaten sind ebenso wie die Bestandsdaten den personenbezogenen Daten zuzurechnen. Im Gegensatz zu den Bestandsdaten unterliegen die Verkehrsdaten jedoch dem besonderen Schutz von Art. 10 GG bzw. § 88 TKG.

Die Vorschrift regelt das datenschutzgerechte Erheben und Verwenden und gibt den pflichtigen Unternehmen gleichzeitig Zulässigkeitsvoraussetzungen vor.
U.a. sind dies die folgenden:

- Das Erheben von Verkehrsdaten kann nur zulässig sein, soweit dies für einen der in Abschnitt 2 von Teil 7 des TKG genannten Zwecke erforderlich ist.
- Unter bestimmten weiteren Bedingungen kann die Ermittlung von Kommunikationsprofilen einzelner Teilnehmer und die Analyse von Verkehrsströmen zulässig sein, § 96 Abs. 3 S. 1 TKG.
- Die Verkehrsdaten sind i.d.R. vom Diensteanbieter nach Beendigung der Verbindung unverzüglich zu löschen, § 96 Abs. 1 S. 3 TKG. Auf den Leitfaden des/der BfDI und der BNetzA für eine datenschutzgerechte Speicherung von Verkehrsdaten (Stand 19.12.2012) wird verwiesen (abrufbar unter www.bundesnetzagentur.de/vds).

4.2.3 Entgeltermittlung und Entgeltabrechnung (§ 97 TKG)

Verkehrsdaten sind in aller Regel Grundlage für Datenverarbeitungstatbestände im Zusammenhang mit der Entgeltermittlung und -abrechnung. Die Vorschrift ist insofern eine bereichsspezifische Verwendungserlaubnis für Verkehrsdaten (§ 96 Abs. 1 TKG s.o.).
In dieser Hinsicht ist folgendes zu beachten:

- Sind bei der Erstellung von Telekommunikationsrechnungen oder der Erbringung von Telekommunikationsdienstleistungen Dritte eingebunden (z. B. durch Diensteanbieter ohne eigene Netzinfrastruktur), dann sind technische und organisatorische Schnittstellen-Beziehungen zwischen Auftraggeber (Diensteanbieter) und Auftragnehmer (Erfüllungsgehilfe) eindeutig zu regeln.
- Nicht benötigte Daten nach § 97 Abs. 3 TKG sind unverzüglich zu löschen.

4.2.4 Standortdaten (§ 98 TKG)

Standortdaten (§ 3 Nr. 19 TKG) können zu Bewegungsprofilen zusammengeführt werden, welche Rückschlüsse auf soziale Beziehungen oder Gewohnheiten zulassen. Standortdaten haben daher eine besonders hohe datenschutzrechtliche Relevanz.

- Standortdaten, die in Bezug auf die Nutzer von öffentlichen Telekommunikationsnetzen oder öffentlich zugänglichen Telekommunikationsdiensten verwendet werden, dürfen nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Umfang und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Teilnehmer dem Anbieter des Dienstes mit Zusatznutzen seine Einwilligung erteilt hat.
- Es ist ein Prozess zu gestalten, um die Verarbeitung von Standortdaten für jede Verbindung zum Netz oder für jede Übertragung auf einfache Weise und unentgeltlich zeitweise vom Nutzer zu untersagen.
- Die Übermittlung von Standortdaten für die Rufnummern nach § 98 Abs. 3 TKG (Notrufnummern 112 oder 110 oder der Rufnummer 124 124 und 116 117) ist sicherzustellen.
- Es ist sicherzustellen, dass die Verarbeitung von Standortdaten auf das erforderliche Maß beschränkt wird.

4.2.5 Einzelverbindungsnachweis (§ 99 TKG)

Der Teilnehmer wird mittels Einzelverbindungsnachweis (EVN) über Einzelheiten der in Rechnung gestellten Telekommunikationsdienstleistungen informiert. Der EVN dient daher der Kontrolle. Die Erstellung des EVN muss allerdings regelmäßig auf der Grundlage von Verkehrsdaten erfolgen. Da diese dem Fernmeldegeheimnis unterliegen, sollen in diesem Zusammenhang besondere datenschutzrechtliche Regeln beachtet werden
(§ 99 Abs. 1 TKG). Dies gilt insbesondere, wenn bestimmte Rechte der Mitbenutzer eines Telefonanschlusses betroffen sind (§ 99 Abs. 2 TKG).
Im Hinblick auf § 99 TKG wird auf folgendes hingewiesen:

- Dem Teilnehmer sind die gespeicherten Daten derjenigen Verbindungen, für die er entgeltpflichtig ist, nur dann mitzuteilen, wenn er vor dem maßgeblichen Abrechnungszeitraum in Textform einen Einzelverbindungsnachweis verlangt hat. Nur auf Wunsch dürfen ihm auch die Daten pauschal abgegoltener Verbindungen mitgeteilt werden.
- Auf Anfrage des Teilnehmers ist der Einzelverbindungsnachweis zur Verfügung zu stellen.
- Dem Teilnehmer muss nach Anfrage eines EVN die Möglichkeit gegeben werden, die von ihm gewählten Rufnummern ungekürzt oder gekürzt um die letzten drei Ziffern zu erhalten.
- Falls der EVN elektronisch versendet wird, müssen Maßnahmen zum Schutz des Fernmeldegeheimnisses und personenbezogener Daten getroffen werden.
- Durch Regelungen beim Pflichtigen ist die Nichterkennbarkeit der Verbindungen nach § 99 Abs. 2 TKG im EVN sicher zu stellen. Die Nichterkennbarkeit der Verbindungen ist sichergestellt, wenn die Verbindung im EVN nicht ausgewiesen ist.
- Die Liste der geschützten Beratungsstellen nach § 99 Abs. 2 S. 4 TKG ist quartalsweise vom pflichtigen Unternehmen bei der Bundesnetzagentur in einem automatisierten Verfahren abzurufen.
- Änderungen sind vom pflichtigen Unternehmen unverzüglich im Abrechnungsverfahren zu berücksichtigen.

4.2.6 Mitteilen ankommender Verbindungen (§ 101 TKG)

Die Vorschrift gewährt dem Teilnehmer in bestimmten Fällen nach einem vorgeschriebenen Verfahren ein Anspruch auf Auskunft über eingehende Anrufe (Fangschaltungsverfahren). Durch die gesetzliche Ausgestaltung dieses Fangschaltverfahrens sollen Teilnehmer die Möglichkeit erhalten, bei bedrohenden oder belästigenden Anrufen eine Auskunft über den

verursachenden Anschluss zu erhalten. Das Verfahren kommt insbesondere bei unterdrückten Rufnummern in Betracht und stellt für die Betroffenen oft die einzige Möglichkeit dar, erfolgversprechend rechtliche Schritte einzuleiten. Zu den Details wird auf den Gesetzestext verwiesen.

Die Bundesnetzagentur sowie der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit sind über die Einführung und Änderung des Verfahrens zur Sicherstellung des Fangschaltungsverfahrens unverzüglich in Kenntnis zu setzen.

4.2.7 Automatische Anrufweiterschaltung (§ 103 TKG)

Die Vorschrift bezweckt den Schutz des Teilnehmers vor ungewollter Weiterschaltung von Anrufen für einen Dritten auf seinen Anschluss. Die Schutzvorschrift steht allerdings unter dem Vorbehalt der technischen Realisierbarkeit.

4.2.8 Nachrichtenübermittlungssysteme mit Zwischenspeicherung (§ 107 TKG)

Manche Diensteanbieter bieten dem Kunden eine Möglichkeit, bestimmte Telekommunikationsinhalte für einen späteren Gebrauch zu speichern. Nachrichtenübermittlungssysteme werden insofern nicht in Echtzeit genutzt. Ein Speichern von Telekommunikationsinhalten kann jedoch auch eine erhebliche Gefahr für personenbezogene Daten sowie für das Fernmeldegeheimnis sein. Dieser Gefahr möchte § 107 TKG begegnen. Insofern wird auf das Folgende hingewiesen:

- Anbieter von Zwischenspeicherungsdiensten haben sicherzustellen, dass ausschließlich der Teilnehmer Inhalt, Umfang und Art der Verarbeitung bestimmt.
- Diensteanbieter haben die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um Fehlübermittlungen und das unbefugte Offenbaren von Nachrichteninhalten innerhalb seines Unternehmens oder an Dritte auszuschließen.

4.3 Sicherheitsanforderungen zum Schutz der Telekommunikationsinfrastruktur und der Verfügbarkeit der Telekommunikationsdienste

4.3.1 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten (§ 100 TKG)

Zum Erkennen, Eingrenzen oder Beseitigen von Störungen darf der Diensteanbieter im erforderlichen Umfang Bestands-, Verkehrs- und Steuerdaten erheben und verwenden. § 100 Abs. 1 TKG normiert insofern einen datenschutzrechtlichen Erlaubnistatbestand. Dieser ist in bestimmten Fällen mit einer Berichtspflicht verknüpft. Allgemeine Hinweise zur Berichtspflicht nach § 100 Abs. 1 TKG und deren Geltung sind unter www.bundesnetzagentur.de/TKG100 abrufbar.

Zum Erkennen und Eingrenzen von Störungen ist dem Betreiber einer Telekommunikationsanlage unter engen Voraussetzungen auch das Aufschalten auf bestehende Verbindungen gestattet. Eventuell entstandene Aufzeichnungen sind jedoch unverzüglich zu löschen. Mit diesem datenschutzrechtlichen Eingriff ist eine Informationspflicht gegenüber dem betrieblichen Datenschutzbeauftragten verbunden (vgl. insgesamt § 100 Abs. 2 TKG).

Liegen Anhaltspunkte für Leistungserschleichung oder Betrug vor, so kann der Diensteanbieter zur Sicherung seines Anspruches unter bestimmten Voraussetzungen Bestands- und Verkehrsdaten verwenden. In diesem Zusammenhang sind Informationspflichten gegenüber der Bundesnetzagentur und dem/der Bundesbeauftragten für den Datenschutz zu beachten.

4.3.2 Beträchtliche Sicherheitsverletzungen (§ 109 Abs. 5 TKG)

Netzbetreiber und Diensteerbringer haben sowohl tatsächlich eingetretene als auch mögliche beträchtliche Sicherheitsverletzungen unverzüglich der Bundesnetzagentur und dem Bundesamt für Sicherheit in der Informationstechnik mitzuteilen. Auf das aktuell gültige Umsetzungskonzept zur Meldung von Vorfällen wird verwiesen (Stand: 10.11.2017, Version: 4.0, ABl. BNetzA Nr. 22 v. 22.11.2017).

4.3.3 Daten- und Informationssicherheit (§ 109a TKG)

Die Vorschrift regelt bestimmte Informationspflichten im Falle einer Verletzung des Schutzes personenbezogener Daten („Datenschutzpanne“ oder „Security Breach“). Dem pflichtigen Unternehmen obliegen in diesem Zusammenhang bestimmte Benachrichtigungspflichten gegenüber dem Betroffenen, aber auch gegenüber der Bundesnetzagentur und dem/der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Auf die Hinweise der Bundesnetzagentur, abrufbar unter www.bundesnetzagentur.de/109a. („Benachrichtigungspflichten im Fall einer Verletzung des Schutzes personenbezogener Daten“) wird verwiesen.

Gehen Verletzungen der IT-Sicherheit von einem nutzerbetriebenen datenverarbeitenden System aus, so ergibt sich für das pflichtige Unternehmen eine Informationspflicht des Nutzers aus § 109a Abs. 4 TKG. Dem pflichtigen Unternehmen wird durch die Umleitung innerhalb der eigenen Netze die Möglichkeit eingeräumt, den betroffenen Nutzer, zunächst zu identifizieren und ihn anschließend in die Lage zu versetzten, die Störung zu beseitigen (sog. „Sinkholing“).

Nicht erforderlich ist eine individuelle Untersuchung der Technik oder eine individuelle Beratung durch den Anbieter. Soweit eine Benachrichtigung der betroffenen Nutzerinnen und Nutzer innerhalb von wenigen Tagen technisch nicht möglich ist, werden die Anbieter nur ihre Teilnehmerinnen und Teilnehmer informieren und auf Hilfsmittel hinweisen können.

Die Formulierung „soweit ihm diese bereits bekannt sind“ macht deutlich, dass zur Ermittlung der Nutzer nur auf solche Verkehrsdaten zugegriffen werden darf, die vom Unternehmen bereits aufgrund anderer Vorschriften erhoben und gespeichert wurden. Eine Erhebung weiterer Daten ausschließlich zum Zweck der Durchführung einer Benachrichtigung ist somit nicht zulässig (BT-Drs. 18/4096, S. 37).

§ 109a Abs. 5 TKG gestattet, den Datenverkehr bei Vorliegen einer Störung einzuschränken, umzuleiten oder zu unterbinden. Angesichts steigender Zahlen von IT-Sicherheitsvorfällen sollen diese Befugnisse deren Behebung insbesondere dann ermöglichen, wenn ein Nutzer, von dessen Systemen die Störung ausgeht, diese trotz einer erfolgten Information nicht beseitigt oder eine unverzügliche Beseitigung nicht zu erwarten ist und zur Beseitigung oder Verhinderung der Beeinträchtigung ein Eingriff in die Nutzung des Telekommunikationsdienstes erforderlich ist.

Das pflichtige Unternehmen kann ferner nach § 109a Abs. 6 TKG den Datenverkehr zu Störungsquellen einschränken oder unterbinden, um der Entstehung von Störungen in den Telekommunikations- und Datenverarbeitungssystemen der Nutzer zu begegnen. Die Befugnis wurde pflichtigen Unternehmen eingeräumt, da Angreifer in der Regel modulare

Angriffswerkzeuge nutzen, um Telekommunikations- und Datenverarbeitungssysteme zu infizieren (BT-Drs. 18/11808, S. 11).

5 Umsetzung von Sicherheitsanforderungen

Aus § 109 Abs. 4 TKG ergeben sich für Betreiber öffentlicher Telekommunikationsnetze und Erbringer öffentlich zugänglicher Telekommunikationsdienste unterschiedliche Pflichten, welche zeitlich abgestuft zu erfüllen sind. Grundsätzlich gilt sowohl für Netzbetreiber als auch für Diensteerbringer eine Pflicht zur Erstellung eines Sicherheitskonzeptes. Ebenso grundsätzlich ist von beiden ein Sicherheitsbeauftragter zu benennen. Nur für den Netzbetreiber sieht das Gesetz mit Betriebsaufnahme eine Vorlagepflicht für das erstellte Sicherheitskonzept bei der Bundesnetzagentur vor. Für den Diensteerbringer besteht keine gesetzliche Vorlagepflicht. Er kann aber von der Bundesnetzagentur hierzu verpflichtet werden. Neben diesen Erstellungs-, Benennungs- und Vorlagenpflichten ist auch eine Erklärungspflicht zu erfüllen. Sie bezieht sich auf die tatsächliche Umsetzung der sicherheitskonzeptionellen Überlegungen. Ändern sich die Gegebenheiten, so sieht das Gesetz für das betreffende Unternehmen eine Anpassungspflicht vor.

Die sicherheitskonzeptionellen Pflichten nach § 109 Abs. 4 TKG dienen der Ermittlung und Strukturierung geeigneter und angemessener Maßnahmen zum Schutz von Fernmeldegeheimnis, Datenschutz und Funktionsfähigkeit von Netzen und Diensten. Der vorliegende Katalog für Sicherheitsanforderungen ist Vorgabe zur Erfüllung dieser Pflichten.

Die Bundesnetzagentur prüft die Vorlage und regelmäßig auch die Umsetzung des unternehmerischen Sicherheitskonzepts. Stellt sie in diesem Zusammenhang ein Sicherheitsmangel fest, so kann sie die Beseitigung des festgestellten Mangels verlangen. Hiervon zu unterscheiden ist die Überprüfung durch eine qualifizierte unabhängige Stelle nach § 109 Abs. 7 TKG. Im Fokus dieser Überprüfung steht nicht das Sicherheitskonzept des Unternehmens oder dessen Umsetzung. Gegenstand dieser Untersuchung ist allein die Frage, ob die Sicherheitsanforderungen aus § 109 Abs. 1 bis 3 TKG im Einzelfall erfüllt sind. Die Überprüfung nach § 109 Abs. 7 TKG soll daher die Sicherheitseinschätzung des Unternehmens mit einer Dritten abgleichen. Auch im Rahmen dieser Prüfung ist auf Kataloginhalte zurückzugreifen. Der Katalog ist daher sowohl Handlungs-, als auch Prüfungsgrundlage.

5.1 Umsetzung von Sicherheitsanforderungen

Das Gesetz gibt dem Sicherheitskonzept einen bestimmten Inhalt vor. Im Einzelnen ergibt sich dieser aus § 109 Abs. 4 Nr. 1 – 3 TKG: Das Konzept muss insofern einen deskriptiven Bericht (§ 109 Abs. 4 Nr. 1 TKG), eine Gefährdungsanalyse (§ 109 Abs. 4 Nr. 2 TKG) und korrespondierend hierzu die im Einzelfall festgelegten Schutzmaßnahmen (§ 109 Abs. 4 Nr. 3 TKG) vorweisen. Auf die Grundlagen der praktischen Umsetzung dieser Anforderungen soll nachfolgend eingegangen werden.

5.1.1 Beschreibung der betriebenen öffentlichen Telekommunikationsnetze

Der gesetzlichen Vorgabe aus § 109 Abs. 4 Nr. 1 1. HS TKG ist regelmäßig mit der Erstellung und Vorlage eines Netzstrukturplanes genüge getan. Der erstellte Plan sollte zumindest folgende Strukturelemente beschreiben:

1. Alle Telekommunikations- und Datenverarbeitungs-Systeme (Vermittlungseinrichtungen, Dienste-Server, Netzwerkmanagement) und alle eingesetzten DV-Anlagen (Kundendatenverwaltung, Billing), welche in das Netz eingebunden sind.
2. Alle Verbindungen zwischen den Systemen (LAN-Verbindungen, Backbone-Techniken, auch Funkstrecken).
3. Alle Außenverbindungen (Schnittstellen) der Systeme (Art der Verbindung, Internet, Remote, Roaming).
4. Größe und Art des Netzes (Anzahl Teilnehmer; Mobilfunk- Richtfunk- oder Kabelnetz etc.).
5. Geographische Ausdehnung des Netzes (lokal, regional, national oder international).

Die Komplexität des Netzplans kann hierbei durch Gruppenbildung vereinfacht werden (z.B. nach Typ, Konfiguration, Netz, Lokation, Rahmenbedingungen, Anwendungen, Dienste, etc.). Ebenso können bei größeren Netzen getrennte Teilpläne (z.B. für Auftragsdatenverarbeitung, Abrechnungssysteme, Backbone-Netze etc.) sinnvoll sein.

5.1.2 Beschreibung der erbrachten öffentlich zugänglichen Telekommunikationsdienste

Grundsätzlich sind alle öffentlichen Telekommunikationsdienste, welche vom Unternehmen erbracht werden, inhaltlich zu beschreiben gemäß § 109 Abs. 4 Nr. 1 2. HS TKG. Zur Erstellung der Gefährdungsanalyse ist es sinnvoll, nicht nur auf Inhalte, sondern auch auf

den jeweiligen Teilnehmerkreis abstrakt einzugehen. Werden lediglich Dienste erbracht, so ist dennoch darauf hinzuweisen, welche TK- Netze hierbei zum Einsatz kommen.

5.1.3 Einstufung der Kritikalität

Aus dem Sicherheitskonzept hat hervorzugehen, von welchen Gefährdungen auszugehen ist, § 109 Abs. 4 Nr. 2 TKG. Zur Erstellung dieser Prognose wird die Vornahme einer Gefährdungsanalyse – regelmäßig bestehend aus einer Schutzbedarfs-, Bedrohungs- und Risikoanalyse – erforderlich. Der bereits festgestellte deskriptive Befund (5.1.1. und 5.1.2) ermöglicht hierbei eine abstrakte Gefährdungsanalyse und eine Zuordnung zu bestimmten Gefährdungslagen (Kritikalitäten). Maßgeblich für die Bestimmung einer Kritikalität ist die Bedeutung des zu schützenden Telekommunikationsnetzes oder –dienstes. Im Grundsatz können öffentliche Telekommunikationsnetze und –dienste folgenden Kritikalitätsstufen zugeordnet werden:

Standardkritikalität: Alle öffentlichen Telekommunikationsnetze und -dienste.

Gehobene Kritikalität: Öffentliche Telekommunikationsnetze und –dienste, sofern sie für das Gemeinwohl eine größere Bedeutung haben.

Erhöhte Kritikalität: Öffentliche Telekommunikationsnetze und –dienste, sofern sie für das Gemeinwohl eine herausragende Bedeutung haben.

Standardkritikalität

Aus verfassungsrechtlicher Sicht muss im Mindestmaß der Bedeutung der durch § 109 Abs. 1 und 2 TKG zu schützenden Rechtsgüter (Fernmeldegeheimnis, Datenschutz und Funktionsfähigkeit des Netzes) für den Einzelnen Rechnung getragen werden. Eine (untere) Standardkritikalität müsste insofern diese Bedeutung zugrunde legen und die Beachtung damit korrespondierender Grundlagen sicherstellen. Sicherheitsanforderungen dieser Art ergeben sich im Wesentlichen aus dem Hauptteil des Kataloges für Sicherheitsanforderungen.

Gehobene Kritikalität

Wird das/der zu schützende Netz/Dienst von einer größeren Zahl von Teilnehmern genutzt, so steigt die Bedeutung des jeweiligen Netzes/Dienstes. Neben der Bedeutung für den Einzelnen bestehen auch Gemeinwohlinteressen. Diese Gemeinwohlinteressen können ab

einer bestimmten Anzahl gewichtig werden. Ein Anhaltspunkt für die Bestimmung einer bedeutenden Teilnehmerzahl kann sich aus dem Post- und Telekommunikationssicherstellungsgesetz (PTSG) ergeben. Denn das PTSG dient u.a. der Funktionsfähigkeit des Gemeinwesens durch Sicherstellung einer grundlegenden Versorgung mit Telekommunikationsdiensten. Der Anwendungsbereich des Gesetzes knüpft in diesem Schutzzusammenhang an das Angebot von Telekommunikationsdiensten für mehr als 100.000 Teilnehmer an. Die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) greift bei der Bestimmung von Schwellenwerten ebenfalls auf die genannten Werte des PTSG zurück. Es erscheint daher angemessen, bei Angeboten von Telekommunikationsdiensten oder Betreiben von Telekommunikationsnetzen mit einer entsprechenden Teilnehmerzahl eine besondere Bedeutung des Netzes oder des Dienstes im Sinne von § 109 Abs. 2 S. 5 TKG zu vermuten und eine gehobene Kritikalität anzunehmen.

Erhöhte Kritikalität

Neben der Teilnehmerzahl können auch Besonderheiten des zu schützenden Telekommunikationsnetzes/-dienstes auf eine bestimmte Bedeutung für das Gemeinwohl hindeuten oder zumindest die Annahme einer besonderen Bedeutung weiter erhärten. Dem öffentlichen Mobilfunknetz kommt in diesem Zusammenhang eine Sonderstellung zu. Denn beim Mobilfunknetz ist von einer querschnittlichen Verwendung in allen Bereichen des öffentlichen Lebens auszugehen. Die Verfügbarkeit und Sicherheit dieses Netzes betrifft daher mit hoher Wahrscheinlichkeit nicht nur den Einzelnen, sondern Staat, Wirtschaft und Gesellschaft gleichermaßen.
Eine enorme Sonderstellung kommt dem Betrieb von 5G-Netzen im Sinne der EU-Empfehlung 2019/534 vom 26. März 2019 zu. 5G-Netze sind in diesem Sinn das künftige Rückgrat unserer zunehmend digitalisierten Volkswirtschaften und Gesellschaften. Sie werden Milliarden von Objekten und Systemen mit einander und auch in den Kritischen Infrastrukturen der Sektoren Energie, Wasser, Ernährung, Gesundheit, Finanz- und Versicherungswesen, Transport und Verkehr sowie dem Sektor Informationstechnik und Telekommunikation sensible Informationen verarbeiten und Sicherheitssysteme unterstützen. Werden daher öffentlich zugängliche 5G- Mobilfunknetze mit einer Teilnehmerzahl von mehr als 100.000 Teilnehmern betrieben, so kann eine herausragende Bedeutung dieser Telekommunikationsnetze für das Gemeinwohl indiziert sein.

Lässt sich aus der Teilnehmerzahl und/oder den Besonderheiten des zu schützenden Telekommunikationsnetzes/-dienstes eine herausragende Bedeutung ableiten, so kann von einer erhöhten Kritikalität ausgegangen werden. Einer erhöhten Kritikalitätsstufe unterfallen

derzeit lediglich öffentliche Telekommunikationsnetze des Mobilfunks der 5. Generation mit Frequenzzuteilungen.

5.1.4 Konkrete Gefährdungsanalyse

Bei der sich anschließenden, konkreten Gefährdungsanalyse geht es - unabhängig von der vorher erfolgten abstrakten Zuordnung zu einer bestimmten Kritikalität - darum, die im Einzelfall tatsächlich betriebenen Komponenten zu ermitteln und zu bewerten.
Es sind daher zunächst alle sicherheitsrelevanten Komponenten des Unternehmens zu ermitteln. Sicherheitsrelevante Komponenten in diesem Sinn können alle Teilsysteme / Systeme oder Geschäftsprozesse mit Bezug zum Fernmeldegeheimnis, Datenschutz und zur Verfügbarkeit von TK- Netzen und TK- Diensten sein. Sicherheitsrelevante Komponenten können sich aber auch aus der Organisation ergeben. Insofern ist die jeweilige Sicherheitsorganisation des Unternehmens (Abschnitt 3.1) ebenfalls einer entsprechenden Gefährdungsanalyse zuzuführen. Prognostiziert werden soll im Einzelfall die Sicherheit von Daten, Systemen und Einrichtungen (Abschnitt 3.3) oder des jeweiligen Betriebes (Abschnitt 3.4). Weitere Hinweise zu diesen Themen liefern die BSI-Standards, sowie die Bausteine des BSI IT-Grundschutz-Kompendiums, unter anderem bezüglich Infrastruktur, IT-Systemen, Netzen und Anwendungen.
Auch hier liefert das BSI IT-Grundschutz-Kompendium wichtige Hinweise auf elementare Gefährdungen aus den Bereichen höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen, vorsätzliche Handlungen.

5.1.5 Gefährdungsanalyse des Gesamtsystems

Eine Gefahrenlage kann sich nicht nur isoliert aus gefährdeten betrieblichen Einzelkomponenten oder aus der abstrakten Zuordnung eines Netzes ergeben. Auch das Zusammenwirken verschiedener Teilprozesse kann bestimmte Gefährdungen auslösen und weitere Schutzmaßnahmen bedingen. In dieser Hinsicht ist daher eine zusätzliche Bewertung des Gesamtsystems erforderlich.
Nicht immer können alle Gefahrenquellen identifiziert werden. Ein entsprechendes Dunkelfeld sollte daher berücksichtigt werden. In einer abschließenden Risikobewertung ist dieses bestehende Restrisiko näher zu beschreiben und zu bewerten. Ziel sollte jedoch eine Identifizierung aller Gefährdungen oder aber eine Reduzierung auf ein quantifizierbares und akzeptables Maß sein.

5.1.6 Festlegung und Beschreibung der technischen Vorkehrungen oder sonstigen Schutzmaßnahmen

1. Nach Abschluss der Gefährdungsanalyse müssen vom pflichtigen Unternehmen geeignete, erforderliche und angemessene Schutzmaßnahmen ausgewählt und implementiert werden.
Maßgeblich für die Auswahl und Festlegung ist grundsätzlich immer eine Beurteilung des Einzelfalls.

Bei der Festlegung der Maßnahme ist der Stand der Technik zu berücksichtigen. Mit der Verpflichtung zur Berücksichtigung des Standes der Technik wird eine dynamische Anpassung an die sich wandelnden technischen Möglichkeiten und Risiken notwendig. Die Beurteilung der Schutzmaßnahmen ist insofern nicht abschließender, sondern fortlaufender Natur. Der Rückgriff auf den Stand der Technik umfasst hierbei aber nicht Verfahren, die in der Praxis noch nicht eingesetzt werden. Dem Stand der Technik entsprechende Maßnahmen müssen sowohl marktreif als auch in der Praxis erprobt sein.

Bei der Festlegung von Maßnahmen spielt auch die Interessenlage des Unternehmens eine Rolle. Die im Einzelfall zu treffenden Schutzmaßnahmen sind nur dann angemessen, wenn der technische und wirtschaftliche Aufwand in einem angemessenen Verhältnis zur Bedeutung der zu schützenden Rechte und zur Bedeutung der zu schützenden Einrichtungen für die Allgemeinheit steht. Ein Missverhältnis zwischen zu betreibendem Aufwand und Nutzen für die Allgemeinheit darf nicht bestehen.

Für neu festzulegende Schutzmaßnahmen kann in diesem Zusammenhang im Einzelfall ein Bestandsschutz berücksichtigt werden. Schutzmaßnahmen, welche auf der Grundlage des „Kataloges von Sicherheitsanforderungen“ (Version 1.1 v. 07.01.2016) erstellt wurden, können daher im Einzelfall weiterhin als angemessen erachtet werden. Voraussetzung ist jedoch, dass sich keine aktuellen Änderungen der betriebenen öffentlichen TK- Netze oder der erbrachten öffentlich zugänglichen TK- Dienste und damit eine Änderung der Gefährdungslage feststellen lassen. Voraussetzung ist ferner, dass der Lebenszyklus der eingesetzten Technik in den betriebenen Netzen oder den angebotenen Diensten überschaubar ist. Das erstellte Sicherheitskonzept muss in diesen Fällen nicht ersetzt oder erneut vorgelegt werden. Abweichungen aufgrund eines Bestandsschutzes sind jedenfalls zu dokumentieren und darzulegen, dass die bestehenden Maßnahmen hinreichend sind.

2. Auf Grundlage der abstrakten Gefährdungsanalyse können nachfolgende Grundsätze für die Auswahl von Schutzmaßnahmen gelten:

Standardkritikalität: Die zu treffenden technischen, organisatorischen, personellen und infrastrukturellen Maßnahmen müssen geeignet sein, ein allgemein anerkanntes Sicherheitsniveau zu gewährleisten. Eine Auswahl konkreter Empfehlungen bietet der IT-Grundschutz des BSI. Die Bausteine des IT-Grundschutz-Kompendiums sind in zehn Schichten aufgeteilt und beschäftigen sich mit unterschiedlichsten Themen der Informationssicherheit – von Anwendungen (APP) über Industrielle IT (IND) bis hin zu Sicherheitsmanagement (ISMS). Im Einzelfall kann zum Schutz des Fernmeldegeheimnisses ein höheres Schutzniveau erforderlich sein.

Gehobene Kritikalität: Die zu treffenden Maßnahmen müssen geeignet sein, einen allgemein anerkannten Grundschutz sowie einen erhöhten Schutz für die Bereiche, die maßgeblich für die gehobene Einstufung der Kritikalität relevant sind, zu gewährleisten. Zusätzlich sind erforderliche und angemessene Maßnahmen gegen erhebliche Störungen infolge von Naturkatastrophen, besonders schweren Unfällen, Sabotagehandlungen, terroristischen Anschlägen oder sonstigen vergleichbaren Ereignissen zu treffen. Geeignete und angemessene Maßnahmen in dieser Hinsicht sind auch für den Spannungs- oder Verteidigungsfall vorzusehen. Betroffen sind hierbei insbesondere Maßnahmen der Notfallvorsorge. Hilfe bei der Auswahl konkreter Maßnahmen bietet das BSI IT-Grundschutz-Kompendium.

Erhöhte Kritikalität: Die zu treffenden Maßnahmen müssen geeignet sein, einen allgemein anerkannten Schutz zu gewährleisten, der zusätzlich zum allgemeinem Schutzbedarf (erhöhter Grundschutz) auch der besonderen Kritikalität Rechnung trägt. Betreiber öffentlicher TK- Netze und Erbringer öffentlich zugänglicher TK- Dienste, die dieser Gruppe zuzuordnen sind, haben zusätzlich die Sicherheitsanforderungen und Maßnahmen gemäß Anlage 2 einzuhalten.

TK-Diensteanbieter mit IP-Infrastruktur haben bei der Festlegung von Schutzmaßnahmen zusätzlich die Anforderungen und Hinweise gemäß Anlage 1 „Anforderungen an TK-Diensteanbieter mit IP-Infrastruktur“ zu berücksichtigen.

Entscheidend für die Festlegung der Schutzmaßnahmen ist jedoch nicht die abstrakte Zuordnung zu einer Gefahrenlage, sondern immer das Ergebnis der konkreten, individuellen Gefährdungsanalyse. Die Zuordnung eines Netzes oder Dienstes zu einer bestimmten Kritikalität kann jedoch indizierende Wirkung haben. Ergänzend ist in allen Fällen die Gesamtprognose zu berücksichtigen.

Das pflichtige Unternehmen ist grundsätzlich nicht gezwungen, die Festlegung von Schutzmaßnahmen auf der Grundlage der vorstehend beschriebenen Analyse zu betreiben. Eine Festlegung kann auch auf der Grundlage geeigneter Standards und Normen (z.B. BSI-Standards, BSI-IT-Grundschutz-Methodik, DIN ISO/IEC-Normen) erfolgen.

5.1.7 Sicherheitskonzept erstellen

Nach Abschluss der Gefahrenanalyse und Festlegung der im Einzelfall zu treffenden Maßnahmen ist das Konzept zu erstellen. Es muss sich dabei um ein inhaltlich zusammenhängendes Dokument handeln. Lediglich mündliche Mitteilungen oder fernmündliche Erklärungen entsprechen nicht diesen Anforderungen.

5.1.8 Benennung des Sicherheitsbeauftragten

Nicht unmittelbarer Bestandteil des Sicherheitskonzepts ist die Benennung des Sicherheitsbeauftragten. Die Benennung hat jedoch, ebenso wie die Konzepterstellung, mit Aufnahme des Betriebes oder Angebot des Dienstes zu erfolgen. Insofern besteht zwischen diesen Pflichten ein zeitlicher, aber auch inhaltlicher Zusammenhang. Dem Sicherheitsbeauftragten sollten u.a. bestimmte Koordinations-, Kontroll- und Fachaufgaben zukommen. Der Sicherheitsbeauftragte oder der benannte Stellvertreter sollte gleichzeitig Ansprechpartner der Bundesnetzagentur sein.
Dieser Aufgabenwahrnehmung entsprechend sollte die Stelle die notwendigen Fachkenntnisse sowie das Verständnis der Unternehmensabläufe nachhalten. Das Wissen der Stelle um die Entwicklungen in der IT-Sicherheit, die Prozesse im Unternehmen und die rechtlichen Rahmenbedingungen muss aktuell gehalten werden. Es sind die Voraussetzungen für einen direkten Kontakt zur Unternehmensleitung zu schaffen.

5.1.9 Umsetzungserklärung

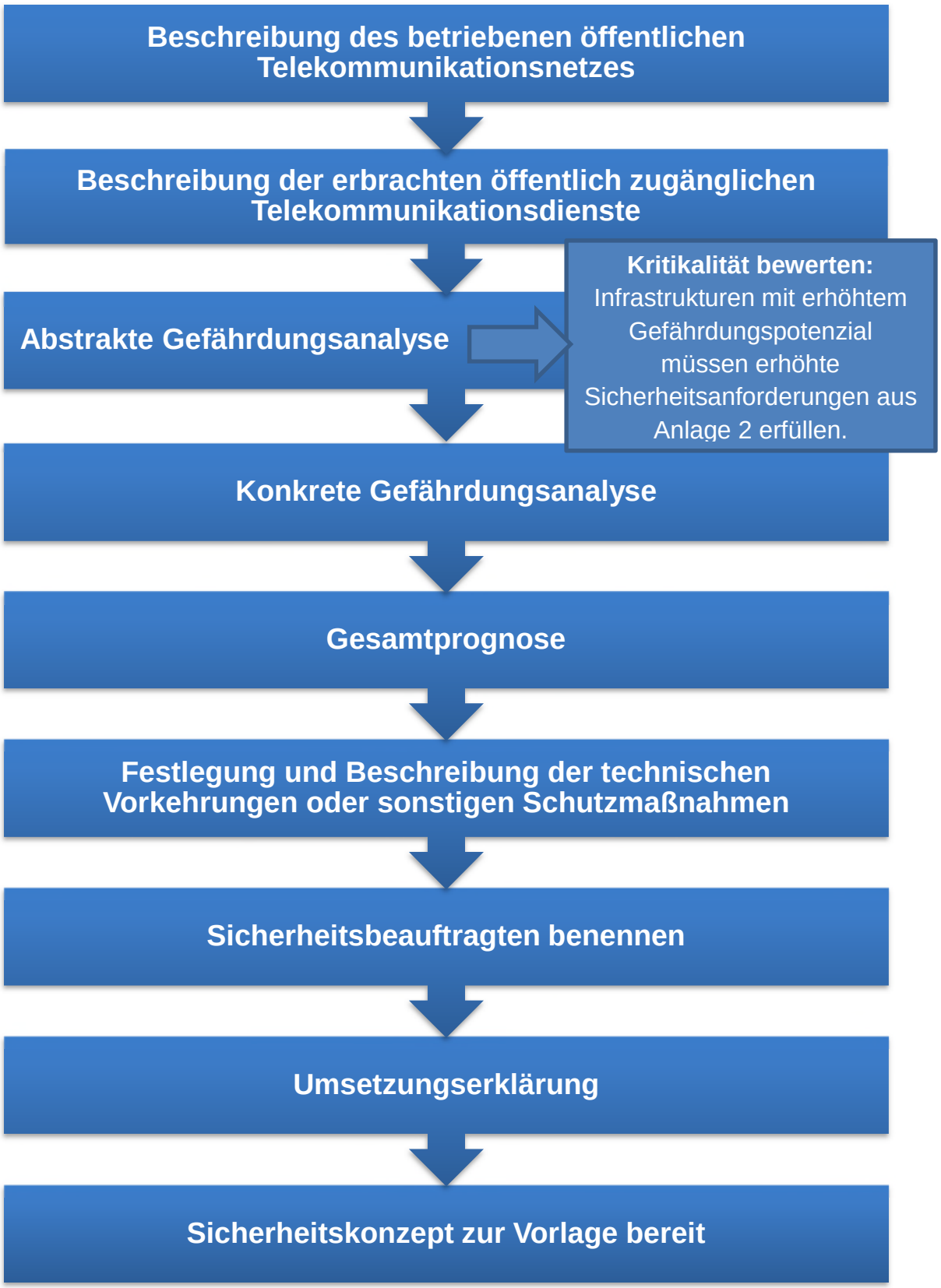
Mit dem Sicherheitskonzept ist eine Erklärung vorzulegen, dass die darin aufgezeigten technischen Vorkehrungen und sonstigen Schutzmaßnahmen umgesetzt sind oder unverzüglich umgesetzt werden. Die Erklärung muss in Schriftform erfolgen.

5.1.10 Sicherheitskonzept an Veränderungen anpassen

Die Sicherheit von Telekommunikationsnetzen und -diensten ist ein kontinuierlicher Verbesserungsprozess. Das Sicherheitskonzept muss daher regelmäßig überprüft und bei Änderungen angepasst werden. Es muss sichergestellt sein, dass auf technische

Entwicklungen, erkannte Schwachstellen und aufgedeckte Sicherheitslücken reagiert wird und geeignete Schutzmaßnahmen ergriffen werden.
Um den Erfolg der Schutzmaßnahmen in einem sich ständig ändernden Umfeld (Geschäftsprozesse, IT-Landschaften, Gesetze und Vorgaben, Bedrohung etc.) dauerhaft sicherzustellen, ist zu gewährleisten, dass in regelmäßigen Abständen die Wirksamkeit der umgesetzten Sicherheitsmaßnahmen festgestellt und bewertet wird. Bei erkannten Sicherheitsproblemen sind systematisch Verbesserungsmaßnahmen zu ergreifen, umzusetzen und zu dokumentieren. Sofern sich die dem Sicherheitskonzept zugrundeliegenden Gegebenheiten ändern, hat der Verpflichtete das Konzept anzupassen und der Bundesnetzagentur unter Hinweis auf die Änderungen erneut vorzulegen.

5.1.11 Vorgehensweise zur Erstellung des Sicherheitskonzepts



6 Inkrafttreten und Übergangsregelungen

Der Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten tritt mit Veröffentlichung im Amtsblatt der Bundesnetzagentur in Kraft. Die Verpflichteten haben die Anforderungen des Katalogs spätestens ein Jahr nach dessen Inkrafttreten zu erfüllen, soweit im Katalog keine speziellen Übergangsregelungen genannt sind.

Informationsquellen:

ENISA Technical Guideline on Security measures for Article 4 and Article 13a:

BSI Standard 200-2:

BSI IT-Grundschutz-Kompendium:

Deutsche Fassung EN ISO/IEC 27001:2017

Deutsche Fassung EN ISO/IEC 27002:2017

7 Begriffsbestimmungen

ENISA

European Agency for Cybersecurity / Agentur der Europäischen Union für Cybersicherheit (vormals European Network, Information Security Agency / Europäische Agentur für Netz und Informationssicherheit.

Verkehrsdaten, § 3 Nr. 30 TKG

Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden.

Diensteanbieter, § 3 Nr. 6 TKG

Jeder, der ganz oder teilweise geschäftsmäßig

- Telekommunikationsdienste erbringt oder
- an der Erbringung solcher Dienste mitwirkt.

Teilnehmer, § 3 Nr. 20 TKG

Jede natürliche oder juristische Person, die mit einem Anbieter von **öffentlich zugänglichen** Telekommunikationsdiensten einen Vertrag über die Erbringung derartiger Dienste geschlossen hat**.**

Bestandsdaten, § 3 Nr. 3 TKG

Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden.

Telekommunikationsanlagen, § 3 Nr. 23 TKG

Technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können.

Telekommunikationsdienste, § 3 Nr. 24 TKG

In der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen.

Personenbezogene Daten

Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Schutzziele

Allgemeine Schutzziele sind der Schutz personenbezogener Daten und der Schutz des Fernmeldegeheimnisses. Besondere Schutzziele sind der Schutz der Telekommunikationsinfrastruktur vor Störungen und Risiken sowie die Verfügbarkeit der Telekommunikationsdienste.

Anlage 1: Anforderungen an TK-Diensteanbieter mit IP-Infrastruktur

Anlage 2: Zusätzliche Sicherheitsanforderungen für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial

Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten

nach
§ 109 Telekommunikationsgesetz (TKG)
Version 2.0

Anlage 1

Anforderungen an TK-Diensteanbieter mit IP-Infrastruktur

Stand: 29.04.2020

Inhaltsverzeichnis

1 Einleitung

Die Anbindung eines TK-Systems an das Internet oder die Erbringung von TK-Diensten im Internet birgt erhebliches Gefahrenpotential für die angeschlossenen TK-, DV-Systeme und deren Nutzer.

Ein Überblick der aktuellen Gefährdungen finden sich beispielsweise in den jährlich herausgegeben Lageberichten des BSI[1], und der ENISA[2].

Aufgrund dieser spezifischen Gefährdungslage sowie aufgrund der Bedeutung des Internets im geschäftlichen und privaten Bereich sind durch die TK-Anbieter mit IP-Infrastruktur geeignete Sicherheitsvorkehrungen zu treffen. Diese Anlage beschreibt technische und organisatorische Maßnahmen zur Verbesserung der Internetsicherheit. Diese Maßnahmen sind entsprechend dem jeweiligen Stand der Technik umzusetzen.

Ergänzende Empfehlungen sind u. a. den Schriftenreihen zur Internetsicherheit (ISi-Reihe) und den Cybersicherheitsempfehlungen für Internet-Service Provider des BSI zu entnehmen.

---

[1] BSI Lagebericht (https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html)

[2] „ENISA Threat Landscape Report“ (https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape)

2 Infrastruktur

2.1 Routing und Protokolle

Stehen zur Implementierung eines Dienstes verschiedene Standards oder Protokollvarianten zur Verfügung, so ist nach sorgfältiger Abwägung eine gemäß Stand der Technik als am sichersten einzuschätzende Lösung zu implementieren.

2.1.1 Verschlüsselungstechnik

Der TK-Anbieter muss an sicherheitsrelevanten Stellen eine Verschlüsselung von Daten nach Stand der Technik vornehmen. Insbesondere müssen Passwörter nach aktuellem Stand der Technik zumindest gehasht und mit einem Salt versehen und gespeichert werden.
Neben einer Verschlüsselung der Daten selbst, bietet sich auch die Verschlüsselung auf dem Transportweg über TLS an. Hierbei erfolgt die Verschlüsselung für den Nutzer transparent (d.h. ohne sein Zutun). Häufig genutzte Protokolle, die das unterstützen, sind HTTPS und SMTPS. Die Art der Verschlüsselung und das zugehörende Schlüsselmanagement müssen dem Schutzbedarf entsprechend geeignet sein. Hierbei ist der jeweilige Stand der Technik zu beachten. Weitere Hilfestellung bietet u. a. die technische Richtlinie TR-02102 des BSI.

2.1.2 Schutz vor DoS/DDoS-Angriffen

Generell hat der TK-Anbieter Maßnahmen zur Abwehr (Mitigation) von DoS/DDoS-Angriffen zu treffen. Solche Mitigation-Konzepte können entweder vom Internetbetreiber selbst oder von einem darauf spezialisierten Dienstleister implementiert und betrieben werden.

2.1.2.1 Resilienz der Infrastruktur gegen DoS- / DDoS-Angriffe

Die Infrastruktur des TK-Anbieters muss zum Schutz gegen DDoS-Angriffe ausreichend dimensioniert sein. Die Kapazitäten von Systemen, die im Fokus von DDoS-Angriffen stehen könnten, müssen so ausgelegt werden, dass ihre Funktionsfähigkeit auch bei einer mittelschweren Attacke ohne weitere Maßnahmen weiterhin gewährleistet ist.

2.1.2.2 Schutz vor IP-Spoofing

Um beispielsweise Reflections-Angriffe zu unterbinden, müssen TK-Diensteanbieter mit IP-Infrastruktur Maßnahmen treffen, die das Fälschen von Absenderadressen verhindern oder erschweren. Die Anforderungen aus den IETF-RFCs RFC2827 und RFC3704 sind umzusetzen.

2.1.2.3 Deaktivieren nicht genutzter Dienste

Die TK-Anbieter sollten eigene Server gegen Missbrauch absichern, indem z.B. nicht benötigte Dienste deaktiviert werden. Ihre Kunden sollten auf offene Ports und erreichbare Dienste (selbst ermittelt oder auf Basis externer Quellen) hingewiesen werden, von denen eine potentielle Gefahr für Dritte ausgeht.

2.1.2.4 Schutz betrieblich erforderlicher Dienste

Für den Netzbetrieb erforderliche Dienste müssen durch geeignete Maßnahmen und Komponenten vor DoS-/DDoS-Angriffen geschützt werden.

Ein Beispiel für Maßnahmen ist die Verwendung von Zugriffsbeschränkungen bzw. ACLs.

Bei den Komponenten kann es sich beispielsweise um Paketfilter oder DDoS-Mitigation-Devices handeln.

2.1.2.5 Detektion von Botnetzen

Die TK-Diensteanbieter mit IP-Infrastruktur müssen, unter Beachtung der Maßgaben in § 100 Abs. 1 TKG, eine geeignete Sensorik betreiben, um Botnetze zu detektieren. Im Einzelfall ist zum Erkennen und Eingrenzen von Störungen nach Maßgabe von § 100 Abs. 2 TKG auch das Aufschalten auf bestehende Verbindungen gestattet. Dies darf jedoch nur dann geschehen, wenn eine betriebliche Notwendigkeit besteht und mildere Mittel, wie z. B. eine Auswertung von Verkehrs- oder Steuerdaten eines informationstechnischen Protokolls nicht zum Ziel führen. Datenschutzrechtliche Schutzvorschriften wie die unverzügliche Löschung aufgezeichneter Daten und die Information des betrieblichen Datenschutzbeauftragten sind zu beachten, vgl. § 100 Abs. 2 TKG.

2.1.3 Gleichbehandlungsgrundsatz

Datenpakete von und an Kunden muss der TK-Anbieter unverändert und gleichberechtigt übertragen, unabhängig davon, woher diese stammen oder welche Anwendungen die Pakete generiert haben. Ausgenommen hiervon ist der VOIP-Dienst des TK-Anbieters, der über gesonderte Netze und/oder mit einer reservierten Bandbreite betrieben werden kann.

2.1.4 Inter-Domain-Routing

Es sind Maßnahmen zur Verhinderung der Manipulation von BGP-Routen zu treffen. Hier bietet sich beispielsweise die Verwendung von RPKI an.

2.2 Beobachtung, Berichterstattung und Kooperation

Um Angriffe oder Fehler zu erkennen, sollten die Verkehrsdaten im Rahmen der gesetzlichen Möglichkeiten und soweit dies für die Erbringung des jeweiligen Dienstes erforderlich ist, regelmäßig auf Auffälligkeiten hin beobachtet werden. Bei festgestellten Unregelmäßigkeiten sind geeignete Maßnahmen zum Schutz zu ergreifen (z.B. Netzverkehr unterbinden, Verkehr zu Störern einschränken oder unterbinden). Hierbei ist insbesondere die DSGVO und § 100 Abs. 1 TKG und bei den Maßnahmen § 109a Abs. 4 - 6 TKG zu beachten. Hier sollte die Empfehlung im Leitfaden des BfDI und der BNetzA für eine datenschutzgerechte Speicherung von Verkehrsdaten[3] beachtet werden, die Daten nach spätestens 7 Tagen zu löschen, wenn keine konkreten Anhaltspunkte für Angriffe oder Fehler vorliegen.

Im Einzelfall kann auch hier zum Erkennen und Eingrenzen von Störungen unter den Voraussetzungen von § 100 Abs. 2 TKG (s.o. unter 2.1.2.5) der Telekommunikationsinhalt aufgezeichnet werden

Weiterhin sollten die in dieser Anlage beschriebenen Maßnahmen umgesetzt werden, um ungewünschte Veränderungen durch Hersteller, Management-Dienstleister oder staatliche Akteure (z.B. aus den Herstellerländern) detektieren bzw. ausschließen zu können.

2.2.1 Implementierung einer Monitoring-Infrastruktur

2.2.1.1 Umfang

Eine geeignete Monitoring Infrastruktur (MI) muss vorgehalten werden. Diese sollte dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden. Eine geeignete MI muss ferner für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen. Die vorgesehenen Maßnahmen sollten tatsächlich und ggf. auch unter Zeitdruck umsetzbar sein.

Die MI muss alle für den Betrieb des Netzwerkes wesentlichen Komponenten erfassen sowie auch Komponenten, die personenbezogene Daten (z.B. Nutzerkennungen) an externe Vertragspartner übermitteln, etwa im Kontext von netzwerkübergreifender Signalisierung. Als für das Sicherheitsmonitoring geeignete Datenquellen kommen u.a. möglicherweise BGP-Router, Server für DNS, E-Mail, HTTP(S), SIP(S), SSH, IPsec in Betracht.

[3] Siehe Punkt B.I.2 im Leitfaden vom 19.12.2012.

Signifikante Abweichungen vom normalen Netzbetrieb (z.B. ungewöhnliche Datenflüsse, untypische Datenpakete auf bestimmten Ports, auffälliges Verhalten kritischer Netzkomponenten usw.) müssen permanent registriert, analysiert und dokumentiert werden. Dabei ist darauf zu achten, dass die Daten nur für den erforderlichen Zeitraum gespeichert werden. Sofern keine konkreten Anhaltspunkte für Angriffe oder Fehler vorliegen, sind die Daten nach spätestens 7 Tagen zu anonymisieren (z.B. durch Erstellen von statistischen Auswertungen) oder zu löschen.

2.2.1.2 Tools und Dokumentation

Die für ein Monitoring eingesetzten Tools müssen geeignete Parameter bzw. Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Die Arbeitsweise, das Zusammenspiel der Monitoring Tools und eine ggf. vorgenommene Verarbeitung der Daten sollte im Sicherheitskonzept dokumentiert werden. Ebenfalls dokumentiert werden sollten Schwellwerte und ähnliche Parameter, die zur Justierung der MI (z.B. Häufigkeit von Einzelereignissen bis ein Alarm ausgelöst wird, Justierung des Verhältnisses von True Positives zu False Negatives) genutzt werden.

Es ist ferner zu dokumentieren, wie mit erkannten Auffälligkeiten umgegangen wird. Es ist zu kennzeichnen, welche Maßnahmen von der MI automatisch eingeleitet werden, und welche einen Alarm auslösen, der eine manuelle Intervention nach sich zieht.

Die MI sollte daneben eine einzelfallunabhängige Statistik generieren, welche eine Identifizierung eines bestimmten Gefahrenbildes oder Modus Operandi ermöglicht. Kommen binäre Klassifikatoren zum Einsatz, so sollten diese mittels einer gemeinsamen Betrachtung der Eckdaten (TPR, FPR, TNR, FNR) und einer geeigneten Darstellung (z.B. ROC-Kurve) bewertet werden.

2.2.1.3 Weiterentwicklung

Die von der MI generierten Daten sollten zur Optimierung des Verhältnisses von True Positives und False Negatives regelmäßig einem Review unterworfen werden. Zur Identifizierung von False Negatives sollten ergänzend externe Datenquellen verwandt werden. Auch in diesen Fällen sollten die zur Optimierung ergriffenen Maßnahmen (z.B. Justierung von Schwellwerten; die Erfassung weiterer Parameter; der Einsatz weiterer oder die Abschaltung von nicht mehr zielführenden Monitoring Tools) und etwaige Änderungen der MI dokumentiert werden.

Eine MI muss rechtlich zulässig und datenschutzkonform sein. Aus telekommunikationsrechtlicher Sicht orientiert sich die rechtliche Zulässigkeit einer MI an § 100 Abs. 1 und 2 TKG

2.2.2 Aufzeichnung / Protokollierung von Management-Aktivitäten

Sämtliche Management-Aktivitäten an Netzkomponenten müssen protokolliert und entsprechend ihrer Bedeutung für die Sicherheit der Gesamtinfrastruktur über einen hinreichend langen Zeitraum archiviert werden, um mögliche Sicherheitsvorfälle auch im Nachhinein rekonstruieren zu können.

2.2.3 Protokollierung der Konfigurationsdateien

Die Soll-Konfiguration einer jeden Netzkomponente sollten dokumentiert und gegen unbefugten Zugriff geschützt abgespeichert werden.

2.2.4 Soll- / Ist-Abgleich der Komponenten

Hinreichend häufig sollten Revisionen der Netzinfrastruktur durchgeführt werden, die u.a. einen Soll-Ist-Abgleich der aktuellen Konfigurationsdateien sämtlicher Netzkomponenten mit den gemäß 2.2.3 archivierten Referenzdateien umfassen.

2.2.5 Verhaltensprüfung der Komponenten

Über den Soll-Ist-Vergleich der Konfigurationsdateien hinaus sollte regelmäßig ein Vergleich des tatsächlichen mit dem vorgesehen Verhalten einzelner Komponenten durchgeführt werden. Dazu sollen Test Cases definiert werden, in denen das konforme Verhalten beschrieben ist.

2.2.6 Identifizierung infizierter Systeme und Aufklärung des Kunden über Bedrohungen bei erkannter Infektion

Zusätzlich zu den genannten Vorkehrungen zum eigenen Schutz sollten TK-Anbieter das Netz auch im Hinblick auf infizierte Systeme von Kunden beobachten. Die dazu erforderlichen Maßnahmen sind nach Stand der Technik und unter Beachtung der gesetzlichen Vorgaben zu gestalten. Werden dem TK-Anbieter Störungen bekannt, die von Datenverarbeitungssystemen der Nutzer ausgehen, ist er nach TKG §109a Abs. 4 zur unverzüglichen Benachrichtigung der Nutzer verpflichtet, soweit dies technisch möglich und zumutbar ist. Auch hat er in diesem Fall die Nutzer auf angemessene, wirksame und zugängliche technische Mittel hinzuweisen, mit denen sie diese Störungen erkennen und beseitigen können. Die gesetzlichen Meldepflichten (siehe Katalog Kap. 3.5.3) sind zu beachten.

2.2.7 Kooperationen bei TK-anbieterübergreifenden Störungen

Treten Störungen auf, von denen mehrere TK-Anbieter betroffen sein könnten, beispielsweise aufgrund von DDoS-Angriffen (siehe hierzu auch 2.1.2.), ist eine TK-Anbieter übergreifende Zusammenarbeit notwendig. Diese sollte auch einen providerübergreifenden Austausch zu infizierten Geräten umfassen.

Hierzu müssen Ansprechpartner und Vorgehensweisen im Vorfeld untereinander abgestimmt werden. Dazu zählt auch die Benennung eines mindestens zu den Büro-Arbeitszeiten reaktionsfähigen Abuse-Kontaktes, über den eingehende Meldungen (ggf. automatisiert) bearbeitet werden.

Es liegt in der Verantwortung des TK-Anbieters, vernetzte Anbieter zu kontaktieren, um die entsprechenden Kontaktpersonen zu ermitteln. Letztere haben den ersten TK-Anbieter im Gegenzug unverzüglich über Änderungen zu informieren. Es muss stets sichergestellt sein, dass im Notfall ein direkter und unverzüglicher Kontakt unter den TK-Anbietern möglich ist.

2.2.8 Kooperation mit Anti-Malware-Herstellern

Mithilfe der umgehenden Weiterleitung von Malware-Samples an AV-Hersteller sollten diese bei der zeitnahen Verbesserung von Detektionsmaßnahmen unterstützt werden.

3 Dienstleistungen für Endnutzer

3.1 Allgemeine Sicherheitsvorkehrungen

Neben der Authentisierung mit Hilfe von Benutzername und Passwort sollten, wenn technisch möglich, den Kunden stärkere Authentifizierungsverfahren wie beispielsweise kryptographische Authentifizierungsverfahren oder Verfahren der Zwei-Faktor-Authentifizierung (Besitz und Wissen) angeboten werden.

3.2 Internetzugang

3.2.1 Neukundeninformation

Neukunden sollten schriftlich mit Informationen zu Risiken im Internet, bestehenden Schutzmöglichkeiten sowie Hinweisen zu Entfernungsmöglichkeiten von Schadsoftware versorgt werden.

3.2.2 Information des Kunden bei Verdacht einer Schadsoftware-Infektion

Bei vorliegendem Verdacht auf eine Schadsoftware-Infektion eines Kunden-Endgeräts sollte der Kunde benachrichtigt werden.

3.3 VoIP

3.3.1 Bandbreite, Erreichbarkeit von Notrufnummern

Der TK-Anbieter sollte einen Teil der zur Verfügung stehenden Bandbreite für die VOIP-Kommunikation reservieren. Vor allem die Erreichbarkeit von Notrufnummern muss sichergestellt sein.

3.3.2 Vertraulichkeit der Kommunikation

Ergänzend zu Abschnitt 2.1.1 sollten im Rahmen des technisch möglichen und wirtschaftlich vertretbaren VoIP-Daten sowohl bei der Übertragung zwischen Provider-Netzen als auch – sofern das CPE des Kunden die technischen Voraussetzungen dafür bietet – zwischen Kunden-CPE und SBC des Providers verschlüsselt übertragen werden.

3.3.3 Übermittlung der Rufnummer

Die Signalisierung für CLIP/CLIR muss bei abgehenden Verbindungen korrekt eingestellt werden und bei ankommenden Verbindungen korrekt berücksichtigt werden. Weiterhin sind

die netzseitige (network provided number) und die kundenspezifische Rufnummer (user provided number) korrekt zu übermitteln.

3.3.4 Schutz vor TDOS

Soweit technisch möglich und wirtschaftlich angemessen, sollten TK-Anbieter – z.B. durch ein entsprechendes Monitoring am SBC – automatisierte Massenanrufe an einem Anschluss zum Zwecke, diesen lahmzulegen (sog. TDOS-Attacken), erkennen und unterbinden können.

3.4 DNS-Dienste

3.4.1 Schutz vor Spoofing und Erschweren von Reflection/Amplification-Angriffen

Zum Schutz vor gespooften DNS-Anfragen müssen TK-Anbieter sicherstellen, dass DNS-Resolver, soweit sie sich in der eigenen betrieblichen Verantwortung befinden, nicht offen erreichbar („Open Resolver“) sind, sondern die Erreichbarkeit auf den eigenen Kundenkreis beschränkt ist. Ein permanentes Monitoring der DNS-Server muss gewährleistet sein und sollte es ermöglichen, Reflection/Amplification-Angriffe frühzeitig zu erkennen. Hinweise ergeben sich z.B. bei einer Häufung von Anfragen aus bestimmten Quellen, bezüglich bestimmter Resource-Records, unerlaubter rekursiver Anfragen u.ä. In diesen Fällen müssen Gegenmaßnahmen, wie die Einschränkung und Filterung von Anfragen, getroffen werden. Dies gilt ebenso für Dienste wie NTP, SSDP usw. die gleichfalls immer häufiger für Reflection-Angriffe missbraucht werden.

3.4.2 Schutz vor DNS-Cache Poisoning

Um die Robustheit des Servers gegenüber DNS-Cache-Poisoning Angriffen zu erhöhen, sollte die Port-Randomisierung aktiviert sein. Die Verkehrsmenge sollte regelmäßig beobachtet werden, um Cache-Poisoning Angriffe frühzeitig zu entdecken. Insbesondere bei breitbandig angebundenen DNS-Resolvern ist eine Cache-Poisoning Attacke trotz aktivierter Port-Randomisierung weiterhin möglich. Zur Risikoreduzierung sollten außerdem Obergrenzen für die Haltezeit von zwischengepufferten Daten im DNS-Cache festgelegt werden.

3.4.3 Einsatz von DNSSEC

Innerhalb der DNS-Infrastruktur eines Netzbetreibers muss eine Validierung von DNSSEC-Signaturen flächendeckend erfolgen. Der TK-Anbieter sollte seine Kunden über die Vorteile von DNSSEC aufklären sowie diese zu einer Nutzung anhalten.

4 Akronyme

RFC Dokument zur Beschreibung von Internet-Standards

TPR True Positive Rate

FPR False Positive Rate

TNR True Negative Rate

FNR False Negative Rate

ROC Receiver Operating Characteristic

Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten

nach
§ 109 Telekommunikationsgesetz (TKG)
Version 2.0

Anlage 2
Zusätzliche Sicherheitsanforderungen für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial

Stand: 13.05.2020

Inhaltsverzeichnis

1 Anwendungsbereich

Nachfolgend werden zusätzliche Sicherheitsanforderungen für Netze und Dienste mit erhöhter Kritikalität beschrieben. Die Reihenfolge der beschriebenen zusätzlichen Sicherheitsanforderungen orientiert sich am Lebenszyklus (Produktion, Auslieferung und Inbetriebnahme) der zu beurteilenden Komponenten.

2 Zertifizierung von kritischen Komponenten

2.1 Grundsätzliches

Zuständige nationale Behörde für die IT-Sicherheitszertifizierung kritischer Komponenten ist das Bundesamt für Sicherheit in der Informationstechnik (BSI). Das BSI ist ebenfalls zuständig für die nationale Anerkennung von Prüfstellen im Rahmen der nationalen IT-Sicherheitszertifizierung.
Das BSI erstellt und veröffentlicht im Benehmen mit der Bundesnetzagentur für die betroffenen Netze im Geltungsbereich dieser Anlage eine Technische Richtlinie. Diese enthält Anforderungen zur Zertifizierung von kritischen Komponenten einschließlich Anforderungen an die Einsatzumgebung und an den Betrieb als Voraussetzung für die Gültigkeit von Zertifikaten. Darüber hinaus beschreibt sie Auflagen zur Nachweiserbringung von Zertifikaten nach europäischen Zertifizierungsschemata (CSA). Die nachfolgenden Abschnitte beschreiben den Prozess zur Identifikation der kritischen Komponenten und Regelungen zu deren Einsatz, ausgehend von der Auflistung (siehe nachfolgend) der kritischen Funktionen in einem Telekommunikationsnetz.

2.2 Liste der kritischen Funktionen

Die Bundesnetzagentur erstellt gemeinsam mit dem BSI ein Dokument, das die kritischen Funktionen in einem Telekommunikationsnetz auflistet.

Kritische Funktionen werden durch BNetzA und BSI auf der Grundlage einer gemeinsamen Gefährdungsanalyse und auf der Grundlage des jeweils aktuellen Stands der Technik identifiziert und in die Liste aufgenommen.
Die Liste wird nach übereinstimmender Einschätzung von BNetzA und BSI kontinuierlich aktualisiert, insbesondere auch dann, wenn sich wesentliche Voraussetzungen verändert

haben. Ergebnisse nationaler oder internationaler Risikoanalysen wie zum Beispiel der ENISA oder BEREC werden hierbei berücksichtigt.
Der oder dem BfDI wird die Möglichkeit der Beteiligung an der Erstellung und Aktualisierung der Liste eingeräumt.
Hersteller, Verbände der Betreiber öffentlicher Telekommunikationsnetze und Verbände der Anbieter öffentlich zugänglicher Telekommunikationsdienste erhalten Gelegenheit zur Stellungnahme. Die Liste wird im Amtsblatt der Bundesnetzagentur bekannt gegeben.

2.3 Identifikation von kritischen Komponenten

Komponenten, die kritische Funktionen teilweise oder in vollem Umfang realisieren, müssen als kritische Komponenten identifiziert und dokumentiert werden. Der Netzbetreiber zeigt den geplanten Einbau der kritischen Komponente bei BSI und BNetzA an.

Übergangsreglung: Diese Anforderung ist spätestens ein Jahr nach Veröffentlichung der Liste der kritischen Funktionen umzusetzen.

2.4 Zertifizierung von kritischen Komponenten

I) Komponenten zur Realisierung kritischer Funktionen dürfen nur dann eingesetzt werden, wenn diese von einer anerkannten Prüfstelle auf IT-Sicherheit überprüft und von einer anerkannten Zertifizierungsstelle im Einklang mit der Verordnung (EU) 2019/881 (Cybersecurity Act) zertifiziert worden sind.
Sollten keine entsprechenden Zertifizierungsschemata verfügbar sein, so müssen pflichtige Netzbetreiber und Diensteerbringer beim Einsatz kritischer Komponenten vorübergehend sonstige geeignete und angemessene technische Vorkehrungen und sonstige Maßnahmen zur Gefahrenabwehr treffen.
Im Rahmen der Produktzertifizierung werden oftmals Anforderungen an die Einsatzumgebung bzw. an den sicheren Betrieb von Produkten gestellt. Nur durch die Einhaltung der im Zertifikat oder durch den Hersteller beschriebenen Auflagen kann ein sicherer Betrieb gewährleistet werden.
Details zu den Anforderungen aus 2.4, insbesondere zu den anzuwendenden Zertifizierungsschemata, werden in der Technischen Richtlinie des BSI geregelt.

II) Regelungen:

Hinsichtlich der Anforderungen zum Einsatz zertifizierter kritischer Komponenten gelten folgende Regelungen:

Inbetriebnahme von Komponenten nach dem 31.12.2025

Für kritische Komponenten, die nach dem 31.12.2025 in Betrieb genommen werden, gelten die Anforderungen zum Einsatz zertifizierter kritischer Komponenten gemäß 2.4 Ziffer I.

Inbetriebnahme von Komponenten bis zum 31.12.2025

Kritische Komponenten, die bis zum Ablauf des 31.12.2025 in Betrieb genommen werden oder wurden, sollen ab dem Zeitpunkt, ab dem zwei geeignete, entsprechend zertifizierte Produkte unterschiedlicher Hersteller am Markt verfügbar sind, spätestens jedoch mit Ablauf des 31.12.2025, die Anforderungen aus 2.4 Ziffer I erfüllen. Kommen ab diesem Zeitpunkt bis zum 31.12.2025 nicht zertifizierte Produkte zum Einsatz, hat der Pflichtige dies zu begründen sowie nachzuweisen und zu dokumentieren, dass dadurch keine zusätzlichen Gefährdungen zu erwarten sind und dadurch auch keine relevanten Sicherheitsverletzungen gemäß § 109 Abs. 5 TKG beim Pflichtigen auftreten können. Für Bestandskomponenten, die nicht mehr neu verbaut werden, wird keine nachträgliche Zertifizierung verlangt. Erhält eine bereits im Netz eingesetzte kritische Komponente keine Zertifizierung oder verliert sie diese, muss die Komponente bis 2025 im Netz ersetzt werden. Dies gilt auch für Bestandskomponenten.

Die Bundesnetzagentur ergreift Maßnahmen und andere Anordnungen nach dem TKG, um die Einhaltung dieser Vorgaben sicherzustellen.

3 Vertrauenswürdigkeit von Herstellern und Lieferanten

Mit der Zertifizierung einer kritischen Komponente oder Funktionalität ist keine direkte Aussage zur Vertrauenswürdigkeit der jeweiligen Bezugsquelle (Lieferant) verbunden. Die Verwendung von kritischen Komponenten aus unbekannten oder nicht vertrauenswürdigen Quellen kann jedoch erhebliche Gefahrenquellen eröffnen. Für den Einsatz in einem sensiblen Umfeld ist daher neben der Zertifizierung vor allem auch die Bezugsquelle der kritischen Komponente wesentlich.
Bezugsquelle einer kritischen Komponente kann u.a. Hersteller (§ 434 Abs. 1 S. 2 BGB) oder Verkäufer bzw. Lieferant (§ 445a Abs. 1 S. 1 BGB) sein. Betreiber öffentlicher Telekommunikationsnetze und Erbringer öffentlich zugänglicher Telekommunikationsdienste mit erhöhter Kritikalität sind vor diesem Hintergrund gehalten, insbesondere Hersteller und Verkäufer bzw. Lieferanten von kritischen Komponenten vor Bezug angemessen auszuwählen. Bestandteil einer angemessenen Auswahl ist auch eine geeignete Untersuchung der Vertrauenswürdigkeit der Bezugsquelle. Das verpflichtete Unternehmen hat zum Nachweis der Vertrauenswürdigkeit der Bezugsquelle von dieser eine umfassende Erklärung einzuholen. Die Erklärung muss sich auf alle sicherheitsrelevanten Komponenten und ggf. Funktionalitäten beziehen sowie die Bezugsquelle selbst vollständig (Hersteller inkl. Zulieferer und ggf. Verkäufer bzw. Lieferant) erfassen.
Im Folgenden werden nicht abschließend Inhalte einer Erklärung der Vertrauenswürdigkeit einer Bezugsquelle aufgeführt. Verstöße gegen die Erklärung sollten mit Vertragsstrafen geahndet werden. Die konkreten Inhalte sind vom pflichtigen Unternehmen im jeweiligen Einzelfall festzulegen.

1. Verpflichtung der Bezugsquelle, mit dem Bedarfsträger auf sicherheitstechnischem Gebiet intensiv zu kooperieren und insbesondere frühzeitig über neuartige Produkte, Technologien und Updates bestehender Produktlinien zu informieren.

2. Versicherung der Bezugsquelle, dass keine Informationen aus seinen Vertragsverhältnissen mit dem Bedarfsträger oder einer seiner Stellen an Dritte weitergegeben werden.

3. Verpflichtung der Bezugsquelle, durch organisatorische und rechtliche Maßnahmen sicherzustellen, dass vertrauliche Informationen von oder über seine(n) Kunden nicht

auf eigene Veranlassung oder Veranlassung Dritter in das Ausland gelangen oder ausländischen Stellen im Inland zur Kenntnis gelangen.

4. Versicherung der Bezugsquelle, dass diese rechtlich und tatsächlich in der Lage ist, eine Weitergabe von vertraulichen Informationen von oder über seinen Kunden an Dritte abzulehnen. Insbesondere bestehen zum Zeitpunkt der Abgabe der Erklärung keine Verpflichtungen, Dritten solchen Informationen zu offenbaren oder in anderer Weise zugänglich zu machen. Dies gilt nicht, soweit hierfür gesetzliche Offenlegungspflichten zu Strafverfolgungszwecken bestehen, es sei denn, solche Offenlegungspflichten bestehen gegenüber ausländischen Nachrichten- oder Sicherheitsbehörden. In Zweifelsfällen weist die Bezugsquelle auf die gesetzliche(n) Offenlegungspflicht(en) vor Abgabe der Erklärung hin.

5. Verpflichtung der Bezugsquelle, den Bedarfsträger sofort schriftlich zu benachrichtigen, wenn die Einhaltung der erklärten Verpflichtung nicht mehr gewährleistet werden kann, insbesondere, wenn für ihn eine Notwendigkeit oder Verpflichtung entsteht oder er eine solche hätte erkennen können, die ihn an der Einhaltung dieser Verpflichtung hindern könnte.

6. Verpflichtung der Bezugsquelle, auf Anfrage konkrete Angaben über die Produktentwicklung der sicherheitsrelevanten Systemanteile seiner Produkte zu machen.

7. Verpflichtung der Bezugsquelle, für die Entwicklung und Herstellung der sicherheitskritischen Systemanteile nur besonders vertrauenswürdige Mitarbeiter einzusetzen.

8. Erklärung der Bereitschaft der Bezugsquelle, Sicherheitsüberprüfungen und Penetrationsanalysen im erforderlichen Umfang an seinem Produkt zuzustimmen und in angemessener Weise zu unterstützen.

9. Versicherung der Bezugsquelle, dass das Produkt, für das die Erklärung abgegeben wird, keine vorsätzlich implementierten Schwachstellen besitzt und dass diese zu keinem späteren Zeitpunkt eingebaut werden sowie dass alle bekannten

unbeabsichtigten Schwachstellen behoben worden sind oder in Zukunft unverzüglich beseitigt werden.

10. Verpflichtung der Bezugsquelle, dass sie ihr bekannte bzw. bekannt gewordene Schwachstellen oder Manipulationen unverzüglich dem Bedarfsträger meldet, sodass frühzeitig Maßnahmen zur Eingrenzung und Beseitigung möglicher Folgewirkungen von Qualitätsmängeln ergriffen werden können. Gelangt der Hersteller an Informationen, die die Sicherheit und Funktion seiner Produkte schwächen oder die einen bestimmungsgemäßen Betrieb negativ beeinflussen können, so wird dies dem Bedarfsträger unverzüglich mitgeteilt. Weiterhin verpflichtet sich der Hersteller zur unmittelbaren Bereitstellung von Lösungsvorschlägen.

11. Erklärung, ob und wie die Bezugsquelle hinreichend sicherstellen kann, dass die kritische Komponente über keine technischen Eigenschaften verfügt, die geeignet sind, missbräuchlich auf die Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur (etwa durch Sabotage, Spionage) einwirken zu können

Die in den nachfolgenden Kapiteln beschriebenen Maßnahmen und Anforderungen können nur in Kombination mit der Zusicherung der Vertrauenswürdigkeit umgesetzt bzw. erfüllt werden.
Die Ausführungen gelten sinngemäß und angepasst auch für Erklärungen der Lieferanten.
Die angemessene Auswahl von Herstellern und Lieferanten setzt sich in einer angemessenen Überwachung derselben fort. Werden dem pflichtigen Unternehmen Anhaltspunkte bekannt, die auf eine Missachtung der Eigenerklärung von Herstellern oder Lieferanten hindeuten, so muss umgehend eine Aufklärung des Sachverhalts veranlasst werden und ggf. geeignete Maßnahmen zur Gefahrenabwehr ergriffen werden. Missachtung der Eigenerklärung von Herstellern oder Lieferanten können zu beträchtlichen Sicherheitsverletzungen führen. Auf die Pflicht zur Meldung tatsächlicher oder möglicher beträchtlicher Sicherheitsverletzungen (§ 109 Abs. 5 TKG) wird verwiesen.

4 Produktintegrität

Ein Produkt ist im Laufe seines Lebenszyklus in den jeweiligen Phasen unterschiedlichen Risiken ausgesetzt. Um diese Risiken zu minimieren werden nachfolgend für besonders kritische Phasen Anforderungen an den Betreiber, aber auch an den Funktionsumfang der Komponenten gestellt.

4.1 Allgemein

Der Betreiber muss in die Lage versetzt werden, die Integrität der erworbenen Komponenten jederzeit, beginnend mit der Abnahme, zu verifizieren. Die Prüfungsmöglichkeiten müssen durch den Betreiber in Anspruch genommen und dokumentiert werden.
Damit dies dem Betreiber möglich ist, sind technische Methoden/Verfahrensweisen in das Produkt zu integrieren und die Herangehensweise zur Durchführung der Verifikation geeignet zu dokumentieren.
Gefahrenträchtige Bereiche während der Auslieferung bis zur Inbetriebnahme müssen durch den Betreiber in Unterstützung durch den Hersteller ausdrücklich und gesondert im Sicherheitskonzept dokumentiert werden. Als gefahrenträchtig gelten insbesondere die nachfolgenden Bereiche.

4.2 Auslieferung

Eine Auslieferung liegt vor, wenn die Komponenten den Herrschaftsbereich des Herstellers verlassen. Die Auslieferung endet mit der Abnahme beim Betreiber. Die ausgelieferten Komponenten müssen in diesem Gefahrenabschnitt gegen mögliche Manipulationen oder andere Einwirkungen geschützt sein. Dies kann durch produkteigene oder externe Mechanismen sichergestellt werden. Zur Sicherstellung stehen aktuell bestimmte grundsätzliche Methoden/Verfahrensweisen zur Verfügung.
Für Software-Produkte ist eine geeignete Maßnahme der Einsatz von kryptographischen Verfahren zur Integritätssicherung. Für Hardware-Produkte ist ein geeigneter physischer Schutz vorzusehen, z.B. versiegelte Transportboxen, bewachte Transporte oder ein Selbstschutz des Produktes (möglich z.B. bei SIM-Karten). Die genaue Ausgestaltung dieser Mechanismen kann grundsätzlich herstellerspezifisch sein.

4.3 Abnahme

Eine Abnahme im Sinne dieser Anlage 2 liegt vor, wenn eine Komponente nach Prüfung durch den empfangenden Betreiber betriebsbereit und mangelfrei ist, und der Betreiber die Abnahme ausdrücklich erklärt.
Der Betreiber hat insbesondere zu prüfen, ob die betreffenden Komponenten während der Auslieferung Manipulationen, Einwirkungen oder andere Veränderungen erfahren haben. Dazu stehen grundsätzlich geeignete Kontrollen im Rahmen der bereits genannten Verfahren zur Verfügung.

4.4 Lagerung

Lagerung bezeichnet den Teil der Lieferkette zwischen der Abnahme und der Inbetriebnahme. Auch in diesem Gefahrenabschnitt ist die Integrität der Komponenten durch den Betreiber sicherzustellen. Die Sicherstellung kann auch hier durch produktinterne und/oder durch externe Mechanismen erfolgen. Vor einer möglichen Lagerung müssen zumindest stichprobenartig eine Funktionsprüfung und eine Überprüfung der Integrität der Komponenten erfolgen.

4.5 Inbetriebnahme

Eine Inbetriebnahme findet statt, wenn die Komponenten in den Betriebsablauf des Netzes überführt werden. Hierbei ist erneut eine Integritätsprüfung durch den Betreiber durchzuführen und in das Konfigurationsmanagement aufzunehmen. Auch dazu stehen grundsätzlich geeignete Kontrollen im Rahmen der bereits genannten Mechanismen zur Verfügung.

4.6 Wirkbetrieb

Siehe Kapitel 5 Sicherheitsanforderungen im laufenden Betrieb.

4.7 Außerbetriebnahme

Auch für die Außerbetriebnahme sind ggf. besondere Anforderungen (z.B. sicheres Löschen von Schlüsselmaterial, Konfigurationen, personenbezogene Daten z.B. Verkehrsdaten, etc.) zu berücksichtigen. Hierzu sind entsprechende technische Methoden/Verfahrensweisen in das Produkt zu integrieren und die Herangehensweise zur Durchführung der Außerbetriebnahme gegenüber dem Betreiber geeignet zu dokumentieren.

5 Sicherheitsanforderungen im laufenden Betrieb

Mit einer sicheren Inbetriebnahme ist der dauerhaft sichere Betrieb des öffentlichen Telekommunikationsnetzes nicht gewährleistet. Im laufenden Betrieb ergeben sich vielmehr neue, andersartige Gefahrenquellen. Zur kontinuierlichen Sicherstellung von § 109 Abs. 1 bis 3 TKG sind daher vom pflichtigen Unternehmen ebenfalls geeignete und dem Gefahrenpotential angemessene technische Vorkehrungen und sonstige Maßnahmen zu veranlassen. Geeignet in diesem Sinn ist der Einsatz von Monitoringverfahren.

5.1 Sicherheitsmonitoring

Das pflichtige Unternehmen hat eine Monitoring-Infrastruktur (MI) umzusetzen und zu betreiben, um fortwährend Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. Zusätzlich zu den Vorgaben im Absatz 2.2 der „Anlage: Anforderungen an TK-Anbieter mit IP-Infrastruktur“ gelten folgende Vorgaben:
Die MI muss alle kritischen Komponenten erfassen sowie Komponenten, die personenbezogene Daten (z.B. IMSIs, CDRs, MSISDN, IMEIs) an externe Vertragspartner übermitteln, etwa im Kontext von netzwerkübergreifender Signalisierung oder Roaming. Als für das Sicherheitsmonitoring geeignete Datenquellen kommen u.a. Server für SS7, DEA, SEPP, NRTRDE und Infrastrukturkomponenten wie SMSC oder HLR in Betracht.
Störungen oder Fehler an Telekommunikationsanlagen können sich beispielsweise ergeben aus DoS- und DDoS-Angriffen; Botnetzen; unerwünschten und verpassten Anrufen („Wangiri“); PBX-Hacking; eingehenden Massenanrufen oder SMS an einen bestimmten oder an mehrere Anschlussinhaber (Robocalling, SPIT); ausgehende Massenanrufe oder SMS, potenzieller Call-ID Fälschung; Anomalien im Kontext von angebotenen Anwendungen (z. B. aus dem Bereich M2M-Kommunikation oder IoT).
Bedrohungen ergeben sich ebenfalls aus falschen Basisstationen. Diese sollen durch eine geeignete MI daher auch ohne Mitwirkung der Endgeräte (Hardware oder Software) der Nutzer erkannt werden.

5.2 Kryptographische Mechanismen und Schlüsselmanagement

Das pflichtige Unternehmen muss dessen Schlüsselmanagement in seinem Sicherheitskonzept beschreiben. Der Lebenszyklus kryptographischer Schlüssel sowie die ergriffenen technischen und organisatorischen Maßnahmen zum Schutz dieser Schlüssel muss dokumentiert werden. Die Dokumentation muss beispielsweise Schlüsselmaterial

- in der UICC bzw. eUICC sowie Kopien in der Infrastruktur,
- zur Verschlüsselung der SUPI,
- für den Betrieb im Kontext des Remote SIM Provisionings,
- für den Betrieb des N32-Interfaces und von DIAMETER,
- für den Betrieb der SIP-Infrastruktur
- zur Sicherung der Kommunikation zwischen Netzwerkkomponenten, und
- zur Sicherung der Kommunikation zwischen Netzwerkkomponenten und dem zentralen Netzwerkmanagement

umfassen. Diese Liste dient der Orientierung und erhebt keinen Anspruch auf Vollständigkeit.
Werden Schlüssel vom Anbieter generiert, so muss das für die Generierung genutzte Verfahren dokumentiert werden. Werden vertrauliche Schlüssel oder Zertifikate mit öffentlichen Schlüsseln an Vertragspartner übermittelt, so müssen die hierbei verwendeten technischen und organisatorischen Schutzmaßnahmen dokumentiert werden.
Der Anbieter muss dokumentieren, welche kryptographischen Algorithmen zum Schutz der Vertraulichkeit und der Integrität auf der Luftschnittstelle unter Berücksichtigung der aktivierten Konfiguration unterstützt werden. Nach Möglichkeit sollte hierbei zwischen Access Stratum, Non-Access-Stratum, zwischen Signalisierung und Nutzdaten sowie zwischen verschiedenen Netzwerkgenerationen (2G/3G/4G/5G usw.) unterschieden werden. Bei unterschiedlicher Ausprägung je nach geographischer Region sollten auch die Unterschiede dokumentiert werden.

6 Eingewiesenes Fachpersonal

Das eingesetzte Fachpersonal muss die zur Wahrnehmung der Aufgabe erforderliche Facheignung vorweisen. Dies gilt schon grundsätzlich. Für den Umgang mit kritischen Komponenten und Funktionalitäten muss jedoch im besonderen Maß auf die Festlegung einer angemessenen Kompetenz geachtet werden. Zur sachgerechten Wahrnehmung einer sicherheitsrelevanten Aufgabe mit dem vorliegenden Gefahrenpotential ist die bloße Kenntnis um technische Abläufe hierbei nicht ausreichend. Erforderlich und angemessen ist vielmehr die zusätzliche Mindestkenntnis über die gängigsten Bedrohungsszenarien für Fernmeldegeheimnis, Datenschutz und Funktionsfähigkeit des Netzes.

Nicht nur der Stand der Technik, sondern auch die damit korrespondierenden Gefahrenlagen unterliegen einer dynamischen Entwicklung. Das pflichtige Unternehmen sollte daher nicht nur statisch auf eine angemessene Personalauswahl, sondern auch auf eine fortwährende Überwachung der Eignung von Fachpersonal achten. Durchzuführende Fortbildungsmaßnahmen müssen sich inhaltlich zumindest am Stand der Technik orientieren und die Entwicklung möglicher und bekannter Gefahrenlagen behandeln.

Alle Mitarbeiter, die in sicherheitsrelevanten Bereichen eingesetzt werden, sollten daher im Rahmen regelmäßiger Sensibilisierungs- und Schulungsmaßnahmen über die ihnen obliegende Verantwortung aufgeklärt werden.

Fortbildungs- und Sensibilisierungsmaßnahmen sind in geeigneter Form zu dokumentieren.

Es muss sichergestellt sein, dass Verantwortlichkeiten und Befugnisse für jedermann eindeutig und transparent sind. Eine geeignete und zugängliche Organisations- und Aufgabenbeschreibung kann diese Transparenz schaffen.

Auch auf eine besondere persönliche Eignung des eingesetzten Personals muss geachtet werden. Denn die Wahrnehmung einer sicherheitsrelevanten Aufgabe erfordert sachgerechtes Verhalten vor allem in Ausnahmesituationen. Das eingesetzte Personal sollte daher entsprechend belastbar sein, so dass in Stresssituationen eine Aufgabenwahrnehmung und Entscheidungsfindung sichergestellt ist. Die Teilnahme an regelmäßigen Notfall- oder Krisenübungen kann in diesem Zusammenhang hilfreich sein.

Das eingesetzte Personal muss vertrauenswürdig sein. Im Mindestmaß wird daher zu fordern sein, dass die Identität des betreffenden Personals vor Einsatz in sicherheitsrelevanten Bereichen feststeht. Ein schlüssiger, belegter und überprüfter Lebenslauf kann Sicherheit über die Herkunft des eingesetzten Personals schaffen.

Ist Personal in besonders sicherheitsrelevanten Bereichen eingesetzt, so kann es angemessen sein, die Vorlage eines polizeilichen Führungszeugnisses einzufordern.

Regelverstöße und unzutreffende Angaben des eingesetzten Sicherheitspersonals müssen arbeitsrechtlich mit einer angemessenen und bekannten Sanktion verknüpft sein. Regelverstöße mit strafrechtlicher Relevanz sind konsequent zur Anzeige zu bringen.

7 Redundanzen

Die technische Kompromittierung kritischer Komponenten ist folgenschwer. Zum Schutz gegen Störungen und zur Beherrschung der Risiken müssen daher zwingend geeignete technische Vorkehrungen oder sonstige Maßnahmen getroffen werden. Eine geeignete technische Vorkehrung kann die Vorsorge mit ausreichenden Redundanzen sein. Dies gilt insbesondere dann, wenn kritische Komponenten sehr hohe Anforderungen hinsichtlich der Verfügbarkeit erfüllen müssen. Ein Ziel muss es sein, Störfälle möglichst zu vermeiden oder aber Ausfallzeiten zumindest zu minimieren. Bei erkannten Manipulationen kann mit der Vorhaltung ausreichender Redundanzen eine Ausweichmöglichkeit geschaffen werden.
In einer geeigneten Risikoanalyse sollte möglichst ermittelt werden, ob und inwieweit ein Ausfall kritischer Komponenten ohne Gefährdung der gesetzlichen Schutzziele verantwortet werden kann. Es muss im Weiteren eine Prüfung erfolgen, ob geeignete technische Alternativen für einen Ausfall zur Verfügung stehen. Hilfreich könnte z.B. die Feststellung und Festlegung temporärer alternativer Netzstrecken oder Basisstationen sein. Festgelegt und im Sicherheitskonzept beschrieben werden sollte möglichst, welche Netz- und Systemkomponenten durch betriebsbereite Ersatzkomponenten bzw. im Fehlerfall sofort (automatisch) aktiviert werden können (Hot Standby). Festgelegt und beschrieben werden sollte ebenso, für welche Komponenten eine kurzfristige Verfügbarkeit durch entsprechende Vorhaltung im Lager oder Vereinbarungen mit Lieferanten ausreichend ist. Zu beachten ist, dass bestimmte Eigenschaften von modernen Netzwerken und bestimmte Anwendungsszenarien eine Hochverfügbarkeit der Netze erfordern. Bei Ultra-Reliable and Low-Latency Communications (uRLLC) handelt es sich beispielsweise um sehr zeitkritische Anwendungen mit geringer Latenzzeit. Ein Ausfall sollte daher möglichst ausgeschlossen werden. Das Sicherheitskonzept sollte auf den Einzelfall abgestimmte Anwendungsszenarien vorsehen.

Ein Beispiel für mögliche Redundanzen können Klimageräte sein. In Serverschränken und Multifunktionsgehäusen sollte eine geeignete Überwachung erfolgen. Unregelmäßigkeiten

sollten vorher festgelegte Präventivmaßnahmen auslösen. Die Vorhaltung von redundanten (z. B. mobilen) Klimaeinrichtungen kann geeignet sein, Störungen zu vermeiden.

8 Diversität

Bei Planung und Aufbau der Netze sind „Monokulturen“ durch den Einsatz von kritischen Netz- und Systemkomponenten unterschiedlicher Hersteller zu vermeiden. Daher sind für das Kern-Netz (Backbone und Core Network), das Transportnetz und für Zugangsnetze (Radio Access Networks / Wired Access Networks) jeweils Komponenten oder Systeme von mindestens zwei unterschiedlichen Herstellern zu verwenden, sofern nicht Eigenentwicklungen der MNO zum Einsatz kommen. Diese sollten voneinander unabhängig und auch nicht von einer dritten Stelle im gleichen Maße abhängig sein. Insbesondere kritische Netzfunktionen und Netzelemente sollten aufgrund der realisierten Netztopologie nicht von einem einzelnen Anbieter kritischer Komponenten abhängig sein. Netze sind topologisch so zu gestalten, dass die Diversität auch bei kritischen, d.h. besonders schützenswerten Netzfunktionen und Netzelementen gegeben ist. Dies könnte bei entsprechender zukünftiger Entwicklung des Standes der Technik durch die Anwendung offener Standards, wie etwa Open RAN, unterstützt werden.
Es sollen Maßnahmen erarbeitet werden, welche die kurzfristige nichtvorhandene Verfügbarkeit von Komponenten eines Herstellers kompensieren, um die Funktionsfähigkeit des Netzes aufrechtzuerhalten.