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: 09.10.2019

---

*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 5

2 Funktion und grundlegender Inhalt des Katalogs von Sicherheitsanforderungen 6

3 Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung von personenbezogenen Daten 7

3.1 Organisation 7

3.1.1 Organisations- und Risikomanagement 7

3.1.2 Sicherheitsrollen und Verantwortlichkeiten 8

3.1.3 Lieferantenmanagement 8

3.2 Sicherheit im Personalmanagement 9

3.2.1 Sicherheitsüberprüfung 9

3.2.2 Sicherheitswissen und Sensibilisierung 9

3.2.3 Personelle Veränderungen 9

3.2.4 Umgang mit Verstößen 10

3.3 Sicherheit von Daten, Systemen und Einrichtungen 10

3.3.1 Sicherer Umgang mit sensiblen Daten und Informationen 10

3.3.2 Physische und elementare Schutzanforderungen 10

3.3.3 Versorgungssicherheit (Verfügbarkeit des Gesamtsystems) 11

3.3.4 Zugriffs- und Zugangskontrolle auf Netzwerk- und Informationssystemen 11

3.3.5 Integrität und Verfügbarkeit von Netzwerk- und Informationssystemen 12

3.3.6 Vertraulichkeit der Kommunikation 13

3.4 Betriebsführung 13

3.4.1 Betriebsverfahren 13

3.4.2 Änderungsmanagement 13

3.4.3 Asset Management 14

3.5 Störungen und Sicherheitsvorfälle 14

3.5.1 Erkennen von Sicherheitsvorfällen und Störungen 14

3.5.2 Umgang mit Sicherheitsvorfällen und Störungen 15

3.5.3 Kommunikation und Meldung von Sicherheitsvorfällen 15

3.6 Not- oder Ausfallmanagement 16

3.6.1 Aufrechterhaltung von Telekommunikationsinfrastrukturen und Diensten (Business Continuity Management) 16

3.6.2 Wiederanlauf nach Ausfällen (Disaster Recovery Management) 16

3.7 Überwachungs- und Testverfahren 17

3.7.1 Überwachungs- und Protokollierungsmaßnahmen 17

3.7.2 Notfallübungen 17

3.7.3 Testen von Netzwerk- und IT-Systemen 18

3.8 Beurteilung der Sicherheitsmaßnahmen 18
3.9 Einhaltung gesetzlicher Anforderungen 18
4 Rechtliche Sicherheitsanforderungen aus bereichsspezifischen Regelungen 19
4.1 Sicherheitsanforderungen zum Schutz des Fernmeldegeheimnisses (§ 88 TKG) 19
4.2 Sicherheitsanforderungen zum Schutz der personenbezogenen Daten (§§ 91 ff. TKG) 21
4.2.1 Informationspflichten (§ 93 TKG) 21
4.2.2 Verkehrsdaten (§ 96 TKG) 22
4.2.3 Entgeltermittlung und Entgeltabrechnung (§ 97 TKG) 23
4.2.4 Standortdaten (§ 98 TKG) 23
4.2.5 Einzelverbindungsnachweis (§ 99 TKG) 23
4.2.6 Mitteilen ankommender Verbindungen (§ 101 TKG) 24
4.2.7 Automatische Anrufweiterschaltung (§ 103 TKG) 24
4.2.8 Nachrichtenübermittlungssysteme mit Zwischenspeicherung (§ 107 TKG) 25
4.3 Sicherheitsanforderungen zum Schutz der Telekommunikationsinfrastruktur und der Verfügbarkeit der Telekommunikationsdienste 25
4.3.1 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten (§ 100 TKG) 25
4.3.2 Beträchtliche Sicherheitsverletzungen (§ 109 Abs. 5 TKG) 25
4.3.3 Daten- und Informationssicherheit (§ 109a TKG) 26
5 Umsetzung von Sicherheitsanforderungen 27
5.1 Umsetzung von Sicherheitsanforderungen 27
5.1.1 Beschreibung der betriebenen öffentlichen Telekommunikationsnetze 27
5.1.2 Beschreibung der erbrachten öffentlich zugänglichen Telekommunikationsdienste 28
5.1.3 Abstrakte Gefahrenprognose 28
5.1.4 Konkrete Gefahrenprognose 29
5.1.5 Gesamtprognose 29
5.1.6 Festlegung und Beschreibung der technischen Vorkehrungen oder sonstigen Schutzmaßnahmen 29
5.1.7 Sicherheitskonzept erstellen 31
5.1.8 Benennung des Sicherheitsbeauftragten 31
5.1.9 Umsetzungserklärung 32
5.1.10 Sicherheitskonzept an Veränderungen anpassen 32
5.1.11 Vorgehensweise zur Erstellung des Sicherheitskonzepts 33
6 Übergangsregelungen 34
7 Informationsquellen 35

8 Begriffsbestimmungen.....35
Anlage 1: Maßnahmen zur Anforderungen an TK-Anbieter mit IP-Infrastruktur 37
Anlage 2: Weitergehende Sicherheitsanforderungen für Betreiber von Netzen mit erhöhtem Gefährdungspotenzial.....37

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 (§ 3 Nr. 6 TKG). 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

Die nach § 109 Abs. 4 TKG pflichtigen Unternehmen sollen durch Festlegung von Sicherheitsanforderungen bei der Erfüllung ihrer Pflichten unterstützt werden. Die Bundesnetzagentur hat daher im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und dem/der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit den vorliegenden „Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten als Grundlage für das Sicherheitskonzept nach § 109 Absatz 4 TKG und für die zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen nach § 109 Absatz 1 und 2 TKG“ erstellt.

Grundlegende Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung von personenbezogenen Daten sind im 3. Kapitel beschrieben. Die Beachtung 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 im Kapitel 5. Anlage 1 beschreibt geeignete technische und organisatorische Maßnahmen zur Anforderungen an TK-Anbieter mit IP-Infrastruktur. Die beschriebenen Maßnahmen richten sich daher an Internet-Service-Provider. Zusätzliche Sicherheitsanforderungen enthält die Anlage 2. Die zusätzlichen Sicherheitsanforderungen richten sich ausschließlich 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 richtet sich daher nicht ausschließlich an das pflichtige Unternehmen, sondern kann 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. 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 zu berücksichtigen.

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 achten. Hierzu gehört insbesondere die Benennung des Sicherheitsbeauftragten nach § 109 Abs. 4 TKG; die Planung bzw. der Bau und Betrieb von TK- Netzen oder das Erheben, Verarbeiten und Nutzen von Bestands- und Verkehrsdaten.

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 in einer Liste zu dokumentieren und vorzuhalten. 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 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 aber 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 anzupassen bzw. zu sperren. Ausgegebene Passwörter sind zu ändern und sollen regelmäßig gewechselt werden.
- 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 sind Bestands- und vor allem Verkehrsdaten hoch sensible Daten. 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 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.
- Sofern es angemessen ist, 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 (2 Stufen Authentifizierung).
- 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.

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). 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

Sicherheitsvorfälle und Störungen können den Betrieb erheblich beeinträchtigen und zum Verlust der Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität führen. Es sollte 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 bekannt werden 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 sein. Im Falle einer Sicherheitsverletzung kann es notwendig sein, unter Zeitdruck oder abweichenden 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 im Einzelfall in geeigneter Form bewertet werden. Der für das Bewertungsergebnis vorgegebene Meldeweg muss sodann umgesetzt werden.
- Kritische Sicherheitsvorfälle müssen grundsätzlich untersucht werden. Untersuchung und Ergebnis sollte 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 zumindest 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, 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 getestet bzw. umgeschaltet werden, 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 jedoch 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)

Eine absolute Ausfallsicherheit ist wünschenswert, aber oft nicht garantierbar. 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 Präventivmaßnahme kann die Vorhaltung geeigneter Ersatzgeräte für Infrastruktur und TK-Systeme sein.

- Eine geeignete Präventivmaßnahme 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, geeignete Auswerteinformationen 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)

Die Vorschrift 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 und 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 weiter gibt.
- Schutzmaßnahme gegen eine ungerechtfertigte, entgegen dem Vertragsverhältnis vereinbarte Löschung von Nachrichteninhalten durch den Diensteanbieter kann beispielsweise das Anlegen von Backupsystemen sein.
- Die Vorkonfiguration von Telekommunikationsanlagen oder Endgeräten, die von Telekommunikationsanbietern den Kunden (als Vertragsbestandteil, zur Miete oder zum Kauf) zur Verfügung gestellt werden, sollte Grundsätze wie die Datenvermeidung und eine hohe Sicherheit berücksichtigen. Endgeräte sollten derart vorkonfiguriert werden, dass dem Fernmeldegeheimnis unterliegende Daten nur auf Wunsch des Nutzers gespeichert werden).
- Während etwa die Wahlwiederholung bei Telefonen oder Anruflisten bei Smartphones bei der normalen Bedienung erkennbar sind, können z. B. längere

Anruflisten bei VoIP-Routern von Nutzern unbeachtet bleiben. Dies ist insbesondere der Fall, wenn das Gerät vorkonfiguriert wird und somit keine Notwendigkeit besteht, die Bedienoberfläche eines Routers zu nutzen. Erst bei einer aktiven Wahl des Nutzers sollten solche Anruflisten aktiviert werden.

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 des BDSG kommen ergänzend zur Anwendung. Diese nationale Rechtslage wird überlagert von der seit 25.05.2018 direkt geltenden Datenschutz Grundverordnung (DSGVO). Es ist damit zu rechnen, dass die anstehende 6. TKG – Novelle auch Vorschriften der Verordnung (EU) 2016/679 vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (DSGVO) umsetzt. Insofern steht der 2. Abschnitt des 7. Teils des TKG vor einer Neuordnung.

Festgehalten werden kann jedoch, 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).

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)

Zur Abwehr 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. § 100 Abs. 1 TKG und die mit dieser Vorschrift verbundene Berichtspflicht könnten mit den datenschutzrechtlichen Anpassungen der 6. TKG-Novelle obsolet werden. Allgemeine Hinweise zur Berichtspflicht nach § 100 Abs. 1 TKG und deren Geltung sind unter www.bundesnetzagentur.de 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-, Verkehrs- und Steuerdaten 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 Diensteanbieter 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 („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 § 109 Abs.4 TKG. Dem pflichtigen Unternehmen wird durch die Umleitung innerhalb der eigenen Netzte 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 Diensteanbieter, 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 sicherheitskonzeptionelle Erstellungspflicht. 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. Der Diensteanbieter ist von einer gesetzlichen Vorlagepflicht befreit, 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. Der vorliegende Katalog für Sicherheitsanforderungen soll Handlungsgrundlage zur Erfüllung dieser Pflichten sein.

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 kann auf Kataloginhalte zurückgegriffen werden. Der Katalog kann daher sowohl Handlungs-, als auch Prüfungsgrundlage sein.

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 Gefahrenprognose (§ 109 Abs. 4 Nr. 2 TKG) und korrespondierend hierzu die im Einzelfall festgelegten Präventivmaßnahmen (§ 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, § 109 Abs. 4 Nr. 1 2. HS TKG. Zur Erstellung der Gefahrenprognose ist es sinnvoll, nicht nur auf Inhalte, sondern auch auf den jeweiligen Teilnehmerkreis abstrakt einzugehen. Werden lediglich Dienste erbracht, so ist dennoch darauf hinzuweise, welche TK- Netze hierbei zum Einsatz kommen.

5.1.3 Abstrakte Gefahrenprognose

Auf Grundlage des deskriptiven Befundes (5.1.1. und 5.1.2) ist eine Gefahrenprognose durchzuführen. Diese soll im günstigsten Fall zunächst auf einer abstrakten und einer konkreten Betrachtungsebene erfolgen. In einem ersten Schritt sollte der im Einzelfall erbrachte und zu beurteilende Dienst oder das betriebene Netzwerk einer abstrakten Gefahrenkategorie zugeordnet werden. Im Grundsatz kann diese Zuordnung nachfolgenden Gesichtspunkten erfolgen:

Standardkritikalität: Allgemeine und einfache öffentliche TK-Netzen und TK- Diensten mit einer normalen Bedeutung. Dieser Kategorie können beispielsweise lokale Netze für Sprach- und Datenkommunikation, Anbieter von Internetzugängen oder Rundfunkverteildienste mit geringer bis mittlerer Teilnehmerzahl zugeordnet werden.

Gehobene Kritikalität: Öffentliche TK-Netze und TK- Dienste, welche für das Gemeinwohl eine größere Bedeutung haben. Von öffentlichen TK- Netzen und öffentlich zugänglichen TK-Diensten mit gehobener Kritikalität ist auszugehen, wenn das jeweilige TK- Unternehmen unter den Geltungsbereich des Post- und Telekommunikationssicherstellungsgesetz (PTSG) fällt.

Erhöhte Kritikalität: Zu den TK- Netzen und TK- Diensten mit erhöhter Kritikalität und erhöhtem Gefährdungspotenzial gehören solche Netze und Dienste, die eine sehr hohe

Notwendigkeit für Gesellschaft, Sicherheit, Wirtschaft und Politik haben. Bei Mobilfunknetzen, die unter den Geltungsbereich des Post- und Telekommunikationssicherstellungsgesetzes (PTSG) fallen, ist grundsätzlich von einer hohen Kritikalität auszugehen. Diese Beurteilung ist pauschal durch die große gesamtgesellschaftliche Bedeutung und die querschnittliche Verwendung der Mobilfunktechnologie in allen Bereichen des öffentlichen Lebens begründet.

5.1.4 Konkrete Gefahrenprognose

Bei der sich anschließenden, konkreten Gefahrenprognose 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 wäre die jeweilige Sicherheitsorganisation des Unternehmens (Abschnitt 3.1) ebenfalls einer entsprechenden Gefahrenprognose 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 Gesamtprognose

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 Gefahren 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 Gefahrenanalyse 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.

2. Auf Grundlage der abstrakten Gefahrenanalyse 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-Anbieter mit IP-Infrastruktur haben bei der Festlegung von Schutzmaßnahmen zusätzlich die Anforderungen und Hinweise gemäß Anlage 1 „Anforderungen an TK-Anbieter 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 Gefahrenprognose. 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 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.

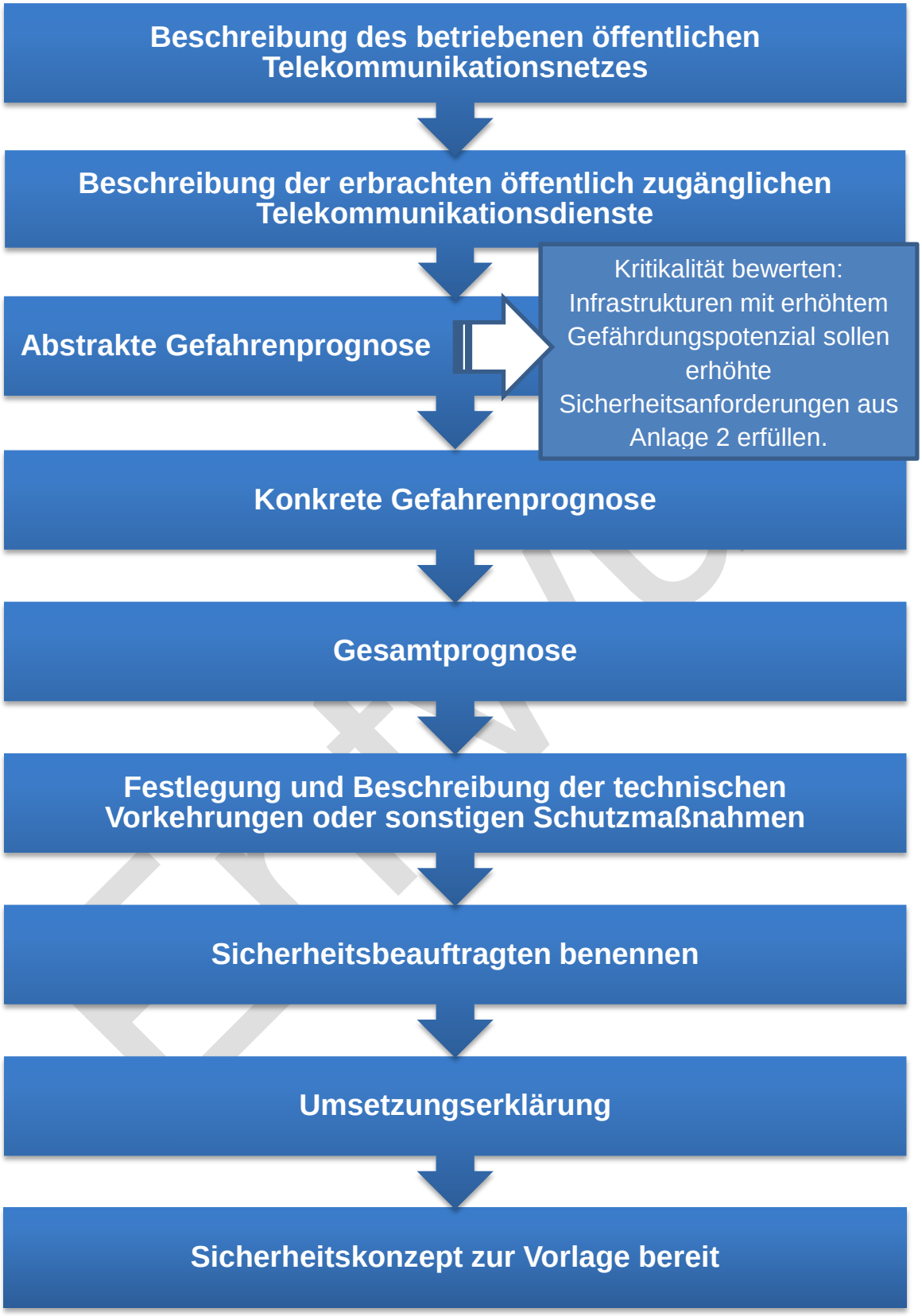
5.1.9 Umsetzungserklärung

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 Übergangsregelungen

Der Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten ist mit Veröffentlichung im Amtsblatt Grundlage für das Sicherheitskonzept nach § 109 Abs. 4 TKG und für die zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen nach § 109 Abs. 1 und 2 TKG.

Betreibern von öffentlichen Telekommunikationsnetzen sowie Erbringern von öffentlich zugänglichen Telekommunikationsdiensten mit erhöhtem Gefährdungspotenzial ist es bis zur Implementierung eines europäisch abgestimmten Zertifizierungsverfahrens sowie einer nationalen Umsetzung durch das BSI nicht möglich, zertifizierte kritische Komponenten im Sinne des vorliegenden Sicherheitskataloges einzusetzen. Um dennoch entsprechende neue Netze und neue Dienste mit kritischen Komponenten realisieren zu können, müssen pflichtige Netzbetreiber und Diensteerbringer beim Einsatz kritischer Komponenten vorübergehend sonstige geeignete und angemessene technische Vorkehrungen und sonstige Maßnahmen zur Gefahrenabwehr treffen.

Übergangsregelungen zum Einsatz kritischer Komponenten finden sich in Anlage 2 (Kapitel 2.5).

7 Informationsquellen

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

https://www.enisa.europa.eu/publications/guideline-on-security-measures-for-article-4-and-article-13a

BSI Standard 200-2:

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard202/ITGStandard202_node.html

BSI IT-Grundschutz-Kompendium:

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html

Deutsche Fassung EN ISO/IEC 27001:2017

Deutsche Fassung EN ISO/IEC 27002:2017

8 Begriffsbestimmungen

ENISA
European Network, Information Security Agency (Europäische Agentur für Netz und Informationssicherheit)

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

Diensteanbieter
Jeder, der ganz oder teilweise geschäftsmäßig

- Telekommunikationsdienste erbringt oder
- an der Erbringung solcher Dienste mitwirkt

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

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

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

Telekommunikationsdienste
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: Maßnahmen zur Anforderungen an TK-Anbieter mit IP-Infrastruktur

Anlage 2: Weitergehende Sicherheitsanforderungen für Betreiber von Netzen mit erhöhtem Gefährdungspotenzial

Anlage 1:

Anforderungen an TK-Anbieter mit IP-Infrastruktur

Stand: 09.10.2019

Inhaltsverzeichnis

1 Einleitung ... 3
2 Infrastruktur ... 4
2.1 Routing und Protokolle ... 4
2.1.1 Verschlüsselungstechnik ... 4
2.1.2 Schutz vor DoS/DDoS-Angriffen ... 4
2.1.3 Gleichbehandlungsgrundsatz ... 5
2.1.4 Inter-Domain-Routing ... 5
2.2 Beobachtung, Berichterstattung und Kooperation ... 5
2.2.1 Implementierung einer Monitoring-Infrastruktur ... 6
2.2.2 Aufzeichnung / Protokollierung von Management-Aktivitäten ... 7
2.2.3 Protokollierung der Konfigurationsdateien ... 7
2.2.4 Soll- / Ist-Abgleich der Komponenten ... 7
2.2.5 Verhaltensprüfung der Komponenten ... 7
2.2.6 Identifizierung infizierter Systeme und Aufklärung des Kunden über Bedrohungen bei erkannter Infektion ... 7
2.2.7 Kooperationen bei TK-anbieterübergreifenden Störungen ... 7
2.2.8 Kooperation mit Anti-Malware-Herstellern ... 8
3 Dienstleistungen für Endnutzer ... 9
3.1 Allgemeine Sicherheitsvorkehrungen ... 9
3.2 Internetzugang ... 9
3.2.1 Neukundeninformation ... 9
3.2.2 Information des Kunden bei Verdacht einer Schadsoftware-Infektion ... 9
3.3 VoIP ... 9
3.3.1 Bandbreite, Erreichbarkeit von Notrufnummern ... 9
3.3.2 Vertraulichkeit der Kommunikation ... 9
3.3.3 Übermittlung der Rufnummer ... 9
3.3.4 Schutz vor TDOS ... 9
3.4 DNS-Dienste ... 10
3.4.1 Schutz vor Spoofing und Erschweren von Reflection/Amplification-Angriffen ... 10
3.4.2 Schutz vor DNS-Cache Poisoning ... 10
3.4.3 Einsatz von DNSSEC ... 10
4 Akronyme ... 11

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. 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.

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 sollten 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 Internet-Betreiber 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 **Filter und adaptive Regeln**

Es sollten geeignete mehrstufige Filter und adaptiven Regelungen (mitigation devices) eingesetzt werden.

2.1.2.5 **Detektion von Botnetzen**

Die Internetbetreiber müssen, unter Beachtung der Maßgaben in § 100 Absatz 1 TKG, eine geeignete Sensorik betreiben, um Botnetze zu detektieren. Im Einzelfall kann zum Erkennen und Eingrenzen von unter den Voraussetzungen von § 100 Absatz 2 TKG (unverzügliche Löschung aufgezeichneter Daten, Informieren des betrieblichen Datenschutzbeauftragten) auch der Telekommunikationsinhalt aufgezeichnet werden. Dies darf jedoch nur in Ausnahmefällen durchgeführt werden, bei denen eine Auswertung von Verkehrsdaten und Steuerdaten eines informationstechnischen Protokolls nicht zum Ziel führt.

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 und 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 Absatz 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[1] beachtet werden, die Daten nach spätestens 7 Tagen zu löschen, wenn keine konkreten Anhaltspunkte für Angriffe oder Fehler vorliegen.

Im Einzelfall kann zum Erkennen und Eingrenzen von unter den Voraussetzungen von § 100 Absatz 2 TKG (unverzügliche Löschung aufgezeichneter Daten, Informieren des betrieblichen Datenschutzbeauftragten) auch der Telekommunikationsinhalt aufgezeichnet werden. Dies darf jedoch nur in Ausnahmefällen durchgeführt werden, bei denen eine Auswertung von Verkehrsdaten nicht zum Ziel führt.

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

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) sollte dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden. Eine geeignete MI sollte 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.

Signifikante Abweichungen vom normalen Netzbetrieb (z.B. ungewöhnliche Datenflüsse, untypische Datenpakete auf bestimmten Ports, auffälliges Verhalten kritischer Netzkomponenten usw.) sollten 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 sollten 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 TKG Abs. 1 und 2.

2.2.2 **Aufzeichnung / Protokollierung von Management-Aktivitäten**

Sämtliche Management-Aktivitäten an Netzkomponenten sollten 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 Absatz 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 weitere Möglichkeiten wie beispielsweise elektronische Identifikationssysteme 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

In Ergänzung zu Abschnitt 2.1.1 sollten 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 muss sichergestellt werden, dass DNS-Resolver 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

Die Validierung von DNSSEC-Signaturen muss 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

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

Stand: 09.10.2019

Inhaltsverzeichnis

1 Anwendungsbereich 3
2 Zertifizierung von kritischen Komponenten 4
2.1 Grundsätzliches 4
2.2 Einsatz von kritischen Komponenten 4
2.3 Liste der kritischen Funktionen und Komponenten 5
2.4 Betrieb von zertifizierten kritischen Komponenten 5
2.5 Übergangsregelungen 6
3 Vertrauenswürdigkeit von Herstellern und Lieferanten 6
4 Produktintegrität 9
4.1 Allgemein 9
4.2 Auslieferung 9
4.3 Abnahme 9
4.4 Lagerung 9
4.5 Inbetriebnahme 10
4.6 Wirkbetrieb 10
4.7 Außerbetriebnahme 10
5 Sicherheitsanforderungen im laufenden Betrieb 10
5.1 Sicherheitsmonitoring 10
5.2 Kryptographische Mechanismen und Schlüsselmanagement 11
6 Eingewiesenes Fachpersonal 11
7 Redundanzen 12
8 Diversität 13

1 Anwendungsbereich

Betreiber von öffentlichen Telekommunikationsnetzen und Anbieter von öffentlichen Telekommunikationsdiensten mit erhöhtem Gefährdungspotential haben zusätzliche technische Vorkehrungen und sonstige Maßnahmen zur Sicherstellung der Anforderungen aus § 109 Abs. 1 bis 2 TKG zu treffen. Von einem erhöhtem Gefährdungspotential wird nach abstrakter Gefahrenprognose bei Netzbetreibern und Dienstanbietern ausgegangen, wenn diese für das Gemeinwohl oder aber den Bestand der Bundesrepublik Deutschland als Industrie- und Technologiestandort eine hervorgehobene Bedeutung haben.
Bei Mobilfunkdiensten, welche aufgrund ihrer Teilnehmerzahl nach § 1 Abs. 1 Nr. 2 des Post- und Telekommunikationssicherstellungsgesetzes (PTSG) in den Geltungsbereich dieses Gesetzes fallen, kann aufgrund der Nutzerzahl und der querschnittlichen Verwendung der Mobilfunktechnologie in allen Bereichen des öffentlichen Lebens diese hervorgehobene Bedeutung vermutet werden. Dem vermuteten Gefährdungspotential entsprechend müssen daher die entsprechenden Mobilfunkanbieter zusätzliche Präventivanforderungen erfüllen. Die Berücksichtigung zusätzlicher Präventivanforderungen ist damit aber nicht auf diese pflichtigen Unternehmen begrenzt. Zeigt die abstrakte, konkrete oder die Gesamtprognose im Einzelfall ein entsprechendes Gefahrenpotential an, so kann das betroffene pflichtige Unternehmen auch in anderen Fällen zur Berücksichtigung ergänzender Präventivanforderungen gehalten sein.
Nachfolgend werden zusätzliche Sicherheitsanforderungen für Netze und Dienste mit erhöhter Kritikalität beschrieben. Die Reihenfolge der beschriebenen zusätzlichen Sicherheitsanforderungen orientiert sich am Verwendungszyklus (Zertifizierung, Produktion, Auslieferung und Inbetriebnahme) der zu beurteilenden Komponenten.
Inhaltlich wird mit der Vorgabe zusätzlicher Sicherheitsanforderungen das Eckpunktepapier der Bundesnetzagentur vom 07.03.2019 (www.bundesnetzagentur.de) umgesetzt.

2 Zertifizierung von kritischen Komponenten

2.1 Grundsätzliches

Primärziel der IT-Sicherheitszertifizierung ist die unabhängige und objektive Überprüfung eines Sicherheitsversprechens. Die Einhaltung eines solchen Versprechens wird im Rahmen eines Zertifizierungsverfahrens durch eine neutrale Prüfstelle evaluiert. Eine Zertifizierungsstelle (im Kontext der IT-Sicherheitszertifizierung ist dies in Deutschland das BSI) begleitet das Verfahren, um eine einheitliche Vorgehensweise und Methodik sicherzustellen.
Eine IT-Sicherheitszertifizierung einer anerkannten nationalen Stelle wird in bestimmten Produktkategorien und Prüftiefen im Rahmen internationaler Abkommen von zahlreichen Nationen, so auch von Deutschland, anerkannt. Mehrfachzertifizierung eines Produktes in verschiedenen Staaten werden dadurch vermieden. Mit dem Inkrafttreten der Verordnung (EU) 2019/881 (Cybersecurity Act) am 27.06.2019 wurde dazu ein einheitliches europäisches Rahmenwerk in der Cybersicherheitszertifizierung eingeführt, in dem die Anerkennung von europäischen Schemata für die Cybersicherheitszertifizierung geregelt ist.
Neben der IT-Sicherheitszertifizierung im Kontext internationaler Abkommen hat das BSI die Möglichkeit, nach einer Technischen Richtlinie zu zertifizieren. In einer Technischen Richtlinie können unter anderem Anforderungen zu IT-Sicherheitseigenschaften von IT-Komponenten, Gesamt- und Teilsysteme gestellt werden, aber auch zur Sicherstellung von Interoperabilität. Dabei kann eine Technische Richtlinie den Nachweis von Zertifikaten aus anderen Zertifizierungsschemata fordern. Somit können nationale Sicherheitsanforderungen auf Basis international anerkannter Standards und Zertifizierungen beschrieben werden.
Das BSI erstellt und veröffentlicht als nationale Zertifizierungsstelle in Deutschland für die betroffenen Netze eine Technische Richtlinie. Diese enthält Anforderungen zur Zertifizierung von sicherheitsrelevanten Systemkomponenten einschließlich Anforderungen an die Einsatzumgebung und an den Betrieb. Darüber hinaus beschreibt sie Auflagen zur Nachweiserbringung von Zertifikaten nach europäischen Zertifizierungsschemata (CSA).

2.2 Einsatz von kritischen Komponenten

Komponenten zur Realisierung kritischer Funktionalitäten dürfen von Betreibern öffentlicher Telekommunikationsnetze bzw. Erbringern öffentlich zugänglicher Telekommunikations-dienste nur eingesetzt werden, wenn sie von einer anerkannten Prüfstelle auf IT-Sicherheit im Einklang mit der Verordnung (EU) 2019/881 (Cybersecurity Act) überprüft und von einer anerkannten Zertifizierungsstelle zertifiziert wurden.
In Deutschland ist das BSI als nationale Zertifizierungsstelle ebenfalls zuständig für die Anerkennung von Prüfstellen im Rahmen der IT-Sicherheitszertifizierung.
Kritisch sind Komponenten insbesondere dann, wenn eine technische Kompromittierung zu

- Datenschutzverletzungen in erheblichem Ausmaß (z.B. automatisiertes Auswerten von Massendaten im Sinne einer Big Data- Anwendung),
- systematischer Ausforschung des Fernmeldeverkehrs oder
- beträchtlichen Sicherheitsverletzungen nach § 109 Abs. 5 TKG

führt oder führen kann. Die Kritikalität einer Komponente ist dabei jeweils durch diejenigen ihrer Funktionen begründet, die das Potential besitzen, bei Versagen oder nicht sachgerechter Realisierung, eine technische Kompromittierung herbeizuführen.

Ist die Realisierung einer solchen Funktion auf mehrere Komponenten verteilt, so ist von der Kritikalität aller dieser Komponenten auszugehen. Dabei ist es grundsätzlich unerheblich, ob Funktionen durch Hard-, Soft- oder Firmware realisiert werden.

2.3 **Liste der kritischen Funktionen und Komponenten**

Die Bundesnetzagentur erstellt gemeinsam mit dem BSI ein Dokument, das in einem ersten Teil die kritischen Funktionen und in einem zweiten Teil die kritischen Komponenten auflistet, die der Realisierung der kritischen Funktionen dienen. Der oder dem BfDI wird die Möglichkeit der Beteiligung eingeräumt.
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. Der oder dem BfDI wird die Möglichkeit der Beteiligung eingeräumt.
Inhaltliche Anpassungen der Liste der kritischen Funktionen werden nur dann vorgenommen, wenn sich nach übereinstimmender Einschätzung von BNetzA und BSI wesentliche Voraussetzungen verändert haben. Der oder dem BfDI wird die Möglichkeit der Beteiligung eingeräumt.
Die Liste wird kontinuierliche aktualisiert. Ergebnisse internationaler Analysen wie zum Beispiel der ENISA oder BEREC werden hierbei berücksichtigt. 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.

2.4 **Betrieb von zertifizierten kritischen Komponenten**

Die Liste der kritischen Komponenten ergibt sich durch Abgleich der aktuell und zukünftig eingesetzten Komponenten mit der Liste der kritischen Funktionen. Komponenten, die kritische Funktionen teilweise oder in vollem Umfang realisieren, müssen in die Liste der kritischen Komponenten aufgenommen werden und unterliegen der Pflicht zur IT-Sicherheitszertifizierung.
Das pflichtige Unternehmen muss alle Komponenten vor ihrem Einsatz mit der Liste der kritischen Funktionen und der Liste der kritischen Komponenten abgleichen. Dient eine Komponente der Realisierung einer kritischen (Teil-) Funktion, so muss diese Komponente in der Liste der kritischen Komponenten aufgeführt sein.
Die Liste der kritischen Funktionen und der Komponenten wird in einer initialen Form spätestens am 01.01.2020 veröffentlicht. Grundlage für die dort enthaltene Liste der kritischen Funktionen bildet das im Jahr 2019 durchgeführte nationale Risiko-Assessment.
Die Liste der kritischen Komponenten wird unter Berücksichtigung durch Meldungen der Hersteller sowie von den Verbänden von Betreiber öffentlicher Telekommunikationsnetze und Erbringer öffentlich zugänglicher Telekommunikationsdienste befüllt.
Im Rahmen der Produktzertifizierung werden oftmals Anforderungen an die Einsatzumgebung bzw. an den sicheren Betrieb der Komponente gestellt. Nur durch die Einhaltung der im Zertifikat oder durch den Hersteller beschriebenen Auflagen kann ein sicherer Betrieb gewährleistet werden. Bei der Festlegung von geeigneten und angemessenen technischen Vorkehrungen und sonstigen Maßnahmen sind diese Auflagen angemessen zu berücksichtigen und im Sicherheitskonzept zu berücksichtigen. Die BNetzA kann anordnen, dass sich die Betreiber öffentlicher TK-Netze und die Erbringer öffentlich zugänglicher Telekommunikationsdienste einer Überprüfung durch eine qualifizierte

unabhängige Stelle oder einer zuständigen nationalen Behörde gemäß § 109 Abs. 7 TKG unterziehen, in der festgestellt wird, ob die Anforderungen nach § 109 Abs. 1 bis 3 TKG erfüllt sind. Die Bewertung einer Überprüfung von Betreibern öffentlicher TK-Netze und Erbringern öffentlich zugänglicher Telekommunikationsdienste mit erhöhtem Gefährdungspotential gemäß § 109 Abs. 7 TKG sowie eine diesbezügliche Feststellung von Sicherheitsmängeln in dem vorgelegten Sicherheitskonzept erfolgt im Einvernehmen mit dem BSI.

2.5 **Übergangsregelungen**

Für Komponenten, die im Sinne von 2.3 als kritische Komponenten zu betrachten sind und vor dem 01.01.2021 ausgeliefert wurden, wird eine Übergangsfrist zur Erlangung eines gültigen Zertifikats gewährt. Voraussetzung für die Gewährung einer Übergangsfrist ist die Aufnahme der entsprechenden Komponenten in die Liste der kritischen Komponenten vor dem 01.01.2021. Diese vor dem 01.01.2021 gelisteten kritischen Komponenten dürfen ohne Einschränkung bis zum 31.12.2025 eingesetzt werden. Für die weitere Nutzung ab dem 01.01.2026 muss in jedem Fall ein gültiges Zertifikat vorliegen. Ab diesem Zeitpunkt ist die weitere Nutzung ohne Zertifikat untersagt.

3 Vertrauenswürdigkeit von Herstellern und Lieferanten

Mit der Zertifizierung einer kritischen Komponente oder Funktionalität ist keine Aussage zur Vertrauenswürdigkeit der jeweiligen Bezugsquelle (Lieferant) verbunden. Im Zertifizierungsverfahren kann maximal die Vertrauenswürdigkeit eines Herstellers hinterfragt werden. 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 sollte mit Vertragsverstößen 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 sicher zu stellen, 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.

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. Hierzu sind durch den Hersteller technische Methoden/Verfahrensweisen in das Produkt zu integrieren und die Herangehensweise zur Durchführung der Verifikation gegenüber dem Betreiber 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 Schlüsselverfahren. 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 muss 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 mit aufgenommen werden. 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 durch den Hersteller 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 sichergestellten 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 Bedrohungen zu identifizieren und zu vermeiden. 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.
Bedrohungen 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 sollte sein Schlüsselmanagement in seinem Sicherheitskonzept beschreiben. Der Lebenszyklus kryptographischer Schlüssel sowie die ergriffenen technischen und organisatorischen Maßnahmen zum Schutz dieser Schlüssel sollten dokumentiert werden. Die Dokumentation sollte 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 sollte das für die Generierung genutzte Verfahren dokumentiert werden. Werden vertrauliche Schlüssel oder Zertifikate mit öffentlichen Schlüsseln an Vertragspartner übermittelt, so sollten die hierbei verwandten technischen und organisatorischen Schutzmaßnahmen dokumentiert werden.
Der Anbieter sollte 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 muss vielmehr die zusätzliche Mindestkenntnis über die gängigsten Bedrohungsszenarien für Fernmeldegeheimnis, Datenschutz und Funktionsfähigkeit des Netzes sein.
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 Personalwahl, 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 daher 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. Vertrauen besteht eher gegenüber Personal aus geordneten wirtschaftlichen Verhältnissen. 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 wäre, 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 Netz- und Systemkomponenten unterschiedlicher Hersteller zu vermeiden. Daher sind soweit möglich zumindest für das Kern-Netz (Core Network) und für das Funkzugangsnetz (Radio Access Network) jeweils Komponenten oder Systeme von mindestens zwei unterschiedlichen Herstellern zu verwenden. Diese sollten voneinander unabhängig und auch nicht von einer dritten Stelle im gleichen Maße abhängig sein.
In den Netzen sollten die Komponenten eines Herstellers maximal zwei Drittel aller Komponenten ausmachen.
Es sollen Maßnahmen erarbeitet werden, welche die kurzfristige nichtvorhandene Verfügbarkeit von Komponenten eines Herstellers kompensieren, um die Funktionsfähigkeit des Netzes aufrechtzuerhalten.