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

nach § 109 Telekommunikationsgesetz (TKG)

Herausgeber:

Bundesnetzagentur

Bundesnetzagentur für Elektrizität, Gas,
Telekommunikation, Post und Eisenbahnen

Stand: 07.01.2016
Version 1.1

Dokumenthistorie

Version	Stand	Ausgabe
1.0	08.05.2013	Erstausgabe
1.1	14.07.2015	Zwischenversion Anpassungsbedarf auf Grund aktueller Sicherheits-belange

Änderungsübersicht

Version	Stand	Änderungen / Ergänzungen (Kapitelnummer)
1.1	14.07.2015	Cybersicherheitsempfehlungen (3.4; 6.1; 8; 9) Ergänzung zu DDoS-Angriffen (Reflection-Angriffe) (7.4; 10; 9.1) Verschlüsselung über Transport Layer Security (TLS) (9.3) Erhöhung der Sicherheit von TK-Endgeräten (9.17)

Inhaltsverzeichnis

1. Zielsetzung und Geltungsbereich

Die ständig wachsende Abhängigkeit der Wirtschaft und Gesellschaft von der Telekommunikation führt zu einem hohen Anspruch an die Qualität von Telekommunikationsnetzen und -diensten. Im Rahmen dessen stellen Teilnehmer und Nutzer von Telekommunikationsdiensten hohe Anforderungen an

- den Schutz des Fernmeldegeheimnisses,
- den Schutz ihrer personenbezogenen Daten und
- eine ordnungsgemäße und fortlaufende Verfügbarkeit von Telekommunikationsdiensten.

Zur Sicherstellung dieser Anforderungen haben Diensteanbieter, Betreiber von öffentlichen Telekommunikationsnetzen und Erbringer von öffentlich zugänglichen Telekommunikationsdiensten die Verpflichtungen nach § 109 TKG zu erfüllen.

Nach § 109 Absatz 6 Satz 1 TKG hat die Bundesnetzagentur im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit einen 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 zu erstellen.

Der vorliegende Katalog hat eine zweifache Funktion. Zum einen wird die Verpflichtung nach § 109 Absatz 6 Satz 1 TKG umgesetzt (Kapitel 8). Zum anderen gibt er den nach § 109 TKG Verpflichteten grundsätzliche Hinweise bzw. Empfehlungen zur Erfüllung der Verpflichtungen nach § 109 TKG. Insbesondere sind dies Hinweise und Empfehlungen

- zu den sicherzustellenden Schutzzielen,
- für die Planung und Umsetzung der technischen Vorkehrungen und sonstigen Maßnahmen zur Erfüllung der Verpflichtungen nach § 109 Absatz 1 bis 3 TKG,
- für die Erstellung des Sicherheitskonzeptes und die Vorlage des Sicherheitskonzeptes bei der Bundesnetzagentur gemäß den Verpflichtungen nach § 109 Absatz 4 TKG, und
- zu den Mitteilungspflichten nach § 109 Absatz 5 TKG.

Die Planung und Umsetzung der technischen Vorkehrungen und sonstigen Maßnahmen zur Erfüllung der Verpflichtungen nach § 109 Absatz 1 und 2 TKG und die Erstellung des Sicherheitskonzeptes gemäß § 109 Absatz 4 Satz 1 TKG kann auch auf der Basis anderer geeigneter Standards, Normen u. ä. (z.B. BSI-Standards, BSI-Grundschutzkataloge, DIN ISO/IEC-Normen) erfolgen. Die Einhaltung der Verpflichtungen nach § 109 Absatz 1 bis 4 TKG ist hierbei jedoch sicherzustellen. Insbesondere ist folgendes zu beachten:

1. Die technischen Vorkehrungen und sonstigen Maßnahmen zur Erfüllung der Verpflichtungen nach § 109 Absatz 1 und 2 TKG müssen die Einhaltung der relevanten Sicherheitsanforderungen gewährleisten.
2. Die technischen Vorkehrungen und sonstigen Maßnahmen zur Erfüllung der Verpflichtungen nach § 109 Absatz 1 TKG müssen den Stand der Technik berücksichtigen.
3. Zur Erfüllung der Verpflichtungen nach § 109 Absatz 2 TKG sind angemessene technische Vorkehrungen und sonstige Maßnahmen zu treffen. Technische

Vorkehrungen und sonstige Schutzmaßnahmen sind angemessen, wenn der dafür erforderliche technische und wirtschaftliche Aufwand nicht außer Verhältnis zur Bedeutung der zu schützenden Telekommunikationsnetze oder -dienste steht.

4. Bei gemeinsamer Nutzung eines Standortes oder technischer Einrichtungen hat jeder Beteiligte die Verpflichtungen nach § 109 Absatz 1 und 2 TKG zu erfüllen, soweit bestimmte Verpflichtungen nicht einem bestimmten Beteiligten zugeordnet werden können.

5. Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Verpflichtungen nach § 109 Absatz 1 TKG verantwortlich. Im Rahmen dessen sind die Verpflichtungen nach § 11 Absatz 2 Bundesdatenschutzgesetz (BDSG) einzuhalten.

6. Werden Telekommunikations- und Datenverarbeitungssysteme, die dem Betreiben von öffentlichen Telekommunikationsdiensten oder dem Erbringen von öffentlich zugänglichen Telekommunikationsdiensten dienen, im Auftrag durch andere Stellen betrieben, gilt § 11 Absatz 1 BDSG entsprechend, d. h, der Auftraggeber ist für die Einhaltung der Verpflichtungen nach § 109 Absatz 2 TKG verantwortlich.

7. Aus dem Sicherheitskonzept muss mindestens hervorgehen

    1. welches öffentliche Telekommunikationsnetz betrieben und welche öffentlich zugänglichen Telekommunikationsdienste erbracht werden,
    2. von welchen Gefährdungen der Schutzziele auszugehen ist und
    3. welche technischen Vorkehrungen oder sonstigen Schutzmaßnahmen zur Erfüllung der Verpflichtungen aus § 109 Absatz 1 und 2 TKG getroffen oder geplant sind.

8. Sofern sich die einem bei der Bundesnetzagentur vorgelegten Sicherheitskonzept zugrunde liegenden Gegebenheiten ändern, ist das Konzept entsprechend anzupassen und der Bundesnetzagentur unter Hinweis auf die Änderungen erneut vorzulegen.

2. Schutzbedarf und Schutzziele

Das Grundgesetz der Bundesrepublik Deutschland (GG) gewährt den Bürgern unter anderem die „Unverletzlichkeit des Fernmeldegeheimnisses (Artikel 10 GG)“, die „Unantastbarkeit der Würde (Artikel 1 GG)“ sowie das „Recht auf freie Entfaltung der Persönlichkeit (Artikel 2 GG)“. Des Weiteren gewährleistet der Bund im Bereich der Telekommunikation flächendeckend angemessene und ausreichende Dienstleistungen (Artikel 87f GG).

Für das Betreiben öffentlicher Telekommunikationsnetze sowie das Erbringen öffentlich zugänglicher Telekommunikationsdienste schreibt § 109 TKG technische Vorkehrungen und sonstige Maßnahmen

- **zum Schutz des Fernmeldegeheimnisses,**
- **gegen die Verletzung des Schutzes personenbezogener Daten,**
- **gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und –diensten führen, auch soweit sie durch äußere Angriffe und Einwirkungen von Katastrophen bedingt sein können,**

als Mindestanforderungen vor.

Im Vordergrund steht hierbei die Beherrschung der Risiken für die Sicherheit von Telekommunikationsnetzen und –diensten. Dabei ist der Stand der Technik zu berücksichtigen.

Ziel und Zweck der zu treffenden Maßnahmen sind insbesondere

- **die Sicherheit vor unerlaubten Zugriffen auf Telekommunikations- und Datenverarbeitungssysteme**
- **die Reduzierung / Minimierung der Auswirkungen von Sicherheitsverletzungen auf Nutzer oder auf zusammengeschaltete Netze**
- **die Gewährleistung eines ordnungsgemäßen Betriebes der Netze und dadurch die Sicherstellung der fortlaufenden Verfügbarkeit der über die Netze erbrachten Dienste**

Die rechtlichen Vorgaben zum Datenschutz ergeben sich als allgemeine Regelungen aus dem Bundesdatenschutzgesetz (BDSG) und als sektorspezifische Regelungen aus dem Teil 7 des TKG. Hiervon sind sowohl die Inhalte als auch die Verkehrs- und Bestandsdaten betroffen, wobei die Inhalte und Verkehrsdaten den erhöhten Anforderungen unterliegen, die sich aus den Vorgaben zum Schutz des Fernmeldegeheimnisses ergeben.

Die Regelungen des BDSG sind von den Telekommunikationsanbietern anzuwenden, sofern im TKG keine sektorspezifischen Regelungen getroffen wurden.

Ansonsten gilt, dass angemessene technische Vorkehrungen und sonstige Maßnahmen in Abhängigkeit vom individuellen Schutzbedarf, der durch eine geeignete Analyse ermittelt wird (z.B. Vorgehensweise gemäß BSI- Standard 100-2), zu treffen sind.
Die Angemessenheit der Maßnahmen ist dann gegeben, wenn der dafür erforderliche 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.

Bei gemeinsamer Nutzung eines Standortes oder technischer Einrichtungen hat jeder Beteiligte die o. a. Verpflichtungen zu erfüllen, soweit bestimmte Verpflichtungen nicht einem bestimmten Beteiligten zugeordnet werden können.

3. Vorgehensweise zur Erfüllung der Verpflichtungen nach § 109 TKG

Die wesentlichen Eckpunkte zur Erfüllung der Verpflichtungen nach § 109 TKG sind nachfolgend in einer Übersicht dargestellt.

3.1 TK-Netzstrukturplan darstellen

TK-System inklusive der angebundenen DV-Systeme, Verbindungen zwischen den Systemen, Außenverbindungen und Anbindungen der Infrastruktur
Welche Datenverarbeitungsanlagen gibt es im Unternehmen, mit welchen Anlagen führen sie die relevanten Geschäftsprozesse (inklusive mittelbarer Aufgaben; z.B. Billing) durch?

3.2 Telekommunikationsdienste beschreiben und eingesetzte Telekommunikationsanlagen darstellen

Welche Telekommunikationsdienste werden mit welchen Telekommunikationssystemen erbracht?
In welchen angebundenen DV-Systemen oder Anlagen werden personenbezogene Daten von Kunden (Bestands- und Verkehrsdaten) erhoben, verarbeitet, genutzt oder gespeichert?

3.3 Sicherheitsteilsysteme bilden

bezüglich übergreifender Aspekte, Infrastruktur, TK / DV-Systeme, Netze und Anwendungen
Welche Betrachtungseinheiten (Teilsysteme) können sinnvoll gebildet werden, um die jeweiligen Schutzmaßnahmen individuell zuordnen zu können?

je Sicherheits-teilsystem

3.4 Schutzziele und Gefährdungen den Sicherheitsteilsystemen zuordnen

Schutzziele:

- Schutz des Fernmeldegeheimnisses
- Schutz personenbezogener Daten
- Schutz vor Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und –diensten führen

Gefährdungen je Teilsystem und Schutzziel

- Elementare Gefährdungen
- Technische Störungen, Ausfälle etc.
- Organisatorische Gefährdungen und menschliche Fehlhandlungen
- Mängel durch Fehler in der Planungsphase
- Sabotage (intern, extern)

3.5 Sicherheitsanforderungen ableiten

Ausgehend von den Gefährdungen der Schutzziele können je Teilsystem die konkreten Sicherheitsanforderungen festgelegt werden

3.6 Schutzmaßnahmen festlegen, beschreiben und umsetzen

3.7 Gesamtsystem bewerten

3.8 System kontinuierlich verbessern

3.9 Mitteilungspflichten

3.1 TK-Netzstrukturplan darstellen

Zu Beginn soll der Verpflichtete eine Übersicht über die Komponenten seines Netzes und deren Verbindungen darstellen. Der Netzplan soll mindestens folgende Komponenten enthalten:

1. Die im Netz eingebundenen TK- und DV-Systeme (Vermittlungseinrichtungen, Dienste-Server, Netzwerkmanagement) und alle eingesetzten DV-Anlagen (Kundendatenverwaltung, Billing)
2. Alle Verbindungen zwischen den Systemen (LAN-Verbindungen, Backbone-Techniken, auch Funkstrecken)
3. Die Außenverbindungen der Systeme (Art der Verbindung, Internet, Remote)

Die Komplexität des Netzplans kann 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.

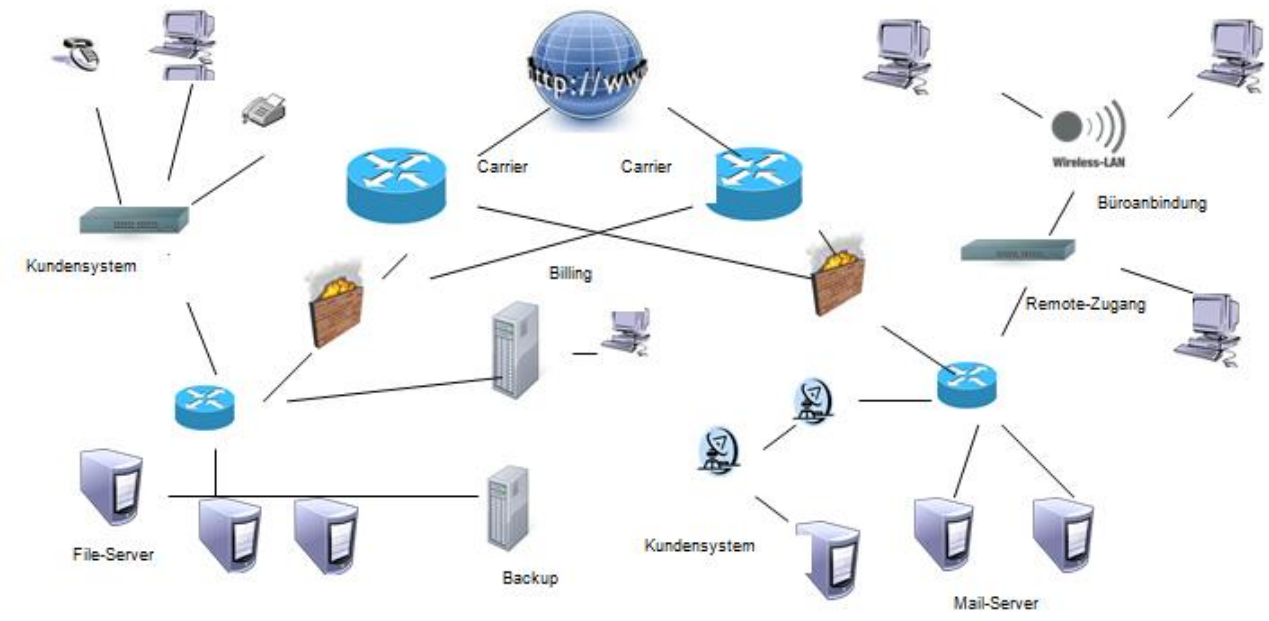

Bild 1: TK- / DV-Netzstrukturplan (Prinzipdarstellung)

3.2 Telekommunikationsdienste beschreiben und eingesetzte Telekommunikationsanlagen darstellen

Um Schutzmaßnahmen sinnvoll zuordnen zu können, sind alle Telekommunikationsdienste, die für die Öffentlichkeit erbracht werden, mit einer Kurzbeschreibung des Dienstes darzustellen.
Die dafür eingesetzten Telekommunikations- und Datenverarbeitungssysteme sind hinsichtlich ihrer Funktion zu beschreiben. Aus der Beschreibung sollte auch hervorgehen, ob die Systeme personenbezogene Daten verarbeiten oder/und speichern.

3.3 Sicherheitsteilsysteme bilden

Wegen der teilweise sehr unterschiedlichen Gefährdungen einzelner Komponenten eines komplexen Systems oder eines Netzes kann es angebracht sein, kleinere Betrachtungseinheiten (Teilsysteme) zu bilden.
Diesen Teilsystemen können dann die jeweiligen Schutzziele - und in der Folge die adäquaten Sicherheitsanforderungen - individuell zugeordnet werden. Das Festlegen der Sicherheitsteilsysteme kann gegebenenfalls unabhängig von technischen Aspekten erfolgen. Wichtig ist dabei eine Einteilung, die hinsichtlich der Sicherheitsanforderungen und Schutzziele plausibel ist. Dies schließt nicht aus, dass mehrere Komponenten zusammen auch gleichzeitig als Sicherheitsteilsystem identifiziert werden können.
Im Falle gemeinsam genutzter Standorte oder gemeinsam genutzter technischer Einrichtungen hat jeder Beteiligte eigene Teilsysteme zu bilden.
Zur Erreichung der Standardsicherheit sind auch solche Komponenten oder Objekte zu berücksichtigen, die nicht unmittelbar der Telekommunikation dienen, aber für den Betrieb mittelbar notwendig sind (z.B. Netzersatzanlagen).

Anmerkung:
Weitere Hinweise für die sinnvolle Bildung von Teilsystemen (Bausteinen) können den IT-Grundschutz-Katalogen des BSI entnommen werden (Bausteinkataloge).

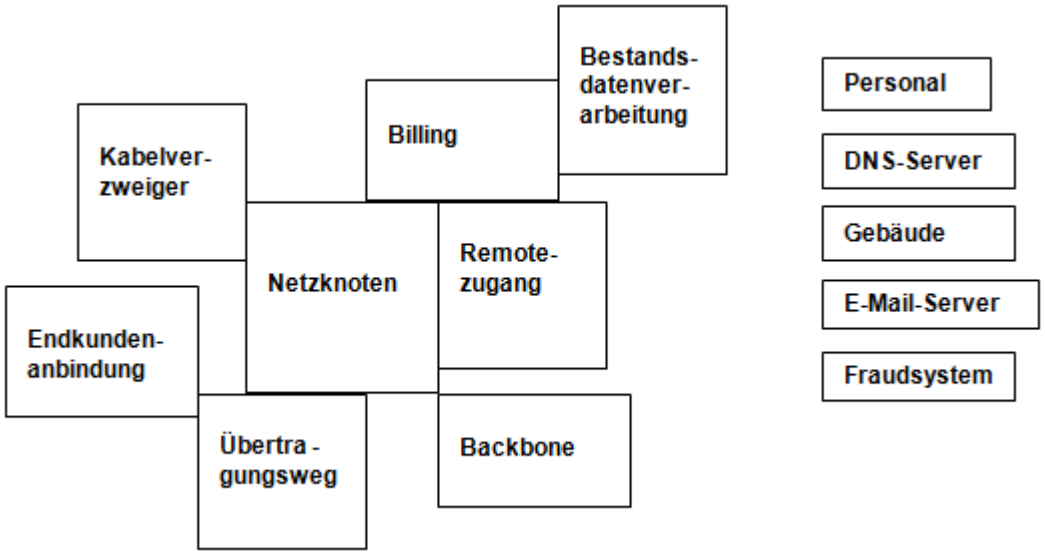

Bild 2: Abgeleitete Teilsysteme: (Beispiele)

3.4 Schutzziele und Gefährdungen den Sicherheitsteilsystemen zuordnen

Für das Erreichen der im § 109 TKG geforderten Standardsicherheit sind nicht immer alle Schutzziele für alle Sicherheitsteilsysteme von Bedeutung. Daher sind in einem ersten Schritt den festgelegten Sicherheitsteilsystemen die betreffenden Schutzziele (siehe Abschnitt 2) zuzuordnen. Werden bestimmte Schutzziele für ein Sicherheitsteilsystem als bedeutungslos angesehen, ist dies zu begründen.

Die möglichen Gefährdungen (vorhandene sowie anzunehmende) sind für jedes Sicherheitsteilsystem zu ermitteln.
Für gemeinsam genutzte Standorte oder technische Einrichtungen ist von allen Beteiligten

kritisch zu prüfen, welche gegenseitige Abhängigkeiten sich für die geforderte Standardsicherheit ergeben, um dann die angemessenen Vorsorgemaßnahmen treffen zu können.

Die Gefährdungen der Schutzziele können zum Beispiel in folgende Gruppen eingeteilt werden:

- Elementare Gefährdungen
- Technische Störungen, Ausfälle
- Organisatorische Gefährdungen und menschliche Fehlhandlungen
- Mängel durch Fehler in der Planungsphase
- Sabotage (intern, extern), Angriffe
- Benutzerverhalten

Anmerkung:
Weitere Hinweise für Gefährdungen in Bezug auf Teilsysteme (Bausteine) können den IT Grundschutz-Katalogen des Bundesamts für Sicherheit in der Informationstechnik (BSI) entnommen werden (Gefährdungskatalog).
Gefährdungen im Zusammenhang mit der Nutzung des Internets können der ISi-Schriftenreihe und den Cybersicherheitsempfehlungen für Internetservice Provider des BSI entnommen werden.

3.5 Sicherheitsanforderungen je Teilsystem ableiten

Aus den Ergebnissen der Untersuchungen und der Überlegungen hinsichtlich möglicher Gefährdungen sind Sicherheitsanforderungen für die verwendeten Sicherheitsteilsysteme abzuleiten.

3.6 Schutzmaßnahmen festlegen, beschreiben und umsetzen

Auf der Basis der festgelegten Sicherheitsanforderungen sind konkrete Maßnahmen zur Erfüllung der Verpflichtungen nach § 109 Absatz 1 und 2 TKG zu treffen.

Die Sicherheitsmaßnahmen müssen geeignet sein, die Gefährdungen der Sicherheitsteilsysteme angemessen zu reduzieren. Sie sind den vorhandenen Komponenten oder Objekten zuzuordnen. Sollten Sicherheitsteilsysteme als nicht ausreichend geschützt bewertet werden, sind weitere geeignete Schutzmaßnahmen vorzusehen.

Die umgesetzten oder bis zu einem bestimmten Zeitpunkt umzusetzenden Sicherheitsmaßnahmen sind darzulegen. Zur Erreichung einer angemessenen Standardsicherheit soll Technologie zur Anwendung kommen, die dem Stand der Technik entspricht.

Für gemeinsam genutzte Standorte oder gemeinsam genutzte technische Einrichtungen ist eine sorgfältige Prüfung der sich aus der Überschneidung der Technik ergebenden Risiken hinsichtlich der geforderten Standardsicherheit erforderlich. Die gemeinsam genutzten Komponenten oder Infrastrukturelemente sind zu benennen und die getroffenen Schutzmaßnahmen zur Erreichung der Schutzziele detailliert zu beschreiben.

Schutzmaßnahmen können wie folgt gegliedert sein:

- Maßnahmen bei der Infrastruktur
- Organisatorische Regelungen

- Regelungen für das Personal
- Technische Maßnahmen
- Notfallmaßnahmen

Anmerkung:
Weitere Hinweise zu Schutzmaßnahmen bezogen auf Teilsysteme (Bausteine) können den Grundschutzkatalogen des BSI entnommen werden (Maßnahmenkatalog). Maßnahmen im Zusammenhang mit der Nutzung des Internets können der ISi-Schriftenreihe des BSI entnommen werden.

3.7 Gesamtsystem bewerten

Auch wenn jedes Sicherheitsteilsystem einzeln die Sicherheitsanforderungen erfüllt, kann das Gesamtsystem noch Sicherheitsmängel aufweisen. Aus diesem Grund ist zusätzlich eine Bewertung des Gesamtsystems erforderlich, d.h. das Zusammenwirken der Sicherheitsteilsysteme, wie auch die Wirkung der angewendeten Schutzmaßnahmen, ist hinsichtlich der Erreichung einer angemessenen Standardsicherheit für das Gesamtsystem zu untersuchen.

Daraus ergibt sich gegebenenfalls die Notwendigkeit für weitere zusätzliche Schutzmaßnahmen, welche über die eines Teilsystems hinausgehen. Denkbar sind Schutzmaßnahmen, die über mehrere, an verschiedenen Orten installierte Sicherheitsteilsysteme wirken oder die erst beim Zusammenwirken von Sicherheitsteilsystemen erforderlich werden.

In der abschließenden Risikobewertung soll das bestehende Restrisiko erkannt und bewertet werden. Ziel ist es, dieses Risiko so weit zu reduzieren, dass das verbleibende Restrisiko quantifizierbar und akzeptierbar wird.

3.8 System kontinuierlich verbessern

Um den Erfolg der Schutzmaßnahmen in einem sich ständig ändernden Umfeld (Geschäftsprozesse, IT-Landschaften, Gesetze und Vorgaben, Bedrohung etc.) dauerhaft sicherzustellen, muss gewährleistet sein, dass in regelmäßigen Abständen die Wirksamkeit der umgesetzten Sicherheitsmaßnahmen festgestellt und bewertet wird. Bei erkannten Sicherheitsproblemen müssen systematisch Verbesserungsmaßnahmen ergriffen, umgesetzt und dokumentiert werden.
Hierbei ist der aktuelle Stand der Technik zu berücksichtigen.

3.9 Mitteilungspflichten

Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat nach § 109 Absatz 5 TKG der Bundesnetzagentur eine Sicherheitsverletzung einschließlich Störungen von Telekommunikationsnetzen oder -diensten unverzüglich mitzuteilen, sofern hierdurch beträchtliche Auswirkungen auf den Betrieb der Telekommunikationsnetze oder das Erbringen von Telekommunikationsdiensten entstehen.

Die Bundesnetzagentur **kann** von dem Verpflichteten einen detaillierten Bericht über die Sicherheitsverletzungen und die ergriffenen Abhilfemaßnahmen verlangen. Erforderlichenfalls unterrichtet die Bundesnetzagentur das Bundesamt für Sicherheit in der Informationstechnik, die nationalen Regulierungsbehörden der anderen Mitgliedstaaten der Europäischen Union sowie die Europäische Agentur für Netz- und Informationssicherheit über die Sicherheitsverletzungen.

Die Bundesnetzagentur kann die Öffentlichkeit informieren oder die Verpflichteten zu dieser Unterrichtung auffordern, wenn sie zu dem Schluss gelangt, dass die Bekanntgabe der Sicherheitsverletzung im öffentlichen Interesse liegt.
Die Bundesnetzagentur legt der Kommission, der Europäischen Agentur für Netz- und Informationssicherheit und dem Bundesamt für Sicherheit der Informationstechnik einmal pro Jahr einen zusammenfassenden Bericht über die eingegangenen Mitteilungen und die ergriffenen Abhilfemaßnahmen vor.

Wer öffentlich zugängliche Telekommunikationsdienste erbringt, hat nach § 109a TKG, im Fall einer Verletzung des Schutzes personenbezogener Daten unverzüglich die Bundesnetzagentur und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit von der Verletzung zu benachrichtigen.
Ist anzunehmen, dass durch die Verletzung des Schutzes personenbezogener Daten Teilnehmer oder andere Personen schwerwiegend in ihren Rechten oder schutzwürdigen Interessen beeinträchtigt werden, hat der Anbieter des Telekommunikationsdienstes zusätzlich die Betroffenen unverzüglich von dieser Verletzung zu benachrichtigen.

In Fällen, in denen in dem Sicherheitskonzept nachgewiesen wurde, dass die von der Verletzung betroffenen personenbezogenen Daten durch geeignete technische Vorkehrungen gesichert, insbesondere unter Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens gespeichert wurden, ist eine Benachrichtigung nicht erforderlich.
Unabhängig davon kann die Bundesnetzagentur den Anbieter des Telekommunikations-dienstes unter Berücksichtigung der wahrscheinlich nachteiligen Auswirkungen der Verletzung des Schutzes personenbezogener Daten zu einer Benachrichtigung der Betroffenen verpflichten. Die Benachrichtigung an die Betroffenen muss mindestens enthalten:

1. Die Art der Verletzung des Schutzes personenbezogener Daten
2. Angaben zu den Kontaktstellen, bei denen weitere Informationen erhältlich sind
3. Empfehlungen zu Maßnahmen, die mögliche nachteilige Auswirkungen der Verletzung des Schutzes personenbezogener Daten begrenzen

In der Benachrichtigung an die Bundesnetzagentur und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit hat der Anbieter des Telekommunikationsdienstes zusätzlich zu den Angaben die Folgen der Verletzung des Schutzes personenbezogener Daten und die beabsichtigten oder ergriffenen Maßnahmen darzulegen.

Die Anbieter der Telekommunikationsdienste haben ein Verzeichnis der Verletzungen des Schutzes personenbezogener Daten zu führen, dass Angaben zu Folgendem enthält:

1. Umstände der Verletzungen
2. Auswirkungen der Verletzungen
3. Ergriffene Abhilfemaßnahmen

Diese Angaben müssen ausreichend sein, um der Bundesnetzagentur und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit die Prüfung zu ermöglichen, ob die geltenden Bestimmungen eingehalten wurden. Das Verzeichnis enthält nur die zu diesem Zweck erforderlichen Informationen und muss nicht Verletzungen berücksichtigen, die mehr als fünf Jahre zurückliegen.

Anmerkung:
Hinweise für die Umsetzung der Verpflichtungen nach den §§ 109 Absatz 3 und 109a TKG finden sich in den ENISA Publikationen „Technical Guidelines for Reporting Incidents“ bzw. „Recommandations for technical implementation of Art.4”. [1]

3.10 Informationssicherheits-Managementsystem

Mit der ISO-27000-Normenreihe existiert eine Sammlung internationaler Standards, die Sicherheitsmaßnahmen für den Schutz der IT definiert. Sie liefert Empfehlungen für die Einrichtung, Umsetzung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung eines Informationssicherheits-Managementsystems (ISMS) zum Schutz der gesamten IT-Organisation. Die Gestaltung und Umsetzung eines ISMS hängen von den Bedürfnissen und Zielen, Sicheranforderungen, eingesetzten Verfahren und der Größe und Struktur der Organisation ab.
Die ISO 27001 formuliert dabei die Anforderungen, die ein ISMS erfüllen sollte. Ergänzend dazu finden sich in den weiteren Publikationen Leitfäden für die konkrete Umsetzung (ISO 27002 IT-Sicherheitsverfahren – Leitfaden für das Informationsmanagement) aber auch branchenspezifische Anpassungen (ISO 27011 ISMS -Anforderungen für Telekommunikationsunternehmen).

Die BSI Standards bauen auf den genannten ISO-Normen auf und zeigen wie eine Umsetzung dieser Standards funktionieren kann.

[1] ENISA (European Network and Information Security Agency)

4. Sicherheitskonzept

Wer öffentliche Telekommunikationsnetze betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat eine **Sicherheitsbeauftragte** oder einen **Sicherheitsbeauftragten** zu benennen und ein **Sicherheitskonzept** zu erstellen, aus dem hervorgeht:

1. Welche öffentlichen Telekommunikationsnetze betrieben und welche öffentlich zugänglichen Telekommunikationsdienste erbracht werden
2. Von welchen Gefährdungen auszugehen ist
3. Welche technischen Vorkehrungen oder sonstigen Schutzmaßnahmen zur Erfüllung der Verpflichtungen getroffen oder geplant sind

4.1 Sicherheitskonzept erstellen

Das Sicherheitskonzept dient dem Betreiber zur Bewusstseinsbildung über die sicherheitsrelevante Bedeutung einzelner Sicherheitsteilsysteme und zur Beurteilung der Sicherheit und Integrität von Netzen und Diensten sowie der fortlaufenden Verfügbarkeit der über diese Netze erbrachten Dienste.

Alle ermittelten Sicherheitsteilsysteme sind zu beschreiben sowie alle gemäß Kapitel 3 durchgeführten und geplanten Schritte und die Bewertungen zu dokumentieren. Die angewendeten Schutzmaßnahmen sind zu nennen und wenn notwendig zu erläutern. Verbleibende Restrisiken sind zu benennen und zu bewerten.

Die Organisation eines Störfallmanagements und das Mitteilungsverfahren für Sicherheitsverletzungen von Telekommunikationsnetzen oder –diensten sind zu beschreiben.

Anmerkung:
Die im Kapitel 3 beschriebene Vorgehensweise dient als Grundlage für die Erstellung des Sicherheitskonzeptes.

4.2 Sicherheitskonzept vorlegen

Wer ein öffentliches Telekommunikationsnetz betreibt, hat der Bundesnetzagentur das Sicherheitskonzept unverzüglich nach Aufnahme des Netzbetriebs vorzulegen.
Wer öffentlich zugängliche Telekommunikationsdienste erbringt, kann nach der Bereitstellung des Telekommunikationsdienstes von der Bundesnetzagentur verpflichtet werden, das Sicherheitskonzept vorzulegen.
Mit dem Sicherheitskonzept ist eine Erklärung vorzulegen, dass die darin aufgezeigten technischen Vorkehrungen und sonstigen Schutzmaßnahmen umgesetzt sind oder unverzüglich umgesetzt werden.

Stellt die Bundesnetzagentur im Sicherheitskonzept oder bei dessen Umsetzung Sicherheitsmängel fest, so kann sie deren unverzügliche Beseitigung verlangen.
Sofern sich die dem Sicherheitskonzept zu Grunde liegenden Gegebenheiten ändern, hat der Verpflichtete das Konzept anzupassen und der Bundesnetzagentur unter Hinweis auf die Änderungen erneut vorzulegen.
Die Bundesnetzagentur kann die Umsetzung des Sicherheitskonzeptes überprüfen.

Die Bundesnetzagentur kann anordnen, dass sich die Betreiber öffentlicher Telekommunikationsnetze oder die Anbieter öffentlich zugänglicher Telekommunikationsdienste einer Überprüfung durch eine qualifizierte unabhängige Stelle oder eine zuständige nationale Behörde unterziehen, in der festgestellt wird ob die Anforderungen des Sicherheitskonzeptes erfüllt

sind. Der Verpflichtete hat eine Kopie des Überprüfungsberichts unverzüglich an die Bundesnetzagentur zu übermitteln. Die Kosten dieser Überprüfung trägt der Verpflichtete.

4.3 TK - Unternehmen, deren Infrastruktur für die Allgemeinheit / Öffentlichkeit von besonderer Bedeutung ist

Höhere Sicherheitsanforderungen als die unter dem Begriff der Standardsicherheit angeführten, sind an jene Netze bzw. Dienste zu stellen, die für die Allgemeinheit von wesentlicher Bedeutung sind. Betreiber dieser Netze bzw. Anbieter dieser Dienste sind verpflichtet darzulegen, inwieweit die im Einzelnen beschriebenen Schutzvorkehrungen über ein Standardniveau hinausgehen.

4.4 Diagramm für die Erstellung eines Sicherheitskonzeptes

In dem nachfolgenden Diagramm ist beispielhaft der Ablauf zur Erstellung eines Sicherheitskonzeptes dargestellt. In den einzelnen Feldern wird Bezug auf die relevanten Abschnitte / Absätze des Katalogs genommen.

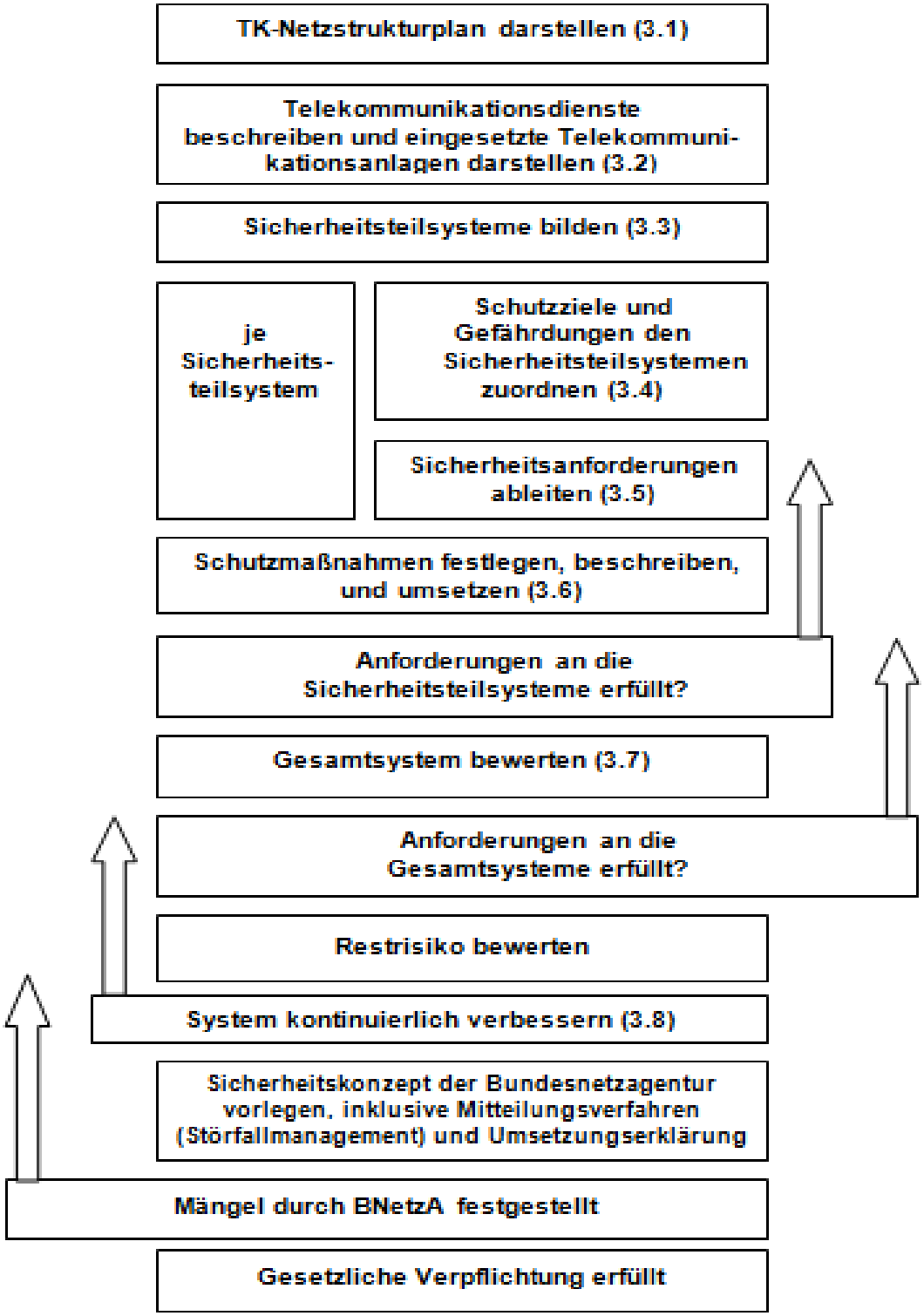

Bild 3: Ablaufdiagramm für die Erstellung eines Sicherheitskonzeptes

5. Risikomanagement[1]

Obwohl durch Regelungen des TKG **nicht** gefordert, wird die Implementierung eines Risikomanagementsystems zur Erhöhung der Sicherheit des Unternehmens, auch unter Berücksichtigung von Aspekten des Datenschutzes, Fernmeldegeheimnisses sowie der Telekommunikations-Infrastruktur, ausdrücklich empfohlen. Grundlage von Risikomanagementsystemen ist dabei die Definition einer Risikopolitik als Bestandteil der unternehmerischen Geschäftspolitik, die Leitlinien zum Umgang mit Risiken festlegt.

Elemente des Risikomanagements sind die Risikoanalyse, die Risikosteuerung und Risikobewältigung, die Risikoüberwachung sowie die Risikofinanzierung:

- In der Risikoanalyse sind sämtliche für das Unternehmen relevanten Risiken (einschließlich der im Sicherheitskonzept beschriebenen Gefährdungen) zu identifizieren, zu analysieren und individuell zu bewerten.
- Die Risikosteuerung dient der Risikovermeidung oder –minderung ggf. auch der Risikoabwälzung auf Dritte (z.B. Kunden, Lieferanten oder Versicherungen). Ein verbleibendes Restrisiko ist zu tolerieren.
- Im Rahmen der Risikoüberwachung sind Frühwarn- und Kontrollsysteme einzurichten (z.B. auch eine branchenspezifische oder branchenübergreifende Kommunikation; Mitarbeit in den einschlägigen Gremien des UP KRITIS, Teilnahme am branchenspezifischen TK-SPOC der BNetzA).
- Das Konzept zur Risikofinanzierung stellt sicher, dass erforderliche Investitionen auch langfristig gewährleistet werden.

5.1 Notfallplanung

Wenn Einrichtungen, die zur Erbringung der TK- Dienste mittelbar oder unmittelbar erforderlich sind, gestört sind, sollte der Betreiber Maßnahmen ergreifen, um deren Auswirkungen so gering wie möglich zu halten. Um die Folgen einer Störung in einem Notfall oder einer Krise beherrschen zu können, sollten ausreichende Informationen über die Einrichtungen allen internen und externen Stellen, die in eine Notfallbewältigung involviert sind (Gefahrenabwehrbehörden), zur Verfügung gestellt werden. Für mögliche Notfallszenarien sollten Alarm- und Gefahrenabwehrpläne erstellt werden.
Hierzu gehört auch eine funktionierende und effektive Krisenkommunikation sowie ggf. die Einrichtung einer Meldestelle für den Krisenfall.
Darüber hinaus wird die Erstellung, Umsetzung und regelmäßige Prüfung von Notfallkonzepten für einen möglichen Personalausfall empfohlen.
Schulungen zum Notfallplan sowie die Sensibilisierung durch zielgruppenspezifische Informationsangebote sind zusätzliche Komponenten, die die Chancen für eine erfolgreiche Bewältigung einer Notfallsituation erhöhen.
Schließlich sollen Notfallsituationen simuliert und die Bewältigung der Notfall- / Krisensituationen geübt werden. Durch Auswertung der Übungsergebnisse sowie die Berücksichtigung der gewonnenen Erfahrungen im Notfallplan kann im Rahmen der „kontinuierlichen Verbesserung“ eine Optimierung der Notfallplanungen gewährleistet werden.

---

1 Schutz Kritischer Infrastrukturen-Basisschutzkonzept, Empfehlungen für Unternehmen, Bundesministerium des Innern, Alt-Moabit 101 D, 10559 Berlin, August 2005

Schließlich wird auch die Teilnahme an branchenbezogenen oder branchenübergreifenden Übungen empfohlen, z.B. im Rahmen des UP KRITIS- Arbeitsgruppen.

5.2 Risiko- und Krisenkommunikation

Sowohl im Vorfeld von Krisenereignissen (auch schon während des regulären Betriebes als Warn- und Alarmsystem) als auch nach Eintritt schwerer Schadensfälle kommt einer angemessenen und möglichst effizienten Kommunikation innerhalb des Unternehmens und zu Externen (Geschäftspartner, Kunden, Öffentlichkeit, öffentliche Stellen etc.) eine besondere Bedeutung zu. Zur Gewährleistung des Informationsflusses innerhalb der Telekommunikationsbranche, zur Bundesnetzagentur und zum BSI sowie zu Betreibern anderer kritischer Infrastrukturen, die zur Aufrechterhaltung des TK- Betriebes von Bedeutung sind, wird die Teilnahme am Kommunikationssystem zur Alarmierung und Krisenbewältigung gemäß UP KRITIS empfohlen. Die BNetzA betreibt hierzu einen SPoC für die Telekommunikationsbranche.

5.3 Ausfall- und Business Continuity Management

Um den Geschäftsbetrieb auch im Krisenfall weitgehend aufrechtzuerhalten, zumindest jedoch einen Notbetrieb einrichten und möglichst schnell die vollständige Funktionsfähigkeit wieder herstellen zu können, müssen frühzeitig Konzepte einer Ausfallplanung und Maßnahmen im Rahmen der Business Continuity festgelegt werden. Ausfallpläne sollten insbesondere Alternativkonzepte zur Gestaltung zentraler Geschäftsprozesse bei Ausfall von kritischen Bereichen im Unternehmen sowie von Zulieferern und Dienstleistern berücksichtigen.

Empfohlen werden insbesondere folgende Punkte:

- Für besonders sensible Bereiche sollten redundante Systeme bereitgehalten werden (ggf. auch räumlich getrennt).
- Für den Betrieb von technischen Einrichtungen sollte eine ausreichende Menge von Betriebsstoffen vorgehalten werden. Hierbei ist besonders auf Auswirkungen großflächiger Ereignisse, die über mehrere Tage andauern, zu achten (zum Beispiel unpassierbare Zufahrtswege oder lang anhaltende Stromausfälle).
- Zur Vorbeugung von Personalausfällen, zum Beispiel durch Epidemien, sollen ausreichende Personalkapazitäten, insbesondere in Schlüsselpositionen, vorgehalten werden. Durch geeignete Qualifizierungen sollen Vertretungen ermöglicht werden.
- Ausfall- und Notfallpläne sollen regelmäßig überprüft und neuen Entwicklungen / Erfahrungen angepasst werden.

6. Sicherheitsteilsysteme

Kapitel 3 des Katalogs befasst sich detailliert mit der Vorgehensweise bei der Ermittlung der Sicherheitsanforderungen. Im Fokus stehen hierbei Telekommunikationsnetze und –dienste sowie Telekommunikationsanlagen. Aufgrund der durch §109 Absatz 1 und 2 TKG vorgegebenen Schutzziele lässt sich eine Gefährdungsanalyse durchführen, die eine Basis bildet für die Zuordnung konkreter Sicherheitsanforderungen. Letztlich werden bezüglich der einzelnen Schutzanforderungen Schutzmaßnahmen zu definieren sein, die diesen gerecht werden und einen angemessenen Grad an Sicherheit gewährleisten.

Um die hier beschriebene Vorarbeit zur Erstellung eines Sicherheitskonzeptes möglichst effektiv und effizient zu gestalten, erscheint es in vielen Fällen sinnvoll, das zu betrachtende Gesamtsystem in Teilsysteme zu untergliedern. Grundsätzlich lassen sich unter Berücksichtigung der Regelungen des § 109 Absatz 1 und 2 TKG drei Bereiche von Sicherheitsteilsystemen definieren:

1. Sicherheitsteilsysteme zur Beschreibung der Rahmenbedingungen und allgemeinen technischen Bestandteilen
2. Sicherheitsteilsysteme zur Beschreibung von Telekommunikations- und Datenverarbeitungssystemen, die mittelbar oder unmittelbar für die Erbringung einer Telekommunikationsdienstleistung erforderlich sind
3. Sicherheitsteilsysteme zur Beschreibung von Datenverarbeitungsanlagen

Die hier aufgeführten drei Bereiche von Sicherheitsteilsystemen sind von den Unternehmen frei wähl- und konfigurierbar. Je nach der zugrundeliegenden Struktur und Zielsetzung des zu betrachtenden Gesamtsystems kann ein einziger Bereich der o. g. Sicherheitsteilsysteme aber auch zwei oder alle drei Bereiche von Relevanz sein.

Nachfolgend werden die Bereiche der o. g. Sicherheitsteilsysteme in den Kapiteln 6.1 bis 6.3 einer näheren Betrachtung unterzogen. Dabei werden exemplarisch Sicherheitsteilsysteme benannt, die vor allem als Leitlinie für mögliche Ansatzpunkte bei der Erstellung eines Sicherheitskonzeptes dienen sollen. In der Praxis bietet sich die Möglichkeit, einzelne Sicherheitsteilsysteme weiter zu untergliedern oder mehrere Sicherheitsteilsysteme (ggf. auch aus unterschiedlichen Bereichen) zusammen zu fassen. Das Unternehmen hat die Möglichkeit, technische Einrichtungen wie z.B. Telekommunikations- und Datenverarbeitungssysteme aber auch Gebäude, Räume, Anwendungen und Personal systematisch unter Berücksichtigung von Sicherheitsanforderungen zu verknüpfen.

Wie oben bereits angedeutet, erhebt die in den Kapiteln 6.1 bis 6.3 dargestellte exemplarische Auflistung von Sicherheitsteilsystemen und technischen sowie sonstigen Elementen einzelner Sicherheitsteilsysteme keinen Anspruch auf Vollständigkeit. Grundsätzlich können auch Sicherheitsteilsysteme benannt werden, die in diesen Kapiteln nicht aufgeführt sind, die aber im zu betrachtenden Gesamtsystem vorhanden sind und einer separaten Betrachtung unterzogen werden sollten.

Die beispielhaft aufgeführten Sicherheitsteilsysteme unter 6.2 und 6.3 orientieren sich an den Begriffen des TKG sowie des BDSG. Je nach gewählter Granularität können verschiedene technische Einrichtungen unter verschiedenen Beispielen der Sicherheitsteilsysteme dargestellt sein (vergleiche z.B. „Telekommunikationsnetz“ und „Übertragungswege“). Welches der beschriebenen Beispiele bei welcher Granularität sinnvoller Weise vom Verpflichteten bei der Gefährdungsanalyse herangezogen wird, ist in starkem Maße von den unternehmensspezifischen Rahmenbedingungen abhängig.

6.1 Sicherheitsteilsysteme zur Beschreibung der Rahmenbedingungen und allgemeinen technischen Bestandteilen

Zur Spezifizierung des Bereiches der Sicherheitsteilsysteme zur Beschreibung von Rahmenbedingungen und allgemeinen technischen Bestandteilen bietet es sich an, die IT-Grundschutzkataloge des BSI heran zu ziehen unter:

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

Die darin enthaltenen Bausteinkataloge B1 bis B5 beinhalten jeweils Beschreibungen und Elemente, die bei der Bildung von unternehmensspezifischen Sicherheitsteilsystemen berücksichtigt werden können:

1. B 1: Übergreifende Aspekte (z.B. Organisation, Personal)
2. B 2: Sicherheit der Infrastruktur (z.B. Gebäude, Haustechnik, Klimatechnik)
3. B 3: Sicherheit der DV-Systeme
4. B 4: Sicherheit im Netz
5. B 5: Sicherheit in Anwendungen

Soweit technische Ausprägungen in den Katalogen B1 bis B5 betroffen sind, beziehen sich diese auf allgemeine Aspekte. Sicherheitsteilsysteme, die den Bereich Telekommunikations- und Datenverarbeitungssysteme betreffen, orientieren sich maßgeblich am TKG sowie am BDSG und werden in den Kapiteln 6.2 und 6.3 beschrieben.

Weitere Hinweise zur Beschreibung der Teilsysteme können aus der BSI-Schriftenreihe zur Internet-Sicherheit (ISi-Reihe) und den Cybersicherheitsempfehlungen für Internetservice Provider entnommen werden.

6.2 Sicherheitsteilsysteme zur Beschreibung von Telekommunikations- und Datenverarbeitungssystemen

Diese Kategorie von Sicherheitsteilsystemen zielt im Wesentlichen auf die Beschreibung von Telekommunikations- und Datenverarbeitungssysteme ab.
Eine Gliederung wie nachfolgend dargestellt ist möglich:

1. Telekommunikations- und Datenverarbeitungssysteme, die dem Betrieb von öffentlichen Netzen oder der Erbringung von öffentlich zugänglichen Telekommunikationsdiensten dienen
2. Gemeinsam mit anderen Diensteanbietern genutzte Standorte und technische Einrichtungen
3. Tätigkeiten im Auftrag durch andere Stellen

6.2.1 Telekommunikations- und Datenverarbeitungssysteme, die dem Betrieb von öffentlichen Netzen oder der Erbringung von öffentlich zugänglichen Telekommunikationsdiensten dienen

Das Sicherheitsteilsystem von Telekommunikations- und Datenverarbeitungssystemen kann unternehmensspezifisch in weitere kleinere Sicherheitsteilsysteme differenziert werden. Eine solche weitere Untergliederung kann von der Unternehmensgröße, von dem Angebot der vom Unternehmen bereitgestellten Dienste, von den dazu betriebenen technischen Einrich-

tungen, von qualitäts- und sicherheitsspezifischen Anforderungen und vielen anderen Aspekten abhängig sein. Deshalb werden an dieser Stelle lediglich einige weitere „Sub“-Sicherheitsteilsysteme benannt, die jeweils mit Beispielen zu einzelnen Elementen dieser Untergruppe belegt sind.

- **Telekommunikationsanlagen die Nachrichten senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren**

Beispiele für einzelne Elemente dieses „Sub-Sicherheitssystems“:

Die folgenden Beispiele sind überwiegend aus dem Bereich der Begriffsdefinitionen des TKG entnommen. Die einzelnen Begrifflichkeiten sind nicht klar voneinander abgegrenzt. Das Element „Übertragungsweg“ ist beispielsweise als Teilmenge in der Definition des Elementes „Telekommunikationsnetz“ enthalten.

Telekommunikationsnetz
Die Gesamtheit von Übertragungssystemen und gegebenenfalls Vermittlungs- und Leitwegeinrichtungen sowie anderweitiger Ressourcen, einschließlich der nicht aktiven Netzbestandteile, die die Übertragung von Signalen über Kabel, Funk, optische und andere elektromagnetische Einrichtungen ermöglichen, einschließlich Satellitennetzen, festen, leitungs- und paketvermittelten Netzen, einschließlich des Internet und mobilen terrestrischen Netzen, Stromleitungssystemen, soweit sie zur Signalübertragung genutzt werden, Netzen für Hörfunk und Fernsehen sowie Kabelfernsehnetzen, unabhängig von der Art der übertragenen Information.

Übertragungswege
Telekommunikationsanlagen in Form von Kabel- oder Funkverbindungen mit ihren übertragungstechnischen Einrichtungen als Punkt-zu-Punkt oder Punkt-zu-Mehrpunktverbindungen mit einem bestimmten Informationsdurchsatzvermögen (Bandbreite oder Bitrate) einschließlich ihrer Abschlusseinrichtungen.

Telekommunikationslinien
Unter- oder oberirdisch geführte Telekommunikationskabelanlagen einschließlich ihrer zugehörigen Schalt- und Verzweigungseinrichtungen, Masten und Unterstützungen, Kabelschächte und Kabelkanalrohre.

Zusammenschaltung
Derjenige Zugang, der die physische und logische Verbindung öffentlicher Telekommunikationsnetze herstellt, um Nutzern eines Unternehmens die Kommunikation mit Nutzern desselben oder eines anderen Unternehmens oder die Inanspruchnahme von Diensten eines anderen Unternehmens zu ermöglichen; Dienste können von den beteiligten Parteien erbracht werden oder von anderen Parteien, die Zugang zum Netz haben. Zusammenschaltung ist ein Sonderfall des Zugangs und wird zwischen Betreibern öffentlicher Telekommunikationsnetze hergestellt.

Vermittlungseinrichtung
In Vermittlungsnetzen zentrale Netzknoteneinrichtung, die den Benutzern des Netzes überwiegend zeitlich beschränkte Kommunikationsmöglichkeiten mit anderen Benutzern oder Anschlüssen ihrer Wahl einräumt.

Netzabschlusspunkt
Der physische Punkt, an dem einem Teilnehmer der Zugang zu einem Telekommunikationsnetz bereitgestellt wird; in Netzen, in denen eine Vermittlung oder Leitwegebestimmung er-

folgt, wird der Netzabschlusspunkt anhand einer bestimmten Netzadresse bezeichnet, die mit der Nummer oder dem Namen eines Teilnehmers verknüpft sein kann.

- **Nachrichtenübermittlungssysteme mit Zwischenspeicherung**

Hierzu gehören technische Einrichtungen oder Systeme, die im Rahmen der Erbringung von Telekommunikationsdiensten der Zwischenspeicherung von Nachrichteninhalten dienen.

Beispiele für einzelne Elemente dieses „Sub"-Sicherheitssystems:

E-Mail-Server
Fax-Server
SMS-Server
Sprachbox-Systeme

- **Sonstige Einrichtungen für einen ordnungsgemäßen Betrieb**

Hierzu gehören Hardware- und Softwarekomponenten, die für einen ordnungsgemäßen Betrieb von Telekommunikationsnetzen und die fortlaufende Verfügbarkeit von Telekommunikationsdiensten erforderlich sind.

Beispiele für einzelne Elemente dieses „Sub-Sicherheitssystems":

DNS-Server
Rufnummernportierungsserver
Netzmanagementsysteme
Service-Schnittstellen

- **System- und Netzwerkmanagement**

Zum System- und Netzwerkmanagement zählen die Verwaltung, der technische Betrieb sowie die Überwachung und Steuerung von Telekommunikations- und Datennetzen sowie IT-Netzen. Im Einzelnen fallen hierunter vielfältige technische Komponenten aber auch Softwarekomponenten, die oft im Zusammenspiel aufgabenspezifisch in einzelne sicherheitsrelevante Elemente eingeteilt werden können.

Beispiele für einzelne Elemente dieses „Sub-Sicherheitssystems":

Einrichtungen zur Verwaltung der Netzkonfiguration
Fehlermanagement
Abrechnungsmanagement
Leistungsmanagement (Performance der Netze)
Sicherheitsmanagement (Authentifizierung von Nutzern z. B. Radius-Server)

6.2.2 Gemeinsam mit anderen Diensteanbietern genutzte Standorte und technische Einrichtungen

Bedingt durch die fortschreitende technische Entwicklung im Telekommunikationsbereich und immer kürzer werdenden technischen Innovationszyklen sowie der Vielfalt und Komplexität von Telekommunikationsdiensten sind die im Marktsegment der Telekommunikation involvierten Unternehmen bestrebt, Synergieeffekte zu nutzen und die jeweiligen Diensteangebote für potentielle Kunden möglichst günstig anzubieten. Das führt dazu, dass viele Betreiber von Telekommunikationsanlagen und/oder Datenverarbeitungssystemen Standorte

und/oder technische Einrichtungen gemeinsam nutzen, um auf diese Weise Kosten einzusparen und die Produktivität zu steigern.

§ 109 Absatz 3 TKG gibt hinsichtlich solcher Konstellationen vor, dass die Verpflichtungen nach Absatz 1 und 2 dieses Paragraphen gemeinsam zu erfüllen sind, sofern ein Standort oder technische Einrichtungen von Betreibern der Anlagen gemeinsam genutzt werden und die Verpflichtungen nicht einem bestimmten Betreiber zugeordnet werden können.

Diese gemeinsame Nutzung von Standorten und Technik soll in den jeweiligen Sicherheitskonzepten der beteiligten Unternehmen beschrieben werden. Wie bereits in Kapitel 6.2.1 lässt sich auch hier das Sicherheitsteilsystem von gemeinsam mit anderen Diensteanbietern genutzten Standorten und technischen Einrichtungen unternehmensspezifisch in weitere kleinere Sicherheitsteilsysteme oder Elemente differenzieren.

Beispiele für einzelne Elemente dieses Sicherheitssystems:

Antennenstandorte
Kollokationsräume
Konzentratoren
Netzzusammenschaltungspunkte
Datenverarbeitungssysteme

6.2.3 Tätigkeiten im Auftrag durch andere Stellen

Vereinzelt bedienen sich die verpflichteten Unternehmen sogenannter, Auftragsdatenverarbeiter also anderen Unternehmen, die bestimmte Tätigkeiten im Auftrag durchführen. Das können beispielsweise Tätigkeiten sein, die das Erheben, Verarbeiten und die Nutzung personenbezogener Daten erfordern. In diesem Rahmen ist der Betrieb von Telekommunikationsanlagen und Datenverarbeitungssystemen aber auch der Betrieb von Datenverarbeitungsanlagen denkbar. Beim Betrieb von Datenverarbeitungsanlagen rückt unmittelbar der Schutz personenbezogener Daten in den Fokus. § 11 BDSG nimmt den Auftraggeber hinsichtlich der Vorschriften des BDSG und anderer Vorschriften zum Datenschutz in die Verantwortung, sofern er personenbezogene Daten im Auftrag durch andere Stellen erheben, verarbeiten oder nutzen lässt.

Eine solche Verlagerung von Aufgaben nach außen erfordert eine erhöhte Sorgfalt bei der Beurteilung und Einschätzung der Gefährdungen und entsprechend extern ausgerichtete Schutzanforderungen.

6.3 Sicherheitsteilsysteme zur Beschreibung von Datenverarbeitungsanlagen

Diese Kategorie von Sicherheitsteilsystemen zielt im Wesentlichen auf die Beschreibung von Datenverarbeitungsanlagen ab. Im Allgemeinen sind Datenverarbeitungsanlagen speziell konfigurierte Hard- und Softwarekomponenten, die im Zusammenspiel - als Einheit - der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten dienen.

Die hier relevanten Sicherheitsteilsysteme können wie folgt gegliedert werden:

1. Datenverarbeitungsanlagen, die zur automatischen Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten dienen
2. Datenträger und Akten
3. Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten

4. Gemeinsame Nutzung eines Standortes oder technischer Einrichtungen

6.3.1 Datenverarbeitungsanlagen, die zur automatischen Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten dienen

Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten ist innerhalb von Telekommunikations- und Datenverarbeitungssystemen sowie im Rahmen der Erbringung von Telekommunikationsdiensten in vielen Bereichen eine notwendige Praxis. Im Rahmen der Kundenverwaltung, der Störungsbearbeitung, zu statistischen Zwecken, im Qualitätsmanagement zur Optimierung von Diensten und in vielen anderen Bereichen werden personenbezogene Daten erhoben, verarbeitet und vielfältig genutzt.

Das Sicherheitsteilsystem von Datenverarbeitungsanlagen kann unternehmensspezifisch in weitere kleinere Sicherheitsteilsysteme aufgeteilt werden. Deshalb wird auch hier, wie bereits im Kapitel 3.2.1, in weitere „Sub“-Sicherheitsteilsysteme unterteilt. Unternehmensspezifisch können weitere oder auch andere Sicherheitsteilsysteme gebildet werden;

- Kundendatenverwaltung
- Entgeltermittlung- und –abrechnung (Billing)
- Missbrauchserkennung und –unterbindung (Fraud-System)
- Rufnummerermittlung bei ankommenden Verbindungen (Fangschaltung)
- Auskunftserteilung (Call Center)
- Störungsstatistik zur Qualitätssicherung
- Eintrag der Teilnehmer in öffentliche gedruckte oder elektronische Verzeichnisse
- Vergabe von Tätigkeiten an externe Dienstleister
- Dokumente und Aufzeichnungen (fallspezifisch und nicht automatisiert)

Jeweils voneinander abgegrenzt können die hier genannten „Sub“-Sicherheitsteilsysteme einer separaten Gefährdungsbetrachtung unterzogen werden. Je nach Bedarf können die o.g. Sicherheitsteilsysteme weiter untergliedert oder in einer weiteren letzten Ebene mit Elementen aufgefüllt werden, die sich technisch, administrativ oder aufgabenspezifisch zusammenfassen lassen.

6.3.2 Datenträger und Akten

Das Sicherheitsteilsystem der Datenträger soll insbesondere sogenannte externe Speichermedien umfassen. Diese werden in der Regel zur Sicherung oder zum Transport personenbezogener Daten benutzt. Auch dieser Bereich lässt sich exemplarisch weiter differenzieren. Bei den nachfolgenden Beispielen kann es sich wiederum um Sicherheitsteilsysteme handeln; das hängt im Einzelnen oft vom Umfang und der Kaskadierung solcher Speichersysteme ab. In großen Unternehmen nehmen Speichermedien oft einen erheblichen Raum in Anspruch und rechtfertigen alleine deshalb schon eine separate Betrachtung als Sicherheitsteilsystem:

- Externe Festplatten
- Magnetbänder
- Speicherkarten
- USB-Stick

Das Sicherheitsteilsystem der *Akten* soll hier „papierbasierte“ Sammlungen personenbezogener Daten, die nach bestimmten Merkmalen sortiert zugänglich sind, umfassen. Hierunter können beispielsweise folgende weitere „Sub“-Sicherheitssysteme oder Elemente eingeordnet werden:

- Vertragsunterlagen der Kunden
- Einzelverbindungsnachweise
- Beschwerden von Kunden
- Unternehmensinterner Schriftverkehr mit Kundendaten

6.3.3 Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten

Die auf Basis der Datenverarbeitungssysteme realisierten Sicherheitsteilsysteme zum *Erheben, Verarbeiten* und *Nutzen* von personenbezogenen Daten haben in diesen drei Bereichen wiederum jeweils spezielle inhaltliche Ausrichtungen. So ist das Erheben von Daten kein „Selbstzweck“ sondern notwendig, um den ordnungsgemäßen Ablauf von Diensten zu gewährleisten. Hier kann es sinnvoll sein, diese Zweckausrichtung der Komponenten *Erheben, Verarbeiten* und *Nutzen* in separaten Sicherheitsteilsystemen zu beschreiben. Anliegend sind hierzu einige Beispiele aufgeführt:

- Erheben von Daten für die Begründung, inhaltliche Ausgestaltung oder Änderung von Vertragsverhältnissen (Bestandsdaten)
- Erheben von Daten bei der Erbringung von Telekommunikationsdiensten (Verkehrsdaten)
- Erheben von Daten, die den Standort eines Endgerätes angeben (Standortdaten)
- Verarbeiten / Nutzen von Bestandsdaten / Verkehrsdaten für die Entgeltermittlung und –abrechnung einschließlich Einzelverbindungsnachweis für das Aufdecken einer rechtswidrigen Inanspruchnahme eines Telekommunikationsnetzes oder -dienstes (Fraud), für das Mitteilen ankommender Verbindungen (Fangschaltung), für die Beratung der Teilnehmer, zu Werbe- und Marketingzwecken, zur Marktforschung, zur bedarfsgerechten Gestaltung von Telekommunikationsdiensten, zur Bereitstellung von Diensten mit Zusatznutzen (Mehrwert- und Premiumdienste), für die Bereitstellung in öffentliche Teilnehmerverzeichnisse und zur Auskunftserteilung)
- Verarbeiten/Nutzen von Standortdaten

Aus den hier aufgeführten Beispielen wird leicht ersichtlich, dass diese abhängig von der Zweckausrichtung des Verfahrens konfiguriert werden können. Zum Teil sind die sich hier ergebenden Sicherheitsteilsysteme immer noch sehr breitbandig angelegt und lassen weitere Unterteilungen zu.

6.3.4 Gemeinsame Nutzung eines Standortes oder technischer Einrichtungen

Wie bereits im Kapitel 6.2.2 *„Gemeinsam mit anderen Diensteanbietern genutzte Standorte und technische Einrichtungen“* erörtert, ist dieses Thema auch im Bereich von zu beschreibenden Sicherheitsteilsystemen bezüglich *Datenverarbeitungsanlagen* von Relevanz. Auf entsprechende Erläuterungen und Beispiele kann diesbezüglich auf Kapitel 6.2.2 zurückgegriffen werden.

7. Gefährdungen (Beispiele)

Die hier beispielhaft aufgeführten Gefährdungen dienen dazu, den Sicherheitsteilsystemen entsprechende Gefahrenlagen zuzuordnen.
Als weitere Hilfestellung zur Feststellung von Gefährdungen pro Sicherheitsteilsystem und Schutzziel sollen die Grundschutzkataloge des BSI dienen.

7.1 Elementare Gefährdungen

7.1.1 Blitz

Der Blitz ist die wesentliche Gefährdung für Objekte mit Telekommunikationskomponenten während eines Gewitters. Nicht an jedem Ort ist das Blitzschlagrisiko gleich hoch. Auch die Eigenschaften des direkten Umfeldes von Objekten beeinflussen die Wahrscheinlichkeit eines Blitzeinschlages.

7.1.2 Sturm

Besonders für technische Einrichtungen, die im Außenbereich angebracht sind (z.B. Antennen), stellt Sturm eine Gefährdung dar.

7.1.3 Feuer

Feuer und Brandrauch in Betriebsgebäuden der Telekommunikation stellt eine unmittelbare Gefahr für deren technische Einrichtungen dar. Zusätzlich können auch in darunter liegenden Gebäudeteilen Löschwasserschäden entstehen.

Begünstigende Faktoren einer Brandausbreitung können sein:

- Offene Brandabschnittstüren
- Unsachgemäße Lagerung brennbarer Materialien
- Mangelhafter vorbeugender Brandschutz
- Fehlen von Brandmeldeeinrichtungen
- Mangelhafte Löscheinrichtungen

7.1.4 Wasser

Wasserschäden in Betriebsgebäuden der Telekommunikation stellen eine besondere Gefährdung für die Betriebssicherheit / Verfügbarkeit dar.

Diese Gefährdungen können verursacht werden durch:

- Regen, Hochwasser, Überschwemmung
- Störungen in der Wasserversorgung oder Abwasserentsorgung
- Defekte an der Heizungsanlage
- Defekte an Klimaanlagen mit Wasseranschluss
- Defekte an Sprinkleranlagen
- Löschwasser bei einer Brandbekämpfung

7.1.5 Witterungseinflüsse

Witterungseinflüsse können eine Gefährdung für den Betrieb von Telekommunikationseinrichtungen darstellen. Hervorgerufen durch meteorologische Veränderungen oder durch ungünstige Witterungsbedingungen vermag das Wetter erheblichen Einfluss auf Teile von Telekommunikationsnetzen und auf deren Betrieb zu nehmen (Beeinträchtigung von Richtfunk- und Satellitenfunkübertragungsstrecken durch Schneefall, Nebel, starken Regen).

7.2 Gefährdungen durch technische Störungen, Ausfälle etc.

7.2.1 Kabelbrand

Kabelbrand in einem Telekommunikationsnetz entsteht überwiegend durch Beflammung (z.B. während Instandhaltungsarbeiten); ebenso ist auch eine Selbstentzündung z.B. durch Kurzschluss möglich. Es besteht die Gefahr der Ausbreitung über Kabeltrassen / -roste, aber auch über parallel verlaufende Leitungen anderer Versorgungssysteme.

7.2.2 Ausfall zentraler Komponenten

Fallen einzelne zentrale Komponenten eines Telekommunikationsnetzes aus, so ist unter Umständen ein Ausfall des gesamten Netzes nicht mehr zu verhindern. Als zentrale Komponenten gelten unter anderem:

- Einrichtungen der Stromversorgung
- DV-Systeme, die der Netzsteuerung und –überwachung dienen
- Vermittlungs- und Übertragungseinrichtungen

Eine Störung von Komponenten mit zentraler Bedeutung führt häufig zu einem Totalausfall von Telekommunikationsnetzen.

7.2.3 Unzulässige Temperatur und Luftfeuchte

Jedes Gerät hat einen Temperaturbereich, innerhalb dessen seine ordnungsgemäße Funktion gewährleistet ist. Gefahren stellen z.B. Aufheizungen durch große Fensterfronten in nicht klimatisierten Räumen dar. Auch das Öffnen von Fenstern kann zu unzulässigem Raumklima (z.B. Zugluft, Spritzwasser, Staub) und damit zur Beschädigung von Betriebsanlagen führen.

7.2.4 Ausfall externer Versorgungsnetze

Trotz der hohen Versorgungssicherheit kann es zu Unterbrechungen der Stromversorgung kommen. Zum Beispiel werden Stromversorgungskabel durch Bauarbeiten beschädigt. Diese Unterbrechungen können längere Zeit andauern und verursachen erhebliche Störungen im Telekommunikationssystem, insbesondere wenn keine Ersatzschaltungsmöglichkeiten zur Verfügung stehen. Stromunterbrechungen können Ausfälle oder Schäden im Telekommunikationsnetz bewirken. Zu berücksichtigen sind auch der Einfluss eines Stromausfalls auf Einrichtungen, die der Klimatisierung von Technikräumen dienen und der Status dieser Ein-richtungen nach Wiederherstellung der regulären Stromversorgung.

7.2.5 Ausfall interner Versorgungsnetze

In Gebäuden ist eine Vielzahl von Netzen vorhanden, die der Ver- und Entsorgung dienen. Die Netze weisen in der Regel gegenseitige Abhängigkeiten auf, wodurch sich einzelne Betriebsstörungen kaskadiert ausbreiten können.

7.2.6 Ausfall vorhandener Sicherungseinrichtungen

Durch technische Defekte oder äußere Einflüsse (z.B. aufgrund von Alterung, Fehlbedienung, mangelhafter Instandhaltung, Manipulation, Stromausfall) kann es zum Ausfall von Sicherungseinrichtungen kommen, so dass die Schutzwirkung herabgesetzt ist oder komplett ausfällt.

7.2.7 Spannungsschwankungen, Überspannung, Unterspannung

Durch Schwankungen der Versorgungsspannung kann es zu Funktionsstörungen der Nachrichtenübertragung kommen. Die Ursache dafür kann in allen Bereichen des Stromversorgungsnetzes entstehen, vom Netz des Energieversorgungsunternehmens bis hin zum Anschlussstromkreis einzelner technischer Einrichtungen.

7.2.8 Ausfall der Netzersatzanlagen

Der Ausfall von Netzersatzanlagen stellt eine besondere Gefährdung dar. Er führt im Bedarfsfall zum sofortigen Ausfall der technischen Einrichtungen (z.B. Vermittlungs- und Übertragungseinrichtungen, Klimaanlagen), da keine Überbrückungsmöglichkeit für die Zeit bis zur Wiederkehr der Stromversorgung besteht.

7.2.9 Verlust gespeicherter Daten

Der Verlust gespeicherter Daten kann erhebliche Auswirkungen auf den Telekommunikationsbetrieb haben. Sind z.B. Betriebsdaten per Softwareeingriff geschalteter Verkehrswege verloren, so kann dies Auswirkung auf den gesamten Netzbetrieb haben. Es sind falsche Verbindungen, aber auch Ausfälle denkbar. Dabei können die Gründe für den Verlust gespeicherter Daten vielfältiger Art sein.

7.2.10 Leitungsbeschädigungen

Je mehr ungeschützte Kabel installiert sind, desto größer ist die Gefahr einer Beschädigung. Diese Kabelschäden führen nicht unbedingt sofort zu einem Ausfall von Leitungsverbindungen. Auch die zufällige Entstehung von Verbindungen (z.B. durch fehlerhafte Reparatur) ist möglich.

7.2.11 Protokollabweichungen

Protokollabweichungen sind alle absichtlich oder zufällig auftretenden Veränderungen des Protokolls, welche Einflussnahme auf die interne Steuerung eines Netzknotens, auf die Abrechnung von Telekommunikationsdienstleistungen, auf schützenswerte Nutzerdaten sowie auf statistische Auswertungen ermöglichen. Dies kann durch Einbringen von Schadprogrammen, veränderten Nachrichten oder Verändern der Nachrichtensequenz über Nutzeranschlüsse, Netz- oder Fernwartungszugänge verursacht werden.

7.3 Organisatorische Gefährdungen, Änderungen des Umfelds und menschliche Fehlhandlungen, Mängel durch Fehler in der Planungsphase

7.3.1 Unzureichende organisatorische Regelungen

Übergreifende organisatorische Regelungen und Vorgaben sind für die Sicherheit von Telekommunikationssystemen von grundsätzlicher Bedeutung. Diese Regelungen geben z. B. Abläufe zu Verhaltensweisen bei der Fehlerbeseitigung vor, sie regeln aber auch Zuständigkeiten bis hin zur Verteilung von Kontrollaufgaben. Regelungsdefizite können schadensfördernde Auswirkungen auf die Betriebsabläufe haben.

7.3.2 Unzureichende Kenntnis über Regelungen

Die Festlegung von Regelungen allein sichert den störungsfreien Arbeitsablauf noch nicht. Die für einen Funktionsträger geltenden Regelungen müssen diesem auch bekannt sein. Ist dies nicht sichergestellt, ist darin eine Gefährdung zu sehen.

7.3.3 Unzureichende Instandhaltung

Die Funktionsfähigkeit der eingesetzten Technik muss gewährleistet sein. Durch regelmäßige Instandhaltung wird der Erhalt der Funktionsfähigkeit ständig überprüft. Werden Instandhaltungsarbeiten nicht oder nur unzureichend durchgeführt, können während des Betriebs der Einrichtungen Schäden oder Folgeschäden entstehen.
Neben Instandhaltungsarbeiten an der vorhandenen technischen Infrastruktur (Hardware) kommt auch der Pflege der eingesetzten Softwarelösungen eine große Bedeutung zu. Werden Softwareupdates nicht eingespielt oder kommen nicht vollständig geprüfte Updates zum Einsatz, kann dies zur Beeinträchtigung von Komponenten und damit zur Verletzung von Schutzzielen führen.

7.3.4 Zutritt Unbefugter

Gelangen Unbefugte in Gebäude oder Räume mit sicherheitsrelevanten Einrichtungen, können Gefährdungen durch vorsätzliche Handlungen oder durch unbeabsichtigtes Fehlverhalten entstehen.

7.3.5 Unerlaubte Ausübung von Rechten

Rechte (z.B. Zutritts-, Zugangs- und Zugriffsberechtigungen) werden als organisatorische Maßnahmen eingesetzt, um einen sicheren und ordnungsgemäßen Telekommunikationsbetrieb zu gewährleisten. Werden solche Rechte von nicht autorisierten Personen missbräuchlich ausgeübt, können sich Gefährdungen ergeben, welche die Vertraulichkeit und Integrität von Daten oder die Vermittlungsleistung beeinträchtigen.

7.3.6 Unkontrollierter Einsatz von Betriebsmitteln

Betriebsmittel - gleich welcher Art - dürfen nur entsprechend dem Verwendungszweck eingesetzt werden. Wird der Einsatz von Betriebsmitteln nicht ausreichend kontrolliert, können als Folge vielfältige Gefährdungen auftreten.

7.3.7 Mangelhafte Anpassung an organisatorische Veränderungen

Die speziell für den Einsatz von Telekommunikations- und Informationstechnik vorgeschriebenen organisatorischen Regelungen, aber auch das gesamte Umfeld eines Unternehmens oder einer Behörde unterliegen ständigen Änderungen. Werden diese Änderungen ungenügend berücksichtigt oder Anpassungen an diese Änderungen ungenügend dokumentiert, ergeben sich Gefährdungen.

7.3.8 Kapazitätsengpass

Bei der Planung von Netzen wird die Kapazitätsfestlegung oft lediglich am aktuellen Bedarf ausgerichtet.

Dabei wird nicht bedacht, dass z. B.:

- Erweiterungen eines Netzes wegen steigenden Bedarfs nicht auszuschließen sind.
- Die Kapazität eines Netzes aufgrund steigenden Datenvolumens nicht mehr ausreicht.
- Höhere Anforderungen an das Netz die Verlegung anderer Kabel erforderlich machen.
- Bei Teilbeschädigungen von Kabeln, neben dem Ersatzkabel, das bisherige Kabel als redundante Teilstrecke beibehalten werden sollte.
- Im Katastrophenfall ein stark erhöhter Kommunikationsbedarf besteht.

Gefährdet ist hier insbesondere die Verfügbarkeit, die während der Erweiterungsarbeiten stark reduziert sein kann.

7.3.9 Unzureichende Dokumentationen, Speicherung der Historie

Besondere Gefahren bestehen bei unzureichender Dokumentation der

- Betriebssoftware (und ihrer Historie)
- Konfiguration (und ihre Historie)
- Verlegung von Kabeln in Gebäuden und öffentlichen Wegen
- Rangierungen in Verteilungen (mechanisch oder logisch)

Derartige mangelhafte Dokumentationen erschweren eine Prüfung, Instandhaltung und Reparatur.

7.3.10 Unzureichend geschützte Vorfeldeinrichtungen oder Komponenten

Sind Vorfeldeinrichtungen oder Komponenten des Telekommunikationsnetzes (auch deren Stromversorgung) in Gebäuden mit Publikumsverkehr frei zugänglich bzw. in unverschlossenen Räumen installiert, ist es Unbefugten möglich, gegebenenfalls diese Einrichtungen zu öffnen, Manipulationen vorzunehmen und dadurch Betriebsstörungen herbeizuführen.

7.3.11 Unzureichend geschützte Verteileinrichtungen

Der unter 7.3.10 beschriebene Sachverhalt trifft in gleicher Weise auch auf Verteileinrichtungen im Anschlussleitungsnetz zu. Da diesen Verteileinrichtungen aus sicherheitsrelevanter Sicht besondere Bedeutung zukommt, wird diese Gefährdung explizit erwähnt.

7.3.12 Nachrichtenverlust durch Störfelder

Beeinflussungen durch elektrische oder magnetische Felder können gegebenenfalls Auslöser von Netzstörungen sein. Solche Störungen können auch im Anschlussleitungsnetz auftreten.

7.3.13 Leitungsbeeinträchtigung durch Umfeldfaktoren

Die Übertragungseigenschaften von Kabeln mit elektrischer Signalübertragung können durch elektrische und magnetische Felder negativ beeinflusst werden (z. B. Blitzeinschlag in Erdseil mit Glasfaserkern).

7.3.14 Informationsverlust bei zu geringer Speicherkapazität

Ist die Speicherkapazität zu gering gewählt, kann dies ebenfalls zu den unter 7.2.9 bereits geschilderten Auswirkungen führen.

7.3.15 Verletzung des Fernmeldegeheimnisses

Die Verletzung des Fernmeldegeheimnisses ist ein Straftatbestand. Mögliche Ursachen dieser Verletzung können unter anderem sein:

- Fehlende Unterweisung und Sensibilisierung der Mitarbeiter
- Unzureichende Administration der Zugriffsrechte
- Mangelnde Kontrolle der Mitarbeiter
- Fehlende oder mangelhafte Schutzvorkehrungen (organisatorisch und technisch)

Aufgrund ihrer wachsenden Verbreitung ist zunehmend auch der Transport von Telefoniedaten über IP-basierte Netze (z. B. der Kommunikation mittels Voice over IP (VoIP)) von der Gefahr der Verletzung des Fernmeldegeheimnisses betroffen.

7.3.16 Vertraulichkeitsverlust von Daten

Der Vertraulichkeitsverlust von Daten stellt eine Gefährdung dar. Insbesondere durch Fehlverhalten von Personal können falsche bzw. nicht gewünschte Datensätze, die dem Empfänger nicht zur Kenntnis gelangen sollen, dennoch übertragen werden.

Beispiele:

- Fehlende Unterweisung und Sensibilisierung der Mitarbeiter
- Mangelhafte Entsorgung von Datenträgern
- Ungeschützte Fernübertragung von sensiblen Daten
- Unsichere Archivierung von Datenträgern

7.3.17 Integritätsverlust von Daten

Personen erreichen bewusst oder zufällig administrativ höhere Zugriffsmöglichkeiten und können den Nachrichten- bzw. den Dateninhalt manipulieren. Der durch die Manipulation verursachte Integritätsverlust ist unabhängig davon, ob die Zugriffsmöglichkeit zeitlich begrenzt oder unbegrenzt ist.

Beispiele:

- Fehlende Administration der Rechte des Datenzugriffs
- Mangelnde Kontrolle der Mitarbeiter

7.3.18 Löschung von Daten, Zerstörung von Einrichtungen sowie Übertragungswegen

Durch sorglosen oder unsachgemäßen Umgang kann es zu Beeinflussungen bis zu Zerstörungen von Systemteilen bzw. Programmabläufen kommen, welche das Leistungsvermögen von Telekommunikationsanlagen erheblich beeinträchtigen. Die hierbei verursachten Störungen können über den Verlust oder die Verfälschung systemrelevanter Daten bis zu kompletten Dienst- oder Netzausfällen führen. Abweichungen von abgestimmten Vorgehensweisen, fehlerhafte Interpretation von Arbeitsinhalten, Abweichungen von Qualitätsanforderungen können weitere Ursachen für Störungen sein.

7.3.19 Nichtbeachtung von Schutzmaßnahmen

Aufgrund von Nachlässigkeit und fehlenden Kontrollen ist damit zu rechnen, dass Personen die Schutzmaßnahmen nicht oder nicht im vollen Umfang beachten. Daraus resultieren Schwachstellen innerhalb des Telekommunikationssystems, die zu leicht vermeidbaren Schäden führen können.

7.3.20 Mangelhafte Sorgfalt im Umgang mit Datenträgern

Zum Umgang mit Datenträgern zählen:

- Geeignete Lagerung
- Geregelter und kontrollierter Zugriff
- Sachgerechte Entsorgung
- Sicherer Versand
- Sach- und fachgerechte Handhabung

Dabei ist Datenträgern, die Bestands- und Verkehrsdaten beinhalten, besondere Beachtung zu gewähren.

7.3.21 Authentizität

Das Betreiben von Netzen mit unzureichenden Mechanismen zur Identifikation und Prüfung der Authentizität des Bedienpersonals (und der Nutzern) stellt eine Gefährdung dar. So stellen im Falle zu simpler Log-In- und Passwortkombinationen diese ein hohes Potential für einen unerlaubten Zugriff dar.
In Abhängigkeit von der Bedeutung der Einrichtungen kann eine fehlende Authentifikation des Bedieners eine nicht unerhebliche Gefährdung des Gesamtsystems darstellen.

7.3.22 Inkompatibilität

Fehlende Kompatibilität (physikalisch oder logisch) von Komponenten oder Netzelementen kann zu einer Instabilität des TK-Netzes führen.

Beispiel:

Kommunikationsprotokolle (z. B. Zeichengabesystem Nr. 7) enthalten Kodierungsbereiche, die für Erweiterungen und zukünftige Anwendungen reserviert sind. Werden diese Bereiche unzulässig benutzt, so kann die Stabilität im Netz bzw. an den Netzgrenzen durch unzureichende Kompatibilität von Endgeräten gefährdet werden.

7.3.23 Ungünstige Netzkonfiguration

Eine ungünstige Netzkonfiguration kann durch Versäumnisse bei der Netzplanung Überlastsituationen und Störungsempfindlichkeit auslösen. Eine Netzkonfiguration ohne Mechanismen zur Ersatzschaltung, zu geringen Kapazitäten für Überlaufverkehr sowie zu geringer Flexibilität kann Ursache sein.

7.3.24 Serviceschnittstellen

Die besondere Gefährdung an Serviceschnittstellen ist dadurch gegeben, dass ein logischer Zugriff auf das Telekommunikationssystem oder einzelne Komponenten erfolgen kann, ohne dass eine physikalische Manipulation vorangegangen ist. So besteht die Möglichkeit, dass Unbefugte über eine Nutzeranschalteeinrichtung mit einem Computer und entsprechender Hard / Software die internen Netzsteuerungen manipulieren könnten.

7.3.25 Unzureichende Standortsicherheit

Die Wahl eines geeigneten Standortes von Anlagen oder Anlagenteilen ist von großer Bedeutung. Hierbei haben z.B. Wetter- und Geländebedingungen besondere Bedeutung.

7.3.26 Unzureichende Vorsorge gegen Gefährdungen der Schutzziele an gemeinsam genutzten Technik-Standorten

Ausfälle oder andere Beeinträchtigungen von technischen Einrichtungen eines einzelnen Netzbetreibers an einem Standort stellen für sich alleine betrachtet u. U. noch keine größere Minderung der Versorgung der Öffentlichkeit mit TK-Dienstleistungen dar. Fallweise, d.h. abhängig von der Wirkbreite der technischen Störung, können die Ausfälle durch Nutzung anderer Kommunikationsnetze zumindest teilweise kompensiert werden. Nutzen jedoch mehrere Betreiber Räumlichkeiten oder bestimmte technische Netzteile oder Netzelemente an einem Standort gemeinsam, so können Betriebsstörungen zu einem möglicherweise weitreichenden Ausfall der gesamten TK-Versorgung einer Region führen.

7.3.27 Unzureichende Überprüfung der Identität

Wer Telekommunikations- und Datenverarbeitungssysteme für Dritte zur Verfügung stellt, muss durch geeignete Maßnahmen sicherstellen, dass er die Identität seiner Servicenehmer in ausreichendem Maße überprüft. Der Zugriff auf angemietete Telekommunikations- und Datenverarbeitungssysteme unter Vortäuschung einer falschen Identität kann der missbräuchlichen Verwendung dienen und stellt somit eine Gefährdung im Sinne der definierten Schutzziele dar.

7.3.28 Drohende Adressknappheit

Die Adressen aus dem bisher verwendeten Bereich für IPv4 werden in absehbarer Zukunft bedingt durch die weiterhin steigende Nachfrage nach neuem Adressraum ausgehen. Dies hat zwar keine direkte Auswirkung auf die bestehenden Teile des Internets, wird aber ein weiteres Wachstum unter Verwendung des eingesetzten Protokolls IPv4 zumindest stark behindern. Daher soll die Einführung von IPv6 vorangetrieben werden.

7.3.29 Monokulturen bei Herstellern/ Zulieferern

Die Konzentration auf nur wenige Hersteller von Komponenten und bei diesen auf nur wenige Geräteserien stellt ein Risikopotential für den Betrieb von Telekommunikations- und Datenverarbeitungssystemen dar. Der Einsatz von durchweg internationalen Anbietern für aktive Komponenten öffnet aus lokaler Sicht ein weiteres Problemfeld, ebenso wie die Verwendung von Hardware aus der Produktion von nicht vertrauenswürdigen Herstellern.

7.4 Sabotage, Manipulation, Anschläge, Vandalismus, Cyber-Angriffe auf die Infrastruktur und strafbare Handlungen intern oder extern

Bei allen in diesem Abschnitt genannten Gefährdungen ist zu berücksichtigen, dass sowohl eine interne als auch externe Einwirkung auf die Netze und Dienste vorkommen kann.

7.4.1 Diebstahl

Der Diebstahl von Anlagen, Anlagenteilen, Endgeräten, Zubehör, Software oder Daten verursacht nicht nur wirtschaftlichen Schaden, sondern vor allen Dingen sicherheitsrelevante Effekte aufgrund mangelnder Verfügbarkeit. Daneben können Schäden durch Vertraulichkeitsverlust entstehen.

7.4.2 Einbruch

Ein Einbruch geht häufig verschiedenen Gefährdungen der Telekommunikation wie Diebstahl oder Manipulation voraus. Schutzmaßnahmen, die gegen einen Einbruch gerichtet sind, wirken dadurch auch gegen mögliche Folgegefährdungen.

7.4.3 Terroristische Anschläge

Ob und in welchem Umfang Telekommunikationseinrichtungen der Gefahr eines Anschlages ausgesetzt sind, hängt neben der Lage und dem Umfeld der Gebäude stark von ihren Aufgaben, der aktuellen Bewertung in der Öffentlichkeit und den politisch-sozialen Umständen ab.

7.4.4 Vandalismus

Bezüglich der Gefährdung ähnelt Vandalismus dem terroristischen Anschlag, nur dass er nicht wie dieser gezielt eingesetzt wird, sondern meist Ausdruck blinder Zerstörungswut ist. Sowohl Außentäter (z.B. enttäuschte Einbrecher, außer Kontrolle geratene Demonstranten) als auch Innentäter (z.B. frustrierte oder alkoholisierte Mitarbeiter) kommen in Betracht. Die tatsächliche Gefährdung durch Vandalismus ist schwer abschätzbar, da dem Vandalismus in der Regel keine zielgerichtete Motivation zugrunde liegt. Persönliche Probleme oder ein schlechtes Betriebsklima können hierfür Ursachen sein.

7.4.5 Manipulationen an Netzknoten und Betriebsräumen

Für Manipulationen von technischen Einrichtungen in Netzknoten, von Hard- und Software und an Einrichtungen und Vorrichtungen in / an den Betriebsräumen kommen sowohl Innen- wie auch Außentäter in Betracht. Zum einen kann es die Zerstörung von technischen Einrichtungen sein, zum anderen die vorsätzliche Schädigung von Software, aber auch Eingriffe, die eine Verletzung des Fernmeldegeheimnisses darstellen.

7.4.6 Manipulationen an Übertragungswegen

Die Übertragungswege im Anschlussleitungsnetz beinhalten - historisch gewachsen - unzureichend geschützte Leitungen und Verteiler. Die dort mögliche Manipulation stellt eine Gefährdung für Nutzer, Betreiber und Anbieter im Telekommunikationsbereich dar.

7.4.7 Abhören

Das Abhören stellt eine Verletzung des Fernmeldegeheimnisses dar. Nur mit einem hohen technischen Aufwand - wenn überhaupt - kann ein direktes oder indirektes „Anzapfen der Leitungen“ nachgewiesen werden. Dies gilt in besonderem Maße für Funkübertragungen.

7.4.8 Missbräuchlicher Telekommunikationsverkehr

Die Erzeugung von Verkehrslasten, insbesondere mit dem Ziel des Missbrauchs, kann zu einer übermäßigen Belegung von Nutz- und Signalisierungskanälen führen. Je nach Ausmaß (z.B. Überlast) kann das Netz destabilisiert werden. Für den sonstigen Telekommunikationsverkehr stehen die Netzressourcen dann nicht mehr in ausreichendem Umfang zur Verfügung.

7.4.9 Manipulation oder Löschung von Daten

Erlangen Innentäter oder nicht autorisierte Dritte Zugang zu betriebsnotwendigen Daten, stellt das eine große Gefahr dar. Manipulierte oder gelöschte Daten können zum Ausfall wichtiger Systeme führen.

7.4.10 DoS/ DDoS

Angriffe, die gezielt darauf gerichtet sind, die Verfügbarkeit von Telekommunikations- und Datenverarbeitungssystemen im Internet zu stören, werden Denial-of-Service-Angriffe (DoS) genannt. Oft sind solche Angriffe nur unter Zuhilfenahme einer Vielzahl verschiedener Rechnersysteme, etwa durch die Kontrolle eines Botnetzes, realisierbar.

Eine weitere Art von DDoS-Angriffen sind die sogenannten Reflection Angriffe. Hierbei sendet der Angreifer Anfragen mit gefälschten Absenderadressen an öffentlich erreichbare Server (häufig DNS- oder NTP-Server). Diese Server antworten dann an die gefälschte Adresse. Typischerweise sind die Antworten sehr viel größer als die Anfragen, was zu einer Verstär-kung des Angriffs führt. Auch bei Reflection Angriffen können Botnetze eingesetzt werden. Aufgrund der Effektivität dieses Angriffsverfahrens kann mit der gleichen Anzahl am Angriff beteiligter Systeme eine höhere Wirkung erzeugt werden.

7.4.11 Manipulation und Missbrauch von DNS-Einträgen

Das DNS-Protokoll weist prinzipielle Schwächen auf. Daher werden regelmäßig neue Schwachstellen gefunden, die die Manipulation von DNS-Einträgen ermöglichen, wodurch Datenpakete gezielt falsch geleitet werden können.

7.4.12 Fehlkonfigurationen oder Manipulation von Verkehrsrouten

Kommt es beim Festlegen und Umsetzen von Routen zu Fehlern, können Teile des Netzes aus dem Routing verschwinden, betroffene Datenpakete werden falsch oder gar nicht mehr transportiert. Werden falsche Routingeinträge über spezielle Routingprotokolle, wie z.B. BGP, an andere Router verteilt, können weite Teile des Internets betroffen sein.

7.5 Gefahren basierend auf Nutzerverhalten

7.5.1 Schadsoftware

Die Kompromittierung eines Systems birgt eine Vielzahl von Gefahren und kann die wirksame Einhaltung der definierten Schutzziele erschweren bzw. in vielen Fällen verhindern. Auch für die Betreiber von Telekommunikations- und Datenverarbeitungssystemen muss daher die Infektion mit Schadsoftware als wachsende Gefahr angesehen werden. Schadprogramme auf den angeschlossenen Kundensystemen können die Infrastruktur der TK-Anbieter durch das Versenden von Spam oder das Durchführen von DDoS-Angriffen ebenfalls schädigen.

7.5.2 Spam oder Spit

Die massenweise Verbreitung von unerwünschter Werbung erfolgt mittlerweile nicht mehr ausschließlich auf dem Weg des Mailversands (Spam) sondern auch über VoIP-Verbindungen werden vermehrt unerwünschte Werbebotschaften verbreitet (Spit). Durch das massenhafte Auftreten können die Systeme der TK-Anbieter stark belastet werden oder sogar ausfallen.

7.5.3 Spoofing

Als Spoofing (englisch für manipulieren, verschleiern oder vortäuschen) werden in der Informations- und Telekommunikationstechnik verschiedene Täuschungsversuche zur Verschleierung der eigenen Identität und zum Fälschen übertragener Daten bezeichnet. Das Ziel beim Spoofing besteht darin, die Integrität und Authentizität der Informationsverarbeitung zu untergraben. Spoofing-Angriffe können beispielsweise mittels Fälschung der MAC-Adresse (MAC-Spoofing) oder der IP-Adresse (IP-Spoofing) erfolgen.

7.5.4 Hacking gegen Komponenten des Netzbetreibers

Hacking bezeichnet im Kontext der Informationssicherheit Angriffe, die darauf abzielen, vorhandene Sicherheitsmechanismen zu überwinden, um in ein DV-System einzudringen, seine Schwächen offen zu legen und es gegebenenfalls zu übernehmen. Hacking stellt somit eine Bedrohung für die Systemhoheit des Netzbetreibers dar.

Angriffe durch Hacking können zum einen gegen Einrichtungen gerichtet sein und zum anderen auf die Serverkomponenten, die im betroffenen Netzwerk zum Einsatz kommen.

8. Sicherheitsanforderungen

Ausgehend von den in § 109 Absatz 1 und 2 TKG verankerten Zielen

1. Schutz des Fernmeldegeheimnisses,
2. Schutz personenbezogener Daten,
3. Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen oder Diensten führen (ordnungsgemäßer Betrieb),

werden nachfolgend unter Berücksichtigung der gesetzlichen Regelungen des BDSG sowie des 7. Teil TKG die relevanten Sicherheitsanforderungen beschrieben.

Auf der Grundlage dieser Sicherheitsanforderungen sind bezüglich der definierten Sicherheitsteilsysteme erforderliche (Schutzziel 1 und 2) oder angemessene (Schutzziel 3) technische Vorkehrungen und sonstige Maßnahmen herzuleiten.

Gemäß TKG sind technische Maßnahmen oder sonstige Schutzmaßnahmen dann angemessen, wenn der dafür erforderliche technische und wirtschaftliche Aufwand nicht außer Verhältnis zur Bedeutung der zu schützenden Telekommunikationsnetze oder -dienste steht. Der Stand der Technik ist zu berücksichtigen.

Grundsätzlich können Maßnahmen aus den IT-Grundschutzkatalogen des BSI, aus der Schriftenreihe zur Internet-Sicherheit (ISi-Reihe) und der Cybersicherheitsempfehlungen für Internetservice Provider des BSI, der ISO-IEC Norm 27002 (Leitfaden für das Informationssicherheitsmanagement) oder anderen Maßnahmenkatalogen entnommen werden.

Darüber hinaus werden zu treffende technische Vorkehrungen und sonstige Maßnahmen in den nachfolgenden Absätzen beispielhaft konkretisiert. Dabei dienen die Konkretisierungen der Orientierung, sie sind nicht abschließend und erheben nicht den Anspruch, allein gültiger oder bester Lösungsansatz zu sein.

Weitere Sicherheitsanforderungen aufgrund sonstiger (gesetzlicher) Regelungen, die beim Führen eines Unternehmens zu berücksichtigen sind, werden nachfolgend nicht behandelt und sind auch nicht Bestandteil eines Sicherheitskonzeptes nach § 109 Absatz 4 TKG.

Die Auswahl und der Einsatz geeigneter technischer Vorkehrungen und sonstiger Maßnahmen zur Erfüllung der Sicherheitsanforderung unter Berücksichtigung unternehmensspezifischer Rahmenbedingungen obliegen ausschließlich der Zuständigkeit und der Verantwortung des Verpflichteten.

8.1 Sicherheitsanforderungen zum Schutz des Fernmeldegeheimnisses

Da sich der Schutz des Fernmeldegeheimnisses sowohl auf den Inhalt der Telekommunikation als auch auf die näheren Umstände bezieht, sind hier die technischen Einrichtungen zur unmittelbaren Übertragung von Nachrichteninhalten und auch die Einrichtungen zur Erhebung, Verarbeitung und Nutzung von Verkehrsdaten zu berücksichtigen (z.B. Teilnehmeranschluss, Netzabschlusspunkt, Vermittlungs- und Leitwegeinrichtungen, Verbindungsnetz so-wie Billing- oder Fraud-Systeme).

Schon bei der Konzeption von Einrichtungen zur Erbringung von öffentlich zugänglichen Telekommunikationsdiensten sowie der Erhebung, Verarbeitung und Nutzung von Verkehrsdaten ist Belangen des Fernmeldegeheimnisses Rechnung zu tragen. Auch hier gilt

das Prinzip der „Datensparsamkeit“. Dieses Prinzip ist sinngemäß auch bei der (Zwischen-) Speicherung auf Nachrichteninhalte anzuwenden.

Neben Regelungen zur gesetzeskonformen Erhebung, Verarbeitung und Nutzung von Verkehrsdaten sind auch Regelungen zum Löschen von Verkehrsdaten erforderlich. Gesetzlich vorgegebene Löschfristen sind einzuhalten.

Auch Backup-Systeme unterliegen dem Prinzip der Datensparsamkeit sowie den gesetzlichen Vorgaben bezüglich Löschfristen.

Wo geeignete Zutritts- und Zugangsvorkehrungen wie Schließsysteme, Ausweistechnologie, Außenhauthärtung, Passwortmanagement u. ä. nicht ausreichen, ist der Schutz ggf. durch geeignete Verschlüsselungstechniken zu erhöhen (z.B. bei gemeinsam genutzter Teilnehmeranschlussleitung oder bei der Speicherung von Verkehrsdaten).

Bei der Vergabe von Zugangs- und Zugriffsrechten soll das „Need to Know-Prinzip“ gewahrt werden. Widerrechtliche Zugriffe können durch geeignete Monitoringverfahren detektiert werden.

Der gesetzeskonforme Umgang mit Verkehrsdaten ist durch Verfahrensanweisungen für alle Beschäftigten verbindlich vorzugeben.

Generell empfiehlt sich eine entsprechende Schulung und Sensibilisierung der Mitarbeiter, siehe 8.2.1

8.1.1 Inhalte und nähere Umstände der Telekommunikation

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.

Als Schutzmaßnahmen sind Strukturen und Ablaufszenarien denkbar, durch die eine Trennung von Inhalten der Telekommunikation des jeweiligen Telekommunikationsdienstes und den zugrundeliegenden technischen Systemen realisiert werden kann. Zum Schutz der näheren Umstände der Telekommunikation sind Maßnahmen erforderlich, durch die dem Diensteanbieter der Zugriff auf entsprechende Netzebenen oder Netzelemente verweigert wird. Je nach administrativ erteilten Zugriffs- und Leserechten zu einzelnen Bereichen kann ein unterschiedlicher Grad bezüglich des Einblicks in die näheren Umstände zur Telekommunikation erlangt werden.

8.1.2 Unbefugte Weitergabe von Informationen

Es ist sicherzustellen, dass Diensteanbieter Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für Zwecke der geschäftsmäßigen Erbringung der Telekommunikationsdienste, zum Schutz der technischen Systeme, oder soweit eine andere Rechtsvorschrift dies vorsieht, verwenden. Insbesondere sind Maßnahmen erforderlich zum Schutz gegen eine unbefugte Weitergabe von Kenntnissen über Tatsachen, die dem Fernmeldegeheimnis unterliegen, an Andere.

Als Schutzmaßnahme empfiehlt sich eine entsprechende Schulung und Sensibilisierung der Mitarbeiter. Besonderer Wert soll auch auf die effektive Administration der Zugriffsrechte gelegt werden.

8.1.3 Kenntnis über Inhalt oder nähere Umstände der Telekommunikation

Es ist zu verhindern, dass sich Unbefugte Kenntnisse über den Inhalt oder die näheren Umstände der Telekommunikation verschaffen.

Zur Einhaltung dieser Sicherheitsanforderungen bedarf es des Schutzes gegen einen unbefugten Zutritt und Zugang auf:

- Telekommunikationsanlagen (z. B. unerlaubtes Aufschalten auf bestehende Verbindungen)
- Nachrichtenübermittlungssysteme mit Zwischenspeicherung
- Datenverarbeitungsanlagen, die dem Verarbeiten oder Nutzen von Daten, die dem Fernmeldegeheimnis unterliegen (nähere Umstände der Telekommunikation), dienen
- sonstige Datenträger, die der Speicherung von Daten, die dem Fernmeldegeheimnis unterliegen, dienen
- Akten mit Daten, die dem Fernmeldegeheimnis unterliegen

Als Schutzmaßnahmen bezüglich des Zugriffs auf die technische Systeme, über die sich Unbefugte Kenntnisse über den Inhalt oder die näheren Umstände der Telekommunikation verschaffen könnten, ist z.B. ein sogenanntes Rollenprinzip empfehlenswert. Je nach Zuständigkeitsbereich, z.B. Administrierung von Datenbanksystemen, Störungsbehebung von Netz-elementen, Auditierung, werden den Beschäftigten Rollen wie z.B. Operator, Administrator oder Advisor zugewiesen. Zu jeder Rolle gibt es konkrete Sicherheitslevels und Zugangskontrollen bei der Aufgabenwahrnehmung.
Im Bereich der Aktenverwaltung und –verwahrung, die dem Fernmeldegeheimnis unterliegen, sind dem Datenschutz hinreichend genügende Aufbewahrungsbehältnisse zu verwenden sowie entsprechende Räume mit Zutrittskontrolle sinnvoll. Es sollen nur Personen Zugriff haben, die eine ausreichende Belehrung über die Sensibilität dieser Daten im Hinblick auf den Datenschutz und das Fernmeldegeheimnis erhalten haben.

8.1.4 Zwischenspeicherung von Nachrichten

Es ist sicherzustellen, dass Nachrichteninhalte nur zwischengespeichert werden, wenn es für die Durchführung von Telekommunikationsdiensten erforderlich ist.
Schutzmaßnahmen zur Verhinderung nicht notwendiger Zwischenspeicherung von Nachrichteninhalten sollen bereits prophylaktisch bei der Dienste- und Netzplanung erfolgen bzw. bei der Erweiterung von bereits bestehenden Systemen berücksichtigt werden. Übertragungsmedien und Übertragungsraten sowie weitere für das Erbringen eines Dienstes notwendigen Systembestandteile sollten technisch so ausgelegt sein, damit eine möglichst kontinuierliche Verarbeitung und Weiterleitung der Nachrichteninhalte erfolgen kann. Um einzelne übertragungsrelevante Teilsysteme bedarfsgerecht anzupassen, kann ein Monitoring des Verkehrsaufkommens einzelner Dienste sinnvoll sein.

8.1.5 Verarbeitung von zwischengespeicherten Nachrichteninhalten

Es ist sicherzustellen, dass eine Verarbeitung von zwischengespeicherten Nachrichteninhalten ausschließlich in Telekommunikationsanlagen des zwischenspeichernden Diensteanbieters erfolgt, es sei denn, die Nachrichteninhalte werden im Auftrag des Teilnehmers oder

durch Eingabe des Teilnehmers in Telekommunikationsanlagen anderer Diensteanbieter weitergeleitet.

8.1.6 Rechte des Teilnehmers

Es muss sichergestellt werden, dass ausschließlich der Teilnehmer, durch seine Eingabe, Inhalt, Umfang und Art der Verarbeitung bestimmt.

Hierzu sind Schutzmaßnahmen empfehlenswert, die eine Manipulation der Nachrichteninhalte durch Dritte z.B. durch geeignete Identifizierungssysteme (Passwort, PIN, TAN etc.) verhindern.

Es muss sichergestellt werden, dass ausschließlich der Teilnehmer bestimmt, wer Nachrichteninhalte eingeben und darauf zugreifen darf.

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 Entscheidungsfreiheit des Teilnehmers an welche Person er die Zugangskennungen weiter gibt.

8.1.7 Vertragsgemäße Löschung

Es muss sichergestellt werden, dass von dem Diensteanbieter Nachrichteninhalte nur entsprechend dem mit dem Teilnehmer geschlossenen Vertrag gelöscht werden.

Schutzmaßnahmen gegen eine ungerechtfertigte, entgegen dem Vertragsverhältnis vereinbarte Löschung von Nachrichteninhalten durch den Diensteanbieter kann beispielsweise das Anlegen von Backupsystemen sein. Auch die Mehrfachabfrage bei Löschvorgängen kann einer unbeabsichtigten versehentlichen Löschung vorbeugen.

8.1.8 Fehlerübermittlung und unbefugtes Offenbaren

Fehlübermittlungen und das unbefugte Offenbaren von Nachrichteninhalten oder den näheren Umständen der Telekommunikation innerhalb des Unternehmens oder an Dritte müssen ausgeschlossen werden.

Schutzmaßnahmen gegen eine Fehlübermittlung von Nachrichteninhalten können beispielsweise im Einzelnen festzulegende Plausibilitäts- oder Sicherheitsüberprüfungen vor der Versendung des Nachrichteninhaltes sein. Bezüglich einer unbefugten Offenbarung von Nachrichteninhalten sind dem Stand der Technik entsprechende Verschlüsselungsverfahren geeignet. Weitere Hilfestellung bietet u. a. die technische Richtlinie des BSI, TR-02102.

Auch die näheren Umstände einer Kommunikation dürfen nur in berechtigten Fällen offenbart werden, so muss etwa sichergestellt werden, dass eine unterdrückte Rufnummer (mit Ausnahme der gesetzlich geregelten Fälle) nicht dem Angerufenen offenbart wird. Schutzmaßnahmen können die regelmäßige Prüfung der Konfiguration von Telekommunikationssystemen sein.

8.1.9 Datenschutzfreundliche Voreinstellung von TK-Endgeräten

Die Vorkonfiguration von TK-Endgeräten, die von TK-Anbietern den Kunden (als Vertragsbestandteil, zur Miete oder zum Kauf) zur Verfügung gestellt werden, sollte Grundsätze wie die Datenvermeidung und eine hohe Sicherheit berücksichtigen. So sollten die TK-Endgeräte so vorkonfiguriert werden, dass dem Fernmeldegeheimnis unterliegende Daten nur auf Wunsch des Nutzers gespeichert werden, sofern es sich nicht um offensichtliche Listen handelt. 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.

8.2 Sicherheitsanforderungen zum Schutz der personenbezogenen Daten der Teilnehmer und Nutzer von Telekommunikationsdiensten

Zu den zu schützenden personenbezogenen Daten gehören insbesondere Bestands- und Verkehrsdaten. Die Erhebung, Verarbeitung und Nutzung erfolgt u. a. in „Customer Care and Billing- Systemen“, in „Fraud- Systemen (§ 100 TKG)“, in „Systemen zur Mitteilung ankommender Verbindungen (§ 101 TKG)“ oder in „Systemen zur Aufnahme in öffentliche Telefonverzeichnisse“.
Diensteanbieter haben ihre Teilnehmer bei Vertragsabschluss über Art, Umfang, Ort und Zweck der Erhebung und Verwendung personenbezogener Daten zu unterrichten.

Neben Verfahren zur Erhebung, Verarbeitung und Nutzung sind auch Regelungen zur gesetzeskonformen Löschung von Bestands- und Verkehrsdaten festzulegen.

Es wird empfohlen, die Mitarbeiter durch geeignete Unterrichtsmaßnahmen für die Belange des Datenschutzes zu sensibilisieren. Eine Verpflichtungserklärung zur Wahrung des Datenschutzes muss von allen tangierten Mitarbeitern abgegeben werden (§ 5 BDSG). Ebenso sollten betroffene Mitarbeiter auf das Fernmeldegeheimnis verpflichtet (§ 88 TKG) und über die strafrechtlichen Vorschriften (§§ 44, 43 Absatz 2 BDSG, § 206 StGB) informiert werden.

8.2.1 Erhebung personenbezogener Daten

Es dürfen nur personenbezogene Daten erhoben werden, wenn

- das TKG oder eine andere Rechtsvorschrift dies erlaubt und die Daten zur Aufgabenerfüllung erforderlich sind oder
- der Betroffene eingewilligt hat (schriftlich oder elektronisch gemäß § 94 TKG).

Hierbei ist sich an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben (Datensparsamkeit). Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

8.2.2 Speicherung personenbezogener Daten

Personenbezogene Daten dürfen auf Datenverarbeitungsanlagen und sonstigen Datenträgern nur gespeichert werden, wenn

- das TKG oder eine andere Rechtsvorschrift dies erlaubt und es zur Aufgabenerfüllung erforderlich ist oder
- der Betroffene eingewilligt hat.

8.2.3 Löschungsfristen

Es ist sicherzustellen, dass bei gespeicherten personenbezogenen Daten die Löschungsfristen eingehalten werden. In Fällen, in denen an Stelle des Löschens eine Sperrung der Daten tritt (s. etwa § 95 Absatz 3 Satz 2 TKG), ist diese rechtzeitig und wirksam umzusetzen.
Schutzmaßnahmen zur ordnungsgemäßen Löschung (bzw. Sperrung) personenbezogener Daten, entsprechend der gesetzlichen Fristen, können beispielsweise automatisierte Erinnerungsabfragen oder automatisierte Löschverfahren sein. Außerdem sind regelmäßige Prüfungen der Datenbestände sinnvoll.

8.2.4 Verarbeitung und Nutzung

Personenbezogene Daten dürfen nur verarbeitet und genutzt (verwendet) werden, wenn

- das TKG oder eine andere Rechtsvorschrift dies erlaubt und es zur Aufgabenerfüllung erforderlich ist oder
- der Betroffene eingewilligt hat.

Schutzmaßnahmen zur ordnungsgemäßen Verarbeitung und Nutzung der personenbezogenen Daten können durch sorgfältige Gestaltung und Prüfung von Verträgen gewährleistet werden. Eine gegebenenfalls erforderliche Einwilligung des Betroffenen muss rechtzeitig und eindeutig unter Hinweis auf die beabsichtigte Verwendung der Daten erfolgen; verklausulierte und uneindeutige Formulierungen sind zu vermeiden.

8.2.5 Verwendungszweck

Personenbezogene Daten dürfen nur für vorher festgelegte Zwecke verwendet werden.

Hierbei ist sicherzustellen, dass zu unterschiedlichen Zwecken gespeicherte Daten getrennt verwendet werden können. Der Teilnehmer ist gemäß § 94 TKG über den Verwendungszweck zu informieren.

Schutzmaßnahmen zur Sicherstellung der vereinbarten Zweckbestimmung der personenbezogenen Daten sind beispielsweise Anmerkungen zur Verarbeitung und Nutzung einzelner Daten in den Verträgen. Besonders unterschiedliche Verwendungszwecke sollen gut sichtbar und verständlich gekennzeichnet sein. Eine stichprobenartige Überprüfung von Datensätzen personenbezogener Daten mit der Übereinstimmung bezüglich der vereinbarten und gesetzlich zulässigen Verarbeitung und Nutzung könnte beispielsweise in regelmäßigen Zeitabständen erfolgen. Ebenso kann die zweckgebundene Verwendung bestimmter Daten über ein den Zugang und die Nutzung regelndes Rollenkonzept erreicht werden (siehe hierzu auch Punkt 8.2.7).

8.2.6 Zutritt zu Geschäfts- und Betriebsräumen

Es ist zu verhindern, dass Unbefugte Zutritt zu Geschäfts- und Betriebsräumen erlangen:

- In denen Datenverarbeitungsanlagen betrieben werden
- Sonstige Datenträger aufbewahrt werden
- Dokumente und Aufzeichnungen (Akten) aufbewahrt werden

Schutzmaßnahmen zum unbefugten Zutritt zu Geschäfts- und Betriebsräumen sind beispielsweise geeignete Hinweisschilder, dem Schutzbedarf angepasste Zutrittssicherungen wie z.B. Sicherheitsschlösser, Zugangscode-Lesegeräte aber auch Videoaufzeichnungen und Alarmanlagen. Des Weiteren kann eine entsprechende Belehrung des Personals, das Zutritt zu diesen Bereichen haben muss, sinnvoll sein. Entsprechende Vertraulichkeitsbelehrungen und Schulungen zur Sensibilität der personenbezogenen Daten können ebenfalls angebracht sein. Die ausgewählten Schutzmaßnahmen sollen jeweils in angemessener Weise dem Schutzbedarf der personenbezogenen Daten Rechnung tragen.

8.2.7 Zugang und Nutzung

Unbefugten muss der Zugang zu Datenverarbeitungsanlagen verwehrt und die Nutzung der Datenverarbeitungsanlagen verhindert werden (Nutzung von Datenverarbeitungsanlagen durch einen unmittelbaren Zugang auf die Anlagen und durch einen Zugang über eine Fernwartungsschnittstelle (Remote-Zugang) auf die Anlagen).

Die Anmerkungen zu Schutzmaßnahmen unter Punkt 8.2.6 gelten hier sinngemäß, da sich Datenverarbeitungsanlagen in der Regel in besonderen Geschäfts- und Betriebsräumen befinden. Der direkte Zugriff auf Datenverarbeitungsanlagen soll durch geeignete Identifizierungssysteme (Passwort, PIN, TAN etc.) nur authentifizierten Personen erteilt werden. Die Gewährung von Zugriffsrechten sowie die Administrierung von Datenverarbeitungsanlagen sollen personell einer strikten Rollentrennung unterliegen, die wiederum einer Prüfung durch eine unabhängige Person untersteht.

8.2.8 Zugang zu Datenträgern und Akten

Unbefugten muss der Zugang auf sonstige Datenträger und Akten verwehrt werden.

Die Anmerkungen zu Schutzmaßnahmen unter Punkt 8.2.6 und Punkt 8.2.7 gelten hier sinngemäß, da sich sonstige Datenträger und Akten in der Regel in besonderen Geschäfts- und Betriebsräumen sowie im unmittelbaren Umfeld von Datenverarbeitungsanlagen befinden.

8.2.9 Zugriffsberechtigungen zur Benutzung einer DV-Anlage

Es muss sichergestellt werden, dass die zur Benutzung einer Datenverarbeitungsanlage Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (unmittelbarer Zugriff auf Daten und Zugriff über eine Fernwartungsschnittstelle (Remote-Zugang)).

Die Erteilung der Zugriffsberechtigungen zur Benutzung einer Datenverarbeitungsanlage soll einer dafür speziell zuständigen Person unterliegen, die selbst keine Administrierungsrechte innehat. Die Erteilung der Zugriffsrechte soll unter Abstimmung mit dem Fachvorgesetzten auf Basis einer schriftlichen Dokumentation erfolgen. In regelmäßigen zeitlichen Abständen erfolgt eine Überprüfung der erteilten Zugriffsrechte. Sofern ein Fernwartungszugang vorhanden ist, soll der externe Wartungszugang mit Schutzmechanismen versehen sein, die einen unberechtigten Zugriff auf die Datenverarbeitungsanlage und die abgelegten Daten verweigern.

8.2.10 Zugriffsrechte auf Datenträger und Akten

Es muss sichergestellt werden, dass die auf „sonstige Datenträger und Akten“ Zugangsberechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

Die Anmerkungen zu Schutzmaßnahmen unter Punkt 8.2.9 gelten hier sinngemäß.

8.2.11 Schutz gespeicherter personenbezogener Daten

Es ist sicherzustellen, dass gespeicherte personenbezogene Daten nicht unbefugt gelesen, kopiert, übermittelt, verändert oder gelöscht werden können.

Eine Maßnahme hierzu ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren bei gespeicherten Daten. Weitere Hilfestellung bietet u. a. die technische Richtlinie des BSI, TR-02102.

8.2.12 Schutz von Akten

Es ist sicherzustellen, dass Akten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Schutzmaßnahmen, die ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen verhindern, wurden bereits hinreichend oben exemplarisch aufgeführt. Geeignete Authentifizierungsverfahren, Kopier- und Schreibschutz, Zugangskontrollen und viele weitere Schutzmechanismen und Sicherheitsverfahren sind diesbezüglich denkbar. Sofern Akten mit personenbezogenen Daten vernichtet werden müssen, sind diesbezüglich konkrete Schutzmaßnahmen notwendig.

8.2.13 Schutz gespeicherter personenbezogener Daten bei elektronischer Übermittlung und Transport

Es ist sicherzustellen, dass gespeicherte personenbezogene Daten bei der elektronischen Übermittlung oder während ihres Transports nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Eine Maßnahme hierzu ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren. Weitere Hilfestellung bietet u.a. die technische Richtlinie des BSI, TR-02102.

8.2.14 Schutz von Akten beim Transport

Es ist sicherzustellen, dass Akten während ihres Transports nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Schutzmaßnahmen zur Sicherung der Akten während des Transports können beispielsweise spezielle Transportboxen sein, die einen Zugriff von unberechtigten Personen verhindert. Sofern Akten zur Vernichtung transportiert werden, sind Boxen geeignet, die bereits beim Befüllen die Akten unleserlich machen. Das zum Transport der Akten betraute Personal soll ebenfalls entsprechende Sicherheits- und Vertraulichkeitsunterweisungen erhalten. Sofern die Akten zu einem anderen Standort verlegt werden, ist eine Liste über die abgehenden und

eingehenden Akten zu führen, die nur von hierzu berechtigtem Personal erstellt und geprüft werden soll.

8.2.15 Nachvollziehbarkeit bei Veränderung und Löschung (Protokollierung)

Es ist sicherzustellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungsanlagen eingegeben, verändert oder gelöscht worden sind.

Für eine nachträgliche Prüfung, ob und vom wem Daten in einer Datenverarbeitungsanlage eingegeben, geändert oder gelöscht worden sind, können Protokolldatensätze dienlich sein. Bei jedem Dateneingabevorgang wird ein Datensatz erzeugt, in dem Informationen über Datum und Zeit sowie die Person enthalten ist, die eine Eingabe, Änderung oder Löschung vorgenommen hat. Dabei ist es in vielen Fällen sinnvoll, die Rolle der Dateneingabe und -änderung von der Rolle der Datenlöschung zu trennen. Auch beim Ein- und Ausloggen der Person, die Dateneingaben, -änderungen oder -löschungen vornimmt, kann eine entsprechende Protokoll-Datei erzeugt werden, die Informationen über Datum, Zeitrahmen und Person sowie ausgelöste Aktion beinhaltet.

8.2.16 Schutz personenbezogener Daten vor Zerstörung und Verlust

Es ist sicherzustellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Maßnahmen, die eine zufällige Zerstörung oder den Verlust personenbezogener Daten verhindern, können beispielsweise entsprechende Backupverfahren sein. In regelmäßigen Zeit-abständen wird bei diesen Systemen, je nach sicherheitsrelevanter Einstufung oder Bedeutung für den Unternehmenszweck, eine Wiederherstellung der Daten des Primärsystems sichergestellt. Bei besonders kritischen Daten kann diese Sicherung bis hin zu vollständig redundanten Systemen gehen.

8.3 Sicherheitsanforderungen zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen oder Diensten führen

(ordnungsgemäßer Betrieb von öffentlichen Telekommunikationsnetzen und eine fortlaufende Verfügbarkeit von öffentlich zugänglichen Telekommunikationsdiensten)

Grundsätzlichen können Störungen, die zu erheblichen Beeinträchtigungen des Betriebes von öffentlichen Telekommunikationsnetzen oder zu erheblichen Beeinträchtigungen beim Erbringen öffentlich zugänglicher Telekommunikationsdienste führen, an jeder Stelle des Unternehmens, die mittelbar oder unmittelbar an der Erbringung der Dienstleistung beteiligt ist, einwirken.

Zu berücksichtigen sind daher bei der Durchführung der Gefährdungsanalyse und bei der Festlegung von Schutzmaßnahmen sowohl technische Systeme (z.B. Netz, Switch, Datenverarbeitung, Stromversorgung etc.) als auch organisatorische Faktoren (z.B. Personalbereitstellung, Schulung, Ressourcenmanagement etc.).

Im Rahmen der Bewertung von Schutzmaßnahmen ist grundsätzlich eine Gesamtbetrachtung erforderlich.

8.3.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu Geschäfts- und Betriebsräumen, in denen Telekommunikations- und Datenverarbeitungssysteme betrieben werden, zu verwehren.

Schutzmaßnahmen zum unbefugten Zutritt zu Geschäfts- und Betriebsräumen in denen Telekommunikations- und Datenverarbeitungsanlagen betrieben werden, sind beispielsweise geeignete Hinweisschilder, dem Schutzbedarf angepasste Zutrittssicherungen wie z.B. Sicherheitsschlösser, Zugangscode-Lesegeräte aber auch Videoaufzeichnungen und Alarmanlagen. Generell sollen nur Personen Zutritt haben, die über hinreichende Kenntnisse über die in den Geschäfts- und Betriebsräumen eingesetzten Telekommunikations- und Datenverarbeitungssysteme verfügen oder sich in Begleitung solcher Personen befinden. Die ausgewählten Schutzmaßnahmen sollen jeweils in angemessener Weise dem Schutzbedarf der personenbezogenen Daten Rechnung tragen.

8.3.2 Zugang und Nutzung von TK- und DV-Systemen

Es ist sicherzustellen, dass Unbefugte keinen Zugang zu Telekommunikations- und Datenverarbeitungssysteme haben und Telekommunikations- und Datenverarbeitungssysteme nicht nutzen können.

Telekommunikations- und Datenverarbeitungssysteme, welche

- in Geschäfts- / Betriebsräumen (z. B. Vermittlungseinrichtungen, Übertragungssysteme) oder
- auf öffentlichen Wegen / Privatgrundstücken (z. B. Übertragungswege einschließlich ihrer zugehörigen Einrichtungen wie z. B. Schalt- und Verzweigungseinrichtungen, Kabelschächte, Antennenträgern, Verteiler in Mehrfamilienhäusern)

betrieben werden, sind entsprechend zu schützen.

Neben den bereits unter Punkt 8.3.1 aufgeführten Schutzmaßnahmen zum unbefugten Zutritt zu Geschäfts- und Betriebsräumen, in denen Telekommunikations- und Datenverarbeitungsanlagen betrieben werden, sollen ergänzend geeignete Maßnahmen zur unbefugten Nutzung getroffen werden. Bei technischen Systemen der Vermittlungs- und Übertragungstechnik sollen an besonders zugangskritischen Systemeinheiten entsprechende Schutzvorkehrungen angebracht werden, die einen unberechtigten Zugang verwehren (Verschlusseinrichtungen, Verplombung etc.).

8.3.3 Schutz gegen Störungen

Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und Telekommunikationsdiensten führen, ist entgegen zu wirken, wenn Sie bedingt sind durch:

- Einwirkungen von Katastrophen und elementaren Gefährdungen (höhere Gewalt wie z. B. Feuer, Wasser, Sturm, Blitz, sonstige extreme Witterungseinflüsse)
- Technische Störungen (wie z. B. Ausfall der Stromversorgung, Ausfall der Klimaanlage)
- Organisatorische Mängel
- Menschliche Fehlhandlungen

- Äußere Angriffe (vorsätzliche Handlungen wie z. B. Einbruch, Vandalismus, terroristische Anschläge, Manipulation an Hard- und Software-Komponenten von Telekommunikations- und Datenverarbeitungssystemen)

Schutzmaßnahmen, die einen je nach Gefährdungsgrad und o. g. Gefährdung angemessenen Schutz zugrunde legen, können beispielsweise Gebäude sein, die erdbebensicher ausgelegt wurden sowie gegen das Eindringen von Wasser gesichert sind. Auch feuerhemmende Materialien in den Räumen oder zu den Räumen sowie ein angemessener Schutz gegen Hochspannungsbeeinflussung, wie beispielsweise Blitzeinschlag, können hier exemplarisch aufgeführt werden. Geeignete Notstromaggregate, bzw. ausreichend ausgelegte und gewartete Akkumulatoren, können die Funktionalität von technischen Systemen bei Ausfall der Stromzuführung über einen bestimmten Zeitraum gewährleisten. Organisatorische Mängel und menschliche Fehlhandlungen können vielfach durch sorgsame Planung und bei kritischen Vorgängen durch ein Vieraugenprinzip minimiert werden. Auch besonders ausgebildetes Schutz- und Wachpersonal kann bei sicherheitstechnisch hoch einzustufenden Systemen ein Mittel der Wahl sein.
Auf die entsprechenden Ausführungen in den IT- Grundschutzkatalogen des BSI wird hingewiesen.

8.3.4 Minimierung der Sicherheitsrisiken

Es ist sicherzustellen, dass die Risiken für die Sicherheit von Telekommunikationsnetzen und –diensten und Maßnahmen beherrschbar sind, um die Auswirkungen von Sicherheitsverletzungen für Nutzer oder für zusammengeschaltete Netze so gering wie möglich zu halten.
Zur Einhaltung dieser Sicherheitsanforderungen ist es erforderlich, den ordnungsgemäßen Betrieb von Telekommunikationsnetzen und Telekommunikationsdiensten nach einem Ausfall oder teilweisen Ausfall so schnell als möglich wiederherzustellen.
Schutzmaßnahmen, die eine schnelle Wiederherstellung des ordnungsgemäßen Betriebs von Telekommunikationsnetzen und Telekommunikationsdiensten nach einem Ausfall oder teilweisen Ausfall unterstützen, können z.B. die Vorbereitung geeigneter Notfallszenarien für besonders kritische Systeme sein. Neben der Planung geeigneter Notfallszenarien sind hier auch die Vorhaltung konkreter redundanter Systeme an lokal verzweigten Orten denkbar. Auch hier gilt die Verhältnismäßigkeit einer Maßnahme zum zu schützenden Netz oder Dienst und der Eintrittswahrscheinlichkeit eines zu minimierenden Risikofaktors.
Auf die Ausführungen in Kapitel 5 wird hingewiesen.

Grundsätzlich können Störungen, die zu erheblichen Beeinträchtigungen des Betriebes von öffentlichen Telekommunikationsnetzen oder zu erheblichen Beeinträchtigungen beim Erbringen öffentlich zugänglicher Telekommunikationsdienste führen, an jeder Stelle des Unter-nehmens, die mittelbar oder unmittelbar an der Erbringung der Dienstleistung beteiligt ist, einwirken.
Zu berücksichtigen sind daher bei der Durchführung der Gefährdungsanalyse und bei der Festlegung von Schutzmaßnahmen sowohl technische Systeme (z.B. Netz, Switch, Server Datenverarbeitung, Stromversorgung etc.) als auch organisatorische Faktoren (z.B. Personalbereitstellung, Schulung, Ressourcenmanagement etc.).

Im Rahmen der Bewertung von Schutzmaßnahmen ist grundsätzlich eine Gesamtbetrachtung erforderlich.

9. Verbesserung der Internetsicherheit

Die Anbindung eines TK-Systems an das Internet oder die Erbringung von TK-Diensten im oder im Umfeld des Internets bergen erhebliche Gefahren für die angeschlossenen TK-, DV-Systeme und deren Nutzer. Aufgrund dieser spezifischen Gefährdungslage sowie aufgrund der immensen Bedeutung des Internets im geschäftlichen und privaten Bereich werden nachfolgend Sicherheitsanforderungen sowie Maßnahmen speziell für eine Verbesserung der Internetsicherheit beispielhaft dargestellt. Insofern werden Ausführungen des Kapitels 8 durch sektorspezifische Zusatzanforderungen und Maßnahmen weiter konkretisiert. Dabei bilden die aufgelisteten Sicherheitsempfehlungen die Grundlage für den sicheren Betrieb eines internetbasierten TK- Systems.

Umfassende Maßnahmenempfehlungen sind u. a. in den Schriftenreihen zur Internetsicherheit (ISi-Reihe) und in den Cybersicherheitsempfehlungen für Internetservice Provider des BSI zu finden.

9.1 DoS / DDoS Mitigation

Es gibt verschiedene Arten von DoS / DDoS - Angriffen. Bei sogenannten Reflection Angriffen werden Anfragen mit gefälschten Absenderadressen an Server gesendet, die Anfragen aus dem Internet erlauben. Internet-Betreiber sollten daher das Fälschen von Absenderadressen unterbinden (RFC2827 und RFC3704). Betreiber öffentlich erreichbarer Server sollten diese gegen Missbrauch absichern, indem z.B. nicht benötigte Dienste deaktiviert werden. DoS / DDoS - Angriffe lassen sich nicht gänzlich verhindern. Die Wirkung des Angriffs kann jedoch durch Verwendung geeigneter mehrstufiger Filter und den Einsatz von adaptiven Regelungen (mitigation devices) im Netz deutlich abgemildert werden.

9.2 Netzverkehr beobachten und analysieren (Netzforensik)

Um Angriffe oder Fehler zu erkennen, sollten die Verkehrsdaten (also keine Inhalte) im Rahmen der gesetzlichen Möglichkeiten und soweit dies für die Erbringung des jeweiligen Dienstes erforderlich ist, regelmäßig beobachtet werden. Hierbei ist insbesondere das BDSG und § 100 Absatz 1 TKG zu beachten.
Im Einzelfall kann zum Erkennen und Eingrenzen von unter den Voraussetzungen von § 100 Absatz 2 TKG – insbesondere der unverzüglichen Löschung aufgezeichneter Daten und der Information des betrieblichen Datenschutzbeauftragten - auch der Telekommunikationsinhalt aufgezeichnet werden. Dies sollte jedoch nur in Ausnahmefällen durchgeführt werden, bei denen eine Auswertung von Verkehrsdaten nicht zum Ziel führt.

9.3 Verschlüsselung von Daten (-Verkehr)

Die Verschlüsselung von Daten vermindert das Risiko der unerlaubten Kenntnisnahme personenbezogener Daten einschließlich Daten, die im Zusammenhang mit dem Fernmeldegeheimnis stehen. Durch die Anwendung von Verschlüsselungsverfahren wird ebenso das Verfälschen des Datenverkehrs erschwert.
Wer Telekommunikationsnetze betreibt oder öffentliche Telekommunikationsdienste erbringt sollte sich mit diesem Thema auseinandersetzen und bei entsprechender Gefährdungslage an geeigneter Stelle eine Verschlüsselung der Daten vornehmen.
Neben einer Verschlüsselung der Daten selbst, bietet sich auch die regelmäßige 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 des BSI, TR-02102.

9.4 Authentifizierung und Autorisierung

Bestimmte Anwendungen oder die Vergabe von Zugriffsberechtigungen erfordern die eindeutige Authentifizierung und Autorisierung der Benutzer, um sicherstellen zu können, dass nicht etwa ein Angreifer eine falsche Identität angenommen hat und sich auf diesem Weg u.a. Zugang zu sensiblen Daten oder Diensten, insbesondere innerhalb der Infrastruktur, erschleicht. Neben dem bekannten Verfahren zur Authentisierung mit Hilfe von Benutzername und Passwort können hier weitere Möglichkeiten wie beispielsweise elektronische Identifikationssysteme oder Verfahren der sogenannten Zwei-Faktor-Authentifizierung (Besitz und Wissen) zum Einsatz kommen.

9.5 Aufklärung des Kunden über Bedrohungen und bei erkannter Infektion

Unter Beachtung der rechtlichen Bestimmungen, insbesondere der Datenschutzvorschriften, sollen Anbieter von Telekommunikationsdiensten die Möglichkeit nutzen, technische Hilfsmittel zum Einsatz zu bringen, um infizierte Systeme von Kunden zu identifizieren, und um dem / den betroffenen Kunden bei einer erkannten Infektion seines / ihres Systems entsprechend zu informieren, damit er / sie die Sicherheit seines / ihres Systems wieder herstellen kann / können.

9.6 Kooperationen bei TK-Anbieter übergreifenden Störungen

Treten Störungen auf, von denen mehrere TK-Anbieter betroffen sind, beispielsweise aufgrund von DDoS-Angriffen, ist eine TK-Anbieter übergreifende Zusammenarbeit sinnvoll. Hierzu sollten Ansprechpartner und Vorgehensweisen im Vorfeld untereinander abgestimmt werden.

9.7 Notfallsperrungen von Benutzerzugängen oder Berechtigungen

Erkennt der TK-Anbieter die Infektion eines Nutzersystems, sollte die Information des Kunden an erster Stelle stehen. Kann der Nutzer sein System nicht bereinigen, solle der TK-Anbieter in schwerwiegenden Fällen die Möglichkeit haben, notfalls die vorübergehende Sperrung einzelner Ports oder des generellen Internet-Zugangs des Benutzers vorzunehmen. Möglicherweise sind dazu geeignete Änderungen in den AGB´s notwendig.

9.8 Ausbau von Bandbreiten

Der Ausbau von Bandbreiten, auch außerhalb von Ballungsgebieten, solle im Interesse aller Anbieter von Telekommunikations- und Datenverarbeitungssystemen sein, da durch den weiteren Ausbau der Infrastruktur auch deren generelle Verfügbarkeit weiter erhöht werden kann.

9.9 Verwendung geprüfter und regelmäßig aktualisierter Hard- oder Software

Schwachstellen in Hard- oder Software können durch Angreifer vielfältig ausgenutzt werden. Die Verringerung der Angriffsfläche durch regelmäßige Aktualisierung und ausgiebige Tests der eingesetzten Hard- und Software sollte daher von allen TK-Anbietern als wichtige Sicherheitsmaßnahme umgesetzt werden.

9.10 Netzkomponenten sicher konfigurieren

Der sicheren Konfiguration von Netzkomponenten kommt eine große Bedeutung zu. Werden hier falsche oder nicht ausreichend geprüfte Einstellungen getroffen oder übernommen, können diese beispielsweise Auswirkungen auf die Verfügbarkeit von Netzbereichen oder Diensten im Internet haben sowie Hacking ermöglichen.

9.11 Anti Spam-Lösungen für Anwendersysteme

Der Einsatz von Anti Spam-Lösungen sowie der Einsatz aktueller Antiviren-Programme stellen eine Möglichkeit dar unter anderem den massenhaften Versand unerwünschter Werbe-botschaften und in diesem Zusammenhang auch die Verbreitung von Schadprogrammen einzudämmen. TK-Anbieter sollten diese Möglichkeit nutzen um ihre eigene Infrastruktur zu schützen sowie ihren Kunden zu helfen, die Sicherheit im Internet zu verbessern, indem sie ihnen möglichst einfach zu konfigurierende Sicherheitspakete zur Verfügung stellen.

9.12 Gleichbehandlungsgrundsatz

Datenpakete von und an Kunden solle der TK-Anbieter unverändert und gleichberechtigt übertragen, unabhängig davon, woher diese stammen oder welche Anwendungen die Pakete generiert haben.

9.13 Zeitnahe Einführung von IPv6

Das Problem des bald erschöpften IPv4-Adressraums lässt sich mit dem Einsatz von IPv6 lösen. Nicht zuletzt aufgrund dieser Tatsache sollten sich alle Anbieter von Telekommunikations- und Datenverarbeitungssystemen ausführlich mit der Einführung von IPv6 beschäftigen.

9.14 Verhinderung der Manipulation von BGP-Routern

(Interdomain-)Routing bezeichnet Routing über mehrere autonome Systeme hinweg. Diese Form des Routings wird zumeist vom Internet-Dienstanbieter administriert. Im Internet stellt das sogenannte Border Gateway Protocol (BGP) den de-facto-Standard für Interdomain-Routing dar. Der unbedachte oder nicht ausreichend geprüfte Eingriff in das Routing kann dazu führen, dass Teilbereiche des Netzes nicht mehr erreichbar sind oder Kommunikationswege unbemerkt umgeleitet werden können. Die Ergreifung von Maßnahmen zur Verhinderung der Manipulation von BGP-Routen ist somit eine wichtige Aufgabe für die Anbieter von Internetanschlüssen.

9.15 DNSSEC Maßnahmen

Die kryptografische Sicherung der DNS-Kommunikation mittels der sogenannten DNS Security Extensions (DNSSEC) ist eine wesentliche Maßnahme zur Umsetzung eines sicheren Betriebs der DNS-Infrastruktur.

9.16 Vermeidung von Monokulturen und Einsatz vertrauenswürdiger Hersteller

Der Aufbau von Monokulturen beim Einsatz von Hard- oder Software führt zu einer vermehrten Abhängigkeit von einzelnen Herstellern. Diese Abhängigkeit sollte vermieden werden, um das Risiko von Systemausfällen beispielsweise durch die gezielte Ausnutzung von Schwachstellen in der Hard- oder Software eines bestimmten Herstellers zu minimieren. Des

Weiteren sollte auf den Einsatz von Einrichtungen vertrauenswürdiger Hersteller geachtet werden.

9.17 Erhöhung der Sicherheit von TK-Endgeräten (Breitband-Router)

TK-Endgeräte sind oft die einzige zentrale Sicherheitskomponente zum Schutz des internen Netzes. Daher sollten TK-Anbieter, die TK-Endgeräte ihren Kunden (als Vertragsbestandteil, zur Miete oder zum Kauf) bereitstellen, geeignete Maßnahmen umsetzen, um die Sicherheit dieser Geräte zu erhöhen.
Hierzu ist von TK-Anbietern zu gewährleisten, dass eine zeitnahe Aktualisierung der TK-Endgeräte-Firmware möglich ist. Beispielsweise kann werkseitig eine automatische Firmware-Update-Funktion angeboten und diese im Auslieferungszustand des Gerätes standard-mäßig aktiviert sein. Sofern Firmware-Updates vorzugsweise oder ausschließlich mithilfe eines Auto Configuration Servers (TR-069) verteilt werden, sollte diese Fernwartungsfunktion gegen Angriffe ausreichend abgesichert sein. Insbesondere Sicherheitsupdates müssen schnellstmöglich auf die betroffenen Geräte aufgespielt werden. Störungen bei den Endgeräten der Kunden aufgrund fehlerhafter Firmware sollten vor Aufspielen durch hinreichende Tests vermieden werden.
Als weitere Schutzmaßnahme sollten typischerweise für DDoS-Reflection-Angriffe verwendete Dienste in einem TK-Endgerät geschlossen sowie keine weiteren nicht zwingend erforderlichen Dienste an der WAN-Schnittstelle des Gerätes aktiviert sein.
Die Zugänge zum WLAN sowie auf das Web-Front-End des TK-Endgerätes sollten sicher vorkonfiguriert sein. Zudem sollte der Nutzer bei Erstinbetriebnahme aufgefordert werden, sichere neue Kennwörter für die genannten Zugänge zu vergeben.
Darüber hinaus sollte eine Firewall (Paketfilter) im Auslieferungszustand aktiviert sein. Es dürfen keine Hintertüren (also nicht dokumentierte Zugänge) in TK-Endgeräten vorhanden sein.
Schließlich sollten TK-Anbieter die Endkunden zeitnah informieren, falls die Entwicklung und zur Verfügungsstellung von Firmware-Updates vom TK-Anbieter bezogener Gerätetypen eingestellt werden.

10. Weitere Informationsquellen

Informationen zum TKG, Telekommunikationsgesetzgebung, Amtsblätter:

www.BNetzA.de

www.gesetze-im-internet.de

Informationen zum IT-Grundschutz und der Internet-Sicherheit des BSI:

www.bsi.bund.de/grundschutz

www.isi-reihe.de

www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/ISP-Empfehlung/Internet-Service-Provider

BSI-Standard 100-1 bis 100-4

Informationen zum Datenschutz:

www.bfdi.bund.de

www.datenschutz.de

DIN-; IEC-; ISO-Normen, VdS Richtlinien

www.beuth.de/

DIN ISO/IEC 27001 Informationssicherheits-Managementsysteme - Anforderungen

DIN ISO/IEC 27002 Leitfaden für das Informationssicherheits-Management

UP-KRITIS, Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen

www.upkritis.de

Schutz Kritischer Infrastrukturen - Basisschutzkonzept

www.bmi.bund.de

ENISA Publikationen

www.enisa.europa.eu

Technical Guideline on Incident Reporting

Technical Guideline on Minimum Security Measures

BITKOM Publikationen

www.bitkom.org

Informationen über Verschlüsselung

BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen

11. Begriffsbestimmungen

Standardsicherheit

Standardsicherheit ist dann gewährleistet, wenn einschlägige Normen oder Regelungen zur Umsetzung von Schutzmaßnahmen (z. B.: IT-Grundschutz des BSI oder ISO IEC 27000.ff.) bei durchschnittlichem Schutzbedarf eingehalten werden. Bei entsprechender Begründung (Angemessenheitsprinzip) sind Abweichungen vom empfohlenen Schutzniveau zulässig.

Stand der Technik

Stand der Technik ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, der nach herrschender Auffassung führender Fachleute das Erreichen des gesetzlich vorgegebenen Zieles gesichert erscheinen lässt. Verfahren, Einrichtungen und Betriebsweisen oder vergleichbare Verfahren, Einrichtungen und Betriebsweisen müssen sich in der Praxis bewährt haben oder sollten – wenn dies noch nicht der Fall ist – möglichst im Betrieb mit Erfolg erprobt worden sein.

Im Recht der Europäischen Union wird auch die Formulierung „die besten verfügbaren Techniken“ verwendet. Dies entspricht weitgehend der Generalklausel „Stand der Technik“.

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

Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)

Verletzung des Schutzes personenbezogener Daten

Eine Verletzung der Datensicherheit, die zum Verlust, zur unrechtmäßigen Löschung, Veränderung, Speicherung, Weitergabe oder sonstigen unrechtmäßigen Verwendung personenbezogener Daten führt, die übertragen, gespeichert oder auf andere Weise im Zusammenhang mit der Bereitstellung öffentlich zugänglicher Telekommunikationsdienste verarbeitet werden sowie der unrechtmäßige Zugang zu diesen

Datenerhebung

Beschaffen von Daten über den Betroffenen

Datenverarbeitung

Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten

Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. Speichern; Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung
2. Verändern; das inhaltliche Umgestalten gespeicherter personenbezogener Daten
3. Übermitteln; das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass

    1. die Daten an den Dritten weiter gegeben werden oder
    2. der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft

4. Sperren; das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken
5. Löschen; das Unkenntlichmachen gespeicherter personenbezogener Daten

Datennutzung

Jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt

Kritische Infrastruktur

Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten können

SPOC

Single Point of Contact

UP-KRITIS

Umsetzungsplan KRITIS