Katalog von Sicherheitsanforderungen

(ENTWURFSFASSUNG)

für das Betreiben von

Telekommunikations- und

Datenverarbeitungssystemen

sowie für die Verarbeitung

personenbezogener Daten nach

§ 167 Telekommunikationsgesetz (TKG)

Stand: Oktober 2025

ENTWURF

Version 2025-10

ENTWURF

Bundesnetzagentur für Elektrizität, Gas,
Telekommunikation, Post und Eisenbahnen

Referat 217

Tulpenfeld 4
53113 Bonn
Tel.: +49 228 14-0
Fax: +49 228 14-8872
E-Mail: info@bnetza.de

Version 2025-10

ENTWURF

ENTWURF

Inhaltsverzeichnis

Inhaltsverzeichnis **5**

I ENTWURF DES KATALOGS VON SICHERHEITSANFORDERUNGEN GEMÄß §167 TKG **9**

A Allgemeinverfügung **10**

Gründe: 13

1. Ermächtigungsgrundlage und formelle Rechtmäßigkeit (Ziffern 1) bis 3) des Tenors) 13

2. Materielle Rechtmäßigkeit (Ziffer 1) des Tenors) 14
2.1 Umfang der Regelungswirkung (§ 35 S. 1 VwVfG) sowie Bestimmtheit (§ 37 Abs. 1 VwVfG) 15
2.2 Unbestimmte Rechtsbegriffe 17
2.3 Ermessensausübung 18
2.3.1 Entschließungsermessen 18
2.3.2 Auswahlermessen 19
2.3.3 Kein Ermessensfehlgebrauch: Allgemeine Verhältnismäßigkeitsüberlegungen hinsichtlich aller im Katalog genannten Maßnahmen 20
2.3.4 Widerruf des Sicherheitskataloges Version 2.0 (Ziffer 2) des Tenors) 25
2.3.5 Gesonderte Rechtmäßigkeitserwägungen zu den Gefährdungspotenzialen (Ziffer 3) des Tenors) 25

B Katalog von Sicherheitsanforderungen §167 TKG **28**

1. Einleitung/Allgemeines 29

2. Adressaten 31

3. Bestimmung von Gefährdungspotenzialen 32
3.1 Gefährdungspotenziale 32
3.2 Verhältnismäßigkeitserwägungen zur Bestimmung der Gefährdungspotenziale 34

4. Festlegung grundlegender Einzelheiten der zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen unter Berücksichtigung der verschiedenen Gefährdungspotenziale, § 167 Abs. 1 S. 1 Nr. 1 TKG 37
4.1 Schutz des Fernmeldegeheimnisses und personenbezogener Daten 39
4.2 Unternehmensführung und Risikomanagement 40
4.2.1 Informationssicherheitspolitik 41
4.2.2 Risikomanagement 41
4.2.3 Sicherheitsrollen und Verantwortlichkeiten 42
4.2.4 Sicherheit bei Abhängigkeiten von Dritten 43
4.3 Sicherheit im Personalmanagement 45
4.3.1 Personalmanagement 46
4.3.2 Sicherheitswissen, Sicherheitsausbildung und Prüfung 46
4.3.3 Personelle Veränderungen 47
4.3.4 Umgang mit Verstößen 48
4.4 Sicherheit von Daten, Systemen und Einrichtungen 49
4.4.1 Physische und umgebungsbezogene Sicherheit 51
4.4.2 Sicherheit der Versorgung (Verfügbarkeit des Gesamtsystems) 52
4.4.3 Zugriffs- und Zugangskontrolle zu Netz- und Informationssystemen 52
4.4.4 Integrität und Verfügbarkeit von Netz- und Informationssystemen 54
4.4.5 Sicherstellung der Vertraulichkeit 54
4.4.6 Schutz von sicherheitsrelevanten Daten 55
4.5 Betriebsführung 57
4.5.1 Betriebsverfahren 58

ENTWURF

4.5.2 Änderungsmanagement ... 58
4.5.3 Asset Management ... 59
4.6 Lifecycle-Management für Hard- und Software ... 61
4.7 Management von Zwischenfällen ... 63
4.7.1 Verfahren für das Management von Zwischenfällen ... 64
4.7.2 Fähigkeit zur Erkennung von Zwischenfällen ... 65
4.7.3 Meldung von Zwischenfällen und Kommunikation ... 65
4.7.4 Kooperation bei TK-anbieterübergreifenden Störungen ... 66
4.8 Notfall- und Ausfallmanagement ... 68
4.8.1 Strategie zur Aufrechterhaltung der Netze, der Dienste und Notfallpläne ... 69
4.8.2 Wiederanlauf nach Ausfällen (Disaster Recovery Management) ... 70
4.8.3 Backup-Strategie ... 71
4.9 Überwachungs-, Prüf- und Testverfahren ... 72
4.9.1 Systeme zur Angriffserkennung, Überwachungs- und Protokollierungsmaßnahmen ... 73
4.9.2 Notfallübungen ... 74
4.9.3 Testen von Netzwerk- und Informationssystemen ... 74
4.9.4 Beurteilung der Schutzmaßnahmen ... 75
4.9.5 Überwachung der Einhaltung ... 76
4.10 Bewusstsein für Bedrohungen (Threat Awareness) ... 77
4.10.1 Informationen über Bedrohungen (Threat Intelligence) ... 78
4.10.2 Unterrichtung der Nutzer über Bedrohungen ... 78

5. Festlegung von zusätzlichen Einzelheiten und Maßnahmen für 5G-Netze ... 79
5.1 Bestimmung von kritischen Komponenten ... 79
5.2 Prozess zur Identifizierung von kritischen Komponenten im betriebenen Netz ... 85
5.3 Zertifizierung von kritischen Komponenten ... 86
5.3.1 Übergangsregelung zur Zertifizierung von kritischen Komponenten ... 86
5.4 Diversität ... 87
5.5 Technische Maßnahmen für die Sicherheit in 5G-Netzen ... 88
5.5.1 Schutz der Identität und Privatheit der Teilnehmer ... 88
5.5.2 Schutz der Vertraulichkeit der Nutz- und Signalisierungsdaten ... 92
5.5.3 Schutz der Integrität der Nutz- und Signalisierungsdaten ... 93
5.5.4 Schutz des Zugriffs auf Netzwerkfunktionen im 5G-Kernnetz ... 95
5.5.5 Schutz der SBA-Kommunikation im 5G-Kernnetz ... 96
5.5.6 Schutz der Kommunikation zwischen Zugangsnetzwerk und Kernnetz sowie zwischen Zugangsnetzwerken ... 97
5.5.7 Schutz der Kommunikation innerhalb eines Zugangsnetzwerks ... 99
5.5.8 Schutz der Kommunikation zwischen dem 5G-Kernnetz und Nicht-5G-Netzwerkelementen ... 100
5.5.9 Schutz der Roaming Signalisierung ... 102
5.5.10 Schutz des Remote SIM Provisionings ... 103
5.5.11 Schutz vor Angriffen auf die Ausführungsumgebung bei Virtualisierung und Containerisierung ... 105
5.5.12 Schutz bei Nutzung von Virtualisierungs- oder Cloud-Diensten ... 106

6. Empfehlungen und Hinweise ... 109
6.1 Lokales Breitband 26 GHz ... 109
6.2 Zugrundeliegende Normen, Standards und Guidelines ... 109

Glossar ... 110

Abkürzungsverzeichnis ... 111

C Anhang - Technische Spezifikation für paketvermittelte Netze zum Katalog der Sicherheitsanforderungen ... 113

1. Einleitung ... 113

2. Maßnahmen gegen Distributed Denial of Service (DDoS) Angriffe ... 115
2.1 Ertüchtigung der eigenen Infrastruktur ... 115
2.2 Mitigation ... 115

ENTWURF

2.3 Absicherung ausnutzbarer Systeme ... 115

3. Inter-Domain-Routing ... 117
3.1 Schutz der BGP-Session ... 117
3.2 Bereitstellung von Routing-Informationen ... 117
3.3 Verhinderung der Weitergabe falscher Routing-Informationen ... 117
3.4 Verhindern von Datenverkehr mit gefälschten Quell-IP-Adressen ... 118
3.5 Bereitstellung aktueller Kontaktinformationen ... 118

4. Domain Name System – Resolver ... 120
4.1 Technische Voraussetzungen ... 120
4.2 DNSSEC ... 120
4.3 Cache-Poisoning ... 121
4.4 Privacy ... 121

5. Domain Name System - Autoritative DNS-Server ... 123
5.1 Technische Voraussetzungen ... 123
5.2 Schutz vor Ausnutzung ... 123
5.3 DNSSEC ... 124

6. E-Mail-Sicherheit ... 125
6.1 Maßnahmen zum Schutz vor Malware und zur Abwehr von Spam und Phishing ... 125
6.1.1 Scan von E-Mails auf Malware (Viren, Würmer, Trojaner) und zu Hinweisen auf Spam oder Phishing ... 125
6.1.2 Prüfung eingehender E-Mails mit einem Spam-Filter ... 125
6.1.3 Maßnahmen gegen Spam-Verbreitung durch Kunden ... 126
6.1.4 Umgang mit verdächtigen Emails ... 127
6.1.5 Kundenbenachrichtigung ... 127
6.2 Vertraulichkeit des E-Mail-Verkehrs ... 129

7. Bewusstsein für Bedrohungen (Awareness) ... 132
7.1 Etablieren eines Schwachstellen-Managements ... 132
7.1.1 Systematisches Sammeln und Auswerten der Schwachstellenmeldungen von Herstellern und CERTs ... 132
7.1.2 Informationsaustausch und Zusammenarbeit mit anderen Anbietern und Betreibern ... 133

Begriffsbestimmungen für Anhang (Technische Spezifikation) ... 134

Abkürzungsverzeichnis ... 136

II KONSULTATION ... 139

VERZEICHNISSE ... 141

Abbildungsverzeichnis ... 142

Impressum ... 143

ENTWURF

ENTWURF

I Entwurf des Katalogs von Sicherheitsanforderungen gemäß §167 TKG

Die im Katalog von Sicherheitsanforderungen festgelegten Maßnahmen werden regelmäßig überprüft und angepasst, um mit dem Stand der Technik Schritt zu halten.

ENTWURF

Dieser Entwurf umfasst die Allgemeinverfügung des Kataloges von Sicherheitsanforderungen unter Abschnitt A, den eigentlichen Katalog von Sicherheitsanforderungen gemäß §167 TKG unter Abschnitt B sowie einen Anhang zur technischen Spezifikation für paketvermittelte Netze zum Katalog der Sicherheitsanforderungen unter Abschnitt C.

A Allgemeinverfügung

ENTWURF

Die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Bundesnetzagentur) legt gemäß § 167 Absatz 1 Satz 1 Telekommunikationsgesetz (TKG) im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit Folgendes fest:

1. Der in Abschnitt B angefügte Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten, mitsamt dem Anhang (Technische Spezifikation für paketvermittelte Netze) in Abschnitt C, tritt mit Bekanntgabe in Kraft.

2. Innerhalb der Umsetzungsfrist gemäß § 167 Abs. 2 TKG gelten für die Adressaten nach Ziffer 1) die Pflichten aus dem mit Allgemeinverfügung Nr. 63/2021 erlassenen Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten vom 29.04.2020 (Sicherheitskatalog Version 2.0) weiter, falls die Adressaten nach Ziffer 1) in den Adressatenkreis des Sicherheitskatalogs Version 2.0 fallen und soweit die Adressaten nach Ziffer 1) die Vorgaben des Katalogs aus 1.) noch nicht erfüllt haben.

   Der mit Allgemeinverfügung Nr. 63/2021 vom 25.08.2021 (ABl. BNetzA Nr. 16/2021) erlassene Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten vom 29.04.2020 (Sicherheitskatalog Version 2.0), zuletzt geändert durch die Allgemeinverfügung Nr. 57/2022 vom 29.06.2022 (ABl. BNetzA Nr. 12/2022), wird mit Wirkung zum DATUM (Inkrafttreten SiKa-neu plus ein Jahr) widerrufen.

ENTWURF

3. Auf Grundlage des § 167 Abs. 1 S. 1 Nr. 3 TKG werden die verschiedenen Gefährdungspotenziale der öffentlichen Telekommunikationsnetze und öffentlich zugänglichen Telekommunikationsdienste im Einvernehmen mit dem BSI sowie der/dem BfDI wie folgt festgelegt:

   a) **Normales Gefährdungspotenzial**: Ein Anbieter von öffentlich zugänglichen Telekommunikationsdiensten oder ein Betreiber öffentlicher Telekommunikationsnetze, weist ein normales Gefährdungspotenzial auf, wenn er weniger als 10 Personen beschäftigt und sein Jahresumsatz bzw. seine Jahresbilanzsumme 2 Mio. EUR nicht überschreitet.

   b) **Gehobenes Gefährdungspotenzial**: Ein Anbieter von öffentlich zugänglichen Telekommunikationsdiensten oder ein Betreiber öffentlicher Telekommunikationsnetze, hat ein gehobenes Gefährdungspotenzial, sofern er eine Bedeutung für das Gemeinwohl darstellt. Jedenfalls weist er ein gehobenes Gefährdungspotenzial auf, wenn er

      i) weniger als 50 Mitarbeiter beschäftigt und

      ii) einen Jahresumsatz oder eine Jahresbilanzsumme von jeweils 10 Millionen Euro oder weniger aufweist.

   c) **Erhöhtes Gefährdungspotenzial**: Ein Anbieter von öffentlich zugänglichen Telekommunikationsdiensten oder ein Betreiber öffentlicher Telekommunikationsnetze, weist ein

erhöhtes Gefährdungspotenzial auf, sofern er eine herausragende Bedeutung für das Gemeinwohl hat.

Ein erhöhtes Gefährdungspotenzial liegt jedenfalls in diesen Fällen vor:

i) Betreiber eines öffentlichen Mobilfunknetzes der 5. Generation (5G Netz)

ii) Betreiber eines sonstigen öffentlichen Telekommunikationsnetzes oder Anbieter von öffentlich zugänglichen Telekommunikationsdiensten, wenn er

(1) mindestens 50 Mitarbeiter beschäftigt oder

(2) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweist oder

(3) ein Betreiber kritischer Einrichtungen gemäß Artikel 2 Nummer 1 der RICHTLINIE (EU) 2022/2557 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates ist oder

Für diese Unternehmen mit erhöhtem Gefährdungspotenzial gilt die im Sicherheitskatalog (Abschnitt B), Kapitel 5.1. genannte Tabelle 1: Liste der festgelegten kritischen Funktionen, § 167 Abs. 1 Nr. 2 TKG.

ENTWURF

Die Bundesnetzagentur weist auf Folgendes hin:

1. Diese Verfügung gilt gemäß § 210 Satz 3 TKG in Verbindung mit § 41 Abs. 4 Satz 4 VwVfG am DATUM, dem Tag nach ihrer Veröffentlichung auf der Internetseite der Bundesnetzagentur sowie ihrer Bekanntmachung im Amtsblatt der Bundesnetzagentur, als öffentlich bekannt gegeben. Sie tritt damit am DATUM in Kraft.

2. Die Verpflichteten haben die Vorgaben des Katalogs spätestens ein Jahr nach dessen Inkrafttreten zu erfüllen (§ 167 Abs. 2 TKG).

3. Die vollständige Entscheidung wird auf der Internetseite der Bundesnetzagentur veröffentlicht.

Gründe:

I.

Mit Allgemeinverfügung Nr. 63/2021 wurde am 25.08.2021 ein Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten (Sicherheitskatalog Version 2.0) erlassen. Im Zuge der TKG-Novelle 2021 wurden die Bestimmungen zur öffentlichen Sicherheit gemäß §§ 165 ff. TKG teilweise neu gefasst, so dass eine Anpassung an die gesetzlichen Vorgaben erforderlich war. Dazu hat die Bundesnetzagentur, im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der/dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, nach § 167 Abs. 1 TKG den Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen und für die Verarbeitung personenbezogener Daten als Grundlage für das Sicherheitskonzept erstellt. Der Katalog von Sicherheitsanforderungen wird im Folgenden als „Sicherheitskatalog“ bezeichnet.

II.

1. Ermächtigungsgrundlage und formelle Rechtmäßigkeit (Ziffern 1) bis 3) des Tenors)

ENTWURF

Die Ermächtigungsgrundlage für den Erlass des Sicherheitskatalogs ist § 167 Abs. 1 TKG. Wer Telekommunikationsdienste erbringt oder daran mitwirkt, hat nach § 165 Abs. 1 S. 1 TKG angemessene technische Vorkehrungen und sonstige Maßnahmen zu treffen. Die Einzelheiten der nach § 167 Abs. 1 S. 1 Nr. 1 TKG i.V.m. § 165 Abs. 1 bis 7 TKG zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen legt die Bundesnetzagentur (BNetzA) im Einvernehmen mit dem BSI und der bzw. dem BfDI durch Allgemeinverfügung in einem Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten fest. Im Einzelnen:

- § 167 Absatz 1 Satz 1 Nummer 1 TKG: Einzelheiten der nach § 165 Absatz 1 bis 7 TKG zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen unter Beachtung der verschiedenen Gefährdungspotenziale der öffentlichen Telekommunikationsnetze und öffentlich zugänglichen Telekommunikationsdienste,
- § 167 Absatz 1 Satz 1 Nummer 2 TKG: welche Funktionen kritische Funktionen im Sinne von § 2 Absatz 13 Satz 1 Nummer 3 Buchstabe b des BSIG sind, die von kritischen Komponenten im Sinne von § 2 Absatz 13 des BSIG realisiert werden, und
- § 167 Absatz 1 Satz 1 Nummer 3 TKG: wer als Betreiber öffentlicher Telekommunikationsnetze und als Anbieter öffentlich zugänglicher Telekommunikationsdienste mit erhöhtem Gefährdungspotenzial einzustufen ist.
- § 167 Absatz 1 Satz 2 TKG: Der Sicherheitskatalog kann auch Anforderungen zur Offenlegung und Interoperabilität von Schnittstellen von Netzkomponenten einschließlich einzuhaltender technischer Standards enthalten.

Dieser Sicherheitskatalog ist gemäß § 167 Abs. 1 S. 1 TKG ein Verwaltungsakt in Form einer Allgemeinverfügung nach § 35 S. 2 VwVfG.

Die Bundesnetzagentur hat den Entwurf des Sicherheitskatalogs am 19.11.2025 im Amtsblatt der Bundesnetzagentur (22/2025) sowie auf der Website der Bundesnetzagentur (https://www.bundesnetzagentur.de/sicherheitsanforderungen) veröffentlicht. Die Marktteilnehmer hatten die Möglichkeit, innerhalb eines Monats zu dem Entwurf Stellung zu nehmen. Damit hat die Bundesnetzagentur den Herstellern, den Verbänden der Betreiber öffentlicher Telekommunikationsnetze und den Verbänden der Anbieter öffentlich zugänglicher Telekommunikationsdienste nach § 167 Abs. 1 S. 3 TKG Gelegenheit zur Stellungnahme gegeben.

Die Ermächtigungsgrundlage für den Widerruf des Sicherheitskataloges Version 2.0 (Ziffer 2) des Tenors) ergibt sich aus § 49 Abs. 1 VwVfG (Widerruf eines rechtmäßigen Verwaltungsaktes).

2. Materielle Rechtmäßigkeit (Ziffer 1) des Tenors)

Der Sicherheitskatalog enthält die wesentlichen tatsächlichen und rechtlichen Entscheidungsgründe gemäß § 39 Abs. 1 S. 2 VwVfG. Die ermessensleitenden Gesichtspunkte werden genannt (§ 39 Abs.1 S. 3 VwVfG).

Adressaten der Allgemeinverfügung sind nach § 165 Abs. 1 S. 1 Nr. 1 TKG alle, die Telekommunikationsdienste erbringen oder daran mitwirken. Daneben erfasst § 165 Abs. 2 Nr. 2 TKG Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste.

ENTWURF

§ 3 Nr. 61 TKG definiert Telekommunikationsdienste als in der Regel gegen Entgelt über Telekommunikationsnetze erbrachte Dienste, die - mit der Ausnahme von Diensten, die Inhalte über Telekommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben - folgende Dienste umfassen:

a) Internetzugangsdienste,

b) interpersonelle Telekommunikationsdienste und

c) Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste, die für Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden.

Diese neue Begriffsbestimmung, die eine Umsetzung von Art. 2 Nr. 4 EKEK ist[1], führt dazu, dass nun ein größerer Adressatenkreis als bisher erfasst wird. Insbesondere sind jetzt auch nummernunabhängige interpersonelle Telekommunikationsdienste dazu verpflichtet, technische Vorkehrungen und sonstige

[1] BT-Drs. 19/26108, S. 236.

Maßnahmen zum Schutz des Fernmeldegeheimnisses und gegen die Verletzung des Schutzes personenbezogener Daten zu treffen. Hintergrund ist die wachsende Bedeutung dieser Dienste.[2]

Die neuen Adressaten, die nummernunabhängige interpersonelle Kommunikationsdienste erbringen, üben üblicherweise keine tatsächliche Kontrolle über die Signalübertragung über Netze aus. Daher stuft der europäische Gesetzgeber das Risiko für solche Dienste als „in gewisser Hinsicht [...] geringer" ein als für herkömmliche elektronische Kommunikationsdienste[3]:

Wenn dies auf der Grundlage der tatsächlichen Bewertung der bestehenden Sicherheitsrisiken gerechtfertigt ist, sollten die Maßnahmen von Anbietern nummernunabhängiger interpersoneller Kommunikationsdienste daher weniger strikt sein. Derselbe Ansatz sollte sinngemäß auch für interpersonelle Kommunikationsdienste gelten, die Nummern nutzen und die keine tatsächliche Kontrolle über die Signalübertragung ausüben.[4]

Darüber hinaus werden von den Vorgaben des Katalogs zum Schutz des Fernmeldegeheimnisses und personenbezogener Daten (§ 165 Abs. 1 TKG) die an der Diensteerbringung Mitwirkenden erfasst, d.h. beispielsweise Mitarbeiter und Erfüllungsgehilfen. Zudem sind z.B. Wiederverkäufer, die für ihre Kundenverwaltung und ihr Rechnungswesen Daten erheben und verwenden, erfasst. Dies geschieht vor dem Hintergrund, dass diese Anbieter ebenfalls personenbezogene Daten erheben und ggf. Informationen erlangen, die dem Fernmeldegeheimnis unterliegen (Rechnungslegung, Geschäftszahlen).[5] Die Vorschrift erfasst demgegenüber nicht Hersteller von Netzkomponenten oder von Endgeräten.[6]

ENTWURF

Dieser große Adressatenkreis wird im Sicherheitskatalog in folgende drei Kategorien eingeteilt, die abhängig vom jeweiligen Gefährdungspotenzial sind. Der Sicherheitskatalog sieht folgende Kategorien vor:

- Normales Gefährdungspotenzial
- Gehobenes Gefährdungspotenzial
- Erhöhtes Gefährdungspotenzial

Abhängig davon, wie die Adressaten eingestuft werden, treffen sie die Verpflichtungen in unterschiedlichem Ausmaß.

Die Adressierung findet demnach zweimal statt; einmal bei der generellen Einstufung in den Kreis aller Verpflichteten und ein zweites Mal bei der Einordnung in die jeweilige Kategorie.

2.1 Umfang der Regelungswirkung (§ 35 S. 1 VwVfG) sowie Bestimmtheit (§ 37 Abs. 1 VwVfG)

Der Gesetzgeber sieht vor, dass der Sicherheitskatalog als Allgemeinverfügung erlassen wird, § 167 Absatz 1 Satz 1 TKG. Der Sicherheitskatalog bildet die Grundlage für technische und organisatorische

---

[2] EKEK, Erwägungsgrund 95.

[3] EKEK, Erwägungsgrund 95.

[4] EKEK, Erwägungsgrund 95. Zwar sind Erwägungsgründe selbst nicht verbindlich, können aber im Rahmen der teleologischen Auslegung herangezogen werden.

[5] Säcker/Körber/Mozek, 4. Aufl. 2023, TKG § 165.

[6] BT-Drs. 19/26108, S. 360.

Schutzmaßnahmen, die die Erbringer und ihre Mitwirkenden von Telekommunikationsdiensten treffen müssen. Sowohl die Bandbreite an möglichen Verpflichteten als auch an denkbaren technischen Maßnahmen ist sehr groß. Der Sicherheitskatalog regelt folgende Bereiche:

1) Den Gesamtkreis der Adressaten

2) Die Einordnung der Adressaten durch Konkretisierung der Gefährdungspotenziale der öffentlichen Telekommunikationsnetze und öffentlich zugänglichen Telekommunikationsdienste wie folgt:

   a) Normales Gefährdungspotenzial

   b) Gehobenes Gefährdungspotenzial

   c) Erhöhtes Gefährdungspotenzial

3) Festlegung von Schutzmaßnahmen, die bei der Erstellung des Sicherheitskonzepts zwingend umzusetzen sind

4) Festlegung von Schutzmaßnahmen, die bei der Erstellung des Sicherheitskonzepts zu berücksichtigen (aber nicht zwingend umzusetzen) sind

Bei der Festlegung von Schutzmaßnahmen kann der Sicherheitskatalog auch lediglich Sicherheitsziele vorgeben, wie sich aus § 166 Absatz 1 Nummer 3 Buchstabe c 2. Halbsatz TKG ergibt.

ENTWURF

Die Nichteinhaltung des Sicherheitskatalogs kann nach § 183 Absatz 1, 5 TKG mit Zwangsgeld belegt werden; im Extremfall ist eine Untersagungsverfügung möglich, § 183 Absatz 4 TKG. Wenn die Adressaten es unterlassen, ihr Sicherheitskonzept, das auf dem Sicherheitskatalog basiert, vollständig und rechtzeitig vorzulegen (§ 166 Absatz 2 S. 1, Absatz 4 Satz 2 TKG), so ist neben § 183 TKG auch § 228 Absatz 2 Nummer 38 TKG einschlägig. Es handelt sich hierbei um eine Ordnungswidrigkeit, die mit einer Geldbuße von bis zu 300.000 Euro belegt werden kann.

Der Katalog kann somit gemäß § 166 Absatz 1 Nummer 3 Buchstabe c 2. HS TKG einerseits lediglich Ziele definieren; andererseits kann seine Nichtdurchsetzung jedoch Zwangsgelder bzw. Geldbußen zur Folge haben, so dass für den Adressaten die Bestimmtheit klar geregelt sein muss. Der Katalog muss deutlich regeln, ob eine Maßnahme unmittelbar verbindlich ist oder „nur“ im Rahmen der Erstellung des Sicherheitskonzepts berücksichtigt werden muss. Im letzteren Fall muss eine Nichtumsetzung von den Adressaten entsprechend dokumentiert werden.

Für die inhaltliche **Bestimmtheit** genügt es, dass aus dem gesamten Inhalt des Verwaltungsakts und aus dem Zusammenhang, vor allem aus der von der Behörde gegebenen Begründung und aus den Beteiligten bekannten näheren Umständen des Erlasses, im Wege einer an den Grundsätzen von Treu und Glauben

orientierten Auslegung hinreichende Klarheit gewonnen werden kann.[7] Hierbei ist entsprechend § 133 BGB auf den erklärten Willen aus der Sicht eines verständigen Empfängers abzustellen.[8]

Aus dem Sicherheitskatalog geht für die Adressaten klar hervor, unter welche Stufe der Gefährdungspotenziale sie fallen. Es ist weiterhin klar definiert, welche Maßnahmen sie umzusetzen und welche sie nur zu berücksichtigen haben.

2.2 Unbestimmte Rechtsbegriffe

Auf Tatbestandsseite sehen die einzelnen Normen des § 165 TKG unbestimmte Rechtsbegriffe vor (z. B. „angemessene technische und organisatorische Vorkehrungen", „sonstige Maßnahmen", „erhebliche Beeinträchtigungen", „Stand der Technik"), die von der Bundesnetzagentur durch den Sicherheitskatalog näher konkretisiert werden müssen. Hierbei kommt ihr ein **Beurteilungsspielraum** zu.

Zwar sieht das Verwaltungsrecht einen solchen Spielraum für Behörden grundsätzlich nicht vor; vielmehr ist eine volle gerichtliche Überprüfbarkeit von Behördenentscheidungen notwendig, um die Rechtsschutzgarantie des Bürgers aus Art. 19 Abs. 4 GG nicht zu unterlaufen. Für einige Fallgruppen sind jedoch Ausnahmen vorgesehen:

Bei Entscheidungen wertender Art durch weisungsfreie, mit Sachverständigen besetzten Ausschüssen liegt die Beurteilungsprärogative bei der Verwaltung. Gleiches gilt für Prognoseentscheidungen und Risikobewertungen. Dass die Bundesnetzagentur zusammen mit den Sachverständigen für Informationstechnik und Datenschutz die unbestimmten Rechtsbegriffe aus §§ 165 ff. TKG auslegt, ist im Gesetz angelegt. So sieht § 167 Abs. 1 S. 1 Nr. 1 TKG vor, dass die Bundesnetzagentur in dem Sicherheitskatalog „Einzelheiten der nach § 167 Abs. 1 bis 7 TKG zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen unter Beachtung der verschiedenen Gefährdungspotenziale" festlegt.

ENTWURF

Eine Besonderheit gilt für den Begriff „**Stand der Technik**". Der Begriff wird in § 165 Abs. 1 S. 2, Abs. 2 S. 3 TKG erwähnt. Das Handbuch der Rechtsförmlichkeit des Bundesministeriums für Justiz enthält Einzelheiten zur Auslegung des Begriffs.[9]

So soll der Gesetzgeber im Allgemeinen nur folgende Generalklauseln für technische Regeln verwenden:

- allgemein anerkannte Regeln der Technik,
- Stand der Technik und
- Stand von Wissenschaft und Technik.

Welche der drei Grundformen zu wählen ist, richtet sich nach dem **Gefährdungspotenzial** der Materie, die geregelt werden soll, und nach der technischen Beherrschbarkeit dieses Gefährdungspotenzials.[10]

---

[7] VGH Mannheim Urt. v. 6.11.2013 – 1 S 1640/12, BeckRS 2013, 58560, beck-online mwN.

[8] VGH Mannheim Urt. v. 6.11.2013 – 1 S 1640/12, BeckRS 2013, 58560, beck-online mwN.

[9] Handbuch der Rechtsförmlichkeit des Bundesministeriums der Justiz, Rn. 252 ff.

[10] Handbuch der Rechtsförmlichkeit des Bundesministeriums der Justiz, Rn. 252.

Das Handbuch führt weiter aus:

*Die Generalklausel „**allgemein anerkannte Regeln der Technik**“ wird für Fälle mit vergleichsweise* **geringem** *Gefährdungspotenzial oder für Fälle verwendet, die auf Grund gesicherter Erfahrungen technisch beherrschbar sind. Allgemein anerkannte Regeln der Technik sind schriftlich fixierte oder mündlich überlieferte technische Beispiel: Die Bezugsnorm ist mangels Gesetzgebungszuständigkeit nichtig; die Ausgangsnorm ist aber kompetenzgerecht erlassen worden. Der Mangel der Bezugsnorm ist für die Ausgangsnorm unerheblich. Festlegungen für Verfahren, Einrichtungen und Betriebsweisen, die nach herrschender Auffassung der beteiligten Kreise (Fachleute, Anwender, Verbraucherinnen und Verbraucher und öffentliche Hand) geeignet sind, das gesetzlich vorgegebene Ziel zu erreichen und die sich in der Praxis allgemein bewährt haben oder deren Bewährung nach herrschender Auffassung in überschaubarer Zeit bevorsteht.*[11]

*Das Anforderungsniveau bei der Generalklausel „**Stand der Technik**“ liegt* **zwischen** *dem Anforderungsniveau der Generalklausel „**allgemein anerkannte Regeln der Technik**“ und dem Anforderungsniveau der Generalklausel „**Stand von Wissenschaft und 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“.*[12]

ENTWURF

*Die Generalklausel „**Stand von Wissenschaft und Technik**“ umschreibt das* **höchste** *Anforderungsniveau und wird daher in Fällen mit sehr hohem Gefährdungspotenzial verwendet. Stand von Wissenschaft und Technik ist der Entwicklungsstand fortschrittlichster Verfahren, Einrichtungen und Betriebsweisen, die nach Auffassung führender Fachleute aus Wissenschaft und Technik auf der Grundlage neuester wissenschaftlich vertretbarer Erkenntnisse im Hinblick auf das gesetzlich vorgegebene Ziel für erforderlich gehalten werden und das Erreichen dieses Ziels gesichert erscheinen lassen“.*[13]

2.3 Ermessensausübung

2.3.1 Entschließungsermessen

§ 167 Abs. 1 TKG sieht vor, dass die Bundesnetzagentur im Einvernehmen mit dem BSI und der/dem BfDI einen Katalog von Sicherheitsanforderungen in Form einer Allgemeinverfügung erlässt. Insoweit sieht der Gesetzgeber kein Entschließungsermessen vor. In Bezug auf den Inhalt besteht jedoch an zwei Stellen ein Entschließungsermessen:

1. § 165 Abs. 3 S. 5 TKG sieht vor, dass die Bundesnetzagentur Einzelheiten für Systeme zur Angriffserkennung im Sicherheitskatalog festlegen kann;

[11] Handbuch der Rechtsförmlichkeit des Bundesministeriums der Justiz, Rn. 255.

[12] Handbuch der Rechtsförmlichkeit des Bundesministeriums der Justiz, Rn. 256.

[13] Handbuch der Rechtsförmlichkeit des Bundesministeriums der Justiz, Rn. 257.

2. § 167 Abs. 1 S. 2 TKG: Der Katalog von Sicherheitsanforderungen kann Anforderungen zur Offenlegung und Interoperabilität von Schnittstellen von Netzkomponenten einschließlich einzuhaltender technischer Standards enthalten.

Der Sicherheitskatalog enthält in Punkt 4.9.1 Ausführungen zu Angriffserkennungen; er erwähnt zudem an verschiedenen Stellen den Punkt der Interoperabilität, ohne beim derzeitigen Stand hierzu weitergehende Anforderungen zu stellen.

2.3.2 Auswahlermessen

Der Bundesnetzagentur kommt darüber hinaus ein Auswahlermessen zu.

Wie bereits festgestellt, ist der Inhalt des Sicherheitskatalogs sehr umfangreich, da er eine erhebliche Spannbreite an Adressaten und möglichen Sachverhalten abdecken muss. Hinzu kommt die ständige Weiterentwicklung der Technik. Wie oben bereits erläutert sieht der Sicherheitskatalog vor, dass die Bundesnetzagentur die unbestimmten Rechtsbegriffe aus § 165 TKG weiter konkretisiert. Bei der Festlegung der „Einzelheiten der nach § 165 Absatz 1 bis 7 TKG zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen unter Beachtung der verschiedenen Gefährdungspotenziale“ steht der Bundesnetzagentur auf der Rechtsfolgenseite ein Ermessen zu.

In dem Sicherheitskatalog werden die angemessenen technischen Vorkehrungen und sonstigen Maßnahmen konkretisiert, die die Adressaten treffen müssen. Hierbei handelt es sich in hohem Maße um gestalterisches Tätigwerden, bei dem die Behörden die Sicherheitsbelange der Bevölkerung und das Funktionieren des Staates gegen die Berufsfreiheit der Adressaten abwägen müssen. Die Bundesnetzagentur wählt hierzu aus einer Vielzahl an möglichen technischen Optionen diejenigen aus, die die Regulierungsziele aus § 2 Abs. 2 TKG am besten miteinander in Einklang bringen. Dies geschieht vor dem Hintergrund einer dynamischen Gefährdungslage, die sich sowohl politisch als auch technisch sehr schnell entwickelt. Für diese prognostische Entscheidung gibt es zudem keine fest verbindlichen technischen Standards.

ENTWURF

Das Ermessen erlaubt einen Auswahl- und Ausgestaltungsspielraum, bei dessen Ausübung sich die Bundesnetzagentur an den **Regulierungszielen** aus § 2 Abs. 2 TKG orientiert. Im vorliegenden Fall fördert die Bundesnetzagentur die Interessen der Nutzer, indem sie die Interessen der öffentlichen Sicherheit wahrt und die Sicherheit der Netze und Dienste gewährleistet (§ 2 Abs. 2 Nr. 3 TKG). Diese Vorgaben werden in den Begriffsbestimmungen in § 3 Nr. 52 TKG weiter ausdifferenziert. Diese Norm definiert die „Sicherheit von Netzen und Diensten“ als die Fähigkeit von Telekommunikationsnetzen und -diensten, auf einem bestimmten Vertrauensniveau alle Angriffe abzuwehren, die folgende Punkte beeinträchtigen:

- die Verfügbarkeit;
- die Authentizität;
- die Integrität
- oder die Vertraulichkeit

dieser Netze und Dienste, der gespeicherten, übermittelten oder verarbeiteten Daten oder der damit zusammenhängenden Dienste, die über diese Telekommunikationsnetze oder -dienste angeboten werden oder zugänglich sind.

2.3.3 Kein Ermessensfehlgebrauch: Allgemeine Verhältnismäßigkeitsüberlegungen hinsichtlich aller im Katalog genannten Maßnahmen

Da ein Auswahlermessen vorliegt, ist die Bundesnetzagentur nach § 40 VwVfG verpflichtet, ihr Ermessen entsprechend dem Zweck der Ermächtigung auszuüben und die gesetzlichen Grenzen des Ermessens einzuhalten. Sie wahrt beim Erlass des vorliegenden Verwaltungsaktes insbesondere die Verhältnismäßigkeit im Rahmen der Grundrechtseingriffe. Zweck der Ermächtigungsgrundlage sind insbesondere der Schutz des Fernmeldegeheimnisses und der Schutz personenbezogener Daten (§ 165 Abs. 1 S. 1 TKG).

(1) Belastender Verwaltungsakt: Eingriff in den Schutzbereich von Art. 12 Abs. 1 GG

Die Verpflichtungen aus dem Sicherheitskatalog können insbesondere in die Berufsfreiheit aus Art. 12 Abs. 1 GG eingreifen. So ziehen die Maßnahmen Kosten nach sich, die an anderer Stelle für Investitionen fehlen; je nachdem, wie umfangreich und kostenintensiv die Maßnahmen sind, kann sich eine Markteintrittsschranke für Neueinsteiger bilden. Kleinere Unternehmen könnten gezwungen sein, den Markt zu verlassen. Darüber hinaus müssen auch die Mitarbeiter geschult sein. Je nach Angebot der Zertifizierer können notwendige Zertifizierungen ggf. nicht sofort eingeholt werden, auch wenn alle Voraussetzungen vorliegen; darüber hinaus müssen Mitarbeiter für die Sicherheitsvorkehrungen eingesetzt bzw. neu eingestellt werden.

Nach Art. 12 Abs. 1 S. 1 GG haben alle Deutschen das Recht, Beruf, Arbeitsplatz und Ausbildungsstätte frei zu wählen. Die Berufsausübung kann gemäß Art. 12 Abs. 1 S. 2 GG durch Gesetz oder aufgrund eines Gesetzes geregelt werden.

ENTWURF

Nach Art. 19 Abs. 3 GG gilt die Berufsfreiheit auch für inländische juristische Personen, soweit sie ihrem Wesen nach auf diese anwendbar ist. Für das Inlandskriterium ist die Sitztheorie entscheidend, d.h. ob sich der effektive (tatsächliche) Sitz in Deutschland (bzw. nach europarechtskonformer Auslegung in der EU)[14] befindet.[15] International tätige juristische Personen haben nur dann ihren Hauptverwaltungssitz im Inland, wenn auch die Mehrheit der Entscheidungen über die Geschäftsführung im Inland fällt.[16] Unternehmen, die ihren Sitz im Sinne eines Aktionszentrums nicht in Deutschland haben, können lediglich subsidiären Schutz aus Art. 2 Abs. 1 GG geltend machen. Wenn ein solches Unternehmen aus einem Drittstaat aber ein zumindest teilrechtsfähiges Tochterunternehmen gründet, das sein Aktionszentrum in Deutschland hat, ist dieser Unternehmensteil jedoch inländisch und nach Art. 12 Abs. 1 GG geschützt.[17] Der Sitz ist für jede juristische Person gesondert festzustellen.[18]

Die **Eingriffsintensität** wurde vom Bundesverfassungsgericht mithilfe der **3-Stufen-Theorie** konkretisiert. [19]

---

[14] Dürig/Herzog/Scholz/Remmert, 103. EL Januar 2024, GG Art. 12 Abs. 1 Rn. 69.

[15] Dreier/Dreier, 3. Aufl. 2013, GG Art. 19 III Rn. 79.

[16] BeckOK GG/Enders, Beck'scher Online-Kommentar GG, 36. Ed. 15.2.2018, Art. 19 Rn. 36; Dreier/Dreier, 3. Aufl. 2013, GG Art. 19 III Rn. 79.

[17] Dürig/Herzog/Scholz/Remmert, 103. EL Januar 2024, GG Art. 12 Abs. 1 Rn. 66.

[18] Ludwigs/Friedman, Die Grundrechtsberechtigung juristischer Personen nach Art. 19 III GG, JA 2018, 807 (807 ff.).

[19] Apotheken-Urteil, BVerfGE 7, 377, Rn. 62 ff., Rn. 72 ff.

Die **1. Stufe** (Berufsausübungsregelungen) betreffen das „**Wie**“ der Berufsausübung und sind gerechtfertigt. Sie betreffen nicht die Frage, wer ihn unter welchen Voraussetzungen ausüben darf; daher sind diese Regelungen bereits gerechtfertigt, wenn sie in zweckmäßiger Weise vernünftige Interessen des Gemeinwohls schützen.

Subjektive Berufswahlregelungen (**2. Stufe**) betreffen das „**Ob**“ der Berufsausübung, wobei Zugangsvoraussetzungen gewisser Berufe an subjektive Kriterien geknüpft werden. Der Zugang zum Beruf hängt damit von bestimmten, in der Person selbst liegenden und damit beeinflussbaren Faktoren ab; dies umfasst beispielsweise Qualifikationsnachweise oder die persönliche Zuverlässigkeit.

Solche Regelungen sind zulässig, wenn sie zum Schutz eines wichtigen, besonders wichtigen oder überragend wichtigen Gemeinschaftsguts erforderlich sind.

Objektive Berufswahlregelungen (**3. Stufe**) knüpfen den Berufszugang an **außerhalb der Person liegende Kriterien**. Dies umfasst beispielsweise Bedarfsregelungen oder den Schutz vor Konkurrenz. Diese Maßnahmen sind gerechtfertigt, wenn sie der „Abwehr nachweisbarer oder höchstwahrscheinlicher schwerer Gefahren für ein überragend wichtiges Gemeinschaftsgut“ dienen.

Der Sicherheitskatalog regelt das „Wie“ und das „Ob“ der Berufsausübung und greift somit auf der **1. und 2. Stufe** in die Berufsfreiheit ein. Damit der Eingriff verhältnismäßig ist, müssen die Regelungen mindestens zum Schutz eines wichtigen Gemeinschaftsguts erforderlich sein.

ENTWURF

(2) Verhältnismäßigkeit des Eingriffs

Legitimer Zweck

Rechtsgrundlage für den Sicherheitskatalog ist § 167 Abs. 1 i.V.m. § 165 TKG. Ein zentraler Zweck des Katalogs ist nach § 165 Abs. 1 Nr. 1 und 2 TKG der Schutz des Fernmeldegeheimnisses. Es handelt sich insofern um eine einfachgesetzliche Ausgestaltung der staatlichen Schutzpflichten aus **Art. 10 GG** (Fernmeldegeheimnis) sowie **Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG** (allgemeines Persönlichkeitsrecht).

In Bezug auf die Regulierungsziele fördert der Sicherheitskatalog die Nutzerinteressen, indem die Bundesnetzagentur die Interessen der öffentlichen Sicherheit wahrt und die Sicherheit der Netze und Dienste gewährleistet (§ 2 Abs. 2 Nr. 3 TKG).

Die Sicherheitsanforderungen schützen aber nicht nur den Einzelnen; da Telekommunikations- und Datenverarbeitungssysteme inzwischen in allen kritischen Bereichen des Staates eingesetzt werden, kann ein Ausfall dort die Sicherheit und das Funktionieren des Staates und seiner Einrichtungen beeinträchtigen. Dies betrifft im Kern die verfassungsrechtlichen Strukturprinzipien aus **Art. 20 Abs. 1 bis 3 GG**. Dieses Ziel findet sich einfachgesetzlich in § 165 Abs. 2 TKG (Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und -diensten führen) sowie in § 165 Abs. 5 TKG (Sicherstellung des ordnungsgemäßen Betriebs der Netze).

Darüber hinaus kann ein Ausfall der von den Sicherheitsvorgaben zu schützenden Telekommunikations- und Datenverarbeitungssysteme dazu führen, dass gewerbliche Kunden des Unternehmens in ihren Eigentums- und Berufsausübungsrechten betroffen werden (**Art. 12 Abs. 1, Art. 14 Abs. 1 GG**). Auch das betreffende Unternehmen wird von den Sicherheitsmaßnahmen geschützt; neben dem Eigenschutz auch dadurch, dass die gesamte Branche ein einheitliches Schutzniveau einhält und der Zukauf von Dienstleistungen ebenfalls

dem Sicherheitsstandard unterliegt. Aufgrund der Interdependenzen sind Anbieter, von dem Sicherheitskatalog betroffen sind, regelmäßig selbst Nutzer von solchen Diensten bei anderen Anbietern. Schon vor diesem Hintergrund ist ein einheitliches Schutzniveau notwendig; andernfalls könnte ein schwaches Sicherheitskonzept von einem Anbieter auf den nächsten „übergreifen“ und diese in ihrer Berufsausübungsfreiheit beeinträchtigen.

Maßnahmen wie redundante Hardware und Backups schützen zudem nicht nur vor Angriffen, sondern auch vor sonstigen Ausfällen.

Geeignetheit

Die Maßnahmen des Sicherheitskataloges müssen konkret geeignet sein, die oben angeführten Sicherheitsziele zu erreichen, d.h. sie müssen zur Zielerreichung zumindest förderlich sein. Die Maßnahmen sind der Erreichung des Zieles der Sicherheit von Netzen und Diensten zumindest förderlich und damit geeignet.

Erforderlichkeit

Es liegen auch keine milderen Mittel vor, die gleichermaßen geeignet wären, um das Ziel zu erreichen.

Der Sicherheitskatalog betrifft eine große Bandbreite an Adressaten und möglichen Sachverhalten. Es sind sowohl sehr große Unternehmen betroffen, die stark sicherheitskritische Infrastruktur betreiben, als auch kleinere Unternehmen, die weniger finanzielle Mittel haben, aber auch nicht in gleichem Ausmaß gefährdet sind.

ENTWURF

Dieser Bandbreite trägt der Sicherheitskatalog Rechnung, indem er die Adressaten abhängig von ihrem Gefährdungspotenzial in unterschiedliche Kategorien einteilt. Dies ist im Gesetz bereits angelegt (§ 167 Abs. 1 S. 1 Nr. 1 TKG: „unter Beachtung der verschiedenen Gefährdungspotenziale“).

Angemessenheit (Verhältnismäßigkeit i.e.S.)

Die Maßnahme ist zudem angemessen, da der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht. Die Angemessenheit der Maßnahmen aus dem Sicherheitskatalog richtet sich nach verschiedenen Kriterien. Auf europarechtlicher Ebene kann hier zunächst Art. 21 Abs. 1 UA 2 NIS-2-RL herangezogen werden. Dieser lautet:

Die in Unterabsatz 1 genannten Maßnahmen müssen unter Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen europäischen und internationalen Normen sowie der **Kosten der Umsetzung** *ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist.* **Bei der Bewertung der Verhältnismäßigkeit dieser Maßnahmen sind das Ausmaß der Risikoexposition der Einrichtung, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen**.

Nach § 165 Abs. 6 S. 1 TKG sind technische Vorkehrungen und sonstige Schutzmaßnahmen angemessen, wenn der dafür erforderliche technische und wirtschaftliche Aufwand nicht außer Verhältnis zur Bedeutung der zu schützenden Telekommunikationsnetze oder -dienste steht.

Allgemein lässt sich demnach festhalten, dass **skalierbare Systeme**, die auf den einzelnen Netzbetreiber angepasst werden können und seine Größe und Systemrelevanz berücksichtigen, für angemessene Maßnahmen sprechen.[20]

Der Sicherheitskatalog skaliert sowohl im Hinblick auf die Adressaten als auch im Hinblick auf die zu treffenden Maßnahmen. So werden zum einen die Adressaten nach Gefährdungspotenzial unterteilt, um zu verhindern, dass nicht risikorelevante Geschäftstätigkeiten unverhältnismäßig belastet werden. Zum anderen enthält der Sicherheitskatalog neben den zwingenden Maßnahmen auch Maßnahmen, die bei der Erstellung des Schutzkonzepts berücksichtigt werden müssen; von diesen Maßnahmen kann der Adressat gegebenenfalls auch abweichen.

Adressatenkreis

Der Adressatenkreis ist durch den Gesetzgeber bereits vorgegeben. Die Einteilung der Adressaten anhand der Gefährdungspotenziale ist ebenfalls bereits im Gesetz angelegt (§ 167 Abs. 1 S. 1 Nr. 1 TKG: „unter Beachtung der verschiedenen Gefährdungspotenziale“ sowie § 165 Abs. 3 S. 2 TKG: „Betreiber [...] mit erhöhtem Gefährdungspotenzial“).

ENTWURF

Die Bundesnetzagentur hat im Sicherheitskatalog Kleinstunternehmen gesondert unter „normalem“ Gefährdungspotenzial gefasst, um die Verpflichtungen möglichst angemessen zur Gefährdung zu gestalten. Doch auch wenn die Adressaten unter ein höheres Gefährdungspotenzial fallen, bedeutet dies nicht, dass Sicherheitsbelange im Rahmen der Abwägung automatisch einen Vorrang gegenüber den anderen Abwägungsbelangen haben.

Verpflichtungen für Adressaten der jeweiligen Kategorien

Hinweis: Hier werden noch die Ergebnisse der Konsultation ergänzt und bei der Verhältnismäßigkeitsprüfung berücksichtigt.

Bei der Ausübung ihres Ermessens wägt die Bundesnetzagentur die Schutzgüter gegeneinander ab, die in den Regulierungszielen in § 2 Abs. 2 TKG genannt sind. Der Sicherheitskatalog dient dazu, die Interessen der öffentlichen Sicherheit zu wahren und die Sicherheit der Netze und Dienste zu gewährleisten (§ 2 Abs. 2 Nr. 3 Buchstabe c TKG). Dabei ist zu beachten, dass absolute Sicherheit nicht erreicht werden kann; es sind grundsätzlich immer noch weitere Sicherheitsmaßnahmen möglich.[21] Die Bundesnetzagentur hat jedoch auch den Auftrag, einen **chancengleichen Wettbewerb** sicherzustellen (§ 2 Abs. 2 Nr. 2 TKG). Vor diesem Hintergrund dürfen die Sicherheitsanforderungen nicht dazu führen, dass eine Markteintrittsschranke entsteht oder das etablierte Wettbewerber den Markt verlassen müssen. Bei der Abwägung von Rentabilität

[20] OLG Düsseldorf Beschl. v. 19.7.2017 – 3 Kart 109/16, BeckRS 2017, 132865 Rn. 58, beck-online zur Angemessenheit des IT-Sicherheitskataloges gemäß § 11 Abs. 1a EnWG.

[21] Geppert/Schütz/Eckhardt, 5. Aufl. 2023, TKG § 165 Rn. 55.

bzw. Wirtschaftlichkeit gegen Sicherheitserwägungen ist es sinnvoll, auf ein Sicherheitsniveau abzuzielen, das die Funktionsfähigkeit der Infrastruktur gegen üblicherweise zu erwartende Gefährdungen garantiert.

Zu beachten ist hierbei auch, dass die Sicherheitsmaßnahmen auch den Adressaten selbst zugutekommen. Die Maßnahmen schützen deren sichere Berufsausübung, nicht nur im Hinblick auf den Schutz vor Angriffen, sondern auch im Falle von sonstigen Datenverlusten.

Um den Mehraufwand für die Marktteilnehmer in Grenzen zu halten, orientiert sich der Sicherheitskatalog an Industriestandards (vgl. Abschnitt 6.2 des Sicherheitskataloges).

Dies entspricht auch den Vorgaben von Art. 21 Abs. 5 UA 3 NIS-2-RL, der sich an die Europäische Kommission richtet:

Bei der Ausarbeitung der in den Unterabsätzen 1 und 2 des vorliegenden Absatzes genannten Durchführungsrechtsakte orientiert sich die Kommission so weit wie möglich **an europäischen und internationalen Normen sowie einschlägigen technischen Spezifikationen**. *[...]*

Eine möglichst einheitliche Übernahme der europäischen und internationalen Normen sowie einschlägigen technischen Spezifikationen erleichtert die Umsetzung und dient dem Funktionieren des Europäischen Binnenmarktes. Da der Sicherheitskatalog nun in europäisches Recht eingebettet ist, besteht auch kein wettbewerbsrechtlicher Nachteil für Marktteilnehmer in Deutschland gegenüber europäischen Wettbewerbern.

ENTWURF

Die Angemessenheit der einzelnen Maßnahmen ist anhand einer Analyse des Schutzbedarfs zu ermitteln.[22] Hier sind insbesondere folgende Faktoren denkbar:[23]

- Das Interesse Dritter an der Kenntnisnahme;
- mögliches Fehlverhalten oder Missbrauch durch eigene Mitarbeiter;
- die Höhe der jeweils zu überwindenden Zugriffsbarrieren sowie
- die Kosten durch technische und organisatorische Schutzvorkehrungen.

Die Bundesnetzagentur hat bei dem Erlass des Sicherheitskatalogs auch darauf geachtet, dass für die Betreiber Rechtssicherheit herrscht. Im Rahmen der einzelnen Maßnahmen ist für die Adressaten deutlich, welche weitergehenden Prozesse erforderlich sind, um den Anforderungen zu genügen. Dies betrifft insbesondere die Sicherheitsüberprüfung von Dritten.

Schließlich muss auch die **dynamische Entwicklung von Technologien** berücksichtigt werden. Neu entwickelte Netz- und Systemkomponenten müssen umgehend geprüft und zertifiziert werden können. Hier wird darauf geachtet, dass die Zertifizierungsstellen den Einsatz neuer Komponenten nicht verzögern. Der Katalog sieht in Punkt 5.3 die Zertifizierung von kritischen Komponenten auf der Grundlage der TR-03163 des

[22] Geppert/Schütz/Eckhardt, 5. Aufl. 2023, TKG § 165 Rn. 55.

[23] Geppert/Schütz/Eckhardt, 5. Aufl. 2023, TKG § 165 Rn. 55.

BSI vor. Zudem gibt es Übergangsregelungen zur Zertifizierung von kritischen Komponenten und Bestandskomponenten dürfen bis zum Stichtag eingesetzt werden.

2.3.4 Widerruf des Sicherheitskataloges Version 2.0 (Ziffer 2) des Tenors)

Die Voraussetzungen für den Widerruf des Sicherheitskataloges Version 2.0 aus § 49 Abs. 1 Verwaltungsverfahrensgesetz liegen vor. Insbesondere handelt es sich bei dem neuen Sicherheitskatalog nicht um einen Verwaltungsakt gleichen Inhalts.

2.3.5 Gesonderte Rechtmäßigkeitserwägungen zu den Gefährdungspotenzialen (Ziffer 3) des Tenors)

In Kapitel 3 des Kataloges von Sicherheitsanforderungen werden die verschiedenen Gefährdungspotenziale der öffentlichen Telekommunikationsnetze und öffentlich zugänglichen Telekommunikationsdiensten näher bestimmt (§ 167 Abs. 1 Nr. 3 TKG), um in der Folge entsprechend des jeweiligen Gefährdungspotenzials angemessene Schutzmaßnahmen zu definieren. Abhängig davon, in welche Kategorie ein Unternehmen fällt, ist der Eingriff in die Grundrechte unterschiedlich tief. In diesem Kapitel werden also die Adressaten des Sicherheitskatalogs nochmals in drei verschiedene Gruppen eingeteilt. Die Einteilung bestimmt, welche Schutzmaßnahmen aus den Kapiteln 4 und 5 für die Adressaten gelten.

Die Einteilung als solches dient dazu, die Skalierbarkeit der Maßnahmen zu gewährleisten, damit der Grundrechtseingriff möglichst geringgehalten werden kann. Dies ist im Gesetz bereits angelegt (§ 167 Abs. 1 S. 1 Nr. 1 TKG: „unter Beachtung der verschiedenen Gefährdungspotenziale“). Art. 3 Abs. 1 NIS-2-Richtlinie definiert „wesentliche“ Einrichtungen, die dem „erhöhten“ Gefährdungspotenzial im Sicherheitskatalog entsprechen. Art. 3 Abs. 2 NIS-2-Richtlinie definiert „wichtige“ Einrichtungen, die dem „gehobenen“ Gefährdungspotenzial entsprechen. Für die weiteren Einrichtungen gilt das normale Gefährdungspotenzial. Der Begriff des „erhöhten“ Gefährdungspotenzials wird in § 165 Abs. 3 S. 2, Abs. 9 S. 2 TKG verwendet.

ENTWURF

Der Sicherheitskatalog sieht folgende Kategorien vor:

- Normales Gefährdungspotenzial
  - weniger als 10 Mitarbeiter und
  - maximal 2 Mio. Euro Jahresumsatz bzw. Jahresbilanzsumme
  - Folge: Einstufung als sonstige öffentliche Telekommunikationsnetze und öffentlich zugängliche Telekommunikationsdienste
- Gehobenes Gefährdungspotenzial
  - weniger als 50 Mitarbeiter und
  - maximal 10 Mio. Euro Jahresumsatz oder Jahresbilanzsumme
  - Folge: Einstufung als öffentliche Telekommunikationsnetze und öffentlich zugängliche Telekommunikationsdienste, die für das Gemeinwohl eine Bedeutung haben
- Erhöhtes Gefährdungspotenzial

- mindestens 50 Mitarbeiter oder
- jeweils über 10 Mio. Euro Jahresumsatz und Jahresbilanzsumme
- Folge: Einstufung als öffentliche Telekommunikationsnetze und öffentlich zugängliche Telekommunikationsdienste, die für das Gemeinwohl eine hohe Bedeutung haben
- Ein erhöhtes Gefährdungspotenzial ergibt sich ebenfalls durch den Betrieb eines Mobilfunknetzes der 5. Generation (5G-Netz).

Diese Indikatoren sind auch sachgemäß. Aus den Kriterien „Mitarbeiteranzahl“ und „wirtschaftliche Kennzahlen“ kann man Rückschlüsse auf die Quantität und Qualität (Wichtigkeit) der Kunden ziehen. Die Wichtigkeit für das Gemeinwohl ergibt sich somit entweder daraus, dass ein signifikanter Anteil der Bevölkerung den Dienst selbst nutzt und/oder dass ein Kunde den Dienst nutzt, der wiederum wichtig für das Gemeinwohl ist. Wenn ein Kunde für das Allgemeinwohl wichtig ist, ist sein Ausfall dementsprechend auch sicherheitskritisch für das Allgemeinwohl.

Auch die Art der Nutzung lässt sich aus den oben genannten Kriterien ableiten. Wenn ein Unternehmen entweder eine große Kundenanzahl hat oder die Kunden sicherheitskritisch sind, werden beispielsweise typischerweise die Dienstleistungen redundant vorgehalten, was sich in der Mitarbeiteranzahl und in der Preisgestaltung widerspiegelt.

ENTWURF

Darüber hinaus sind die Kriterien objektiv feststellbar und bieten daher Rechtssicherheit. Die Kriterien sind zudem bekannt und haben sich auch in anderen, ähnlichen Kontexten zur Abgrenzung bewährt. Sie wurden bereits in einer Empfehlung der Kommission im Jahr 2003 formuliert, in dem verschiedene Kleinstunternehmen sowie kleine und mittlere Unternehmen (KMU) voneinander abgegrenzt wurden.[24] Zwar findet sich die Abgrenzung nicht unmittelbar im TKG, in den angrenzenden Regelungen zur Informationssicherheit werden die Kriterien jedoch gleich mehrfach genannt.

Art. 3 der NIS2-Richtlinie[25] definiert wesentliche und wichtige Einrichtungen. Art. 3 Abs. 1 lit. a) der NIS2-Richtlinie verweist auf Anhang I der Richtlinie. Anhang I der Richtlinie enthält eine Liste verschiedener Unterbranchen mit starker Kritikalität. Damit diese jedoch als wesentliche Einrichtungen gelten, müssen sie nach Art. 3 Abs. 1 lit. a) NIS2-Richtlinie die Schwellenwerte der KMU-Empfehlung für mittlere Unternehmen überschreiten.

---

[24] Art, 2 der Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, Aktenzeichen K(2003) 1422), Amtsblatt Nr. L 124 vom 20/05/2003 S. 0036 – 0041; siehe auch Erwägungsgrund 4.

[25] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie).

Schließlich ist zu berücksichtigen, dass sowohl der Sicherheitskatalog als auch das auf ihm aufsetzende Sicherheitskonzept eine weitere Skalierbarkeit ermöglichen, um im Einzelfall eine unverhältnismäßige Belastung innerhalb der Kategorien zu vermeiden.

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

Rechtsbehelfsbelehrung:

ENTWURF

Gegen diese Allgemeinverfügung kann innerhalb eines Monats nach Bekanntgabe Widerspruch bei der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Tulpenfeld 4, 53113 Bonn oder bei einer sonstigen Dienststelle der Bundesnetzagentur erhoben werden.

Ein Widerspruch hat gemäß § 217 Abs. 1 TKG keine aufschiebende Wirkung.

B Katalog von Sicherheitsanforderungen §167 TKG

ENTWURF

1. Einleitung/Allgemeines

Gemäß § 167 Abs. 1 S. 1 TKG trifft der vorliegende Katalog von Sicherheitsanforderungen (Sicherheitskatalog) die folgenden Festlegungen:

1. Einzelheiten der nach § 165 Abs. 1 bis 7 TKG zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen unter Beachtung der verschiedenen Gefährdungspotenziale der öffentlichen Telekommunikationsnetze und öffentlich zugänglichen Telekommunikationsdienste,
2. welche Funktionen kritische Funktionen im Sinne von § 2 Abs. 13 S. 1 Nummer 3 Buchstabe b des BSI-Gesetzes (BSIG) sind, die von kritischen Komponenten im Sinne von § 2 Abs. 13 des BSIG realisiert werden, und
3. wer als Betreiber öffentlicher Telekommunikationsnetze und als Anbieter öffentlich zugänglicher Telekommunikationsdienste mit erhöhtem Gefährdungspotenzial einzustufen ist.

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

Die Einzelheiten der nach § 167 Abs. 1 S. 1 Nr. 1 TKG i.V.m. § 165 Abs. 1 bis 7 TKG zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen legt die Bundesnetzagentur (BNetzA) im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) durch Allgemeinverfügung in einem Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten fest.

ENTWURF

Zu diesem Zweck definiert § 165 TKG bestimmte Sicherheitsziele und Schutzpflichten. Zunächst verpflichtet § 165 Abs. 1 TKG die Anbieter von Telekommunikationsdiensten und diejenigen, die daran mitwirken, angemessene technische Vorkehrungen und sonstige Maßnahmen zum Schutz des Fernmeldegeheimnisses und gegen die Verletzung des Schutzes personenbezogener Daten zu treffen. Darüber hinaus haben Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste gemäß § 165 Abs. 2 TKG zum Schutz der betriebenen Telekommunikations- und Datenverarbeitungssystemen gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und -diensten führen, auch sofern diese Störungen durch äußere Angriffe und Einwirkungen von Katastrophen bedingt sein können, und zur Beherrschung der Risiken für die Sicherheit von Telekommunikationsnetzen und -diensten angemessene technische und organisatorische Vorkehrungen und sonstige Maßnahmen zu treffen.

In der Vorgehensweise zum Erreichen der Sicherheitsziele und der daraus abzuleitenden Schutzmaßnahmen orientiert sich dieser Katalog an der ENISA „Guideline on security measures under the EECC“ (Stand: 07/2021)[26].

Werden telekommunikationsrechtliche Pflichten aus §§ 165 und 166 TKG im Auftrag eines Verantwortlichen durch andere Personen oder Stellen erfüllt und hierbei Daten verarbeitet, so hat der Verpflichtete für die Einhaltung der telekommunikationsrechtlichen Vorschriften Sorge zu tragen. Unberührt hiervon bleibt die

[26] https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc

unmittelbare datenschutzrechtliche Verantwortlichkeit der beauftragten Person oder Stelle nach allgemeinem Datenschutzrecht.

Die Bundesnetzagentur (BNetzA) kann nach § 165 Abs. 9 TKG anordnen, dass sich die Betreiber öffentlicher Telekommunikationsnetze oder die Anbieter öffentlich zugänglicher Telekommunikationsdienste einer Überprüfung durch eine qualifizierte unabhängige Stelle oder einer zuständigen nationalen Behörde unterziehen. Durch eine solche Überprüfung wird festgestellt, ob die Vorkehrungen und Maßnahmen nach § 165 Abs. 1 bis 7 TKG erfüllt sind. Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial müssen sich alle zwei Jahre einer Überprüfung durch eine qualifizierte unabhängige Stelle oder eine zuständige nationale Behörde unterziehen, in der festgestellt wird, ob die Vorkehrungen und Maßnahmen nach den Absätzen 1 bis 7 erfüllt sind.

Zur besseren Beherrschbarkeit der Risiken für öffentliche Telekommunikationsnetze und öffentlich zugängliche Telekommunikationsdienste sieht § 166 TKG die Erstellung eines Sicherheitskonzeptes, die Bestimmung eines Sicherheitsbeauftragten und die Benennung eines in der Europäischen Union ansässigen Ansprechpartners vor.

Anmerkung:

Bei der Erfüllung seiner telekommunikationsrechtlichen Pflichten hat der Verpflichtete ergänzend die allgemeinen datenschutzrechtlichen Vorgaben des Bundesdatenschutzgesetzes (BDSG), des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes (TDDDG) und der Datenschutz-Grundverordnung (DSGVO) zu beachten.

ENTWURF

Hier ist zu berücksichtigen, dass aufgrund von Art. 95 DSGVO grundsätzlich § 165 TKG als Umsetzung der ePrivacy-Richtlinie Vorrang vor den vergleichbaren Regelungen der DSGVO (insb. Art. 32) hat, soweit sie dasselbe Ziel verfolgen. Weitergehende Informationen finden sich in Kapitel 4.1.

2. Adressaten

Der Katalog von Sicherheitsanforderungen konkretisiert die nach § 165 Abs. 1 bis 7 TKG zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen und richtet sich an alle relevanten Unternehmen im Geltungsbereich des TKG (§ 1 Abs. 2 TKG).

Adressaten des § 165 Abs. 1 (auch i.V.m. Abs. 6 und 7) TKG sind alle Anbieter von Telekommunikationsdiensten und daran Mitwirkende. Adressaten des § 165 Abs. 2 und 3 (auch i.V.m. Abs. 6 und 7) TKG sind Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste. Adressaten der § 165 Abs. 4 und 5 (auch i.V.m. Abs. 6 und 7) TKG sind Betreiber öffentlicher Telekommunikationsnetze.

Betreiber ist gemäß § 3 Nr. 7 TKG ein Unternehmen, das ein öffentliches Telekommunikationsnetz oder eine zugehörige Einrichtung bereitstellt oder zur Bereitstellung hiervon befugt ist.

Anbieter von Telekommunikationsdiensten ist gemäß § 3 Nr. 1 TKG jeder, der Telekommunikationsdienste erbringt.

Die Verpflichtungen aus § 165 Abs. 3 Satz 2 und 4 TKG richten sich nur an Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial. Die verschiedenen Gefährdungspotenziale werden im nachfolgenden Abschnitt 3. festgelegt. Die Festlegung, wer als Betreiber öffentlicher Telekommunikationsnetze und als Anbieter öffentlich zugänglicher Telekommunikationsdienste mit erhöhtem Gefährdungspotenzial einzustufen ist, erfolgt unter 3.1.

ENTWURF

3. Bestimmung von Gefährdungspotenzialen

Aus dem gemäß § 166 Abs. 1 Nr. 3 TKG zu erstellenden Sicherheitskonzept hat hervorzugehen, von welchen Gefährdungen auszugehen ist und welche technischen Vorkehrungen und sonstigen Maßnahmen unter Beachtung der verschiedenen Gefährdungspotenziale der öffentlichen Telekommunikationsnetze und öffentlich zugänglichen Telekommunikationsdienste umgesetzt werden. Dabei stehen die Gefährdungen in direkter Abhängigkeit zur Bedeutung der Netze und Dienste. Die Bedeutung des zu schützenden Telekommunikationsnetzes oder -dienstes ist insofern maßgeblich für dessen Gefährdungspotenzial. Im Grundsatz können öffentliche Telekommunikationsnetze und -dienste folgenden Gefährdungspotenzialen zugeordnet werden:

- **Normales Gefährdungspotenzial:** Alle öffentlichen Telekommunikationsnetze und öffentlich zugängliche Telekommunikationsdienste
- **Gehobenes Gefährdungspotenzial:** Öffentliche Telekommunikationsnetze und öffentlich zugängliche Telekommunikationsdienste, sofern sie für das Gemeinwohl eine Bedeutung haben
- **Erhöhtes Gefährdungspotenzial:** Öffentliche Telekommunikationsnetze und öffentlich zugängliche Telekommunikationsdienste, sofern sie für das Gemeinwohl eine herausragende Bedeutung haben

3.1 Gefährdungspotenziale

Auf Grundlage des § 167 Abs. 1 S. 1 Nr. 3 TKG werden die verschiedenen Gefährdungspotenziale der öffentlichen Telekommunikationsnetze und öffentlich zugänglichen Telekommunikationsdienste im Einvernehmen mit dem BSI sowie der/dem BfDI wie folgt festgelegt:

ENTWURF

- **Normales Gefährdungspotenzial:** Aus verfassungsrechtlicher Sicht muss der Bedeutung der durch § 165 TKG zu schützenden Rechtsgüter (Fernmeldegeheimnis, Schutz personenbezogener Daten und Funktionsfähigkeit der Telekommunikationsnetze und -dienste) für den Einzelnen Rechnung getragen werden. Ein normales Gefährdungspotenzial hat insofern zumindest diese Bedeutung zugrunde zu legen und die Beachtung damit korrespondierender Vorkehrungen und sonstiger Schutzmaßnahmen sicherzustellen.

  Ein Anbieter von öffentlich zugänglichen Telekommunikationsdiensten oder ein Betreiber öffentlicher Telekommunikationsnetze, weist ein normales Gefährdungspotenzial auf, wenn er weniger als 10 Personen beschäftigt und sein Jahresumsatz bzw. seine Jahresbilanzsumme 2 Mio. EUR nicht überschreitet.

- **Gehobenes Gefährdungspotenzial:** Ein Anbieter von öffentlich zugänglichen Telekommunikationsdiensten oder ein Betreiber öffentlicher Telekommunikationsnetze, hat ein gehobenes Gefährdungspotenzial, sofern er eine Bedeutung für das Gemeinwohl darstellt.

  Jedenfalls weist er ein gehobenes Gefährdungspotenzial auf, wenn er

  a) weniger als 50 Mitarbeiter beschäftigt und

  b) einen Jahresumsatz oder eine Jahresbilanzsumme von jeweils 10 Millionen Euro oder weniger aufweist

- **Erhöhtes Gefährdungspotenzial:** Ein Anbieter von öffentlich zugänglichen Telekommunikationsdiensten oder ein Betreiber öffentlicher Telekommunikationsnetze, weist ein erhöhtes Gefährdungspotenzial auf, sofern er eine herausragende Bedeutung für das Gemeinwohl hat.

  Ein erhöhtes Gefährdungspotenzial liegt jedenfalls in diesen Fällen vor:

  a) Betreiber eines öffentlichen Mobilfunknetzes der 5. Generation (5G Netz)

  b) Betreiber eines sonstigen öffentlichen Telekommunikationsnetzes oder Anbieter von öffentlich zugänglichen Telekommunikationsdiensten, wenn er

     i) mindestens 50 Mitarbeiter beschäftigt oder

     ii) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweist oder

     iii) ein Betreiber kritischer Einrichtungen gemäß Artikel 2 Nummer 1 der RICHTLINIE (EU) 2022/2557 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates ist

Die BNetzA legt gemäß § 167 Abs. 1 S. 1 Nr. 1 TKG im Einvernehmen mit dem BSI und der/dem BfDI Einzelheiten der nach § 165 Abs. 1 bis 7 TKG zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen unter Beachtung der verschiedenen Gefährdungspotenziale der öffentlichen Telekommunikationsnetze und öffentlich zugänglichen Telekommunikationsdienste fest. Aus der Bedeutung der Netze und Dienste und den verschiedenen Gefährdungspotenzialen ergeben sich jeweils andere Anforderungen an die Netze und Dienste. Im Bereich des Telekommunikationssektors existiert eine große Diversität an Telekommunikationsunternehmen auf dem Markt. Daher werden von den Verpflichteten nur geeignete, erforderliche und angemessene technische Vorkehrungen und sonstige Maßnahmen erwartet. 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, § 165 Abs. 6 S. 1 TKG. Einen wesentlichen Beitrag zur Bestimmung der jeweils einschlägigen technischen Vorkehrung oder sonstigen Maßnahme soll der vorliegende Katalog von Sicherheitsanforderungen leisten. Die Beurteilung des jeweiligen Einzelfalls obliegt dem betroffenen Unternehmen unter Berücksichtigung des jeweils festgestellten Gefährdungspotenzials.

ENTWURF

Normales Gefährdungspotenzial: Alle Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste unterliegen dem normalen Gefährdungspotenzial. Diese haben mindestens die grundlegenden Schutzmaßnahmen der Kategorie a) der jeweiligen Bereiche im Kapitel 4 des Kataloges von Sicherheitsanforderungen umzusetzen.

Gehobenes Gefährdungspotenzial: Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste, welche dem gehobenen Gefährdungspotenzial unterliegen, müssen zum Erfüllen der Sicherheitsziele mindestens die grundlegenden Schutzmaßnahmen der Kategorie a) und die erweiterten Schutzmaßnahmen der Kategorie b) im Kapitel 4 des Kataloges von Sicherheitsanforderungen der jeweiligen Bereiche umsetzen.

Erhöhtes Gefährdungspotenzial: Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste, welche dem erhöhten Gefährdungspotenzial im Sinne der

Fallgruppen a) oder b) unterliegen, müssen zum Erfüllen der Sicherheitsziele mindestens die grundlegenden Schutzmaßnahmen der Kategorien a), die erweiterten Schutzmaßnahmen der Kategorie b) und die vollumfänglichen Schutzmaßnahmen der Kategorie c) im Kapitel 4 des Kataloges von Sicherheitsanforderungen der jeweiligen Bereiche umsetzen.

Betreiber von 5G-Netzen nach Fallgruppe a) müssen darüber hinaus die Sicherheitsanforderungen aus Kapitel 5 des Kataloges von Sicherheitsanforderungen erfüllen.

3.2 Verhältnismäßigkeitserwägungen zur Bestimmung der Gefährdungspotenziale

In Kapitel 3 des Kataloges von Sicherheitsanforderungen werden die verschiedenen Gefährdungspotenziale der öffentlichen Telekommunikationsnetze und öffentlich zugänglichen Telekommunikationsdiensten näher bestimmt (§ 167 Abs. 1 Nr. 3 TKG), um in der Folge entsprechend des jeweiligen Gefährdungspotenzials angemessene Schutzmaßnahmen zu definieren. Abhängig davon, in welche Kategorie ein Unternehmen fällt, ist der Eingriff in die Grundrechte unterschiedlich tief. In diesem Kapitel werden also die Adressaten des Sicherheitskatalogs nochmals in drei verschiedene Gruppen eingeteilt. Die Einteilung bestimmt, welche Schutzmaßnahmen aus den Kapiteln 4 und 5 für die Adressaten gelten.

Die Einteilung als solches dient dazu, die Skalierbarkeit der Maßnahmen zu gewährleisten, damit der Grundrechtseingriff möglichst geringgehalten werden kann. Dies ist im Gesetz bereits angelegt (§ 167 Abs. 1 S. 1 Nr. 1 TKG: „unter Beachtung der verschiedenen Gefährdungspotenziale“). Art. 3 Abs. 1 NIS-2-Richtlinie definiert „wesentliche“ Einrichtungen, die dem „erhöhten“ Gefährdungspotenzial im Sicherheitskatalog entsprechen. Art. 3 Abs. 2 NIS-2-Richtlinie definiert „wichtige“ Einrichtungen, die dem „gehobenen“ Gefährdungspotenzial entsprechen. Für die weiteren Einrichtungen gilt das normales Gefährdungspotenzial. Der Begriff des „erhöhten“ Gefährdungspotenzials wird in § 165 Abs. 3 S. 2, Abs. 9 S. 2 TKG verwendet.

ENTWURF

Der Sicherheitskatalog sieht folgende Kategorien vor:

- Normales Gefährdungspotenzial
    - weniger als 10 Mitarbeiter und
    - maximal 2 Mio. Euro Jahresumsatz bzw. Jahresbilanzsumme
    - Folge: Einstufung als sonstige öffentliche Telekommunikationsnetze und öffentlich zugängliche Telekommunikationsdienste
- Gehobenes Gefährdungspotenzial
    - weniger als 50 Mitarbeiter und
    - maximal 10 Mio. Euro Jahresumsatz oder Jahresbilanzsumme
    - Folge: Einstufung als öffentliche Telekommunikationsnetze und öffentlich zugängliche Telekommunikationsdienste, die für das Gemeinwohl eine größere Bedeutung haben
- Erhöhtes Gefährdungspotenzial
    - mindestens 50 Mitarbeiter oder
    - jeweils über 10 Mio. Euro Jahresumsatz und Jahresbilanzsumme

- Folge: Einstufung als öffentliche Telekommunikationsnetze und öffentlich zugängliche Telekommunikationsdienste, die für das Gemeinwohl eine herausragende Bedeutung haben

Diese Indikatoren sind auch sachgemäß. Aus den Kriterien „Mitarbeiteranzahl“ und „wirtschaftliche Kennzahlen“ kann man Rückschlüsse auf die Quantität und Qualität (Wichtigkeit) der Kunden ziehen. Die Wichtigkeit für das Gemeinwohl ergibt sich somit entweder daraus, dass ein signifikanter Anteil der Bevölkerung den Dienst selbst nutzt und/oder dass ein Kunde den Dienst nutzt, der wiederum wichtig für das Gemeinwohl ist. Wenn ein Kunde für das Allgemeinwohl wichtig ist, ist sein Ausfall dementsprechend auch sicherheitskritisch für das Allgemeinwohl.

Auch die Art der Nutzung lässt sich aus den oben genannten Kriterien ableiten. Wenn ein Unternehmen entweder eine große Kundenanzahl hat oder die Kunden sicherheitskritisch sind, werden beispielsweise typischerweise die Dienstleistungen redundant vorgehalten, was sich in der Mitarbeiteranzahl und in der Preisgestaltung widerspiegelt.

Darüber hinaus sind die Kriterien objektiv feststellbar und bieten daher Rechtssicherheit. Die Kriterien sind zudem bekannt und haben sich auch in anderen, ähnlichen Kontexten zur Abgrenzung bewährt. Sie wurden bereits in einer Empfehlung der Kommission im Jahr 2003 formuliert, in dem verschiedene Kleinstunternehmen sowie kleine und mittlere Unternehmen (KMU) voneinander abgegrenzt wurden[27]. Zwar findet sich die Abgrenzung nicht unmittelbar im TKG, in den angrenzenden Regelungen zur Informationssicherheit werden die Kriterien jedoch gleich mehrfach genannt.

ENTWURF

Art. 3 der NIS2-Richtlinie[28] definiert wesentliche und wichtige Einrichtungen. Art. 3 Abs. 1 lit. a) der NIS2-Richtlinie verweist auf Anhang I der Richtlinie. Anhang I der Richtlinie enthält eine Liste verschiedener Unterbranchen mit starker Kritikalität. Damit diese jedoch als wesentliche Einrichtungen gelten, müssen sie nach Art. 3 Abs. 1 lit. a) NIS2-Richtlinie die Schwellenwerte der KMU-Empfehlung für mittlere Unternehmen überschreiten.

Schließlich ist zu berücksichtigen, dass sowohl der Sicherheitskatalog als auch das auf ihm aufsetzende Sicherheitskonzept eine weitere Skalierbarkeit ermöglichen, um im Einzelfall eine unverhältnismäßige Belastung innerhalb der Kategorien zu vermeiden.

Neben den Kennzahlen und der Mitarbeiterzahl können auch Besonderheiten des zu schützenden Telekommunikationsnetzes/-dienstes auf eine bestimmte Bedeutung für das Gemeinwohl hindeuten oder zumindest die Annahme einer besonderen Bedeutung weiter erhärten. Dem öffentlichen Mobilfunknetz kommt in diesem Zusammenhang eine Sonderstellung zu. Denn beim Mobilfunknetz ist von einer querschnittlichen Verwendung in allen Bereichen des öffentlichen Lebens auszugehen. Die Verfügbarkeit und Sicherheit dieses Netzes betrifft daher mit hoher Wahrscheinlichkeit nicht nur den Einzelnen, sondern Staat, Wirtschaft und Gesellschaft gleichermaßen. Eine enorme Sonderstellung kommt dem Betrieb von 5G-Netzen

---

[27] Art, 2 der Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, Aktenzeichen K(2003) 1422), Amtsblatt Nr. L 124 vom 20/05/2003 S. 0036 – 0041; siehe auch Erwägungsgrund 4.

[28] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie).

im Sinne der EU Empfehlung 2019/534 vom 26. März 2019 zu. 5G-Netze sind in diesem Sinn das künftige Rückgrat unserer zunehmend digitalisierten Volkswirtschaften und Gesellschaften. Sie werden Milliarden von Objekten und Systemen miteinander verbinden und auch in den Kritischen Infrastrukturen der Sektoren Energie, Wasser, Ernährung, Gesundheit, Finanz- und Versicherungswesen, Transport und Verkehr sowie dem Sektor Informationstechnik und Telekommunikation sensible Informationen verarbeiten und Sicherheitssysteme unterstützen. Der Betrieb öffentlicher 5G-Mobilfunknetze oder das Anbieten öffentlich zugänglicher 5G-Telekommunikationsdienste indizieren daher eine herausragende Bedeutung dieser Telekommunikationsnetze für das Gemeinwohl.

ENTWURF

4. Festlegung grundlegender Einzelheiten der zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen unter Berücksichtigung der verschiedenen Gefährdungspotenziale, § 167 Abs. 1 S. 1 Nr. 1 TKG

Informationssicherheitsmanagement, oder kurz IS-Management, ist der Teil des allgemeinen Risikomanagements, der die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, Geschäftsprozessen, Anwendungen und IT-Systemen gewährleisten soll.

Um ein bedarfsgerechtes Sicherheitsniveau für alle Geschäftsprozesse, Informationen und der Technik zu erreichen, sind in erheblichem Maße auch geeignete organisatorische und personelle Rahmenbedingungen zu schaffen.

Die im Folgenden aufgelisteten Schutzmaßnahmen greifen diese Aspekte auf und berücksichtigen dabei die Grundstruktur des „Guideline on Security Measures under the EECC 4th Edition July 2021“. Die Schutzmaßnahmen gelten für alle Verpflichteten, sind technologieneutral formuliert und müssen evtl. durch spezifische Sicherheitsprofile ergänzt werden. Sie bilden insofern die Grundlage für alle umzusetzenden Schutzmaßnahmen. Die aus den Sicherheitszielen abgeleiteten Schutzmaßnahmen müssen im Weiteren angemessen in dem zu erstellenden Sicherheitskonzept berücksichtigt werden. Die Beurteilung der Angemessenheit einer sicherheitskonzeptionellen Schutzmaßnahme liegt hierbei zunächst in der Eigenverantwortung des Verpflichteten. Dabei handelt es sich um einen kontinuierlichen Beurteilungsprozess, bei dem Strategien und Maßnahmen stetig überprüft und an veränderte Anforderungen angepasst werden.

ENTWURF

Eine Grundlage für das Erreichen der Sicherheitsziele und der hierfür zu ergreifenden Schutzmaßnahmen bildet der IT-Grundschutz des BSI. Auf Grund der technischen Weiterentwicklungen verfließen die Grenzen zwischen reinen IT- und klassischen Telekommunikationssystemen immer stärker und sind in einigen Bereichen bereits nicht mehr eindeutig voneinander zu trennen. Somit bildet der IT-Grundschutz die Basis zur Absicherung dieser Systeme und ist daher, bei den in diesem Kapitel dargestellten Sicherheitszielen und Schutzmaßnahmen, mit zu berücksichtigen.

Darüber hinaus haben die Verpflichteten die im Anhang des Kataloges genannten Vorkehrungen und Maßnahmen umzusetzen. Im Anhang des Kataloges bleibt die Einstufung Verpflichtungen in den unterschiedlichen Gefährdungspotenzialen aus Kapitel 3.2 mit den Kategorien a), b) und c) bestehen.

Für jedes Sicherheitsziel werden spezifische Schutzmaßnahmen aufgeführt, die von den Verpflichteten ergriffen werden müssen, um das Sicherheitsziel zu erreichen.

Diese Schutzmaßnahmen sind mit Blick auf die unterschiedlichen Gefährdungspotenziale in 3 Kategorien (a bis c) mit steigender Komplexität eingeteilt. Die aufgeführten Schutzmaßnahmen in den Stufen sind abhängig vom Gefährdungspotenzial kumulativ umzusetzen.

a) Grundlegende Schutzmaßnahmen (normales Gefährdungspotenzial und höher)

b) Erweiterte Schutzmaßnahmen (gehobenes Gefährdungspotenzial und höher)

c) Nochmals erweiterte Schutzmaßnahmen (erhöhtes Gefährdungspotenzial)

Hintergrund dieser Differenzierung ist die große Heterogenität des Telekommunikationssektors. Um der großen Bandbreite und den sich daraus ergebenden Gefährdungspotenzialen von Geschäftsmodellen gerecht zu werden (große etablierte Telekommunikationsunternehmen, kleine Diensteerbringer, Betreiber von Glasfaserleitungen, Betreiber virtueller Mobilfunknetze, Internetzugangsdiensteanbieter etc.), wurde diese Mehrstufigkeit gewählt.

Aufgrund des technologieneutralen Ansatzes sollten die hier aufgelisteten Schutzmaßnahmen für ein breites Spektrum unterschiedlicher Technologien anwendbar sein. Als Ergänzung dazu existieren detailliertere Leitlinien für bestimmte Netze und Technologien, wie z. B. Mobilfunk.

Dieser Katalog gibt Sicherheitsziele vor und der Verpflichtete muss darlegen, dass mit den von ihm ergriffenen Maßnahmen das jeweilige Sicherheitsziel vollumfänglich erreicht wird.

Die Aufzählung der Schutzmaßnahmen ist nicht abschließend, sondern dienen als Mindestanforderung in den verschiedenen Kategorien der Gefährdungspotenziale und dienen dem Verpflichteten als Orientierungshilfe zum Erreichen der Sicherheitsziele.

Sofern zur Erreichung des Sicherheitszieles abweichende Maßnahmen umgesetzt werden, so hat der Verpflichtete darzulegen, wie er die geforderten Sicherheitsziele erreicht.

Darüber hinaus gehende Schutzmaßnahmen sind möglich und entsprechend des Ergebnisses der Gefährdungsanalyse gegebenenfalls auch notwendig. Daher kann ein Verpflichteter mit normalen Gefährdungspotenzial auch erweiterte Schutzmaßnahmen des gehobenen Gefährdungspotenzials zum Erreichen der Sicherheitsziele anwenden. Für alle Schutzmaßnahmen ist der Stand der Technik zu berücksichtigen.

ENTWURF

Maßnahmen sollen den Stand der Technik berücksichtigen und unter Betrachtung der einschlägigen europäischen und internationalen Normen sowie der Umsetzungskosten ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist. Bei der Bewertung, ob Maßnahmen dem bestehenden Risiko angemessen sind, sind das Ausmaß der Risikoexposition und die Größe des Betreibers oder des Anbieters sowie die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen.

Nach dem Grundsatz der Verhältnismäßigkeit müssen alle staatlichen Maßnahmen einem legitimen Zweck dienen. Sie müssen geeignet sein, den verfolgten Zweck zu erreichen oder ihn zu fördern (Geeignetheit). Die Maßnahmen müssen erforderlich sein, um den Zweck zu erreichen (Erforderlichkeit) und dürfen nicht außer Verhältnis zum Ziel und dem Zweck stehen (Angemessenheit oder Verhältnismäßigkeit im engeren Sinne).

4.1 Schutz des Fernmeldegeheimnisses und personenbezogener Daten

Der Schutz des Fernmeldegeheimnisses und der Schutz personenbezogener Daten nehmen eine herausgehobene Stellung ein. Daher hat jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, angemessene technische Vorkehrungen und sonstige Maßnahmen zu treffen, um das Fernmeldegeheimnis und personenbezogene Daten zu schützen.

Das Erreichen dieser Sicherheitsziele gilt unabhängig vom zu Grunde liegenden Gefährdungspotenzial. Insofern kann es für den Schutz des Fernmeldegeheimnisses und der Schutz personenbezogener Daten im Einzelfall erforderlich und angemessen sein, Maßnahmen eines übergeordneten Gefährdungspotenzials umzusetzen.

Der technische Schutz personenbezogener Daten erfährt mit Geltung der DSGVO eine rechtliche Neuverortung: die datenschutzrechtlichen Verpflichtungen sind im Allgemeinen in der DSGVO und im BDSG geregelt. Für die Sicherheit der Verarbeitung ist insbesondere Artikel 32 DSGVO zu beachten. Für den Telekommunikationsbereich gibt es hingegen eine Ausnahme von der allgemeinen Regel. Artikel 95 DSGVO gibt den Regelungen der ePrivacy-Richtlinie Vorrang, sofern diese das gleiche Ziel verfolgen. Im TKG und TDDDG werden entsprechende Regelungen der ePrivacy-Richtlinie in deutsches Recht umgesetzt. Dies betrifft auch § 165 TKG als Umsetzung von Artikel 4 Abs. 1 und 1a der ePrivacy-Richtlinie. Im Ergebnis bedeutet dies, dass für die Gewährleistung der Sicherheit der Dienste nicht Art. 32 DSGVO, sondern § 165 ff. TKG, und damit auch der vorliegende Katalog von Sicherheitsanforderungen anzuwenden ist. Für weite Teile der Verarbeitung von Bestandsdaten ist dagegen die DSGVO die einschlägige Rechtsgrundlage.

ENTWURF

4.2 Unternehmensführung und Risikomanagement

Der Bereich "Unternehmensführung und Risikomanagement" umfasst die Sicherheitsziele in Bezug auf das Management von Netz- und Informationssicherheitsrisiken.

Legitimer Zweck und Geeignetheit

Diese Regelungen dienen dem legitimen Zweck, die Sicherheit von Netzen und Diensten jederzeit zu gewährleisten und Sicherheitsrisiken frühzeitig zu erkennen, um diese entsprechend abzuwenden. Hierzu sind sie auch geeignet.

Erforderlichkeit

Die in diesem Kapitel enthaltenen Maßnahmen sind erforderlich, da ihr Ziel nicht durch ein anderes, gleich wirksames Mittel erreicht werden kann. Für Unternehmen mit normalem Gefährdungspotenzial ist es erforderlich, ein übergeordnetes Sicherheitskonzept schriftlich festzuhalten und zumindest das Personal in Schlüsselpositionen im Vorfeld darüber zu informieren. Wenn das Unternehmen erst bei Auftreten von konkreten Gefährdungssituationen entsprechend reagieren würde, könnten insbesondere größere Risiken leichter eintreten. Diese müssen vielmehr bereits abstrakt und im Vorfeld einkalkuliert werden, damit sie vermieden bzw. ihre Auswirkungen minimiert werden können. Auch das Personal muss entsprechend vorbereitet sein und jederzeit für die Einhaltung der Sicherheitsbestimmungen und Umsetzung der Maßnahmen Sorge tragen.

ENTWURF

Für Unternehmen mit gehobenem und erhöhtem Gefährdungspotenzial ist es darüber hinaus erforderlich, detaillierte Netz- und Informationssicherheitsrichtlinien festzulegen, über die das gesamte Personal zu informieren ist. Dies stellt sicher, dass das Unternehmen auch bei Ausfall des Schlüsselpersonals und im Bedarfsfall handlungsfähig bleibt. Das Personal ist förmlich in Sicherheitsfunktionen einzusetzen; das Risikomanagement ist regelmäßig zu überprüfen, da das Eintreten von Gefährdungen Auswirkungen auf das Gemeinwohl haben kann.

Für Unternehmen mit erhöhtem Gefährdungspotenzial gilt zudem, um branchenweit Erkenntnisse aus der Gefahrenabwehr nutzen zu können, sind bei der Überprüfung der Netz- und Informationsrichtlinien die Erfahrungen eigener Vorfälle und die der anderen Anbieter zu berücksichtigen. Es ist nicht ausreichend, das gesamte Personal nur zu informieren; vielmehr muss darüber hinaus ein spezieller Krisenstab eingerichtet sowie einen 24/7 verfügbaren Ansprechpartner für den Krisenfall zu benannt werden, um im Bedarfsfall eine schnellere Reaktionszeit zu gewährleisten. Regelmäßige Überprüfungen und eine gesicherte Nachvollziehbarkeit der Lieferkette in sicherheitsbezogenen Aspekten müssen vollumfassend gewährleistet sein, da das Eintreten von Gefährdungen gravierende Auswirkungen auf das Gemeinwohl haben kann. Dabei handelt es sich um eine Regelung, die auch im Eigeninteresse der Unternehmen ist, da auch ein sicherheitsgefährdendes Verhalten in der Lieferkette dazu führen kann, dass sich das Unternehmen dieses Verhalten nach § 278 Bürgerliches Gesetzbuch (BGB) zurechnen lassen muss.

Angemessenheit

Die Maßnahme ist angemessen, wenn der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht.

Durch die Abstufung der Eingriffstiefe in der Ausgestaltung der Sicherheitsziele wurde dieser zwischen dem legitimen Zweck und den Interessen der Verpflichteten Interessenabwägung Rechnung getragen. Unternehmen aus der Kategorie a) müssen nur weniger einschneidende Maßnahmen zur Erreichung des Sicherheitsziels umsetzen. In Anbetracht des erhöhten bzw. höheren Gefährdungspotenzials, dass von Unternehmen der Kategorien b) und c) für die Gewährleistung der Sicherheit von Netzen und Diensten ausgeht, ist diesen Unternehmen auch ein schwerwiegenderer Eingriff in ihre Berufsfreiheit zumutbar.

4.2.1 Informationssicherheitspolitik

Netz- und Informationssicherheitsrichtlinien und themenspezifische Richtlinien müssen definiert, intern veröffentlicht, dem zuständigen Personal mitgeteilt und von diesen anerkannt werden.

Schutzmaßnahmen:

a)

- Festlegung einer übergeordneten Sicherheitsstrategie für die Sicherheit von Netzen und Diensten
- Information an das Personal in Schlüsselpositionen über die Sicherheitsstrategie
- Überprüfung der Sicherheitsstrategie nach Zwischenfällen

b)

- Festlegung detaillierter Informationssicherheitsrichtlinien für Anlagen und Geschäftsprozesse, die zur Aufrechterhaltung der Netze und Dienste erforderlich sind
- Information an das gesamte Personal über die Sicherheitspolitik und die Auswirkungen auf deren Arbeit
- Regelmäßige Überprüfung entsprechend der Gefährdungsanalyse
- Ergebnisse von Tests/Übungen innerhalb der Organisation in Bezug zur Informationssicherheitspolitik bewerten

c)

- Regelmäßige Überprüfung entsprechend der Gefährdungsanalyse von Informationssicherheitsrichtlinien und dabei Verstöße, Ausnahmen, früherer Zwischenfällen und frühere Tests/Übungen berücksichtigen, die andere (ähnliche) Betreiber/Anbieter in der Branche betrafen

4.2.2 Risikomanagement

Jeder Verpflichtete hat sicherzustellen, dass ein Verfahren festgelegt, umgesetzt und gepflegt wird, um Risiken für die Sicherheit von Netzen, Diensten und die Verarbeitung schützenswerter Daten zu erkennen. Hierfür kann unter anderem die Gefährdungsanalyse herangezogen werden.

ENTWURF

Schutzmaßnahmen:

a)

- Erstellung einer Liste der Risiken für die Sicherheit von Netzen und Diensten unter Berücksichtigung der Gefährdungen für alle Bereiche
- Information des Personals in Schlüsselpositionen über die wichtigsten Risiken und wie diese gemindert werden
- Überprüfung von Risikobewertungen nach Änderungen oder Zwischenfällen

b)

- Einrichtung einer Risikomanagement-Methodik und/oder eines Risikomanagement-Tools auf der Grundlage von Industriestandards
- Sicherstellung, dass das Personal in Schlüsselpositionen die Risikomanagement-Methoden und -Tools anwendet
- Sicherstellung, dass die Restrisiken in einem annehmbaren Maß sind und von der Geschäftsleitung akzeptiert und gelebt werden
- Regelmäßige Überprüfung von Risikobewertungen
- Regelmäßige Überprüfung der Risikomanagement-Methodiken und/oder -Tools unter Berücksichtigung von Änderungen und früheren Zwischenfällen
- Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

ENTWURF

4.2.3 Sicherheitsrollen und Verantwortlichkeiten

Für die Sicherheit von Informationen, Geschäftsprozessen, Anwendungen, Aufgaben und Regelungen ist eine personelle Verantwortlichkeit festzulegen.

Schutzmaßnahmen:

a)

- Zuweisung und regelmäßige Überprüfung von Sicherheitsrollen mit den entsprechenden Kompetenzen und Befugnissen und Festlegung von Verantwortlichkeiten beim Personal
- Sicherstellung, dass die Verantwortlichen mit entsprechender Sicherheitsrolle oder deren Vertreter im Falle von Zwischenfällen erreichbar sind

- Informieren des Personals über die Sicherheitsfunktionen in ihrer jeweiligen Organisation und darüber, wann und wer kontaktiert werden soll

b)

- Das Personal wird förmlich in Sicherheitsfunktionen eingesetzt
- Regelmäßige Überprüfung der Struktur der Sicherheitsrollen und Zuständigkeiten auch im Hinblick auf Änderungen und/oder Überarbeitungsbedarfe aufgrund vergangener Zwischenfälle

c)

- Einrichtung eines Krisenstabes und eines Krisen-/Lagezentrums für den Krisenfall sowie Benennung eines 24/7 verfügbaren Ansprechpartners für den Krisenfall
- Einrichtung und regelmäßige Überprüfung eines Prozesses für Zertifikate von Produkten, wenn gesetzliche Vorgaben zur Produktzertifizierung vorliegen

4.2.4 Sicherheit bei Abhängigkeiten von Dritten

Die Bereitstellung von Telekommunikationsnetzen und -diensten kann oft nur unter Rückgriff auf Dritte (z.B. Vordienstleister, Cloud-Anbieter, Kollokation) erfolgen. Daher ist die Einführung und Aufrechterhaltung von Sicherheitszielen für Verträge mit Dritten sicherzustellen, so dass Abhängigkeiten von Dritten die Sicherheit von Netzen und/oder Diensten nicht beeinträchtigen. Sicherheitsziele und Sicherheitsstandards, die für das verpflichtete Unternehmen gelten, sind in solchen Fällen auch für Lieferanten Dritte verpflichtend und vertraglich sicherzustellen.

ENTWURF

Anmerkung:

Anbieter von Telekommunikations-Diensten der 5. Mobilfunkgeneration sind verpflichtet, vertraglich sicherzustellen, dass die Vorgaben aus dem Kapitel 5 für die 5G-Netzbetreiber durch ihre Vordienstleister und Vertragspartner umgesetzt werden.

Schutzmaßnahmen:

a)

- Aufnahme von Schutzmaßnahmen in Verträge mit Dritten, einschließlich Vertraulichkeit und sichere Übertragung von Informationen
- Anlassbezogene Überprüfung und Aktualisierung der Sicherheitsrichtlinien für Dritte unter Berücksichtigung vergangener Zwischenfällen, Änderungen usw.
- Übersicht über Verträge mit Dritten muss vorhanden sein

b)

- Festlegung von Sicherheitsrichtlinien für Verträge mit Dritten
- Sicherstellung der Integrität bei allen Beschaffungen von Dienstleistungen/Produkten
- Sicherstellung der Einhaltung der Richtlinien bei Dritten
- Forderung von spezifischen Sicherheitsstandards in den Prozessen von Dritten
- Abmilderung von Restrisiken, die nicht von der dritten Partei behandelt werden
- Erstellung und Nutzung eines Vertragsmanagements für Verträge mit Dritten

c)

- Sicherheit der Lieferkette, einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern sind zu gewährleisten
- Verfolgung und Dokumentation von Zwischenfällen, die mit Dritten zusammenhängen oder von Dritten verursacht werden
- Regelmäßige Überprüfung und Aktualisierung der Sicherheitsrichtlinien für Dritte unter Berücksichtigung vergangener Zwischenfällen, Änderungen usw.

ENTWURF

4.3 Sicherheit im Personalmanagement

Das Personal liefert einen wesentlichen Beitrag zur Einhaltung der eingangs erwähnten Sicherheitsziele. Aufwendige Schutzmaßnahmen und technische Redundanzkonzepte bringen nur den gewünschten Erfolg, wenn auch das Personal selbst keine Sicherheitslücke im Unternehmen darstellt und sich der Verantwortung seiner sicherheitsrelevanten Tätigkeit bewusst ist. Dieses Kapitel umfasst die Schutzmaßnahmen an die Personalabteilung, die Geschäftsführung und das Personal im Unternehmen. Hierzu gehört auch Personal, welches zur Erledigung bestimmter Aufgaben extern bereitgestellt wird.

Legitimer Zweck

Legitimer Zweck ist die Gewährleistung der Sicherheit im Personalmanagement.

Geeignetheit

Die Überprüfung der Zuverlässigkeit des Personals, sowie die Darreichung eines umfassenden Schulungsangebotes zu fachbezogenen Sicherheitsfragen, sind gemeinsam, mit der Etablierung von Verfahren, zum Umgang mit personellen Veränderungen und Personalverstößen, entsprechend der jeweiligen Gefährdungspotenziale, geeignete Mittel, um Risiken für die Sicherheit zu vermeiden, welche durch Personal verursacht werden.

Erforderlichkeit

ENTWURF

Die Maßnahme ist erforderlich, da ihr Ziel nicht durch ein anderes, gleich wirksames Mittel erreicht werden kann. Für Unternehmen mit normalem und gehobenem Gefährdungspotenzial ist es erforderlich, zumindest das Schlüsselpersonal zu überprüfen, für Unternehmen mit erhöhtem Gefährdungspotenzial ist die Zuverlässigkeitsüberprüfung auch auf Auftragnehmer und Drittanbieter zu erstrecken. Dies ergibt sich aus der zentralen Rolle von Unternehmen mit erhöhtem Gefährdungspotenzial für das Funktionieren der Telekommunikationsinfrastruktur.

Um zu gewährleisten, dass das gesamte Personal über alle notwendigen Sicherheitskenntnisse verfügt, ist das Schlüsselpersonal entsprechend mit Schulungsmaterial zu versorgen. Für Unternehmen mit gehobenem und erhöhtem Gefährdungspotenzial sind regelmäßige Schulungen zu Sicherheitsfragen vorgesehen, damit das gesamte Personal jederzeit über die aktuellen Sicherheitskenntnisse verfügt, um sicherheitskritische Situationen weitestgehend zu vermeiden und im Falle eines Gefahreneintritts entsprechend agieren zu können.

Für den Umgang mit personellen Veränderungen sind bereits im Vorfeld entsprechende Verfahren zu etablieren, die vermeiden sollen, dass bei einem Wechsel des Personals auch nur kurzzeitige Sicherheitslücken entstehen, etwa indem beispielsweise Zugangsrechte oder Ausweise nicht rechtzeitig entzogen werden.

Um zu gewährleisten, dass das Personal die erworbenen Sicherheitskenntnisse auch entsprechend umsetzt, ist ein Verfahren für das Personal zu etablieren, welches gegen Sicherheitsrichtlinien verstoßen hat. Für Unternehmen ab gehobenem Gefährdungspotenzial sind die getroffenen Abhilfemaßnahmen darüber hinaus zu dokumentieren und das Verfahren ist regelmäßig zu überprüfen und aktualisieren. Nur so kann auf Änderungen und Zwischenfälle adäquat reagiert werden.

Angemessenheit

Die vorgesehenen Maßnahmen sind angemessen, da der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht. Hierbei wurde entsprechend des jeweiligen Gefährdungspotenzials berücksichtigt, dass bei kleineren Unternehmen die Zuverlässigkeitsprüfung lediglich auf das Schlüsselpersonal zu beschränken ist. Das Schlüsselpersonal ist mit Schulungsmaterial zu Sicherheitsfragen zu versorgen, erst ab gehobenem Gefährdungspotenzial sind regelmäßige Sicherheitsschulungen erforderlich. Zu beachten ist auch, dass die Schulungen ggf. auch von externen Dienstleistern erbracht werden können, d.h. nicht zwingend für jedes Unternehmen separat konzipiert werden müssen. Der Umgang mit personellen Veränderungen (Entzug der Zugangsrechte) ist zudem auch regelmäßig bereits aus datenschutzrechtlichen Erwägungen heraus umzusetzen.

4.3.1 Personalmanagement

Je nach Aufgabe und Verantwortlichkeit ist eine angemessene Überprüfung der Vertraulichkeit, Unabhängigkeit und Integrität des Personals durchzuführen.

Schutzmaßnahmen:

a)

- Überprüfung der beruflichen Referenzen des Schlüsselpersonals (Systemadministratoren, Sicherheitsbeauftragte, Wachpersonal usw.)

ENTWURF

b)

- Durchführung von Überprüfungen des Personals in Schlüsselpositionen, sofern erforderlich
- Erstellung von Richtlinien und Verfahren für Überprüfungen des Personals
- Überprüfung und Aktualisierung der Maßnahmen/Verfahren für Zuverlässigkeitsüberprüfungen und Referenzprüfungen in regelmäßigen Abständen unter Berücksichtigung von Änderungen und früheren Zwischenfällen

c)

- Zuverlässigkeitsüberprüfungen auch auf Auftragnehmer und Dritte anwenden

4.3.2 Sicherheitswissen, Sicherheitsausbildung und Prüfung

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

Schutzmaßnahmen:

a)

- Versorgung des Schlüsselpersonals mit einschlägigem Schulungsmaterial zu Sicherheitsfragen

b)

- Implementierung eines Schulungsprogramms, welches sicherstellt, dass das Personal in Schlüsselpositionen über ausreichende und aktuelle Sicherheitskenntnisse verfügt
- Organisation von Schulungen im Bereich der Sicherheit von Netzen und Diensten und Sensibilisierungsveranstaltungen für das Personal zu Sicherheitsthemen, die für das Unternehmen wichtig sind
- Überprüfung und Aktualisierung des Schulungsprogramms in regelmäßigen Abständen unter Berücksichtigung von Änderungen und vergangenen Zwischenfällen
- Regelmäßige Prüfung der Sicherheitskenntnisse des Personals
- Schulungsprogramme aktualisieren und Neuerungen anhand des Standes der Technik abdecken
- Regelmäßige Überprüfung des Fachpersonals auf die aktuellen durchgeführten Schulungen und Qualifikation, bevor das Personal Zugang zu sicherheitskritischen Bereichen bekommt

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

ENTWURF

4.3.3 Personelle Veränderungen

Einführung und Aufrechterhaltung eines geeigneten Verfahrens für den Umgang mit personellen Veränderungen oder Änderungen in ihren Rollen und Verantwortlichkeiten.

Schutzmaßnahmen:

a)

- Nach personellen Veränderungen werden unverzüglich Zugangsrechte, Ausweise, Ausrüstungen usw. entzogen, wenn sie nicht mehr erforderlich oder zulässig sind, entsprechende Nachweise sind zu führen
- Einweisung und Unterweisung neuen Personals in die geltenden Richtlinien und Verfahren

b)

- Etablierung eines Verfahrens für Personalwechsel unter Berücksichtigung des rechtzeitigen Entzugs von Zugangsrechten, Ausweisen, Ausrüstung usw.
- Umsetzung von Maßnahmen/Verfahren für die Aus- und Weiterbildung von Personal in neuen Funktionen
- Regelmäßige Überprüfung der Wirksamkeit der Verfahren

c)

- Dokumentation von Verbesserungsmöglichkeiten und direkte Anwendung, falls möglich
- Überprüfung, Bewertung und Anpassung von Maßnahmen/Verfahren für personelle Veränderungen unter Berücksichtigung von Änderungen und früheren Zwischenfällen

4.3.4 Umgang mit Verstößen

Einführung und Aufrechterhaltung eines Verfahrens für das Personal, welches gegen Sicherheitsrichtlinien verstoßen hat. Es soll ein umfassendes Verfahren vorhanden sein, das Zwischenfälle aufdeckt, die durch Verstöße des Personals verursacht wurden.

Schutzmaßnahmen:

a)

- Einrichtung eines Verfahrens, welches Verstöße gegen Richtlinien feststellt und entsprechende Gegenmaßnahmen ergreift

b)

- Einrichtung von Verfahren bei Verstößen des Personals gegen die Richtlinien und Dokumentation der getroffenen Abhilfemaßnahmen
- Regelmäßige Überprüfung und Aktualisierung des Verfahrens auf der Grundlage von Änderungen und früheren Zwischenfälle

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

ENTWURF

4.4 Sicherheit von Daten, Systemen und Einrichtungen

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

Legitimer Zweck

Diese Punkte dienen dazu, die physische und logische Sicherheit von Daten, Netzwerk- und Informationssystemen sicherzustellen.

Geeignetheit

Die Einrichtung und Aufrechterhaltung von physischen und logischen Schutzmaßnahmen, um unbefugten Zugang zu verhindern, ist dazu geeignet, die Sicherheit der Netze, Informationssysteme und Einrichtungen zu fördern. Maßnahmen, um die Geräte und Betriebsmittel vor Stromausfällen und anderen Störungen zu schützen, sind geeignete Mittel, um die Versorgungssicherheit zu fördern. Eindeutige Kennungen und Zugangskontrollmechanismen sind geeignete Mittel, um unberechtigte Nutzung von Geräten und Systemen, eine Offenlegung von vertraulichen Informationen und Störungen zu verhindern sowie Manipulationen vorzubeugen. Die Implementierung von Schutzmaßnahmen gegen Angriffsvektoren wie Viren, Code-Injektionen oder Malware sind geeignet, die Integrität und Verfügbarkeit von Netzwerk- und Informationssystemen zu fördern. Verschlüsselungsalgorithmen sind geeignet, um die Netze und Systeme gegen unerlaubte Zugriffe zu schützen.

ENTWURF

Erforderlichkeit

Die Maßnahme ist erforderlich, da ihr Ziel nicht durch ein anderes, gleich wirksames Mittel erreicht werden kann. Für Unternehmen mit normalem Gefährdungspotenzial ist es erforderlich, Maßnahmen zur Verhinderung von unbefugtem physischem und logischem Zugang zu Einrichtungen und Infrastrukturen zu ergreifen. Unternehmen mit gehobenem und erhöhtem Gefährdungspotenzial müssen, um den Zugang zu schützen, darüber hinaus Strategien entwickeln, die regelmäßig zu kontrollieren und zu überprüfen sind. Unternehmen mit erhöhtem Gefährdungspotenzial müssen diese Strategien regelmäßig aktualisieren, um auf aktuelle Gefährdungen frühzeitig reagieren zu können und auch eine ausfallsichere Fernabschaltung oder Datenlöschung für gestohlene Geräte sicherzustellen.

Zur Gewährleistung der Versorgungssicherheit sind Geräte und Betriebsmittel vor Stromausfällen und anderen Störungen zu schützen. Unternehmen mit gehobenem Gefährdungspotenzial müssen im Hinblick auf den Ausfall des öffentlichen Stromnetzes definieren, welche kritischen Bereiche des Betriebes aufrechterhalten werden müssen, um notwendige Versorgungsgüter vorab zu schützen. Unternehmen mit erhöhtem Gefährdungspotenzial müssen darüber hinaus aktive Kühlung und Notstromgeneratoren bereithalten, um zu gewährleisten, dass die Versorgung jederzeit sichergestellt ist.

Die Implementierung logischer Zugangskontrollmechanismen ist ein geeignetes Mittel, um eine unberechtigte Nutzung von Geräten und Systemen zu verhindern. Nur mithilfe eindeutiger Kennungen von Benutzer und Systemen kann ein nicht autorisierter Zugriff verhindert werden. Unternehmen mit gehobenem Gefährdungspotenzial müssen den Zugang zu Netz und Informationssystemen überwachen. Unternehmen mit erhöhtem Gefährdungspotenzial müssen darüber hinaus die Wirksamkeit ihrer

Zugangskontrollstrategien und -verfahren bewerten und ihre Authentifizierungsmechanismen müssen den allgemein bewährten Verfahren entsprechen, bspw. Multifaktor-Authentifizierung (MFA).

Um die Integrität und Verfügbarkeit von Netzwerk- und Informationssystemen zu schützen, muss bei Unternehmen mit normalem Gefährdungspotenzial etwa durch Eingabekontrollen und Firewalls sichergestellt werden, dass Angriffsvektoren mittels z.B. Viren oder Malware nicht zum Zugriff auf die Systeme genutzt werden können. Dazu sind bei Unternehmen mit gehobenem Gefährdungspotenzial verstärkte Kontrollen der Softwareintegrität erforderlich, um im Vorfeld Angriffsvektoren abzuwehren. Unternehmen mit erhöhtem Gefährdungspotenzial müssen Software-Patching-Verfahren einsetzen, um jederzeit sicherzustellen, dass Softwareprodukte sicherheitsrelevante Patches schnellstmöglich erhalten.

Zur Sicherung gegen unerlaubte Zugriffe sind Verschlüsselungen einzusetzen. Unternehmen mit gehobenem Gefährdungspotenzial müssen Verschlüsselungsrichtlinien und -algorithmen einführen und umsetzen, um ein standardisiertes Verfahren zu gewährleisten, Unternehmen mit erhöhtem Gefährdungspotenzial müssen diese Richtlinien regelmäßig überprüfen und aktualisieren, um den aktuellen Stand der Technik zu gewährleisten.

Sicherheitsrelevante Daten sind mithilfe von Verschlüsselung und Authentifizierungsmaßnahmen zu schützen. Unternehmen mit gehobenem und erhöhtem Gefährdungspotenzial müssen hierfür spezielle Verfahren umsetzen, die regelmäßig zu überprüfen und aktualisieren sind.

Angemessenheit

ENTWURF

Die Maßnahmen sind angemessen, da der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht. Hierbei wurde entsprechend des jeweiligen Gefährdungspotenzials berücksichtigt, dass kleinere Unternehmen zwar auch angemessene Schutzmaßnahmen zur Sicherheit von Daten, Systemen und Einrichtungen treffen müssen, aber Unternehmen mit gehobenem und erhöhtem Gefährdungspotenzial hierfür umfangreichere Strategien und Verfahren bereitstellen müssen. Unternehmen mit erhöhtem Gefährdungspotenzial müssen darüber hinaus ihre Strategien regelmäßig überprüfen, dokumentieren und aktualisieren. Hierbei müssen sie allgemeingültige Standards und Richtlinien berücksichtigen, um das bestmögliche Schutzniveau nach dem Stand der Technik zu erreichen (zu dem Begriff „Stand der Technik“ vgl. bereits oben in den allgemeinen Ausführungen zur Verhältnismäßigkeit). Der Punkt 4.4 enthält anders als andere Punkte Anforderungen an die Unternehmen, die teilweise erhebliche Investitionen sowohl in finanzieller als auch in personeller Hinsicht erfordern. Dies ergibt sich daraus, dass die Datensicherheit sowohl die physische als auch die logische Sicherheit von Daten, Netzwerk- und Informationssystemen umfasst. Um den umfassenden Schutz der Daten zu gewährleisten, genügt es nicht, nur einen Schutz gegen physische Zerstörung einzurichten; vielmehr muss auch ein Manipulationsschutz vorgesehen werden, um die Sicherheit von Netzen und Diensten zu gewährleisten. vgl. § 3 Nr. 52 TKG. Danach bedeutet "Sicherheit von Netzen und Diensten" die Fähigkeit von Telekommunikationsnetzen und -diensten, auf einem bestimmten Vertrauensniveau alle Angriffe abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit dieser Netze und Dienste, der gespeicherten, übermittelten oder verarbeiteten Daten oder der damit zusammenhängenden Dienste, die über diese Telekommunikationsnetze oder -dienste angeboten werden oder zugänglich sind, beeinträchtigen.

Da die unterschiedlichen Gefährdungspotenziale auch unterschiedliche Vertrauensniveaus bedingen, ergibt sich bereits hieraus die unterschiedliche Eingriffstiefe für die unterschiedlich eingestuften Unternehmen.

4.4.1 Physische und umgebungsbezogene Sicherheit

Einrichtung und Aufrechterhaltung einer angemessenen physischen und umgebungsbezogenen Sicherheit der Netze, Informationssysteme und Einrichtungen.

Schutzmaßnahmen:

a)

- Verhinderung von unbefugtem physischen und logischem Zugang zu Einrichtungen und Infrastrukturen
- Einrichtung angemessener Umgebungskontrollen, um vor unbefugtem Zutritt, Einbruch, Feuer, Überschwemmung usw. geschützt zu sein

b)

- Umsetzung einer Strategie für physische Schutzmaßnahmen und Umgebungskontrollen (z.B. Maßnahmen des Objektschutzes, darunter das Aufstellen von Zäunen und Sperren, Instrumente und Verfahren für die Überwachung der Umgebung, der Einsatz von Detektionsgeräten)
- Durchführung von physischen und umgebungsbezogenen Kontrollen
- Verstärkte Kontrollen des physischen Zugangs zu sicherheitskritischen Bereichen
- Überprüfung der Wirksamkeit der physischen und umgebungsbezogenen Kontrollen
- Regelmäßige Bewertung der Wirksamkeit der physischen und umgebungsbezogenen Kontrollen

c)

- Überprüfung und Aktualisierung der Strategie für physische Schutzmaßnahmen und umgebungsbezogene Kontrollen unter Berücksichtigung von Änderungen und vergangenen Zwischenfällen
- Dokumentation von zusätzlichen, risikobasierten Kontrollen für die physische Sicherheit
- Dokumentation von zusätzlichen, angemessenen physischen Infrastrukturkontrollen (z. B. Sicherheit der Infrastruktur und der Verwaltungsgebäude, Alarmanlagen und Videoüberwachung zur Erkennung und Aufzeichnung von Zwischenfällen), insbesondere für unbemannte Anlagenstandorte
- Einrichtung von Kontrollen, die eine ausfallsichere Fernabschaltung (oder Datenlöschung) für gestohlene Geräte ermöglichen und/oder eine erneute Authentifizierung oder Konfiguration nach einem physischen Angriff oder einem Stromausfall erfordern

ENTWURF

- Führung von Nachweisen über Zugangskontrollen, dass Personen, die Räumlichkeiten betreten, sicherheitsüberprüft, geschult und qualifiziert sind und dass jeglicher Zugang, insbesondere durch Dritte streng überwacht wird

4.4.2 Sicherheit der Versorgung (Verfügbarkeit des Gesamtsystems)

Geräte und Betriebsmittel sind vor Stromausfällen und anderen Störungen, die durch Ausfälle von Versorgungseinrichtungen verursacht werden, zu schützen.

Schutzmaßnahmen:

a)

- Sicherstellung von relevanten Lieferungen zur Gewährleistung der Versorgungssicherheit

b)

- Im Hinblick auf den Ausfall des öffentlichen Stromnetzes muss definiert werden in welchem Umfang der Betrieb oder einzelne besonders kritische Bereiche aufrechterhalten werden müssen

- Umsetzung eines Konzepts für die Sicherstellung von wichtigen Lieferungen zur Gewährleistung der Versorgungssicherheit

- Umsetzung von Schutzmaßnahmen zum Schutz notwendiger Versorgungsgüter und unterstützender Einrichtungen (z.B. passive Kühlung, automatischer Neustart nach einer Stromunterbrechung, Notstrombatterien, Dieselgeneratoren, Ersatzkraftstoff usw.)

- Regelmäßige Überprüfung und Aktualisierung der Maßnahmen und Verfahren zur Sicherung wichtiger Güter und zur Gewährleistung der Versorgungssicherheit, unter Berücksichtigung von Änderungen und vergangenen Zwischenfällen

Anmerkung:

In Bezug zur Notstromversorgung ist der Leitfaden „Notstromversorgung in Unternehmen und Behörden“ des Bundesamts für Bevölkerungsschutz und Katstrophenhilfe zu berücksichtigen

c)

- Einführung von Maßnahmen zum Schutz notwendiger Versorgungsgüter (z.B. aktive Kühlung, Notstromgeneratoren, Service-Level-Agreement (SLAs) mit Kraftstofflieferanten, redundante Kühl- und Stromversorgungssysteme)

4.4.3 Zugriffs- und Zugangskontrolle zu Netz- und Informationssystemen

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

ENTWURF

Schutzmaßnahmen:

a)

- Benutzer und Systeme haben eindeutige Kennungen und werden vor dem Zugriff auf Dienste oder Systeme authentifiziert
- Implementierung logischer Zugangskontrollmechanismen für Netz- und Informationssysteme, um nur die autorisierte Nutzung zuzulassen
- Passwörter sind zumindest gehasht und, sofern technisch möglich, mit einem Salt versehen zu speichern
- Umsetzung von Maßnahmen zum Schutz des Zugangs zu Netz- und Informationssystemen, z. B. in Bezug auf Rollen, Rechte, Zuständigkeiten und Verfahren, für die Zuweisung und den Entzug von Zugangsrechten
- Je nach Art des Zugriffs müssen ausreichend sichere Authentifizierungsmechanismen z.B. Multi-Faktor-Authentifizierung eingesetzt werden
- Regelmäßige Überprüfung der erteilten Rollen und Rechte
- Sicherstellung, dass der Zugang von Dritten und/oder der Fernzugriff zu betriebs- und sicherheitsrelevanten Systemen nur für den erforderlichen Zeitraum gewährt wird und keine dauerhaften Zugangsdaten vergeben werden

ENTWURF

b)

- Überwachung des Zugangs zu Netzen und Informationssystemen
- Einrichtung eines Verfahrens zur Genehmigung von Ausnahmen und zur Registrierung von Zugangsverletzungen
- Regelmäßige Kontrollen für den Fernzugriff auf betriebsrelevante Netz- und Informationssysteme durch Dritte

c)

- Bewertung der Wirksamkeit von Zugangskontrollstrategien und -verfahren und Durchführung von Gegenkontrollen der Zugangskontrollmechanismen
- Zugangskontrollverfahren und Zugangskontrollmechanismen müssen überprüft und bei Bedarf unverzüglich überarbeitet werden
- Implementierte Authentifizierungsmechanismen müssen den allgemein bewährten Verfahren für Multifaktor-Authentifizierung (MFA) entsprechen

- Zentrale Lösung für das Privileged Access Management (PAM)

4.4.4 Integrität und Verfügbarkeit von Netz- und Informationssystemen

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

Schutzmaßnahmen:

a)

- Sicherstellung, dass die Software von Netz- und Informationssystemen nicht manipuliert oder verändert wird, z. B. durch den Einsatz von Eingabekontrollen und Firewalls
- Kontinuierliche Überprüfung auf Schadsoftware in (internen) Netzwerken und Informationssystemen
- Absicherung von Servern gegen Missbrauch, z.B. durch Deaktivierung nicht benötigter Dienste

b)

- Implementierung von Schutzmaßnahmen, die einen umfassenden Schutz vor Manipulationen und Änderungen an Systemen bieten und die Verfügbarkeit der Netze und Systeme sicherstellen
- Regelmäßige verstärkte Kontrollen der Softwareintegrität, der Aktualisierung und der Patch-Verwaltung für betriebsrelevante Bereiche in Netzwerken
- Vorhalten ausreichender Redundanzen zum Sicherstellen der Verfügbarkeit betriebsrelevanter Systeme

c)

- Einrichtung effektiver Kontrollen zum Schutz der Integrität der Systeme
- Bewertung und Überprüfung der Wirksamkeit von Maßnahmen zum Schutz der Integrität von Systemen
- Anwendung von Software-Patching-Verfahren, um sicherzustellen, dass Softwareprodukte oder -komponenten nicht verändert wurden (z. B. geeignete kryptografische Methoden zum Schutz der Integrität und Authentizität)

4.4.5 Sicherstellung der Vertraulichkeit

Gegen unerlaubte Zugriffe sind insbesondere Maßnahmen zu treffen, um Telekommunikations- und Datenverarbeitungssysteme zu sichern und Auswirkungen von Zwischenfällen für Nutzer sowie andere Telekommunikationsnetze und -dienste so gering wie möglich zu halten.

ENTWURF

Schutzmaßnahmen:

a)

- Bei der Übermittlung und bei der Speicherung von Daten ist die Vertraulichkeit, der Schutz des Fernmeldegeheimnisses und der Schutz personenbezogener Daten durch Verschlüsselung angemessen sicherzustellen oder ein Zugriff Dritter muss durch andere Maßnahmen sicher ausgeschlossen werden

- Bei geplanten Neuanschaffungen, Ersatz von Telekommunikations- und Datenverarbeitungssystemen oder Umstrukturierung sollen bei der Planung und Umsetzung Maßnahmen zur Verschlüsselung angemessen berücksichtigt werden

- Sofern den Kunden eine Software für mobile Geräte („App“) als Teil des Dienstes zur Verfügung gestellt wird, sind die auf dem Gerät gespeicherten und die übertragenen Daten zu verschlüsseln

Anmerkung: Weitere Informationen zum Stand der Technik der Verschlüsselung liefert die TR-02102.

b)

- Einführung und Umsetzung einer Verschlüsselungsrichtlinie

- Verwendung von Verschlüsselungsalgorithmen unter Berücksichtigung der empfohlenen Mindestlänge des verwendeten kryptografischen Schlüssels

- Anlassbezogene Überprüfung und Aktualisierung der Verschlüsselungsrichtlinie

- Bei Systemen, die eine Auswahl von verschiedenen Sicherheitsstufen bieten, sollte die höchstmögliche Sicherheitsstufe verwendet werden

- Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung

c)

- Regelmäßige Überprüfung und Aktualisierung der Verschlüsselungsrichtlinie

ENTWURF

4.4.6 Schutz von sicherheitsrelevanten Daten

Sicherstellen, dass das kryptografische Schlüsselmaterial und die geheimen Authentifizierungsinformationen in angemessener Weise geschützt sind.

Schutzmaßnahmen:

a)

- Sicherstellung, dass kryptografisches Schlüsselmaterial und geheime Authentifizierungsinformationen (einschließlich des für die Authentifizierung verwendeten kryptografischen Schlüsselmaterials) nicht offengelegt oder manipuliert werden können

- Strenge Kontrolle und Überwachung des Zugangs zu privaten kryptografischen Schlüsseln

b)

- Umsetzung von Verfahren für die Verwaltung von kryptografischen Schlüsseln
- Umsetzung eines Verfahrens für die Verwaltung von Passwörtern
- Regelmäßige Überprüfung und Aktualisierung der Schlüsselverwaltungsrichtlinie
- Regelmäßige Überprüfung und Aktualisierung der Richtlinie zur Verwaltung von Passwörtern
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

ENTWURF

4.5 Betriebsführung

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

Legitimer Zweck

Legitimer Zweck ist es, den ordnungsgemäßen und sicheren Betrieb zu gewährleisten.

Geeignetheit

Die Festlegung und Umsetzung von Betriebsverfahren, von vordefinierten Methoden oder Verfahren bei Änderungen an betriebsrelevanten Systemen sowie von Asset-Management-Verfahren und Konfigurationskontrollen sind geeignete Mittel, um den ordnungsgemäßen und sicheren Betrieb zu gewährleisten.

Erforderlichkeit

Die Maßnahmen sind erforderlich, da ihr Ziel nicht durch ein anderes, gleich wirksames Mittel erreicht werden kann. Für Unternehmen mit normalem Gefährdungspotenzial ist es erforderlich, Betriebsverfahren und die Zuweisung von Zuständigkeiten für den Betrieb wichtiger Systeme festzulegen. Unternehmen mit gehobenem und erhöhtem Gefährdungspotenzial müssen Strategien umsetzen und diese regelmäßig überprüfen sowie aktualisieren, um sicherzustellen, dass alle wichtigen Systeme betrieben und verwaltet werden. Nur durch die Festlegung solcher Strategien im Voraus kann garantiert werden, dass die Netze und Dienste jederzeit aufrechterhalten werden. Unternehmen mit erhöhtem Gefährdungspotenzial müssen zudem Mechanismen einführen, um sicherzustellen, dass auch jede tatsächliche Änderung aufgezeichnet wird und alle Unregelmäßigkeiten untersucht werden.

ENTWURF

Zur Vermeidung von Störungen oder Zwischenfällen müssen Änderungen an Netzwerk- und Informationssystemen, Infrastrukturen, Dokumentationen, Prozessen, Verfahren und Betriebsabläufen mit vordefinierten Methoden oder Verfahren geplant, kontrolliert und gesteuert werden. Würde man das Vorgehen erst zeitgleich mit der auftretenden Änderung festlegen, bestünde die Gefahr, dass ein übereiltes oder ungeeignetes Änderungsmanagement zu Sicherheitsrisiken führt. Unternehmen mit gehobenem und erhöhtem Gefährdungspotenzial müssen vordefinierte Verfahren zur Änderungsverwaltung festlegen, diese dokumentieren, regelmäßig überprüfen und aktualisieren sowie ein Patch-Management-System einrichten und nutzen. Bei Unternehmen mit erhöhtem Gefährdungspotenzial müssen zudem Änderungen an der virtualisierten Netzwerkumgebung in Richtlinien und Verfahren für das Änderungsmanagement enthalten sein.

Um die Verfügbarkeit wichtiger Anlagen und Konfigurationen kritischer Netz- und Informationssysteme zu verwalten, sind ein Asset-Management-Verfahren und Konfigurationskontrollen zu etablieren. Wichtige Anlagen müssen vorab identifiziert und dokumentiert werden. Wichtige Systeme und solche, die personenbezogene Daten enthalten, sind zu konfigurieren und schützen. Unternehmen mit gehobenem und erhöhtem Gefährdungspotenzial müssen entsprechende Verfahren umsetzen, überprüfen und aktualisieren. Unternehmen mit erhöhtem Gefährdungspotenzial müssen zusätzlich Datenspeicher mit den relevanten Einzelheiten und über eingesetzte Technologien und Komponenten einsetzen.

Angemessenheit

Diese Maßnahmen sind angemessen, da der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht. Hierbei wurde bei der Bestimmung der zu etablierenden Maßnahmen das jeweilige Gefährdungspotenzial berücksichtigt. Unternehmen der Kategorie a) müssen sichere Betriebsverfahren und Änderungsmanagement etablieren. Unternehmen mit gehobenem und erhöhtem Gefährdungspotenzial müssen umfassendere Verfahren etablieren. Unternehmen mit erhöhtem Gefährdungspotenzial müssen darüber hinaus noch umfassendere Mechanismen einführen, diese regelmäßig kontrollieren und jederzeit auf dem aktuellen Stand der Technik halten.

4.5.1 Betriebsverfahren

Durch geeignete Betriebsverfahren ist sicherzustellen, dass alle relevanten Betriebsabläufe des jeweiligen Verpflichteten ordnungsgemäß, sicher und kontinuierlich funktionieren.

Schutzmaßnahmen:

a)

- Festlegung von Betriebsverfahren und Zuweisung von Zuständigkeiten für den Betrieb wichtiger Systeme

b)

ENTWURF

- Umsetzung einer Strategie für den Betrieb von Systemen, um sicherzustellen, dass alle wichtigen Systeme gemäß den vordefinierten Verfahren betrieben und verwaltet werden

- Regelmäßige Überprüfung und Aktualisierung der Maßnahmen/Verfahren für den Betrieb der Systeme, die für die Aufrechterhaltung der Netze und Dienste erforderlich sind, unter Berücksichtigung von Zwischenfällen und/oder Änderungen

c)

- Einführung von Mechanismen um sicherzustellen, dass jede tatsächliche Änderung aufgezeichnet wird und dass alle während des Änderungsprozesses aufgetretenen Unregelmäßigkeiten untersucht werden

4.5.2 Änderungsmanagement

Zur Vermeidung von Störungen oder Zwischenfällen müssen Änderungen an Netzwerk- und Informationssystemen, Infrastrukturen, Dokumentationen, Prozessen, Verfahren und Betriebsabläufen geplant, kontrolliert und gesteuert sowie nach Abschluss überprüft werden.

Schutzmaßnahmen:

a)

- Befolgung von vordefinierten Methoden oder Verfahren, wenn Änderungen an betriebsrelevanten Systemen vorgenommen werden
- Sicherheitspatches innerhalb eines angemessenen Zeitraums nach ihrer Verfügbarkeit anwenden, ihre vertrauenswürdige Herkunft und deren Integrität prüfen

b)

- Umsetzung von Maßnahmen/Verfahren für die Änderungsverwaltung, um sicherzustellen, dass Änderungen an betriebsrelevanten Systemen stets nach einem vordefinierten Verfahren vorgenommen werden
- Dokumentation der Verfahren zur Änderungsverwaltung und Festhalten aller Änderungen des Verfahrens
- Regelmäßige Überprüfung und Aktualisierung des Verfahrens für das Änderungsmanagement, dabei sind Änderungen und frühere Zwischenfälle zu berücksichtigen
- Einrichtung und Nutzung eines Patch-Management-Systems
- Implementieren von übergreifenden Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen

ENTWURF

c)

- Änderungen an der virtualisierten Netzwerkumgebung (z. B. durch Patchen von softwaredefinierten Netzwerkkomponenten) müssen in den Richtlinien und Verfahren für das Änderungsmanagement enthalten sein

4.5.3 Asset Management

Einrichtung und Aufrechterhaltung von Asset-Management-Verfahren und Konfigurationskontrollen, um die Verfügbarkeit wichtiger Anlagen und Konfigurationen kritischer Netz- und Informationssysteme zu verwalten.

Schutzmaßnahmen:

a)

- Identifizierung und Dokumentation wichtiger Anlagen und Konfigurationen wichtiger Systeme sowie von Systemen, die personenbezogene Daten enthalten
- Dokumentation der Systeme, die mit den vorgenannten Systemen verbunden sind und für Angriffe missbraucht werden könnten, z.B. in Form eines Netzwerkstrukturplans

b)

- Umsetzung von Maßnahmen/Verfahren für das Asset-Management und die Konfigurationskontrolle
- Regelmäßige Überprüfung und Aktualisierung des Asset-Managements auf Grundlage von Änderungen und vergangenen Zwischenfällen
- Erstellung einer Übersicht der Abhängigkeiten wichtiger Anlagen, Konfigurationen wichtiger Systeme und wichtiger / kritischer Software

c)

- Einrichtung und regelmäßiges Aktualisierung einer Dokumentation, welche Einzelheiten über eingesetzte Technologien und Komponenten enthalten
- Durchführung regelmäßiger Bewertungen der physischen Anlagen mittels Einführung von Strategien/Verfahren im Asset Management
- Kategorisierung der physischen Netzanlagen (z. B. Kernnetzanlagen, Übertragungsknotenpunkte, Vermittlungsstellen, Basisstationen) basierend auf der Gefährdungsanalyse und in Bezug zur Bedeutung der betriebsrelevanten Systeme

ENTWURF

4.6 Lifecycle-Management für Hard- und Software

Da Produkte im Laufe ihres Lebenszyklus in den jeweiligen Phasen unterschiedlichen Risiken ausgesetzt sind, müssen diese Risiken minimiert werden. Für besonders kritische Phasen werden daher nachfolgend Anforderungen an den Verpflichteten, aber auch an den Funktionsumfang der Komponenten, gestellt. Das Lifecycle-Management dient dazu, die Integrität der verwendeten Hard- und Software sicherzustellen.

Legitimer Zweck

Legitimer Zweck ist es, die Sicherheitsrisiken zu minimieren, die in den verschiedenen Lebenszyklen von Hard- und Software entstehen können.

Geeignetheit

Die Festlegung und Umsetzung von Maßnahmen, entsprechend der jeweiligen Gefährdungspotenziale, für die Dauer der Nutzung und den Austauschprozess von Komponenten ist ein geeignetes Mittel, um die Sicherheitsrisiken in den verschiedenen Lebenszyklen von Hard- und Software zu minimieren.

Der Austausch von nicht mehr aktuellen Komponenten sowie die Integritätsprüfung bindet finanzielle und personelle Ressourcen, dient sowohl dem legitimen Zweck, das Gefährdungspotenzial in allen Kategorien zu minimieren.

Erforderlichkeit

ENTWURF

Die Maßnahmen sind erforderlich, da ihr Ziel nicht durch ein anderes, gleich wirksames Mittel erreicht werden kann. Für Unternehmen mit normalem Gefährdungspotenzial ist es erforderlich, die Komponenten nach Ende des Supports auszutauschen, da nach diesem Zeitraum ein sicherer Betrieb nicht mehr gewährleistet werden kann. Unternehmen mit gehobenem Gefährdungspotenzial müssen jederzeit die Integrität der erworbenen Produkte verifizieren können. Nur so kann sichergestellt werden, dass die Komponenten während der Auslieferung nicht manipuliert wurden. Unternehmen mit erhöhtem Gefährdungspotenzial müssen Hardware-Produkte bei der Auslieferung mit einem physischen Schutz etwa Versiegelungen versehen, damit Einwirkungen auf das Produkt auch äußerlich sofort erkennbar sind. Bei der Außerbetriebnahme sind weitere Anforderungen einzuhalten und sensible Daten dauerhaft zu löschen, so dass sie nicht wiederhergestellt werden können.

Angemessenheit

Die Maßnahmen sind auch angemessen, da der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht. Durch die Abstufung der Eingriffstiefe in der Ausgestaltung der Sicherheitsziele wurde dieser Interessenabwägung Rechnung getragen. Unternehmen aus der Kategorie a) müssen nur weniger einschneidende Maßnahmen zur Erreichung des Sicherheitsziels umsetzen. In Anbetracht des höheren Gefährdungspotenzials, dass von Unternehmen der Kategorien b) und c) für die Gewährleistung der Sicherheit von Netzen und Diensten ausgeht, ist diesen Unternehmen auch ein schwerwiegenderer Eingriff in ihre Berufsfreiheit zumutbar.

Schutzmaßnahmen:

a)

- Austausch von Komponenten, wenn diese z.B. nach Ende des Supportzeitraums nicht mehr sicher betrieben werden können

b)

- Der Verpflichtete muss in die Lage versetzt werden, die Integrität der erworbenen Hard- und Software-Produkte jederzeit, beginnend mit der Abnahme, zu verifizieren. Die Prüfungsmöglichkeiten müssen entsprechend in Anspruch genommen und dokumentiert werden.

- Es ist insbesondere zu prüfen, ob die betreffenden Komponenten während der Auslieferung Manipulationen, Einwirkungen oder andere Veränderungen erfahren haben

c)

- Für Hardware-Produkte ist ein geeigneter physischer Schutz bei der Auslieferung vorzusehen, z.B. versiegelte Transportboxen, bewachte Transporte oder ein Selbstschutz des Produktes (z.B. der Einsatz von kryptographischen Verfahren zur Integritätssicherung)

- Für Software-Produkte sind Prinzipien wie Security-by-Design zu berücksichtigen und die Vorgaben des Cyber Resilience Act (CRA) zu beachten

- Die Integrität des Produktes ist bei der Lagerung sicherzustellen.

- Bei der Inbetriebnahme ist erneut eine Integritätsprüfung durchzuführen und in das Konfigurationsmanagement aufzunehmen

- Bei der Außerbetriebnahme sind ggf. besondere Anforderungen (z.B. sicheres Löschen von Schlüsselmaterial, Konfigurationen, personenbezogene Daten z.B. Verkehrsdaten, etc.) zu berücksichtigen

ENTWURF

4.7 Management von Zwischenfällen

Das Management von Zwischenfällen umfasst das eigentliche Managementverfahren, die Fähigkeit, die Zwischenfälle zu erkennen, zu melden und bei TK-anbieterübergreifenden Störungen zu kooperieren.

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

Legitimer Zweck

Legitimer Zweck ist das Erkennen, die Reaktion sowie die Meldung von Störungen und Zwischenfällen zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Informationen und Systemen.

Geeignetheit

Dieser Eingriff dient dem legitimen Zweck, die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Informationen und Systemen zu schützen. Die genannten Strategien sind hierzu auch geeignet.

Die Festlegung und Umsetzung von umfassenden Sicherheitsstrategien entsprechend der jeweiligen Gefährdungspotenziale ist ein geeignetes Mittel den Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Informationen und Systemen sicherzustellen.

ENTWURF

Erforderlichkeit

Die Maßnahme ist erforderlich, da ihr Ziel nicht durch ein anderes, gleich wirksames Mittel erreicht werden kann. Für Unternehmen mit normalem Gefährdungspotenzial ist es erforderlich, Personalressourcen sicherzustellen, die auf die Bewältigung von Zwischenfällen vorbereitet sind und Prozesse einzurichten, um Zwischenfälle zu erkennen. Eine Mitteilung und Berichterstattung an Dritte, Kunden und Behörden kann erforderlich sein, um ähnlichen Zwischenfällen künftig vorzubeugen.

Die Adressaten des Eingriffs müssen Personalressourcen bereitstellen und – bei gehobenem und erhöhtem Gefährdungspotenzial – auch entsprechende Prozesse etablieren. Andere, gleich wirksame Mittel, die Informationen und Systeme gleichermaßen vor Zwischenfällen schützen könnten, sind nicht ersichtlich. Insbesondere dient der transparente Umgang mit Zwischenfällen dazu, ähnlichen Zwischenfällen künftig vorzubeugen.

Unternehmen mit gehobenem Gefährdungspotenzial müssen branchenübliche Systeme und Verfahren für das Management von Zwischenfällen etablieren, um umfassend vorbereitet zu sein. Dazu zählen auch Verfahren für die Kommunikation und Berichterstattung über Zwischenfälle. Für Fälle von Störungen, von denen mehrere Betreiber / Anbieter betroffen sein könnten, müssen Ansprechpartner und Vorgehensweise im Vorfeld untereinander abgestimmt werden, damit im Notfall ein direkter und unverzüglicher Kontakt möglich ist, um möglichst schnell und adäquat auf Gefahrensituationen reagieren zu können.

Unternehmen mit erhöhtem Gefährdungspotenzial müssen darüber hinaus bei Bewertung ihrer Verfahren für das Management ihrer Zwischenfälle auch die Erkenntnisse früherer Zwischenfälle heranziehen, um die

daraus gewonnenen Informationen miteinzubeziehen sowie alle sicherheitsrelevanten Netzaktivitäten überwachen.

Angemessenheit

Die Maßnahme ist angemessen, da der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht. Durch die Abstufung der Eingriffstiefe in der Ausgestaltung der Sicherheitsziele wurde dieser Interessenabwägung Rechnung getragen. Unternehmen aus der Kategorie a) müssen nur weniger einschneidende Maßnahmen zur Erreichung des Sicherheitsziels umsetzen. In Anbetracht des höheren Gefährdungspotenzials, dass von Unternehmen der Kategorien b) und c) für die Gewährleistung der Sicherheit von Netzen und Diensten ausgeht, ist diesen Unternehmen auch ein schwerwiegenderer Eingriff in ihre Berufsfreiheit zumutbar.

Bei der Interessenabwägung wurde berücksichtigt, dass das Aufdecken von IT-Sicherheitslücken im Eigeninteresse des jeweiligen Adressaten liegt.

Vor diesem Hintergrund handelt es sich bei den Anforderungen teilweise um Obliegenheiten, d.h. um Verhaltensanforderungen im eigenen Interesse. Die Eingriffstiefe wurde so ausgestaltet, dass insbesondere sehr kleine Unternehmen keine separaten Prozesse einführen müssen. Vor diesem Hintergrund sind die genannten Maßnahmen insgesamt verhältnismäßig.

ENTWURF

4.7.1 Verfahren für das Management von Zwischenfällen

Einführung, Aufrechterhaltung und Aktualisierung von Verfahren zur Behandlung von Zwischenfällen und deren Weiterleitung an geeignetes Personal.

Schutzmaßnahmen:

a)

- Sicherstellung von Personalressourcen, die auf die Bewältigung von Zwischenfällen vorbereitet sind
- Führung von Aufzeichnungen über alle wichtigen Zwischenfälle
- Anlassbezogene Untersuchung von Zwischenfällen sowie der ergriffenen Maßnahmen

b)

- Umsetzung von Maßnahmen/Verfahren für das Management von Zwischenfällen
- Untersuchung größerer Zwischenfälle und Erstellung von Abschlussberichten, einschließlich der ergriffenen Maßnahmen und Empfehlungen zur Vermeidung künftiger Zwischenfälle dieser Art

c)

- Bewertung der Grundsätze/Verfahren für das Management von Zwischenfällen auf der Grundlage früherer Zwischenfälle

4.7.2 Fähigkeit zur Erkennung von Zwischenfällen

Einrichtung und Aufrechterhaltung eines Systems zur Erkennung von Zwischenfällen.

Schutzmaßnahmen:

a)

- Einrichtung von Prozessen zur Erkennung von Zwischenfällen
- Kontaktmöglichkeit zum Empfang externer Meldungen

b)

- Implementierung branchenüblicher Systeme und Verfahren zur Erkennung von Zwischenfällen
- Einführung von Systemen und Verfahren zur Erfassung und rechtzeitigen Weiterleitung von Zwischenfällen an die zuständigen Stellen
- Regelmäßige Überprüfung der Systeme und Verfahren zur Erkennung von Zwischenfällen und deren Aktualisierung unter Berücksichtigung von Änderungen und vergangenen Zwischenfällen
- Regelmäßige Überprüfung von relevanten Protokollen nach vordefinierten Verfahren im Zusammenhang mit dem Fernzugriff auf das Netz
- Konzepte zur Bewältigung von Zwischenfällen

ENTWURF

c)

- Einführung von Systemen und Verfahren zur Erkennung von Zwischenfällen
- Überwachung der sicherheitsrelevanten Netzaktivitäten

4.7.3 Meldung von Zwischenfällen und Kommunikation

Einrichtung, Aufrechterhaltung und Aktualisierung von Verfahren zur Meldung von Zwischenfällen.

Schutzmaßnahmen:

a)

- Mitteilung und Berichterstattung über anhaltende oder vergangene Zwischenfälle an Dritte, Kunden und/oder Behörden, falls erforderlich

b)

- Umsetzung von Maßnahmen und Verfahren für die Kommunikation und Berichterstattung über Zwischenfälle

- Regelmäßige Überprüfung und Aktualisierung der Melde- und Kommunikationspläne auf der Grundlage von Änderungen oder vergangenen Zwischenfällen

c)

- Bewertung des Verfahrens auf Grundlage von früheren Mitteilungen und Berichten über Zwischenfälle

Anmerkung:

Es gibt unterschiedliche Arten von Zwischenfällen, für die der Verpflichtete entsprechende und geeignete Verfahren einführen muss.

Sollte es bei einem Zwischenfall zu beträchtlichen Auswirkungen auf den Betrieb der Netze oder auf die Erbringung der Dienste kommen, so ist dieser als Sicherheitsvorfall gemäß § 168 TKG einzustufen und unverzüglich der BNetzA und dem BSI mitzuteilen.

Nähere Informationen zu Sicherheitsvorfällen gemäß § 168 TKG finden sich auf der Internetseite der BNetzA unter www.bundesnetzagentur.de/sicherheitsvorfall.

Darüber hinaus sind Anbieter von öffentlich zugänglichen TK-Diensten verpflichtet, im Falle einer Verletzung personenbezogener Daten, unverzüglich die Bundesnetzagentur und die/den BfDI zu benachrichtigen (§169 Abs. 1 TKG).

ENTWURF

4.7.4 Kooperation bei TK-anbieterübergreifenden Störungen

Treten Störungen auf, von denen mehrere Betreiber/Anbieter betroffen sein könnten, beispielsweise aufgrund von DDoS-Angriffen, ist eine übergreifende Zusammenarbeit der Betreiber/Anbieter notwendig. Diese sollte auch einen übergreifenden Austausch der Betreiber/Anbieter zu infizierten Geräten umfassen.

Schutzmaßnahmen:

a)

- Grundlegende Schutzmaßnahmen zur Erreichung des Sicherheitsziels

b)

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

- Es liegt in der Verantwortung des Verpflichteten, vernetzte Betreiber/Anbieter zu kontaktieren, um die entsprechenden Kontaktpersonen zu ermitteln. Letztere haben den ersten Betreiber/Anbieter im Gegenzug unverzüglich über Änderungen zu informieren.

- Es muss stets sichergestellt sein, dass im Notfall ein direkter und unverzüglicher Kontakt unter den Betreibern/Anbietern möglich ist

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

ENTWURF

4.8 Notfall- und Ausfallmanagement

Eine Störung oder ein Zwischenfall kann zum Ausfall des Dienstes oder des Netzbetriebes führen. Eine geeignete Präventionsstrategie sollte Entwicklungen dieser Art berücksichtigen und entsprechende, auf den Einzelfall angepasste Abwehrkonzepte entwickeln. Der Bereich Notfall- und Ausfallmanagement umfasst Kontinuitätsstrategien und Notfallpläne, um größere Ausfälle und natürliche oder vom Menschen verursachte Katastrophen abzuwenden oder abzumildern.

Anmerkung:

Eine Vorgehensweise zum systematischen Aufbau eines umfassenden Notfall- und Ausfallmanagement ist im BSI-Standard 100-4[29] beschrieben.

Legitimer Zweck und Geeignetheit

Dieser Punkt dient dazu, mithilfe von Kontinuitätsstrategien und Notfallplänen größere Ausfälle von Diensten oder des Netzbetriebes und Katastrophen abzuwenden oder abzumildern. Die Festlegung und Umsetzung von umfassenden Sicherheitsstrategien entsprechend der jeweiligen Gefährdungspotenziale ist ein geeignetes Mittel, zu verhindern, dass Störungen oder Zwischenfälle zum Ausfall des Dienstes oder des Netzbetriebes führen.

Erforderlichkeit

ENTWURF

Die Maßnahme ist erforderlich, da ihr Ziel nicht durch ein anderes, gleich wirksames Mittel erreicht werden kann. Für Unternehmen mit normalem Gefährdungspotenzial ist es erforderlich, Notfallpläne und eine Strategie zur Gewährleistung der Aufrechterhaltung der Dienste und Netze umzusetzen, um zu verhindern, dass Störungen und Zwischenfälle zum Ausfall führen. Es sind regelmäßige Backups aller Systeme und Daten zu erstellen, die für den Betrieb des Netzes und/oder die Erbringung der TK-Dienste notwendig sind. Unternehmen mit normalem Gefährdungspotenzial sollen lediglich Backup-Daten und -Systeme räumlich und logisch getrennt von den Systemen des Wirkbetriebes lagern; Unternehmen mit gehobenem und erhöhtem Gefährdungspotenzial müssen dies tun. Damit bleibt der Sicherheitskatalog für Unternehmen mit normalem Gefährdungspotenzial noch unter der 3-2-1-Regel für Backups, die als Best Practice-Regel allgemein akzeptiert wird.[30] Insbesondere vor dem Hintergrund, dass Ransomware-Angriffe in den letzten Jahren stark zugenommen haben und in erheblichem Maße auch Erfolg hatten, ist eine Backup-Strategie für die Sicherheit der Daten und das Funktionieren der Telekommunikationsinfrastruktur in Deutschland ein integraler Bestandteil und darüber hinaus auch im Eigeninteresse jedes Unternehmens. Unternehmen mit gehobenem und erhöhtem Gefährdungspotenzial müssen darüber hinaus Notfallpläne für betriebsrelevante Systeme und Prozesse umsetzen und diese regelmäßig überprüfen und überarbeiten.

[29] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.html

[30] Danach sollen 3 Sicherheitskopien auf 2 verschiedenen Speichermedien vorgenommen werden; eine Sicherheitskopie soll off-site gelagert werden.

Unternehmen mit erhöhtem Gefährdungspotenzial müssen bei der Bewertung ihrer Notfallpläne auch die Erkenntnisse früherer Zwischenfälle heranziehen sowie besondere Vorkehrungen treffen, um zeitkritische Anwendungen abzudecken und eine höhere Netzverfügbarkeit zu gewährleisten.

Angemessenheit

Die Maßnahme ist angemessen, da der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht. Durch die Abstufung der Eingriffstiefe in der Ausgestaltung der Sicherheitsziele wurde dieser Interessenabwägung Rechnung getragen. Unternehmen aus der Kategorie a) müssen nur weniger einschneidende Maßnahmen zur Erreichung des Sicherheitsziels umsetzen. In Anbetracht des höheren Gefährdungspotenzials, dass von Unternehmen der Kategorien b) und c) für die Gewährleistung der Sicherheit von Netzen und Diensten ausgeht, ist diesen Unternehmen auch ein schwerwiegenderer Eingriff in ihre Berufsfreiheit zumutbar

4.8.1 Strategie zur Aufrechterhaltung der Netze, der Dienste und Notfallpläne

Erstellung und Pflege von Notfallplänen und einer Strategie zur Gewährleistung der Kontinuität (Business Continuity Management) von betriebenen Netzen und erbrachter Telekommunikationsdienste sind unumgänglich.

Schutzmaßnahmen:

a)

- Umsetzung einer Strategie zur Aufrechterhaltung der bereitgestellten Telekommunikationsnetze und/oder -dienste

b)

- Umsetzung von Notfallplänen für alle betriebsrelevanten Systeme, Prozesse, Sektoren und Dienste
- Überwachung der Notfallplan-Aktivierung und -Ausführung sowie Registrierung der Zeiten, die für die erfolgreichen bzw. fehlgeschlagenen Wiederherstellungen notwendig sind
- Regelmäßige Überprüfung und Überarbeitung der Strategie zur Aufrechterhaltung der Netze und Dienste, z.B. die Vorsorge mit ausreichenden Redundanzen

c)

- Überprüfung und Überarbeitung von Notfallplänen auf der Grundlage von Änderungen und vergangener Zwischenfälle
- Bereitstellung von besonderen Vorkehrungen, die zu den bestehenden Notfallplänen hinzugefügt werden, um zeitkritische Anwendungen abzudecken, um eine höhere Netzverfügbarkeit für solche Dienste zu gewährleisten

ENTWURF

- Erstellung einer Übersicht über betriebsrelevante Abhängigkeiten (z.B. im Rahmen der Lieferketten, Vordienstleister, Versorgungsgütern für den Notfall usw.), welche sich direkt oder indirekt auf die Verfügbarkeit oder Kontinuität von Netzen/Diensten auswirken können. Entsprechende Abhilfemaßnahmen sind zu definieren und dokumentieren.

4.8.2 Wiederanlauf nach Ausfällen (Disaster Recovery Management)

Der Verpflichtete hat für den Fall von Naturkatastrophen, Sabotage und/oder anderen Katastrophen angemessene Notfallmechanismen zur Wiederherstellung von Telekommunikationsnetzen- und diensten einzurichten und aufrechtzuerhalten.

Schutzmaßnahmen:

a)

- Erstellung und Dokumentation konkreter Planungen für den Wiederaufbau und die Wiederherstellung von Diensten und Netzen nach Zwischenfällen. Entsprechende Dokumentationen müssen im Notfall sofort verfügbar sein.

- Dokumentation von Wiederanlaufzeiten für die zentralen Dienste und Netze

b)

ENTWURF

- Umsetzung von Maßnahmen/Verfahren für den Einsatz von Disaster Recovery Management, u.a. Erstellung eines Notfallhandbuches

- Implementierung von Disaster Recovery Management Systeme. Ersatzweise können diese auch von Dritten zur Verfügung gestellt werden (z.B. von nationalen Notfallnetzen).

- Regelmäßige Tests zur Überprüfung, dass die Notfallmaßnahmen wirksam sind und die gemäß Dokumentation vorgesehenen Wiederanlaufzeiten eingehalten werden

- Regelmäßige Überprüfung und Aktualisierung der Disaster-Recovery-Fähigkeiten unter Berücksichtigung von Änderungen, vergangenen Zwischenfällen sowie den Ergebnissen von Tests und Übungen

c)

- Einrichtung von ausreichend dimensionierten Disaster-Recovery-Kapazitäten zur Abfederung von äußeren Angriffen und Einwirkungen von Katastrophen

- Pläne für den Fall einer Katastrophe, die den laufenden Betrieb des Netzes und des Dienstes beeinträchtigt

4.8.3 Backup-Strategie

Es sind regelmäßige Backups aller Systeme und Daten zu erstellen, die für den Betrieb der TK-Netze bzw. die Erbringung der TK-Dienste notwendig sind.

Auf die gesetzlich vorgegebenen Lösch- und Speicherfristen ist hierbei zu achten, insbesondere sollte die Speicherdauer der Backups in einem angemessenen Verhältnis zur Speicherdauer der personenbezogenen Daten stehen.

Schutzmaßnahmen:

a)

- Die Backup-Daten und -Systeme sollen räumlich und logisch getrennt von den Systemen des Wirkbetriebes gelagert werden
- Die Backup-Medien und -Systeme sind in angemessenen Zeitabständen auf einwandfreie Funktion zu überprüfen
- In angemessenen Zeitabständen ist zu überprüfen, dass im Falle einer Störung des Wirkbetriebs mit den Backups ein unterbrechungsfreier Weiterbetrieb der Netz- und Telekommunikationsdienste gewährleistet ist
- Alle Backup-Verfahren sind zu dokumentieren und diese Dokumentation mit den Backup-Daten aufzubewahren

ENTWURF

b)

- Backup-Daten und -Systeme müssen räumlich und logisch getrennt von den Systemen des Wirkbetriebes gelagert werden
- Etablierung georedundanter Backup-Lösungen zur Minimierung von Unterbrechungen der TK-Dienste durch Ausfälle zentraler Technikstandorte

c)

- Keine darüberhinausgehenden Maßnahmen erforderlich

4.9 Überwachungs-, Prüf- und Testverfahren

Um Systeme und Prozesse möglichst sicher zu gestalten und stets zu optimieren, müssen Überwachungs-, Prüf- und Testverfahren von Netz- und Informationssystemen und -einrichtungen eingeführt werden.

Legitimer Zweck

Legitimer Zweck ist die Einführung von Überwachungs-, Prüf- und Testverfahren von Netz- und Informationssystemen und -einrichtungen, um Systeme und Prozesse möglichst sicher zu gestalten.

Geeignetheit

Die Festlegung und Umsetzung von umfassenden Sicherheitsstrategien entsprechend der jeweiligen Gefährdungspotenziale ist ein geeignetes Mittel, um Systeme und Prozesse möglichst sicher zu gestalten.

Erforderlichkeit

Die Maßnahme ist erforderlich, da ihr Ziel nicht durch ein anderes, gleich wirksames Mittel erreicht werden kann. Für Unternehmen mit normalem Gefährdungspotenzial ist es erforderlich, Systeme und relevante Schnittstellen, die zum Betrieb erforderlich sind, zu identifizieren und diese zu überwachen. Es sind Festlegungen für das Testen von Systemen erforderlich, wenn neue Netze oder Systeme angeschlossen werden.

ENTWURF

Unternehmen mit gehobenem und erhöhtem Gefährdungspotenzial müssen Systeme zur Angriffserkennung einsetzen sowie Programme implementieren, um Sicherungs- und Notfallpläne regelmäßig zu üben. Hier ist ein deutlicher Sprung in den Anforderungen gegenüber Unternehmen mit normalem Gefährdungspotenzial zu sehen. Daraus ergibt sich, dass das Einrichten von entsprechenden Tools und die zugehörige Überwachung als eigenständige Punkte im Katalog genannt werden. Unternehmen mit erhöhtem Gefährdungspotenzial müssen Systeme zur Angriffserkennung nach bestimmten Richtlinien umsetzen und auch Lieferanten und Dritte in die Notfallübungen einbeziehen.

Im Hinblick auf die Notfallpläne besteht der Unterschied zwischen den Gefährdungspotenzialen darin, dass Unternehmen mit einem normalen Gefährdungspotenzial lediglich abstrakte Übungen durchführen müssen, während die größeren Unternehmen – die als Angriffsziele auch attraktiver sind – darüber hinaus auch konkrete Szenarien durchspielen müssen. Unternehmen mit erhöhtem Gefährdungspotenzial müssen zudem auch Lieferanten und Dritte mit einbeziehen, um die Sicherheit der gesamten Prozesskette zumindest grundlegend zu gewährleisten.

Das Testen von Netzen und Informationssystemen, bevor diese eingeführt werden, dient dazu, den laufenden Betrieb zu gewährleisten. In der Vergangenheit hat sich gezeigt, dass dieser Punkt nicht nur dazu dient, Manipulationen z.B. durch Schadsoftware vorzubeugen; vielmehr kann so die Kompatibilität und das Verhalten der Software im bestehenden System geprüft werden, bevor sie im Produktivsystem eingesetzt wird.

Die Schutzmaßnahmen müssen den Stand der Technik (vgl. die Ausführungen zur allgemeinen Verhältnismäßigkeit) berücksichtigen. Sie müssen sich zudem der wachsenden Bedrohungslage anpassen. Vor diesem Hintergrund müssen Unternehmen mit normalem Gefährdungspotenzial sicherstellen, dass

regelmäßige Sicherheitstests durchgeführt werden. Unternehmen mit gehobenem/erhöhtem Gefährdungspotenzial müssen zudem die Sicherheitstests selbst überprüfen und ggf. anpassen.

Die Einhaltung und Umsetzung rechtlicher und regulatorischer Anforderungen sind als solches Teil eines ordnungsgemäß ausgeführten Gewerbebetriebs; insoweit enthält der Sicherheitskatalog für Unternehmen mit normalem Gefährdungspotenzial keine darüberhinausgehenden Anforderungen. Dass Unternehmen mit gehobenem/erhöhtem Gefährdungspotenzial die Überwachung optimieren müssen, stellt hingegen eine eigene Regelung dar, deren Eingriffstiefe jedoch gering ist.

Angemessenheit

Die Maßnahme ist angemessen, da der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht. Durch die Abstufung der Eingriffstiefe in der Ausgestaltung der Sicherheitsziele wurde dieser Interessenabwägung Rechnung getragen. Unternehmen aus der Kategorie a) müssen nur weniger einschneidende Maßnahmen zur Erreichung des Sicherheitsziels umsetzen. In Anbetracht des höheren Gefährdungspotenzials, dass von Unternehmen der Kategorien b) und c) für die Gewährleistung der Sicherheit von Netzen und Diensten ausgeht, ist diesen Unternehmen auch ein schwerwiegenderer Eingriff in ihre Berufsfreiheit zumutbar.

4.9.1 Systeme zur Angriffserkennung, Überwachungs- und Protokollierungsmaßnahmen

Zur Erkennung von Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und -diensten führen können, sowie zur Beherrschung von Risiken für die Sicherheit von Netzen und Diensten, müssen alle zu deren Betrieb bzw. deren Erbringung relevanten Systeme und Netze überwacht werden. Dazu kann die Erhebung von Protokoll- und Protokollierungsdaten zur Identifikation und Bewertung von sicherheitsrelevanten Ereignissen (SRE) und der Einsatz von Systemen zur Angriffserkennung erforderlich sein. Bei Umsetzung dieser Maßnahmen sind sowohl die datenschutzrechtlichen Anforderungen, als auch die Anforderungen zum Fernmeldegeheimnis zu beachten.

ENTWURF

Schutzmaßnahmen:

a)

- Identifikation von Systemen und relevanter Schnittstellen, die zum Betrieb der Telekommunikationsnetze und/oder zur Erbringung der Telekommunikationsdienste relevant sind
- Überwachung dieser Systeme bzw. Schnittstellen

b)

- Empfehlung zum Einsatz und Betrieb von Systemen zur Angriffserkennung Details sind der Orientierungshilfe zu Systemen zur Angriffserkennung des BSI[31] zu entnehmen

[31] https://www.bsi.bund.de/oh-sza

c)

- Einsatz und Betrieb von Systemen zur Angriffserkennung mindestens gleichwertig zur Stufe 4 des Umsetzungsgradmodells der Orientierungshilfe zu Systemen zur Angriffserkennung des BSI. Gleichwertig sind sie dann, wenn sie insbesondere über ebenbürtige Angriffserkennungskapazitäten verfügen und so ein äquivalentes Sicherheitsniveau sicherstellen können.

4.9.2 Notfallübungen

Schutzmaßnahmen zur Aufrechterhaltung und zum Wiederanlauf von Infrastrukturen und Diensten nach Zwischenfällen, Ausfällen und Notfällen müssen vorhanden und umgesetzt sein.

Es müssen in regelmäßigen Abständen die festgelegten und umgesetzten Maßnahmen für Sicherungs- und Notfallpläne, auch in Zusammenarbeit mit Dritten, überprüft werden, um sicherzustellen, dass diese gültig und in widrigen Situationen wirksam sind.

Schutzmaßnahmen:

a)

- Übung und Testung von Backup- und Notfallplänen, um sicherzustellen, dass die Systeme und Prozesse funktionieren und das Personal auf größere Ausfälle und Unwägbarkeiten vorbereitet ist

ENTWURF

b)

- Implementierung eines Programmes zur regelmäßigen Übung von Sicherungs- und Notfallplänen, wobei realistische Szenarien verwendet werden sollen

- Sicherstellung, dass die aus den Übungen gewonnenen Erkenntnisse von den verantwortlichen Personen aufgegriffen und die entsprechenden Prozesse und Systeme entsprechend aktualisiert werden

- Regelmäßige Überprüfung und Aktualisierung der Übungspläne unter Berücksichtigung von Änderungen, vergangenen Ereignissen und Zwischenfällen, die im Übungsprogramm nicht berücksichtigt wurden

c)

- Einbeziehung von Lieferanten und anderer Dritter in die Übungen ein, z.B. Geschäftspartner und Kunden

- Teilnahme an Tests/Übungen mit anderen (ähnlichen) Betreibern/Anbietern in der Branche

4.9.3 Testen von Netzwerk- und Informationssystemen

Änderungen oder Entwicklungsarbeiten an bestehenden Netzwerk- oder Informationssystemen sind mögliche Risikofaktoren. Es müssen daher Festlegungen für das Testen von Netzwerk- und

Informationssystemen getroffen werden insbesondere, wenn neue Netze oder Systeme angeschlossen werden.

Schutzmaßnahmen:

a)

- Testung der Netzwerk- und Informationssysteme, bevor diese eingeführt oder an bestehende Systeme angeschlossen werden

b)

- Umsetzung von Maßnahmen/Verfahren zum Testen von Netzwerk- und Informationssystemen
- Implementierung von Tools für automatisierte Tests
- Regelmäßige Überprüfung und Aktualisierung der Maßnahmen/Verfahren für das Testen, unter Berücksichtigung von Änderungen und vergangenen Zwischenfällen

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

ENTWURF

4.9.4 Beurteilung der Schutzmaßnahmen

Die Schutzmaßnahmen müssen den Stand der Technik berücksichtigen und müssen sich damit einhergehend der wachsenden Bedrohungslage anpassen. Vor diesem Hintergrund müssen Festlegungen und Aufrechterhaltung einer angemessenen Strategie für die Durchführung von Sicherheitsbewertungen der Netzwerke und der Informationssysteme getroffen werden.

Schutzmaßnahmen:

a)

- Sicherstellung, dass wichtige Systeme regelmäßigen Sicherheitsüberprüfungen und Sicherheitstests unterzogen werden, insbesondere bei der Einführung neuer Systeme und nach Änderungen

b)

- Umsetzung von Maßnahmen/Verfahren für Sicherheitsbewertungen und Sicherheitstests
- Regelmäßige Überprüfung und Aktualisierung der Maßnahmen/Verfahren für Sicherheitsbewertungen und Sicherheitstests unter Berücksichtigung von Änderungen und vergangenen Zwischenfällen
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Maßnahmen im Bereich der Sicherheit von Netzen und Diensten, welche auf einem gefahrenübergreifenden Ansatz beruhen, der darauf

abzielt, die Netzwerk- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen

c)

- Bewertung der Wirksamkeit von Schutzmaßnahmen und Sicherheitsverfahren
- Bewertung der Sicherheitstests

4.9.5 Überwachung der Einhaltung

Einführung und Umsetzung von Verfahren zur Überwachung der Einhaltung von Normen und gesetzlichen Vorschriften.

Schutzmaßnahmen:

a)

- Überwachung der Einhaltung und Umsetzung von rechtlichen Anforderungen

b)

- Kontinuierliche Überwachung der Einhaltung von Normen und rechtlichen Anforderungen
- Regelmäßige Überprüfung und Aktualisierung der Maßnahmen/Verfahren für die Einhaltung der Vorschriften und die Prüfung, unter Berücksichtigung von Änderungen und früheren Zwischenfällen

c)

- Bewertung der Maßnahmen/Verfahren zur Einhaltung der Vorschriften und zur Prüfung

ENTWURF

4.10 Bewusstsein für Bedrohungen (Threat Awareness)

Dieser Bereich umfasst Sicherheitsziele im Zusammenhang mit der Aufklärung von Bedrohungen und dem Kontakt zu Endnutzern, um Informationen über die wichtigsten Bedrohungen für die Sicherheit von Netzen und Diensten weiterzugeben.

Legitimer Zweck

Der Punkt „Bewusstsein für Bedrohungen“ umfasst Informationen über Bedrohungen sowie die Unterrichtung der Nutzer über Bedrohungen. Dies dient dazu, Informationen über die wichtigsten Bedrohungen für die Sicherheit von Netzen und Diensten zu erhalten sowie an Endkunden weiterzugeben, indem umfassende Sicherheitsstrategien festgelegt und umgesetzt werden. Diese sind zudem wiederum an die jeweiligen Gefährdungspotenziale angepasst.

Geeignetheit

Die Festlegung und Umsetzung von umfassenden Sicherheitsstrategien entsprechend der jeweiligen Gefährdungspotenziale ist ein geeignetes Mittel, um die Sicherheit von Netzen und Diensten zu erreichen.

Erforderlichkeit

Die Maßnahme ist erforderlich, da ihr Ziel nicht durch ein anderes, gleich wirksames Mittel erreicht werden kann.

ENTWURF

Für Unternehmen mit normalem Gefährdungspotenzial ist es erforderlich, Bedrohungsanalyseprogramme durchzuführen und im Rahmen der Aufklärung die Endnutzer von Netzen und Diensten über Sicherheitsbedrohungen zu informieren.

Unternehmen mit gehobenem und erhöhtem Gefährdungspotenzial müssen entsprechende Programme und Maßnahmen zur regelmäßigen Unterrichtung der Nutzer über Sicherheitsbedrohungen umsetzen; Unternehmen mit erhöhtem Gefährdungspotenzial müssen darüber hinaus diese Maßnahmen regelmäßig überprüfen und aktualisieren.

Angemessenheit

Bei der Maßnahme handelt es sich um Informationsmechanismen, die weder in finanzieller noch in personeller Hinsicht unangemessen sind. Insbesondere sind die Maßnahmen auch hier an die jeweiligen Gefährdungspotenziale angepasst. Die Maßnahme ist angemessen, da der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht. Durch die Abstufung der Eingriffstiefe in der Ausgestaltung der Sicherheitsziele wurde dieser Interessenabwägung Rechnung getragen. Unternehmen aus der Kategorie a) müssen nur weniger einschneidende Maßnahmen zur Erreichung des Sicherheitsziels umsetzen. In Anbetracht des höheren Gefährdungspotenzials, das von Unternehmen der Kategorien b) und c) für die Gewährleistung der Sicherheit von Netzen und Diensten ausgeht, ist diesen Unternehmen auch ein schwerwiegenderer Eingriff in ihre Berufsfreiheit zumutbar.

4.10.1 Informationen über Bedrohungen (Threat Intelligence)

Einrichtung und Pflege geeigneter Mechanismen zur Überwachung und Sammlung von Informationen über relevante Bedrohungen für die Sicherheit von Netzen und Diensten.

Schutzmaßnahmen:

a)

- Durchführung einer regelmäßigen Bedrohungsanalyse

b)

- Umsetzung eines Prozesses zur Aufklärung und Analyse von Bedrohungen (z.B. Bedrohungsanalysesoftware)
- Regelmäßige Überprüfung und Aktualisierung des eingeführten Bedrohungsanalyseprozesses

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

4.10.2 Unterrichtung der Nutzer über Bedrohungen

ENTWURF

Die Nutzer sind über besondere und bedeutende Sicherheitsbedrohungen für das Netz oder den Dienst, die sich auf die Nutzer auswirken können, zu informieren. Den Nutzern sind Maßnahmen mitzuteilen, welche diese zum Schutz der Sicherheit ihrer Kommunikation ergreifen können.

Schutzmaßnahmen

a)

- Unterrichtung der Nutzer von Telekommunikationsnetzen und -diensten über besondere und erhebliche Sicherheitsbedrohungen für das Netz oder den Dienst, die sie betreffen können und über mögliche Abhilfemaßnahmen

b)

- Umsetzung von Maßnahmen/Verfahren zur regelmäßigen Unterrichtung der Nutzer über Sicherheitsbedrohungen für das Netz oder den Dienst, die sie betreffen könnten

c)

- Regelmäßige Überprüfung und Aktualisierung der Maßnahmen/Verfahren zur regelmäßigen Information der Nutzer über Sicherheitsbedrohungen für das Netz oder den Dienst, die sie betreffen könnten

5. Festlegung von zusätzlichen Einzelheiten und Maßnahmen für 5G-Netze

Das nachfolgende Kapitel 5 richtet sich an Betreiber öffentlicher Mobilfunknetze der 5. Generation („5G-Netz"). „5G-Netz" im Kontext des Kataloges ist die Gesamtheit aller Netzinfrastrukturelemente und Technologien, die die Implementierung und Umsetzung des 5G-Standards[32] einschließlich der jeweiligen Betriebsarten (s.u.) im Rahmen der europäischen 5G-Harmonisierung ermöglicht. Die Implementierung des 5G-Standards unterliegt den rechtlich bindenden Harmonisierungs- und Regulierungsentscheidungen.

Für 5G-Netze sind Architekturoptionen[33] für die Betriebsarten 5G Non-Standalone (5G NSA) und 5G Standalone (5G SA) definiert, die einzeln, nebeneinander oder dynamisch konfigurierbar das Netz oder Teilnetze bilden.

Neben den durch die 3GPP spezifizierten Funkzugangsnetzen können weitere Zugangsnetze (Non-3GPP-Access und Open-RAN)[34] in ein 5G-Netz integriert werden und können damit Teil des 5G-Netzes im Kontext des Kataloges werden. Sofern diese Zugangsnetze bzw. Komponenten davon vom 5G-Netzbetreiber bereitgestellt werden, gelten die Regelungen des Kataloges der Sicherheitsanforderungen entsprechend für diese Zugangsnetze bzw. den entsprechenden Komponenten.

5.1 Bestimmung von kritischen Komponenten

Komponenten, die teilweise oder in vollem Umfang die nachfolgend festgelegten kritischen Funktionen realisieren, müssen im Sicherheitskonzept als kritische Komponenten identifiziert und dokumentiert werden.

ENTWURF

Kritische Komponenten i. S. v. § 2 Abs. 13 S. 1 Nr. 3 Buchstabe b BSIG dürfen von einem Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial nur eingesetzt werden, wenn sie vor dem erstmaligen Einsatz von einer anerkannten Zertifizierungsstelle überprüft und zertifiziert wurden (§ 165 Abs. 4 TKG).

Die nachfolgende Tabelle (Abbildung 1: Liste der festgelegten kritischen Funktionen, § 167 Abs. 1 Nr. 2 TKG) wurde von BNetzA, BSI und BfDI gemeinsam erstellt. Für die Erstellung wurde der Stand der Technik weitestgehend berücksichtigt. Die Liste wird gemeinsam kontinuierlich aktualisiert, insbesondere, wenn sich wesentliche Voraussetzungen verändert haben.

Die nachfolgende Liste bezieht sich auf 5G-Netzwerkkomponenten sowie die zum 5G-Netzbetrieb notwendigen Systeme. Entsprechend sind 4G-Netzwerkkomponenten und auch die ausschließlich zum Betrieb von 4G-Netzen notwendigen Systeme ausdrücklich von der Liste ausgenommen.

---

[32] 3GPP Release 15 ff.

[33] In der 3GPP Standardisierung und der GSMA werden diese Optionen mit 1, 2, 3, 3a, 3x, 4, 4a, 5, 6, 7, 7a, 7x, 8 und 8a bezeichnet und finden sich in 3GPP RP-161266, 5G architecture options – full set, Joint RAN/SA meeting, 14.06.2016 und der 3GPP TR 38.801.

[34] Für Non-3GPP-Access (trusted, untrusted, wireline) siehe u.a. ETSI TS 123 501 und ETSI TS 123 401/402

Kategorie		Funktion
A	Core network functions (Kernnetzfunktionen) [1)]	• Authentifizierungs-, Roaming- und Sitzungsverwaltungsfunktionen für Endnutzer • Datentransportfunktionen für Endnutzereinrichtungen • Zugriffsrichtlinienverwaltung • Registrierung und Autorisierung von Netzwerkdiensten • Speicherung von Endnutzer- und Netzwerkdaten • Verbindung mit Mobilfunknetzen von Drittanbietern • Exposition der Kernnetzfunktionen gegenüber externen Anwendungen • Zuordnung von Endgeräten zu Netzwerk-Slices
B	Network functions virtualization (NFV), Management and network orchestration (MANO)	• Management und Orchestrierung virtualisierter Netzwerkfunktionen
C	Management systems and supporting services	• Sicherheitsfunktionen des Management-Systems • Zertifikatsverwaltung
D	Radio Access Network (RAN)	• 5G-RAN-Management • Funktionen der gNodeB
E	Transport and transmission functions	• 5G-spezifische Sprach- und Datentransportfunktionen in der Backbone Infrastruktur / Rechenzentren
F	Internetwork exchanges	• IP-Netzwerk außerhalb der MNO-Räumlichkeiten (Netzwerkdienste von Dritten) • Firewall Infrastruktur beim Übergang zu Fremdnetzen
1) unabhängig vom Ort der Realisierung innerhalb des 5G-Netzes (z.B. eine Realisierung im RAN oder MEC)		

Quelle: Bundesnetzagentur

Abbildung 1: Liste der festgelegten kritischen Funktionen, § 167 Abs. 1 Nr. 2 TKG

ENTWURF

Als Auslegungshilfe zur Liste der kritischen Funktionen sei auf folgende Ergänzungen verwiesen:

Kategorie A - Core network functions (Kernnetzfunktionen)

Grundlegend sind alle im 3GPP-Architekturmodell beschriebenen Core-Funktionen kritisch. Weiterführend können auch nicht-3GPP spezifizierte Funktionen kritische Kernnetzfunktionen darstellen. Deshalb müssen bei der praktischen Ableitung für das jeweilige Netz Ergänzungen vorgenommen werden.

Beispielhaft werden zu den einzelnen Anstrichen der Liste der kritischen Funktionen in Kategorie A die folgenden Funktionen dem Core zugeordnet:

- Authentifizierungs-, Roaming- und Sitzungsverwaltungsfunktionen für Endnutzer
    - Access and Mobility Management Function (AMF),
    - Session Management Function (SMF),
    - Authentication Server Function (AUSF),
    - Unified Data Management (UDM),

    - Security Edge Protection Proxy (SEPP)
- Datentransportfunktionen für Endnutzereinrichtungen
    - User Plane Function (UPF),
    - Access and Mobility Management Function (AMF)
- Zugriffsrichtlinienverwaltung
    - Policy Control Function (PCF),
    - Unified Data Management (UDM)
- Registrierung und Autorisierung von Netzwerkdiensten
    - Network Repository Function (NRF)
- Speicherung von Endnutzer- und Netzwerkdaten
    - Unified Data Repository (UDR),
    - Unstructured Data Storage Function (UDSF),
    - Service Communication Proxy (SCP),
    - Network Data Analytics Function (NWDAF)
- Verbindung mit Mobilfunknetzen von Drittanbietern
    - Security Edge Protection Proxy (SEPP)
- Exposition der Kernnetzwerkfunktionen gegenüber externen Anwendungen
    - Network Exposure Function (NEF),
    - Application Function (AF)
- Zuordnung von Endgeräte zu Netzwerk-Slices
    - Network Slice Selection Function (NSSF),
    - Network Slice Admission Control Function (NSACF),
    - Network Slice-specific and SNPN Authentication and Authorization Function (NSSAAF)

ENTWURF

- Sichere Verbindung zu Zugangsnetzwerken anderer Standards
  - Non-3GPP Interworking Function (N3IWF),
  - Trusted Non-3GPP Gateway Function (TNGF)

Kategorie B - Network functions virtualization (NFV), Management and network orchestration (MANO)

Funktionen der MANO ermöglichen das allumfassende Management und die Orchestrierung der VNF und CNF in der NFV-Architektur. Die MANO instanziiert die Netzwerkservices durch Automatisierung, Bereitstellung und Koordination von Workflows zu den Virtualized Infrastructure Managern (VIM) und VNF-Managern. Weiterhin verbinden die MANO-Funktionen die NFV-Architektur mit den vorhandenen Operating Support Systems (OSS) / Business Support Systems (BSS).

Ferner zählen dazu auch die Managementfunktionen für die Infrastruktur virtualisierter bzw. containerisierter Managementfunktionen.

Kategorie C - Management systems and supporting service

ENTWURF

Auf alle Management-Systeme (Management-Systeme zur Sicherheit des Gesamt-Systems und aller Teilsysteme) sind starke Angriffsszenarien vorhanden. Deshalb ist die Absicherung dieser Systeme ein wichtiger Sicherheitsfaktor (Zugriffe, Rollen, Absicherung des Systems selbst etc.).

In diese Kategorie fallen alle Managementfunktionen, die nicht bereits in Kategorie B oder Kategorie D benannt sind. Beispielhaft können genannt werden: Elementmanager des Kernnetzes und des Transportnetzes.

Kategorie D - Radio Access Network (RAN)

Unter 5G-RAN-Management sind alle Management-Systeme für die verwalteten Komponenten mit RAN-Funktionalität zu verstehen, unabhängig davon, an welcher Stelle im Gesamtsystem das jeweilige Management-System angesiedelt ist. Das 5G-RAN-Management beinhaltet dementsprechend alle Systemfunktionalitäten, die RAN-Komponenten über Schnittstellen steuern und kontrollieren können. Dies umfasst auch alle Funktionalitäten, um Komponenten des RAN (via AI oder ML) intelligent und adaptiv zu gestalten.

Beispielhaft beinhaltet das 5G-RAN-Management:

- Alle Netzwerk-Management-Systeme zur Steuerung des RAN (bspw. Performancemanagement und Sicherheitsmanagement)

- Site-Management-RAN (Integrität, Perimeter, Verfügbarkeit, etc.)
- Steuerung und Parametrisierung der gNodeB
- Zugangssteuerung und Interfaces vom Core zum RAN
- Priorisierung von Kryptoalgorithmen im RAN
- RAN-Konfigurationsdaten-Management und Interfaces

Darüber hinaus sind alle Funktionen des gNodeB als kritische Funktion einzuordnen. Zusätzliche Funktionen in RAN Architekturen, die auf dem 3GPP Standard aufbauen oder alternativ verwendet werden, wie zum Beispiel Open RAN, können ebenfalls kritische Funktionen enthalten.

Kategorie E - Transport and transmission functions

5G-spezifische Sprach- und Datentransportfunktionen in der Backbone Infrastruktur des Mobilfunknetzbetreibers und Rechenzentren des Mobilfunknetzbetreibers umfassen Funktionen des Transports und der Übertragung von Daten (umgesetzt z.B. in Routern, Switches).

ENTWURF

Als Rechenzentren des Mobilfunknetzbetreibers werden alle Rechenzentren angesehen, in denen die kritischen Funktionen ausgeführt werden. Sprach- und Datentransportfunktionen des Zugangsnetzes fallen nicht hierunter.

Kategorie F - Internetwork exchange

Der Peripherieschutz spielt eine zentrale Rolle bei der Absicherung von Übergängen zwischen der Netzwerkinfrastruktur des MNO und Fremdnetzen. Diese Schnittstellen stellen einen potenziellen Schwachpunkt dar, da hier unterschiedliche Netzwerkinfrastrukturen mit potenziell divergierenden Sicherheitsstandards aufeinandertreffen.

Es geht daher um alle Übergänge zu anderen Netzwerkinfrastrukturen außerhalb der tatsächlichen Hoheit des MNO. Gegenstand der Betrachtung ist die jeweilige Schnittstelle zum Fremdnetz insbesondere die Firewall-Infrastruktur beim Übergang zum Fremdnetz. Das Fremdnetz ist nicht Betrachtungsgegenstand. Hier greifen die dortigen Sicherheitskonzepte. Werden in diesem Zusammenhang Erfüllungsgehilfen in Anspruch genommen, so ist über rechtlich-vertragliche Regelungen die Beachtung aller einschlägigen Schutzmaßnahmen sicherzustellen.

Beispielhaft für Peripherieschutz können benannt werden:

- Nutzung von IP-Netz-Anbietern
- IPX Provider

- Roaming Hubs
- Edge Computing
- Internet Exchange Points
- Direktes Peering mit anderen Providern
- Hosted SEPP

Ergänzend zu den Firewall-Systemen sind hier ebenfalls IDS/IPS zu benennen die ungewöhnliches Verhalten oder signaturbasierte Bedrohungen erkennen und aktiv verhindern können.

ENTWURF

5.2 Prozess zur Identifizierung von kritischen Komponenten im betriebenen Netz

Betreiber öffentlicher 5G-Mobilfunknetze müssen einen Prozess für die Identifizierung von kritischen Komponenten einführen und umsetzen, basierend auf den Vorgaben in diesem Kapitel.

Zur Identifizierung von kritischen Komponenten ist die Liste der kritischen Funktionen zu nutzen. Der hier beschriebene Prozess verfolgt das Ziel, eine konsistente Anwendung durch alle Netzbetreiber zu erreichen.

Der Prozess integriert sich in den Gesamtprozess zur Erstellung eines Sicherheitskonzeptes gemäß § 166 Abs. 1 Nr. 3 TKG.

Der Prozess zur Identifizierung und der damit verbundenen Zertifizierung von kritischen Komponenten, wie hier beschrieben, ist unabhängig zu sehen von der Pflicht der Umsetzung der Schutzmaßnahmen aus dem Kapitel Festlegung grundlegender Einzelheiten der zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen unter Berücksichtigung der verschiedenen Gefährdungspotenziale, § 167 Abs. 1 S. 1 Nr. 1 TKG. Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial können ihre Verpflichtung zur Identifikation von kritischen Komponenten nicht durch den Einsatz von mitigierenden Maßnahmen umgehen, da diese Maßnahmen nur das Risiko eines Sicherheitsvorfalls reduzieren, jedoch nicht die der Komponente innewohnende Kritikalität beeinflussen.

Nachfolgend werden die einzelnen Schritte zur Identifizierung kritischer Komponenten beschrieben:

ENTWURF

Schritt 1: Identifizierung der Komponenten des Netzes

Nach Beschreibung des Netzes und der Bestimmung des Gefährdungspotenzials gemäß Kapitel Bestimmung von Gefährdungspotenzialen sind für die Netze mit erhöhtem Gefährdungspotenzial alle im Netz vorhandenen Komponenten zu ermitteln.

Die Identifizierung der Komponenten des Netzes erfolgt durch den Netzbetreiber. Dieser Schritt erlaubt dem Netzbetreiber, eine Anpassung auf dessen individuelle Netzarchitektur vorzunehmen. Es sind grundsätzlich alle im Netz vorhandenen Komponenten zu betrachten, unabhängig davon, ob kritische Funktionen realisiert sind oder nicht.

Schritt 2: Identifizierung von kritischen Komponenten mittels kritischer Funktionen

Nachdem alle relevanten Komponenten des Netzes festgelegt wurden, können anhand der Ausführungen in Kapitel 5.1 die Komponenten identifiziert werden, welche kritische Funktionen realisieren. Wenn eine Komponente eine kritische Funktion teilweise oder in vollem Umfang realisiert, so ist diese Komponente grundsätzlich als kritische Komponente zu bewerten.

5.3 Zertifizierung von kritischen Komponenten

Kritische Komponenten im Sinne von § 2 Abs. 13 BSIG dürfen nach § 165 Abs. 4 TKG von einem Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial nur eingesetzt werden, wenn sie vor dem erstmaligen Einsatz von einer anerkannten Zertifizierungsstelle überprüft und zertifiziert wurden. Die Zertifizierung der kritischen Komponenten hat auf Grundlage der TR-03163 des BSI zu erfolgen.

Sollten zum Zeitpunkt des erstmaligen Einsatzes einer kritischen Komponente keine Möglichkeiten zur Zertifizierung verfügbar sein oder der Einsatz vor der Stichtagsregelung (siehe nachfolgendes Unterkapitel) erfolgen, so müssen pflichtige Netzbetreiber und Diensteerbringer beim Einsatz kritischer Komponenten geeignete und angemessene technische Vorkehrungen und sonstige Maßnahmen zur Gefahrenabwehr treffen.

Die Produktzertifizierung gibt Anforderungen an die Einsatzumgebung bzw. an den sicheren Betrieb von Produkten vor. Nur durch die Einhaltung dieser zum Zertifikat gehörenden Vorgaben kann ein zertifikatskonformer Betrieb der Komponente gewährleistet werden.

5.3.1 Übergangsregelung zur Zertifizierung von kritischen Komponenten

Hinsichtlich der Anforderungen zum Einsatz zertifizierter kritischer Komponenten gilt die folgende Übergangsregelung bis zum unten bestimmten Stichtag:

Stichtag

ENTWURF

Als Stichtag für die jeweilige kritische Komponente gilt spätestens der letzte Tag des 24. Monats, nachdem die Zertifizierung des Produktes, zu dem die jeweilige kritische Komponente gehört, nach TR-03163 des BSI erstmals möglich ist, frühestens aber der 01.01.2026. Für die Möglichkeit der Zertifizierung bedarf es sowohl der Veröffentlichung der TR-03163, wie auch der Verfügbarkeit produktbezogener Anforderungsdokumente. Die Veröffentlichung der TR-03163 und der Verweis auf die entsprechenden Anforderungsdokumente mit Benennung des für den Produkttyp geltenden Stichtages erfolgt auf der Webseite des BSI (www.bsi.bund.de). Für die Berechnung und Einhaltung des Stichtages ist es unerheblich, wenn die Dokumente für die Zertifizierung (TR-03163 oder die entsprechenden Anforderungsdokumente) ausgetauscht oder aktualisiert werden.

Einsatz von Bestandskomponenten bis zum Stichtag

Bis zum Ablauf des Stichtages ist der erstmalige Einsatz von zuvor nicht von einer anerkannten Zertifizierungsstelle überprüften und zertifizierten kritischen Komponente („Bestandskomponente“) ohne Zertifizierung zulässig.

Die Zertifizierungspflicht bezieht sich somit auf den erstmaligen Einsatz einer einzelnen kritischen Komponente nach dem Stichtag. Dies gilt auch dann, wenn Typ und Art des erstmaligen Einsatzes einer kritischen Komponente dem der Bestandskomponente entspricht.

Bereits im Einsatz befindliche Bestandskomponenten müssen nicht nachträglich zertifiziert werden.

5.4 Diversität

Bei Planung und Aufbau der Netze sind „Monokulturen“ durch den Einsatz von Komponenten unterschiedlicher Hersteller nach Möglichkeit zu vermeiden. Diese Hersteller sollten voneinander unabhängig und auch nicht von einer dritten Stelle abhängig sein. Insbesondere kritische Komponenten sollten aufgrund der realisierten Netztopologie nicht von einem einzelnen Hersteller kritischer Komponenten abhängig sein. Netze sind topologisch so zu gestalten, dass die Diversität auch bei sensiblen, d.h. besonders schützenswerten Netzfunktionen und Netzelementen, gegeben ist. Bei Fortentwicklung des Standes der Technik sollte unter Einhaltung technischer Standards die Interoperabilität von Schnittstellen von Netzkomponenten vorhanden sein, um die Diversität weiter auszubauen.

Es sind Maßnahmen zu erarbeiten, welche die kurzfristige Nichtverfügbarkeit von Komponenten eines Herstellers kompensieren, um die Funktionsfähigkeit des Netzes aufrechtzuerhalten.

ENTWURF

5.5 Technische Maßnahmen für die Sicherheit in 5G-Netzen

5G sieht Verbesserungen der Sicherheitseigenschaften im Vergleich zu den Vorgängergenerationen vor.

Der Standard sieht hier mehrere Optionen vor, um einen Betrieb konform zu verschiedenen staatlichen Regulierungen zu ermöglichen. Die Auswahl oder Aktivierung erfolgt gemäß den regulatorischen Vorgaben, oder nach Wahl des jeweiligen Netzbetreibers, wenn keine nationale Regulierung oder andere gesetzliche Rahmenbedingungen vorhanden sind.

Für die relevanten Verpflichteten dieser Allgemeinverfügung stellen die folgenden Maßnahmen sicher, dass eine Aktivierung dieser Eigenschaften in allen öffentlichen 5G-Netzen erfolgt.

5.5.1 Schutz der Identität und Privatheit der Teilnehmer

Die Identität des Nutzers ist vor Offenlegung zu schützen, um eine Verfolgung und Identifizierung des Nutzers zu verhindern. Die geheimen Authentisierungsinformationen und das kryptografische Schlüsselmaterial sind in angemessener Weise zu schützen.

Legitimer Zweck

Der legitime Zweck ist es, die Identität der Teilnehmer, die Vertraulichkeit sowie die Authentisierungsinformationen und das kryptografische Schlüsselmaterial vor Offenlegung zu schützen.

Geeignetheit

ENTWURF

Die Festlegung und Umsetzung von spezifischen technischen Maßnahmen ist ein geeignetes Mittel, um die Identität der Teilnehmer, die Vertraulichkeit und die Authentisierungsinformationen zu schützen, hierfür sind insbesondere Schutzmaßnahmen in Form von Verschlüsselung geeignet. Die Festlegung und Umsetzung von Maßnahmen zum Schutz des kryptografischen Schlüsselmaterials selbst, ist ein geeignetes Mittel, um eine wirksame Verschlüsselung zu gewährleisten.

Erforderlichkeit

Die Maßnahme ist erforderlich, wenn ihr Ziel nicht durch ein anderes, gleich wirksames Mittel erreicht werden kann.

Bei der beschriebenen Maßnahme zur Subscription Permanent Identifier (SUPI) / Subscription Concealed Identifier (SUCI)-Verschlüsselung handelt es sich um ein grundlegendes Sicherheitsmerkmal der 5G-Technologie, um insbesondere die Vertraulichkeit der Teilnehmeridentität auf der Luftschnittstelle zu schützen[35] [36]. Teilnehmeridentitäten stellen die Basis für das Erbringen des Dienstes dar und deren Vertraulichkeit ist unumgänglich für das Erreichen der oben beschriebenen Sicherheitsziele.

[35] https://www.nccoe.nist.gov/sites/default/files/2022-04/nist-5G-sp1800-33b-preliminary-draft.pdf

[36] https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Security%20in%205G%20Specifications.pdf

Die beschriebene Maßnahme zur Authentisierung und Schlüsselableitung wurde bereits in der dritten Mobilfunkgeneration (3G) eingeführt und dient unter anderem der Absicherung vor Betrug an den Mobilfunkbetreibern. Damit liegt diese Maßnahme auch im Eigeninteresse der Betreiber.

Die beschriebene Maßnahme zum Schutz der Verschlüsselungsinformationen schützt die Vertraulichkeit der Kommunikation aller Nutzer eines Betreibers, indem das für die Verschlüsselung der Kommunikation verwendete kryptografische Material sicher verwahrt wird. Sollte dieses bekannt werden, kann ein Angreifer jede Kommunikation seines Opfers entschlüsseln. Auch aufgezeichnete Daten können nachträglich entschlüsselt werden.

In einem High-Level/Hardware Security Module ist das kryptographische Material manipulationsresistent, fälschungsgeschützt und zugriffssicher abgelegt.

Um die Auswirkungen auf die Performance durch kryptografische Rechenoperationen zu minimieren, kann ein High-Level/Hardware Security Module (HSM), das für besonders wertvolle sicherheitsrelevante Informationen (Master-Keys, Schlüssel von globaler Bedeutung etc.) und für sehr hohe Performance-Anforderungen konzipiert ist, verwendet werden.

Die beschriebene Maßnahme zur regelmäßigen Erneuerung der Kurzzeit-Benutzerkennung schützt die Identität und Informationen zur Position des Nutzers auf der Luftschnittstelle. Damit ist diese Maßnahme zusammen mit der SUPI/SUCI-Verschlüsselung ein wirksamer Schutz vor Tracking durch Signalisierungsdaten auf der Luftschnittstelle. Im ETSI 5G Standard sind für die meisten Fälle, in denen die 5G Global Unique Temporary Identifier (5G-GUTI) erneuert werden sollte, bereits verpflichtende Erneuerungen vorgeschrieben gemäß.

ENTWURF

Nach dem "periodic registration update" besteht im Gegensatz zu anderen Events, zu denen die 5G-GUTI gesendet wird, keine Verpflichtung zur Erneuerung, wird allerdings im Standard empfohlen gemäß[37]. "periodic registration update" wird regelmäßig durchgeführt, die Periode ist frei wählbar. Wenn die Erneuerung nicht ausgeführt wird, kann dies zu Rückschlüssen auf die Identität und Position des Nutzers führen[38].

Andere Maßnahmen, außer den hier beschriebenen, zur Erreichung des Schutzziels gibt es nach aktuellem Kenntnisstand nicht.

Angemessenheit

Die Maßnahme ist angemessen, wenn der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht.

Die Kosten für die Maßnahme zur SUPI/SUCI-Verschlüsselung stehen nicht außer Verhältnis zum damit bezweckten Schutz der Vertraulichkeit der Kommunikation. Insbesondere sind hinreichend Geräte auf dem Markt verfügbar, die den Vorgaben entsprechen. Die technische Voraussetzung zu dieser Vorgabe ist bereits

[37] https://www.nccoe.nist.gov/sites/default/files/2022-04/nist-5G-sp1800-33b-preliminary-draft.pdf

[38] https://fight.mitre.org/techniques/FGT5012.003/

von allen Herstellern implementiert, die standardkonform mit ETSI TS 133.501 Abs. 5.2.5 + C.3.4.1 sind, da der Standard eine verpflichtende Umsetzung und optionale Aktivierung der Maßnahme vorsieht. Der Verpflichtete muss die Maßnahme im Idealfall lediglich aktivieren.

Die Maßnahme wird bereits teilweise ausgerollt. Des Weiteren hat bereits ein namhafter Endgerätehersteller den Support von Einwahlen in das 5G SA Netz unterbunden, wenn keine SUPI-Verschlüsselung stattfindet.

Die GSMA als internationale Interessenvertretung der Mobilfunkbetreiber empfiehlt ebenfalls die Nullverschlüsselung nicht zu nutzen[39]. Im Bericht[40] zur Sicherheit von 5G ist eine der grundsätzlichen Empfehlungen der ENISA, die Nullverschlüsselung zu vermeiden.

Die beschriebene Maßnahme zur Authentisierung und Schlüsselableitung wurde zumindest teilweise bereits in 3G angewendet.

Die GSMA als internationale Interessenvertretung der Mobilfunkbetreiber empfiehlt die Unterstützung von MILENAGE und TUAK[41].

Der mit dieser Maßnahme zum Schutz der Verschlüsselungsinformationen verbundene Aufwand für die Verpflichteten steht auch nicht außer Verhältnis zum damit verfolgten Zweck.

Im Bericht[42] zur Sicherheit von 5G ist eine der grundsätzlichen Empfehlungen der ENISA, die hier aufgeführte Maßnahmen zur sicheren Authentisierung und Schlüsselableitung und zum Schutz der Verschlüsselungsinformationen umzusetzen.

ENTWURF

Auch liegt die Umsetzung dieser Maßnahme zum Schutz des kryptografischen Materials im Eigeninteresse der Betreiber.

Die technische Voraussetzung zur regelmäßigen Erneuerung der Kurzzeit-Benutzerkennung ist bereits von allen Herstellern implementiert, die standardkonform mit ETSI TS 133.501 Abs. 6.12.3 sind. Der Verpflichtete muss die Maßnahme im Idealfall lediglich aktivieren.

Da die Erneuerung bereits in anderen Fällen, wie Registration Request message des Typen "initial registration", "mobility registration update", sowie Service Request, Verlassen des 5GMM-IDLE Zustands[43], stattfindet und somit die Kosten einer Umsetzung in diesem weiteren Fall gering sind, stehen die Kosten der Maßnahme nicht außer Verhältnis zu dem erreichten Nutzen.

---

[39] https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2022/09/FS.35-v3.0.pdf

[40] https://www.enisa.europa.eu/publications/security-in-5g-specifications

[41] https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2022/09/FS.35-v3.0.pdf

[42] https://www.enisa.europa.eu/publications/security-in-5g-specifications

[43] ETSI TS 133.501 **Fehler! Linkreferenz ungültig.**

Verschlüsselung der permanenten Benutzerkennung

Die permanente Benutzerkennung Subscription Permanent Identifier (SUPI) soll wann immer möglich nicht im Klartext, sondern als Subscription Concealed Identifier (SUCI) verschlüsselt übertragen werden.

Schutzmaßnahmen:

- Der Betreiber muss die Verschlüsselung der SUPI zur SUCI für alle Verbindungen und Verbindungsversuche zwischen Endgeräten mit einer für sein eigenes Netz provisionierten USIM und einem 5G-Kernnetz sicherstellen
- Eine Verschlüsselung mit dem NULL-Schema bietet keinen Schutz für die Teilnehmer und ist daher nicht zulässig, außer beim Vorliegen zwingender gesetzlicher Gründe oder regulatorischer Vorgaben
- Die Verwendung des Profils A basierend auf Curve25519 gemäß [3GPP TS 33.501] Anhang C.3.4.1 wird empfohlen

Sichere Authentisierung und Schlüsselableitung

Für Algorithmen zur Authentisierung und Schlüsselableitung sind evaluierte und geeignete, öffentlich untersuchte Algorithmen zu verwenden.

Schutzmaßnahmen:

ENTWURF

- Die Verwendung der öffentlich analysierten Algorithmen MILENAGE ([3GPP TS 35.205]) zusammen mit den dort genannten „Default Parameter“ oder TUAK ([3GPP TS 35.231]) wird empfohlen (siehe auch GSMA Official Document FS.35 - Security Algorithm Deployment Guidances Version 4.0)
- Für grundsätzliche Anforderungen an Algorithmen sei auf die Technische Richtlinie BSI TR-02102-1 "Kryptographische Verfahren: Empfehlungen und Schlüssellängen" verwiesen

Schutz der Verschlüsselungsinformationen

Als Vertrauensanker ("Root of trust") für die Sicherheitsfunktionen im Netzwerk muss das verwendete kryptographische Material (Schlüssel und Algorithmen) manipulations- und einbruchsicher zentral gespeichert bzw. ausgeführt werden.

Schutzmaßnahme:

- Der Betreiber muss sicherstellen, dass die persistenten Schlüssel und die Verschlüsselungsalgorithmen im Kernnetz manipulations- und einbruchsicher zentral gespeichert bzw. ausgeführt werden und dass nur kryptographisch geeignete Zufallszahlengeneratoren verwendet werden
- Die Verwendung eines High-Level/Hardware Security Modules (HSM) wird empfohlen

Regelmäßige Erneuerung der Kurzzeit-Benutzerkennung

Zum Schutz gegen Ausspähen ist die Kurzzeit-Benutzerkennung für den Netzwerkzugang in regelmäßigen Abständen zu erneuern.

Schutzmaßnahmen:

- Der Betreiber muss sicherstellen, dass die 5G-Kernnetzfunktion AMF auch im Fall „periodic registration update“ die Kurzzeit-Benutzerkennung 5G-GUTI erneuert und an das Teilnehmergerät sendet (siehe [3GPP TS 33.501] 6.12.3)
- Der 3GPP Standard empfiehlt in [3GPP TS 24.501] (T3512) eine Periode von 54 Minuten. Soweit technisch möglich, soll diese Periodendauer nicht überschritten werden.
- Der Betreiber muss sicherstellen, dass die 4G-Kernnetzfunktion Mobility Management Entity (MME) für die Erneuerung der GUTI analog dazu konfiguriert ist (siehe [3GPP TS 33.401] GUTI, Tracking Area Update (TAU))

5.5.2 Schutz der Vertraulichkeit der Nutz- und Signalisierungsdaten

Nutz- und Signalisierungsdaten zwischen dem Nutzer und dem Netzwerk sind vor unbefugtem Zugriff zu schützen.

Schutzmaßnahmen:

ENTWURF

- Der Betreiber muss die Vertraulichkeit der Nutz- und Signalisierungsdaten (User and Control Plane) zwischen dem Teilnehmerendgerät und dem Netzwerk durch geeignete Verschlüsselung sicherstellen (User Plane und Control Plane auf dem Access Stratum; Control Plane auf dem Non-Access Stratum)
- Die Auswahl des Algorithmus 128-NEA2 bzw. 128-EEA2 wird empfohlen ([3GPP TS 33.501] D.2.1.3 bzw. 3GPP TS 33.401] B.1.3.), solange keine Algorithmen mit größerer Schlüssellänge standardisiert sind
- Die Nutzung des NEA0 oder EEA0 (Null-Verschlüsselung / Klartext ohne Verschlüsselung) ist nur beim Vorliegen zwingender technischer Gründe oder regulatorischer Vorgaben gestattet

Legitimer Zweck

Der legitime Zweck ist es, die Vertraulichkeit der Nutz- und Signalisierungsdaten sicherzustellen.

Geeignetheit

Die Festlegung und Umsetzung von Maßnahmen der Verschlüsselung ist ein geeignetes Mittel, um die Vertraulichkeit der Nutz- und Signalisierungsdaten sicherzustellen.

Erforderlichkeit

Die Maßnahme ist erforderlich, wenn ihr Ziel nicht durch ein anderes, gleich wirksames Mittel erreicht werden kann. Andere Maßnahmen, außer den hier beschriebenen, zur Erreichung des Schutzziels gibt es nach aktuellem Kenntnisstand nicht.

Die beschriebene Maßnahme schützt die Vertraulichkeit der Daten und die Privatsphäre des Nutzers[44]. Ausnahmen sind gemäß Standard für den Notruf möglich, da dieser auch ohne vorherige Registrierung im Netz erfolgen kann.

Die GSMA als internationale Interessenvertretung der Mobilfunkbetreiber empfiehlt die Nutzung der Nullverschlüsselung NEA0 und EEA0 zu verbieten. Als Ausnahme wird neben Notrufen von einem nicht registrierten Gerät ein regulatorisches Verschlüsselungsverbot von staatlicher Seite aufgeführt[45]. Im Bericht zur Sicherheit von 5G ist eine der grundsätzlichen Empfehlungen der ENISA die hier aufgeführte Maßnahme umzusetzen. Dabei soll mindestens 128-NEA1 verwendet werden oder ein besserer Algorithmus. Ebenso wird die Nutzung im Standard in TS 133 501 Absatz 5.3.2 der ETSI empfohlen, wo immer die Regulierung es zulässt. Die Ausnahme für den nicht registrierten Notruf ist in TS 133 501 Absatz 10.2.2 im Standard beschrieben.

Angemessenheit

Die Maßnahme ist angemessen, wenn der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht.

Die Kosten für die Maßnahme stehen nicht außer Verhältnis zum damit bezweckten Schutz der Vertraulichkeit der Kommunikation. Insbesondere sind hinreichend Geräte, die in öffentlichen Netzen von Nutzern verwendet werden, auf dem Markt verfügbar, die den Vorgaben entsprechen. Die technische Voraussetzung zu dieser Vorgabe ist bereits von allen Herstellern implementiert, die ETSI (TS 133.501 Abs. 5.3.2) konform sind. Der Verpflichtete muss die Maßnahme im Idealfall lediglich aktivieren.

ENTWURF

5.5.3 Schutz der Integrität der Nutz- und Signalisierungsdaten

Die Integrität der Nutz- und Signalisierungsdaten im Datenverkehr zwischen dem Nutzer und dem Netzwerk ist sicherzustellen.

Schutzmaßnahmen:

- Der Betreiber muss die Integrität der Nutz- und Signalisierungsdaten (User Plane Data und Control Plane) zwischen dem Teilnehmerendgerät und dem Netzwerk durch eine geeignete Integritätssicherung gewährleisten
- Die Verwendung des Algorithmus 128-NIA2 bzw.128-EIA2 wird empfohlen ([3GPP TS 33.501] D.3.1.3 bzw. 3GPP TS 33.401] B.2.3.), solange keine Algorithmen mit größerer Schlüssellänge standardisiert sind
- Die Integritätssicherung muss auch bei voller Datenrate (full-rate) aktiviert sein, sobald die Unterstützung der Integritätssicherung mit voller Rate (full-rate) vom Teilnehmerendgerät signalisiert wird
- Die Nutzung des NIA0 oder EIA0 (Null-Verschlüsslung/Klartext ohne Verschlüsselung) ist nur beim Vorliegen zwingender technischer Gründe oder regulatorischer Vorgaben gestattet

[44] https://www.enisa.europa.eu/publications/security-in-5g-specifications

[45] https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2022/09/FS.35-v3.0.pdf

Legitimer Zweck

Der legitime Zweck ist es, die Integrität der Nutz- und Signalisierungsdaten sicherzustellen.

Geeignetheit

Die Festlegung und Umsetzung von Maßnahmen der Integrität ist ein geeignetes Mittel, um die Vertraulichkeit der Nutz- und Signalisierungsdaten sicherzustellen. Auch bietet die Nutzung einer Nullverschlüsselung keinerlei Schutz und stellt damit keine hinreichende Alternative zur Maßnahme dar.

Erforderlichkeit

Die Maßnahme ist erforderlich, wenn ihr Ziel nicht durch ein anderes, gleich wirksames Mittel erreicht werden kann. Andere Maßnahmen, außer den hier beschriebenen, zur Erreichung des Schutzziels gibt es nach aktuellem Kenntnisstand nicht.

Die beschriebene Maßnahme schützt die Integrität der Nutz- und Signalisierungsdaten und verhindert somit eine Kompromittierung und Veränderung der Daten. Damit werden auch verschiedene Man-in-the-Middle-Angriffe unterbunden[46] [47].

Die GSMA als internationale Interessenvertretung der Mobilfunkbetreiber empfiehlt die Nutzung der Nullverschlüsselung NIA0 und EIA0 zu verbieten. Als Ausnahme wird neben Notrufen von einem nicht registrierten Gerät ein regulatorisches Verschlüsselungsverbot von staatlicher Seite aufgeführt[48]. Im Bericht zur Sicherheit von 5G ist eine der grundsätzlichen Empfehlungen der ENISA die hier aufgeführte Maßnahme umzusetzen. Dabei soll mindestens 128-NIA1 verwendet werden oder ein besserer Algorithmus. Ebenso wird die Nutzung im Standard[49] empfohlen, wo immer die Regulierung es zulässt.

ENTWURF

Angemessenheit

Die Maßnahme ist angemessen, wenn der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht.

Die Kosten für die Maßnahme stehen nicht außer Verhältnis zum damit bezweckten Schutz der Vertraulichkeit der Kommunikation. Insbesondere sind hinreichend Geräte, die in öffentlichen Netzen verwendet werden, auf dem Markt verfügbar, die den Vorgaben entsprechen. Die technische Voraussetzung zu dieser Vorgabe ist bereits von allen Herstellern implementiert, die ETSI (TS 133.501 Abs. 5.3.3) konform sind. Der Verpflichtete muss die Maßnahme im Idealfall lediglich aktivieren.

Darüber hinaus führt die Maßnahme zu keiner erheblichen Minderung der Qualität des erbrachten Dienstes. Wissenschaftliche Betrachtungen der Performanz der einzelnen Algorithmen hinsichtlich des Durchsatzes

---

[46] https://www.enisa.europa.eu/publications/security-in-5g-specifications

[47] https://doi.ieeecomputersociety.org/10.1109/SP.2019.00006

[48] https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2022/09/FS.35-v3.0.pdf

[49] ETSI TS 133.501

und der Latenz ergaben keine signifikanten Auswirkungen auf den Durchsatz. Bei der Latenz waren vertretbare Auswirkungen erkennbar[50]. Der Standard TS 133.501 Abs. 5.3.3 schreibt verpflichtend die Unterstützung des Integritätsschutzes vor.

5.5.4 Schutz des Zugriffs auf Netzwerkfunktionen im 5G-Kernnetz

Um den unerlaubten Zugriff auf Netzwerkfunktionen und die Ausbreitung einer Kompromittierung von einer auf weitere Netzwerkfunktionen zu verhindern (lateral movement), ist das 5G-Kernnetz entsprechend zu schützen.

Schutzmaßnahme:

- Der Betreiber muss die Zugriffe auf die von den Netzwerkfunktionen angebotenen Services durch die Autorisierung mindestens mittels des OAuth2.0 Protokolls gemäß [3GPP TS 33.501] 13.4.1 sicherstellen.

Legitimer Zweck

Der legitime Zweck ist es, die Funktionen im 5G-Kernnetz vor unbefugtem Zugriff zu schützen.

Geeignetheit

Die Festlegung und Umsetzung von Maßnahmen der sicheren Authentisierung nach aktuellen Standards ist ein geeignetes Mittel, um die Funktionen im 5G-Kernnetz vor unbefugtem Zugriff zu schützen. Die Maßnahme dämmt die Ausbreitung von Angriffen durch "lateral movement" innerhalb des Kernnetzes ein, in dem nur Anfragen von autorisierten Komponenten verarbeitet werden. Bei fehlender Autorisierung kann ein Angreifer Zugriff auf beliebige Netzwerkfunktionen bekommen und damit Informationen abgreifen oder Zugriff auf Services blockieren[51].

ENTWURF

Erforderlichkeit

Die Maßnahme ist erforderlich, wenn ihr Ziel nicht durch ein anderes, gleich wirksames Mittel erreicht werden kann. Zur Sicherung gegen unerlaubte Zugriffe ist Autorisierung einzusetzen.

Die enthaltene Maßnahme ist erforderlich, da ihr Ziel nicht durch ein anderes, gleich wirksames Mittel erreicht werden kann. Wenn das Kernnetz nicht durch OAuth 2.0 abgesichert wäre, würde ein Angriff durch „lateral movement“ nicht verhindert werden und größere Risiken leichter eintreten.

Angemessenheit

Die Maßnahme ist angemessen, wenn der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht.

---

[50] https://dl.acm.org/doi/pdf/10.1145/3558482.3581777

[51] https://www.enisa.europa.eu/publications/security-in-5g-specifications

Die technische Voraussetzung zu dieser Vorgabe ist bereits von allen Herstellern implementiert, die ETSI (TS 133.501 Abs. 13.4.1) konform sind. Der Verpflichtete muss die Maßnahme im Idealfall lediglich aktivieren.

Der Schutz vor lateraler Ausbreitung ist ebenfalls eine Sicherheitsforderung in anderen Branchen mit ähnlicher Technologie (z. B. Cloudanbieter). OAuth 2.0 ist ein etabliertes Verfahren

Im Bericht zur Sicherheit von 5G ist eine der grundsätzlichen Empfehlungen der ENISA, die hier aufgeführte Maßnahme umzusetzen.

5.5.5 Schutz der SBA-Kommunikation im 5G-Kernnetz

Durch die offene und verteilte Service Based Architecture (SBA) des 5G-Kernnetzes erhöht sich das Risiko, dass die Kommunikation zwischen Netzwerkfunktionen durch eine kompromittierte Funktion, Schnittstelle oder Ausführungsumgebung angegriffen werden kann. Die Integrität und Vertraulichkeit der Kommunikation im Kernnetz ist auf angemessene Weise zu schützen.

Schutzmaßnahmen:

- Der Betreiber muss den Schutz der Kommunikation im 5G-Kernnetz gemäß [3GPP TS 33.501] 13.1 gewährleisten
- Der Betreiber muss sicherstellen, dass „Mutually authenticated TLS / HTTPS“ genutzt wird, sofern die Netzwerksicherheit nicht auf andere, im Schutzniveau gleichwertige Weise gewährleistet wird[52]

ENTWURF

Legitimer Zweck

Der legitime Zweck ist es, die Kommunikation im 5G-Kernnetz vor unbefugtem Zugriff zu schützen.

Geeignetheit

Die Festlegung und Umsetzung von Maßnahmen zur Sicherstellung der Vertraulichkeit sind ein geeignetes Mittel, um die Kommunikation im 5G-Kernnetz vor unbefugtem Zugriff zu schützen.

Erforderlichkeit

Die Maßnahme ist erforderlich, wenn ihr Ziel nicht durch ein anderes, gleich wirksames Mittel erreicht werden kann.

Die beschriebene Maßnahme bietet eine Absicherung gegen Angriffe auf Netzwerkfunktionen innerhalb des Kernnetzes.

Ist mTLS aktiviert, bietet es Absicherung ohne auf physische Grenzen, wie die Lokalisation der darunterliegenden Hardware, achten zu müssen und damit mehr Freiheit bei der Lastverteilung. Die Lokalität einer Funktionalität ist nicht mehr relevant. "Lateral movement", d.h. die Ausbreitung von Angriffen wird

[52] Diese Anforderung gilt vorrangig zu Absatz 3 und Note 2 in [3GPP TS 33.501] 13.1.0

auch nach dem Eindringen in einen Sicherheitsperimeter erschwert. Dieses Prinzip wird als "Defense in depth" bezeichnet.

Physischer Schutz durch bauliche Maßnahmen als Alternative zur Absicherung der einzelnen Netzwerkfunktionen, wie es der Standard[53] zulässt, reicht nicht aus, da durch verschiedene agile Betriebsszenarien, wie automatische Lastverteilung auf räumlich getrennte Rechenzentren diese Maßnahme keine Wirksamkeit besitzt. Des Weiteren verliert ein physischer Schutz seine Wirkung, falls ein Angriff erfolgreich in einen Sicherheitsperimeter eindringen kann. Außerdem kann es aufgrund der Virtualisierung schneller zu Vermischungen von verschiedenen Sicherheitsperimetern kommen.

Angemessenheit

Die Maßnahme ist angemessen, wenn der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht.

Ist die Kommunikation im Kernnetz unverschlüsselt, besteht u.a. auch die Möglichkeit, durch kompromittierte Funktionen oder Interfaces auf sensitive Informationen wie Sitzungsschlüssel oder die Langzeit-Benutzerkennung zuzugreifen, weshalb die Kosten für die Maßnahme nicht außer Verhältnis zum damit bezweckten Schutz der Vertraulichkeit und Integrität der Kommunikation stehen. Außerdem zeigen wissenschaftliche Betrachtungen, dass die zusätzliche Latenz im Betrieb vernachlässigbar ist. Für den initialen Verbindungsaufbau ist die Latenz höher. Die zusätzliche CPU-Last und Speicherauslastung ist ebenfalls vernachlässigbar[54].

ENTWURF

TLS ist eine bekannte und für den Webseitenaufruf im Internet über das https-Protokoll seit vielen Jahren etablierte Absicherung, siehe [55] und [56] für Statistik. Außerdem ist es für virtualisierte Umgebungen ein etabliertes Verfahren. Im Bericht zur Sicherheit von 5G ist eine der grundsätzlichen Empfehlungen der ENISA die hier aufgeführte Maßnahme umzusetzen.

Die technische Voraussetzung zu dieser Vorgabe ist bereits von allen Herstellern implementiert, die ETSI (TS 133.501 Abs. 13.1) konform sind. Der Verpflichtete muss die Maßnahme im Idealfall lediglich aktivieren.

5.5.6 Schutz der Kommunikation zwischen Zugangsnetzwerk und Kernnetz sowie zwischen Zugangsnetzwerken

Die Vertraulichkeit der Kommunikation zwischen den Zugangsnetzwerken und dem Kernnetzwerk sowie zwischen Zugangsnetzwerken ist vor unerlaubtem Zugriff zu schützen.

Zu den Zugangsnetzwerken zählen in diesem Zusammenhang die Funkzugangsnetzwerke für 4G- und 5G- sowie Non-3GPP-Zugangsnetzwerke, sofern diese Teile des 5G-Netzes sind.

---

[53] ETSI TS 133.501

[54] https://mediatum.ub.tum.de/doc/1740121/1740121.pdf

[55] https://www.ericsson.com/en/blog/2020/8/security-for-5g-service-based-architecture

[56] https://w3techs.com/technologies/details/ce-httpsdefault

Schutzmaßnahmen:

- Der Betreiber muss die Kommunikation zwischen Zugangsnetzwerken und dem Kernnetz durch Transportverschlüsselung absichern
- Der Betreiber muss die Kommunikation zwischen Zugangsnetzwerken durch Transportverschlüsselung absichern
- Für die Transportverschlüsselung ist die Nutzung einer kryptographischen Lösung verpflichtend

Anmerkung: Kryptographische Verfahren im Sinne der Empfehlungen der Technischen Richtlinie TR-02102 des BSI

Legitimer Zweck

Der legitime Zweck ist es, die Kommunikation zwischen Zugangsnetzwerk und Kernnetz sowie zwischen Zugangsnetzwerken vor unbefugtem Zugriff zu schützen.

Geeignetheit

Die Festlegung und Umsetzung von Maßnahmen zur Sicherstellung der Vertraulichkeit sind ein geeignetes Mittel, um die Kommunikation zwischen Zugangsnetzwerk und Kernnetz sowie zwischen Zugangsnetzwerken vor unbefugtem Zugriff zu schützen.

ENTWURF

Erforderlichkeit

Die Maßnahme ist erforderlich, wenn ihr Ziel nicht durch ein anderes, gleich wirksames Mittel erreicht werden kann.

Die beschriebene Maßnahme bietet eine Absicherung gegen Angriffe auf die Integrität und Vertraulichkeit der Kommunikation und verhindert die Kompromittierung und Veränderung von Netzwerkdaten. Man-in-the-Middle Angriffe werden dadurch erschwert.

Gemäß [3GPP TS 33.501] Absätze 9.2, 9.3, 9.4 ist für einige Schnittstellen (N2, N3, Xn) bereits die verpflichtende Absicherung der Integrität, Vertraulichkeit und ein Schutz gegen Replay Attacken vorgeschrieben. Für die Schnittstelle F1-U ist die technische Unterstützung dieser Absicherungen für standardkonforme Produkte verpflichtend umzusetzen, gemäß [3GPP TS 33.501] Absatz 9.8. Mit der verpflichtenden Absicherung der F1-U Schnittstelle wird die Kommunikation des Nutzers ebenfalls vor Angriffen auf Vertraulichkeit und Integrität geschützt.

Non-3GPP Zugangsnetze in der Hoheit des Betreibers sind ebenfalls entsprechend abzusichern, da sich zwar die genutzten Protokolle und grundlegenden Standards unterscheiden, aber die Bewertung hinsichtlich des Risikos ähnlich ist.

Angemessenheit

Die Maßnahme ist angemessen, wenn der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht.

Im Bericht zur Sicherheit von 5G ist eine der grundsätzlichen Empfehlungen der ENISA, die hier aufgeführte Maßnahme umzusetzen.

Die Nutzung von IPSec ist eine etablierte Maßnahme, die zur Absicherung der Kommunikation zwischen Zugangsnetz und Kernnetz genutzt wird.

5.5.7 Schutz der Kommunikation innerhalb eines Zugangsnetzwerks

Sind die Funktionen eines Zugangsnetzwerks verteilt realisiert, ist die Kommunikation zwischen diesen Funktionen zu schützen, unabhängig davon, ob es sich um standarisierte oder proprietäre Schnittstellen handelt.

Zu den Zugangsnetzwerken zählen in diesem Zusammenhang die Funkzugangsnetzwerke für 4G- und 5G- sowie Non-3GPP-Zugangsnetzwerke, sofern diese Teile des 5G-Netzes sind.

Schutzmaßnahmen:

- Der Betreiber muss sicherstellen, dass die im jeweiligen Standard unterstützten Sicherheitsfunktionen aktiviert sind. Dazu zählen:
  - gegenseitige Authentisierung
  - Integritätsschutz
  - Replay-Schutz
  - Vertraulichkeitsschutz

  Stehen dabei mehrere Optionen zur Verfügung, wird die Auswahl der Option mit dem höchsten Schutzniveau empfohlen.
- Bei Schnittstellen ohne spezifizierte Sicherheitsvorgaben oder bei proprietären Schnittstellen innerhalb des Zugangsnetzes ist der Betreiber verpflichtet, eigene Maßnahmen zur Absicherung umzusetzen

ENTWURF

Legitimer Zweck

Der legitime Zweck ist es, die Kommunikation innerhalb eines Zugangsnetzwerks zu schützen.

Geeignetheit

Die Festlegung und Umsetzung von Schutzmaßnahmen zur Aktivierung der Sicherheitsfunktionen sind ein geeignetes Mittel zum Schutz der Kommunikation innerhalb eines Zugangsnetzwerks.

Erforderlichkeit

Die Maßnahme ist erforderlich, wenn ihr Ziel nicht durch ein anderes, gleich wirksames Mittel erreicht werden kann.

Die Maßnahme dient dem Schutz der Integrität und Vertraulichkeit der Kommunikation über die Schnittstellen im RAN, insbesondere auch im Open RAN. Eine fehlende Absicherung könnte zur Kompromittierung und Veränderung von Netzwerkdaten führen und erleichtert Man-in-the-Middle-Angriffe.

Fehlende Authentifizierung und Autorisierung kann dazu führen, dass Maßnahmen zum Schutz der Integrität und Vertraulichkeit wirkungslos werden.

Eine Vielzahl von Risiken und Bewertungen hinsichtlich der Vollständigkeit der in den Konsortialspezifikationen der O-RAN Alliance vorgeschriebenen Sicherheitsmaßnahmen sind in der vom BSI veröffentlichten Open RAN Risikoanalyse[57] und im Threat Model[58] der O-RAN Alliance dargestellt. Deutlich erkennbar ist in der Risikoanalyse, dass die verpflichtend umzusetzenden Maßnahmen nicht ausreichend sind. Hinsichtlich der optionalen Maßnahmen hat die O-RAN Alliance durchaus Verbesserungen seit der Veröffentlichung der Studie umsetzen können. Weitergehende Verpflichtungen zu Aktivierung von Sicherheitsmaßnahmen wurden allerdings nicht in die Spezifikationen aufgenommen.

Auch proprietäre Schnittstellen, für die keine standardisierten Sicherheitsmaßnahmen vorliegen, sind entsprechend abzusichern, da sich zwar die genutzten Protokolle und grundlegenden Standards unterscheiden, aber die Risikobewertung ähnlich ist.

Angemessenheit

ENTWURF

Die Maßnahme ist angemessen, wenn der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht.

Die Weiterentwicklung des O-RAN Systems nach dem Prinzip "Funktionalität vor Sicherheit" erfordert die Ausdehnung der Maßnahme auch auf neue Schnittstellen und proprietäre Schnittstellen, für die noch keine Sicherheitsmaßnahmen von der O-RAN Alliance spezifiziert wurden. Eine Absicherung von Schnittstellen ist in jedem Fall erforderlich, auch wenn keine Vorgaben in den Spezifikationen existieren sollten. Diese ist nötig, um Angriffe zu verhindern oder zu erschweren.

5.5.8 Schutz der Kommunikation zwischen dem 5G-Kernnetz und Nicht-5G-Netzwerkelementen

Das 5G-Kernnetz kann mit einem 4G-Kernnetz und weiteren Nicht-5G-Netzelementen, wie dem IP Multimedia Subsystem (IMS), über Schnittstellen verbunden sein, die die Protokolle DIAMETER oder GPRS Tunneling Protocol (GTP) verwenden.

Die Kommunikation über Schnittstellen zwischen dem 5G-Kernnetz und Nicht-5G-Netzwerkelementen ist in angemessener Weise zu schützen.

Schutzmaßnahmen:

---

[57] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/5G/5GRAN-Risikoanalyse.html?nn=1019518

[58] https://specifications.o-ran.org/download?id=697

- Der Betreiber muss die Sicherheit von Schnittstellen mit GTP oder dem DIAMETER-Protokoll gemäß [3GPP TS 33.501] 9.5 gewährleisten
- Der Betreiber muss eine Absicherung durch eine kryptographische Lösung sicherstellen, sofern die Sicherheit nicht auf andere, im Schutzniveau gleichwertige Weise gewährleistet wird. Die Verwendung von Network Domain Security for IP based protocols (NDS/IP) oder (Datagram) Transport Layer Security ((D)TLS) wird empfohlen[59].

Legitimer Zweck

Der legitime Zweck ist es, die Kommunikation zwischen dem 5G-Kernnetz und weiteren Nicht-5G-Netzelementen zu schützen.

Geeignetheit

Die Festlegung und Umsetzung von Standards zum Schutz der Schnittstellen sind ein geeignetes Mittel, um die Sicherheit der Kommunikation zwischen dem 5G-Kernnetz und Nicht-5G-Netzwerkelementen zu schützen.

Erforderlichkeit

Die Maßnahme ist erforderlich, wenn ihr Ziel nicht durch ein anderes, gleich wirksames Mittel erreicht werden kann.

ENTWURF

Die Maßnahme dient dem Schutz der Integrität und Vertraulichkeit der Kommunikation. Andere Absicherungen, wie physische Absicherung durch bauliche Maßnahmen, sind auf Grund verteilter Rechenzentren und Virtualisierung nicht ausreichend.

DIAMETER und GTP sind ältere Standards. Für beide sind Sicherheitsmängel und Angriffsmöglichkeiten bekannt.

Die GSMA als Interessenvertretung der Mobilfunkbetreiber dokumentiert in [60] weitreichende Sicherheitsmängel, welche unter anderem auf unverschlüsselte Verbindungen zurückzuführen sind.

Angemessenheit

Die Maßnahme ist angemessen, wenn der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht.

Die technische Voraussetzung für die Vorgabe ist bereits von allen Herstellern implementiert, die ETSI (TS 133.501 Abs. 9.5) konform sind. Der Verpflichtete muss die Maßnahme im Idealfall lediglich aktivieren.

---

[59] Diese Anforderungen gelten vorrangig zu Absatz 2 Satz 1 in [3GPP TS 33.501] 9.5

[60] https://www.gsma.com/membership/wp-content/uploads/2018/09/Diameter-2018-eng.pdf

5.5.9 Schutz der Roaming Signalisierung

Mobilfunknetze verschiedener Betreiber sind untereinander verbunden, u.a. für Roaming (National, International, Disaster Roaming). Die Roaming-Signalisierung zu weiteren Mobilfunknetzen ist in angemessener Weise zu schützen.

Schutzmaßnahmen:

- Einrichtung und regelmäßige Überprüfung eines Prozesses zur Dokumentation der Roaming-Partner[61] (inklusive „Disaster Roaming"-Partner)
- Der Betreiber muss den Signalisierungsverkehr zu weiteren Mobilfunknetzbetreibern (Public Land Mobile Network/PLMN) vor Zugriffen durch Dritte schützen
- Der Betreiber muss sicherstellen, dass die eigenen SEPP-Komponenten so konfiguriert sind, dass im Zuge des N32-c Sitzungsaufbaus für direkte N32-Verbindungen nur die TLS Variante für N32-f angeboten wird
    - Für indirekte N32-Verbindungen[62] ist die N32-c Verbindung beim Roaming-Partner und nicht beim Vermittler[63] zu terminieren. In diesem Fall muss die PRINS (ALS) Variante für N32-f angeboten werden.
    - Bei Roaming-Partnern, bei denen es nicht möglich ist, eine direkte N32-c (nach TS 33.501) Verbindung aufzubauen, sind die Gründe hierfür zu dokumentieren

ENTWURF

Legitimer Zweck

Die Maßnahme ist angemessen, wenn der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht.

Die technische Voraussetzung für die Vorgabe ist bereits von allen Herstellern implementiert, die ETSI (TS 133.501 Abs. 13.2) konform sind. Der Verpflichtete muss die Maßnahme im Idealfall lediglich aktivieren.

Geeignetheit

Die Festlegung und Umsetzung von Standards zum Schutz der Schnittstellen und Anwendung von Verschlüsselung sind ein geeignetes Mittel, um die Sicherheit der Kommunikation für die Roaming-Signalisierung zu schützen.

Erforderlichkeit

---

[61] Als Roaming-Partner gilt jeder andere Mobilfunkanbieter, der den Teilnehmern (Subscribern) des Betreibers mittels Roaming den Netzzugang ermöglicht

[62] Eine Roaming-Verbindung gilt als indirekt, wenn mindestens ein weiteres Unternehmen, beispielsweise als "Vermittler", den Signalisierungsverkehr im Auftrag des Betreibers oder im Auftrag des Roaming Partners auswertet und/oder in diesen eingreift.

[63] Ein Vermittler kann beispielsweise ein Roaming Hub, ein IPX Provider oder ein Anbieter von "Roaming Value Added Services" sein

Die Maßnahme ist erforderlich, wenn ihr Ziel nicht durch ein anderes, gleich wirksames Mittel erreicht werden kann.

Die Roaming-Signalisierung ist eine wesentliche Neuerung von 5G zur Reduzierung des bisherigen Angriffspotentials von Roaming[64]. Dies funktioniert u.a. durch Nachverfolgung von Angriffen durch die Mobilfunkbetreiber. Die Maßnahmen zur Dokumentation, sind Grundsatzanforderungen die in erster Linie dazu dienen, Transparenz zu schaffen. Diese ist Voraussetzung dafür, die potenzielle Angriffsfläche zu ermitteln, die durch die Notwendigkeit entsteht, ein globales Roaming anzubieten sowie die SMS-Zustellung durch Nicht-Mobilfunkanbieter (z.B. Registriercodes um Onlineservices freizuschalten). Die Ermittlung von Angriffsflächen sollte auch im Eigeninteresse des Mobilfunkbetreibers liegen.

Die Übertragungswege und Sicherheitsmaßnahmen auf diesen Übertragungswegen sind ausschlaggebend dafür, in welchem Ausmaß die Endnutzer des Heimnetzwerkes Gefahren, die durch Dritte weltweit ausgehen, ausgesetzt sind. Bestimmte dieser Gefahren existieren unabhängig davon, ob die Endnutzer ihr Heimnetz verlassen oder nicht. Eine schlecht gesicherte Roaming-Infrastruktur kann dazu genutzt werden, Nutzer anzugreifen, die gar nicht im Ausland roamen.

Ohne Informationen über diese Übertragungswege und die an der Vermittlung beteiligten Unternehmen kann der Mobilfunknetzbetreiber nicht angemessen auf bestimmte Vorfälle reagieren, beispielsweise wenn bekannt wird, dass ein bestimmter Vermittler unzureichende Sicherheitsmaßnahmen ergreift und so unautorisierte Dritte Zugriff auf die Roaming-Signalisierung erhalten. Auch die Dokumentation der Zwecke (N32Purpose) dient dazu, die potenzielle Angriffsfläche zu ermitteln und im Bedarfsfall geeignete Gegenmaßnahmen zu formulieren.

ENTWURF

Angemessenheit

Die Maßnahme ist angemessen, wenn der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht.

Die Maßnahme greift nur im geringen Umfang in die unternehmerischen Freiheiten der Mobilfunkanbieter ein. Die beschriebenen Dokumentationspflichten betreffen nur Informationen, welche den Mobilfunknetzbetreibern bereits vorliegen müssen, um Roaming überhaupt durchführen zu können.

Diese Maßnahme zur Absicherung der Kommunikation über die N32 Schnittstelle wird in der GSMA erheblich vorangetrieben und wurde daher auch als Eigeninteresse des Mobilfunknetzbetreibers bezeichnet, da eine Absicherung von Schnittstellen in jedem Fall stattfinden muss.

5.5.10 Schutz des Remote SIM Provisionings

Der Prozess der Remote SIM Provisionierung (RSP) ist in angemessener Weise zu schützen. Hierzu hat die GSMA ein einheitliches Vorgehen auf Basis von etablierten Industriestandards festgeschrieben.

Schutzmaßnahmen:

---

[64] https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g

- Es dürfen nur nach GSMA SGP.25 bzw. BSI-CC-PP-0100-2018 CC EAL4 + AVA_VAN.5 zertifizierte eUICC Produkte, die in einer GSMA SAS-UP geprüften Umgebung präpersonalisiert wurden, durch die Hintergrundsysteme im Feld mittels RSP[65] bespielt werden. Diese Hintergrundsysteme müssen im Gegenzug mittels GSMA SAS[66]-SM geprüft werden

Legitimer Zweck

Der legitime Zweck ist es, den Prozess der Bereitstellung von Profil-Daten für den Endnutzer zu schützen. Diese Profil-Daten werden auf die eSIM beim Endnutzer aufgespielt.

Geeignetheit

Die Festlegung und Umsetzung von Standards zum Schutz der Prozesse und Schnittstellen sind ein geeignetes Mittel, um die Sicherheit der Kommunikation während der ferngesteuerten Bereitstellung zu schützen.

Erforderlichkeit

Die Maßnahme ist erforderlich, wenn ihr Ziel nicht durch ein anderes, gleich wirksames Mittel erreicht werden kann.

Die schützenswerten Daten sind die Profil-Daten, welche beim Mobilfunknetzbetreiber oder beauftragten Dritten erstellt werden. Diese müssen sicher übertragen werden zum Endgerät und werden in der eSIM gespeichert. Der Kanal für die Übertragung ist dabei abzusichern.

ENTWURF

Andere Maßnahmen, außer den hier beschriebenen, zur Erreichung des Schutzziels gibt es nicht, nach aktuellem Kenntnisstand.

Angemessenheit

Die Maßnahme ist angemessen, wenn der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht.

Die beschriebene Maßnahme ist bereits bei den Mobilfunknetzbetreibern umgesetzt. Durch eine verpflichtende Regulierung entsteht somit kein Mehraufwand. Einer Abweichung von diesen sinnvollen Vorgaben soll vorgebeugt werden.

Die CC-Zertifizierung von eUICC wird aktuell von der Industrie als angemessen akzeptiert, da ein hohes Vertrauensniveau zwischen unterschiedlichen Anbietern der eUICCs (Hersteller) und Nutzern (MNO) erreicht werden muss.

Die in der Maßnahme genannten Dokumente wurden durch die GSMA, die Interessenvertretung der Mobilfunkbetreiber, unter Beteiligung der Mobilfunkbetreiber selbst erarbeitet und getragen

---

[65] GSMA SGP.21, SGP.22, SGP.23-1, SGP.23-2, SGP.23-3, SGP.24

[66] GSMA FS.04, FS.05, FS.08, FS.09, FS.18

5.5.11 Schutz vor Angriffen auf die Ausführungsumgebung bei Virtualisierung und Containerisierung

Virtualisierte (VNF) oder containerisierte (CNF) 5G-Netzwerkfunktionen sind gegen Gefährdungen und Angriffe im Zusammenhang mit der Ausführungsumgebung zu schützen.

Schutzmaßnahmen:

- Die Ausführungsumgebungen von VNF und CNF sind nach dem Stand der Technik abzusichern, hierbei wird die Erfüllung der Anforderungen bei erhöhtem Schutzbedarf gemäß des IT Grundschutzes[67] empfohlen

  Hinweis: Es existieren umfassende Empfehlungen der ETSI zur 5G-spezifischen Absicherung von virtualisierten und containerisierten Umgebungen[68].

Legitimer Zweck

Der legitime Zweck ist es, die virtualisierten (VNF) oder containerisierten (CNF) 5G-Netzwerkfunktionen in ihrer Ausführungsumgebung zu schützen.

Geeignetheit

Die Festlegung und Umsetzung von Standards zum Schutz der Ausführungsumgebung von CNF und VNF ist ein geeignetes Mittel, um die Kommunikation zu und zwischen den entsprechenden Netzwerkfunktionen zu schützen.

ENTWURF

Erforderlichkeit

Die Maßnahme ist erforderlich, wenn ihr Ziel nicht durch ein anderes, gleich wirksames Mittel erreicht werden kann.

Durch eine unzureichende Absicherung der Virtualisierungsschicht und der Container ist das Erreichen der Schutzziele bei Angriffen gefährdet. So beinhalten beispielsweise im Fall von „Kubernetes“ die Standardeinstellungen weitreichende Sicherheitslücken und Angriffsmöglichkeiten[69].

Die Maßnahmen des IT-Grundschutz sind erforderlich, da ihr Ziel nicht durch ein anderes, gleich wirksames Mittel erreicht werden kann. Unternehmen mit erhöhtem Gefährdungspotenzial müssen ganzheitliche Standards umsetzen, diese regelmäßig überprüfen und aktualisieren, um sicherzustellen, dass alle virtualisierten und containerisierten Systeme betrieben und verwaltet werden. Nur durch die Festlegung solcher Strategien im Voraus kann darauf hingewirkt werden, dass die Netze und Dienste jederzeit aufrechterhalten werden.

---

[67] BSI IT-Grundschutz-Bausteine, Edition 2023; Bausteine SYS.1.5 "Virtualisierung" und SYS.1.6 "Containerisierung"

[68] ETSI ("work in progress") NFV_SEC023 und NFV_SEC025

[69] Hacking von Kubernetes in Standardabsicherung: 5G hacking just got a lot more interesting (Karsten Nohl) https://program.mch2022.org/media/mch2022/submissions/8BEFCG/resources/220723.OpenRAN_Security-MCH2022_Karsten_Nohl_yKotUaV.pdf

Die Maßnahmen sind erforderlich, weil Virtualisierung und Containerisierung zentrale Bestandteile moderner Netzwerkfunktionen sind, im Kontext von 5G-Netzwerkfunktionen, da die Angriffsfläche durch fehlende oder mangelhafte Absicherungen erheblich erhöht wird und Sicherheitsvorfälle in solchen Umgebungen schwerwiegende Folgen für die gesamte IT-Infrastruktur haben können.

Angemessenheit

Die Maßnahme ist angemessen, wenn der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht.

Insbesondere schränkt die Maßnahme den Betreiber nicht in der Auswahl der Möglichkeiten zur Absicherung ein.

Es existieren umfassende Empfehlungen u.a. von der ETSI zur Absicherung von virtualisierten und containerisierten Umgebungen[70] [71]. Außerdem empfiehlt die GSMA als Interessenvertretung der Mobilfunkbetreiber in dem Dokument FS.31[72] grundlegende Sicherheitsmaßnahmen zu Virtualisierung und Containern.

Die Maßnahme zur Anwendung des IT-Grundschutz[73] ist angemessen, da der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht. Der geforderte Standard der Absicherung der Ausführungsumgebung orientiert sich an der Bedeutung des öffentlichen 5G-Mobilfunknetzes für das Gemeinwohl in Deutschland. Deshalb ist die Mindestforderung nach der Standard-Absicherung des IT-Grundschutzes angemessen, da die Basisabsicherung als Einstieg zu niedrig gewählt wäre für einen KRITIS-Sektor.

ENTWURF

5.5.12 Schutz bei Nutzung von Virtualisierungs- oder Cloud-Diensten

Bei teilweiser oder vollständiger Nutzung einer Ausführungsumgebung oder von Netzwerkfunktionen Dritter, wie zum Beispiel bei der Nutzung von Public Cloud-Diensten, ist das 5G-Netz gegen die daraus entstehenden Angriffsvektoren und Verfügbarkeitsrisiken abzusichern.

Schutzmaßnahmen:

- Der Betreiber muss durch technische und organisatorische Maßnahmen nachweisen, dass die Vertraulichkeit und Integrität der Teilnehmerdaten und der Kommunikation jederzeit gewährleistet ist

[70] ETSI GS NFV-SEC023 - Container Security Specification
https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58647

[71] ETSI GS NFV-SEC025 - Secure E2E VNF & NS Management
https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=59208

[72] FS.31 GSMA Baseline Security Controls
https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/06/FS.31-Baseline-Security-Controls-v3.0.pdf

[73] BSI IT-Grundschutz-Bausteine, Edition 2023; Bausteine SYS.1.5 "Virtualisierung" und SYS.1.6 "Containerisierung"

- Der Betreiber muss nachweisen, dass bei der Nutzung von Diensten Dritter weder die Verfügbarkeit noch das Sicherheitsniveau des 5G-Netzes herabgesetzt wird
- Falls der Betreiber Funktionen und Daten an Dritte auslagert, die für die Netzadministration und Netzkonfiguration erforderlich sind, muss der Betreiber zusätzlich diese Funktionen und Daten auch in eigener Hoheit vorhalten
- Der Betreiber muss eine Exit-Strategie nachweisen und Verfahren implementieren, die geeignet sind, den teilweisen oder vollständigen Ausfall der Dienste eines Dritten unverzüglich, ohne Verletzung gesetzlicher oder regulatorischer Verfügbarkeitsanforderungen und gegebenenfalls auch ohne Mitwirkung dieses Dritten, zu kompensieren
- Es wird empfohlen, keine Auslagerung an Dritte vorzunehmen, die nicht ausschließlich nationalem und europäischem Recht unterliegen
- Es wird empfohlen, dem Dritten keine Nutzung von Infrastrukturstandorten außerhalb der EU zu gestatten und diese idealerweise auf Deutschland zu beschränken. Diese Empfehlung gilt auch für den tatsächlichen Arbeitsort aller Administratoren

Legitimer Zweck

Der legitime Zweck ist es, bei teilweiser oder vollständiger Auslagerung der 5G-Ausführungsumgebung an Dritte, insbesondere bei Nutzung von Rechenzentren oder Cloud-Diensten, die nicht unter alleiniger Kontrolle des Netzbetreibers liegen, diese zu schützen.

ENTWURF

Geeignetheit

Die Festlegung und Umsetzung von Maßnahmen zum Schutz der 5G-Ausführungsumgebung, auch unter Nutzung von Dritten, um die Vertraulichkeit und Integrität der Kommunikation zu schützen, sind geeignete Mittel.

Erforderlichkeit

Die Maßnahme ist erforderlich, wenn ihr Ziel nicht durch ein anderes, gleich wirksames Mittel erreicht werden kann.

Eine Nutzung von Public Cloud-Diensten ist für den Mobilfunkbetrieb technisch nicht notwendig, sondern ggf. eine betriebswirtschaftliche Entscheidung (Outsourcing). Andere technische Mittel um den legitimen Zweck zu erreichen, sind zum Beispiel durch das Eigenhosting der entsprechenden Netzwerkfunktionen gegeben. Werden die Netzwerkfunktionen allerdings ausgelagert, so sind die Sicherheitsziele nicht mit gleichwertigen Mitteln zu erreichen.

Die Absicherung einer hohen Verfügbarkeit ist ebenfalls durch das Eigenhosting zu erreichen. Entscheidet sich der Betreiber für die Nutzung des Dienstes Dritter, ist vertraglich eine entsprechende Verfügbarkeit, die nicht geringer sein darf als beim Eigenhosting, festzulegen.

Das Vorhalten der Daten und Funktionen in eigener Hoheit trotz Auslagerung an Dritte ist erforderlich zur Absicherung der Verfügbarkeit bei einem „Exit under stress“. Dies gewährleistet die Verfügbarkeit des Netzes

auch wenn die Daten in der Cloud nicht extrahiert werden können und auf diese nicht zugegriffen werden kann. Diese Maßnahme ist erforderlich, um eine Exit-Strategie im Ernstfall auch ausführen zu können.

Eine Exit-Strategie ist erforderlich, da der Betreiber ansonsten die Handlungshoheit über das eigene Netz an den Cloudbetreiber abgibt und somit in dem Maße, in dem Funktionen ausgelagert wurden, vom Cloudbetreiber abhängig ist. Dies gilt hinsichtlich der Verfügbarkeit sowie für die Wirtschaftlichkeit.

Angemessenheit

Die Maßnahme ist angemessen, wenn der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht.

Eine Absicherung hinsichtlich Vertraulichkeit und Integrität ist generell notwendig, da die Vertraulichkeit und Integrität der Teilnehmerdaten bei unzureichender Absicherung vom Cloudbetreiber eingesehen, verändert und weiterverwendet werden können.

Die Verlagerung der Daten in die Cloud darf die Verfügbarkeit gegenüber der Verfügbarkeit im Eigenhosting nicht verschlechtern, ansonsten ist das Eigenhosting zu wählen.

Das Erstellen einer Exit-Strategie inklusive des Vorhaltens der Daten und Funktionen in eigener Hoheit sichern die Verfügbarkeit des Netzes im Fall einer Nichterreichbarkeit der Daten in der Cloud. Mit dieser Maßnahme wird gewährleistet, dass die Verfügbarkeit durch einen Ausfall der Cloud nicht wesentlich verschlechtert wird gegenüber dem Eigenhosting.

ENTWURF

6. Empfehlungen und Hinweise

6.1 Lokales Breitband 26 GHz

Der Zuteilungsinhaber ist für den Schutz seiner Telekommunikationsinfrastruktur vor Angriffen selbst verantwortlich und trägt die Risiken für die Verfügbarkeit seiner Telekommunikationsdienste. Dieser "Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten" kann als Hilfestellung zur Erreichung des Schutzes herangezogen werden; für öffentliche Funknetze ist er verpflichtend.

6.2 Zugrundeliegende Normen, Standards und Guidelines

Die in diesem Dokument beschriebenen Sicherheitsziele und Maßnahmen wurden von bestehenden Normen und Informationsstandards abgeleitet. Diese können verwendet werden, um die Anforderungen des Kataloges umzusetzen. Sie enthalten u. a. Beispiele für Schutzmaßnahmen, Bedrohungsszenarien 5G, und beschreiben Gefährdungen und Maßnahmen im IT-TK-Umfeld.

Die unten angefügte Abbildung gibt eine Übersicht über die zugeordneten Normen, Standards und Guidelines.

ENTWURF

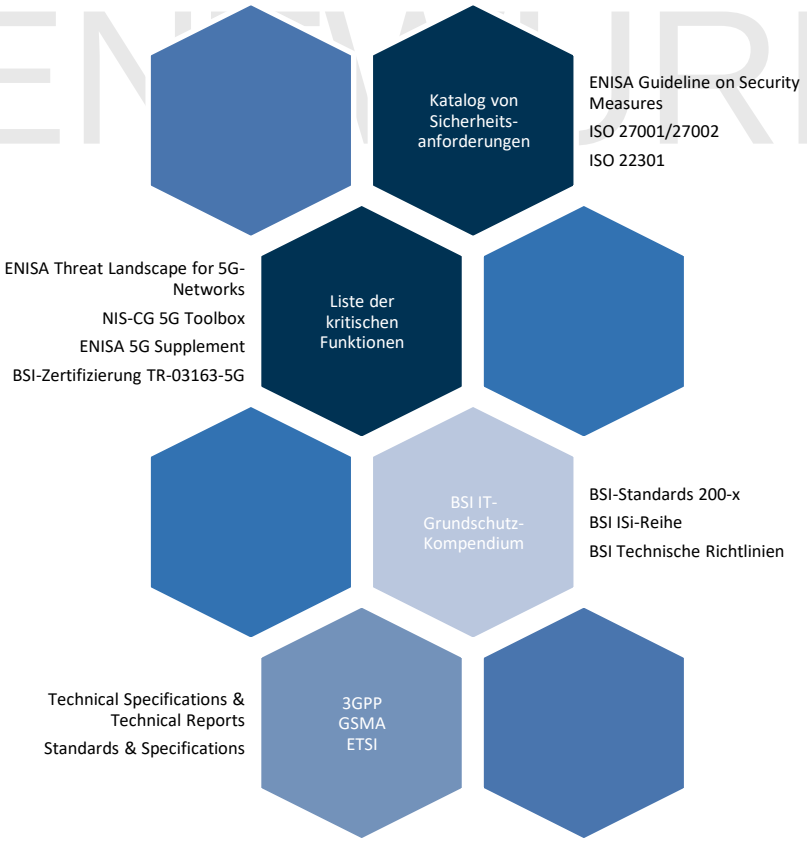

Abbildung 2: Normen, Standards und Guidelines

Glossar

DIAMETER
Authentifizierungs-, Autorisierungs- und Accounting-Protokoll.

gNodeB
Ein „next Generation Node B“ ist die eigentliche 5G-Basisstation, welche Nutzdatentransfer (User Plane) und Signalisierung (Control Plane) für die Kommunikation zum 5G-Teilnehmerendgerät zur Verfügung stellt.

GTP (GPRS Tunneling Protocol)
IP-basiertes Tunnelprotokoll.

N32-c
Control Plane Schnittstelle zwischen SEPPs, zur Durchführung des anfänglichen Handshakes und zur Aushandlung der Parameter, die für die eigentliche N32-Nachrichtenweiterleitung gelten

N32-f
Weiterleitungsschnittstelle zwischen den SEPPs, die für die Weiterleitung der Kommunikation zwischen dem Netzwerk-Funktions-Nutzer (NF service consumer) und dem Netzwerk-Funktions-Bereitsteller (NF service producer) nach Anwendung des Sicherheitsschutzes auf Anwendungsebene verwendet wird.

ENTWURF

PAM
Privileged Access Management, Sicherheitsstrategie um privilegierten Zugriff auf das notwendige Maß zu beschränken

Replay-Schutz
Schutz vor einem Cyber-Angriff, bei dem Netzwerkpakete abgefangen und wiederholt eingespielt werden

SLA
Service-Level-Agreement, eine Vereinbarung über die Qualität und den Preis eines Dienstleistungsvertrags

Abkürzungsverzeichnis

5G NSA	Non-Standalone
5G SA	Standalone
BDSG	Bundesdatenschutzgesetz
BEREC	Body of European Regulators for Electronic Communications (Gremium Europäischer Regulierungsstellen für elektronische Kommunikation)
BfDI	Bundesbeauftragte(r) für den Datenschutz und die Informationsfreiheit
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BR-Drs.	Drucksachen des Deutschen Bundesrates
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung)
BT-Drs.	Bundestagsdrucksache
CER	Critical Entities Resilience
CSA	EU Cybersecurity Act (Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 - Rechtsakt zur Cybersicherheit)
DSGVO	Datenschutz-Grundverordnung
(D)TLS	(Datagram) Transport Layer Security
EKEK	Europäischer Kodex für die elektronische Kommunikation
ENISA	European Agency for Cybersecurity / Agentur der Europäischen Union für Cybersicherheit (vormals European Network, Information Security Agency / Europäische Agentur für Netz und Informationssicherheit)
ETSI	European Telecommunications Standards Institute

ENTWURF

eUICC	embedded Universal Integrated Circuit Card
GTP	GPRS Tunneling Protocol
GSMA	Global System for Mobile Communications Association
GSMA SAS-UP	GSMA Security Accreditation Scheme for Universal Integrated Circuit Card (UICC) Production
GSMA SAS-SM	GSMA Security Accreditation Scheme for Subscription Management
GUTI	Global Unique Temporary Identifier
IT	Informationstechnik
KMU	Kleinstunternehmen sowie kleine und mittlere Unternehmen
MANO	Management and network orchestration
MEC	Multi-access edge computing
MME	Mobile Management Entity
MNO	Mobile Network Operator (Mobilfunknetzbetreiber)
NDS/IP	Network Domain Security for IP based protocols
NF	Network function
NFV	Network functions virtualization
NIS	Netzwerk- und Informationssicherheit
RAN	Radio Access Network
RSP	Remote SIM Provisionierung
SEPP	Security Edge Protection Proxy
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TR	Technische Richtlinie

ENTWURF

C Anhang - Technische Spezifikation für paketvermittelte Netze zum Katalog der Sicherheitsanforderungen

1. Einleitung

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

Ein Überblick der aktuellen Gefährdungen finden sich beispielsweise in den jährlich herausgegebenen Lageberichten des BSI[74] und der ENISA.

Aufgrund dieser spezifischen Gefährdungslage sowie aufgrund der Bedeutung des Internets im geschäftlichen und privaten Bereich sind durch die Betreiber und Anbieter paketvermittelter Netze geeignete Sicherheitsvorkehrungen zu treffen. Der Anhang beschreibt - in Ergänzung der Anforderungen des Hauptteils des Kataloges von Sicherheitsanforderungen nach § 167 TKG (Sicherheitskatalog) – technische Vorkehrungen und sonstige Maßnahmen, die für paketvermittelte Netze (Internet) entsprechend dem jeweiligen Stand der Technik umzusetzen sind. Diese Maßnahmen dienen auch dem Schutz des Fernmeldegeheimnisses bzw. der Verhinderung von Verletzungen des Schutzes personenbezogener Daten.

ENTWURF

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

Die Fokussierung auf technische Aspekte macht es in dem vorliegenden Anhang zum Sicherheitskatalog notwendig, Begriffe zu verwenden, welche zur Beschreibung des Standes der Technik einerseits unerlässlich sind, die andererseits im TKG jedoch keine Verwendung finden. Diese Begriffe werden am Ende des Anhangs in den Begriffsbestimmungen näher erläutert.

Im Anhang werden, wie im Sicherheitskatalog (Kapitel 3), drei Kategorien von Gefährdungspotenzialen unterschieden.

Verpflichtungen in den unterschiedlichen Gefährdungspotenzialen:

- **Normales Gefährdungspotenzial** (im Folgenden mit a bezeichnet): Alle öffentlichen Telekommunikationsnetze und öffentlich zugängliche Telekommunikationsdienste
- **Gehobenes Gefährdungspotenzial** (im Folgenden mit b bezeichnet): Öffentliche Telekommunikationsnetze und öffentlich zugängliche Telekommunikationsdienste, sofern sie für das Gemeinwohl eine größere Bedeutung haben

[74] https://www.bsi.bund.de/lagebericht

- **Erhöhtes Gefährdungspotenzial** (im Folgenden mit c bezeichnet): Öffentliche Telekommunikationsnetze und öffentlich zugängliche Telekommunikationsdienste, sofern sie für das Gemeinwohl eine herausragende Bedeutung haben

ENTWURF

2. Maßnahmen gegen Distributed Denial of Service (DDoS) Angriffe

DDoS-Angriffe können beträchtlichen Schaden verursachen. Die Verpflichteten spielen bei der Mitigation eine zentrale Rolle und tragen dazu bei, das Risiko erfolgreicher DDoS-Angriffe zu verringern und deren Auswirkungen zu reduzieren.

2.1 Ertüchtigung der eigenen Infrastruktur

Viele DDoS-Angriffe ähneln in ihren Symptomen Lastspitzen. Eine einfache Art kleinen und mittleren DDoS-Angriffen erfolgreich zu widerstehen ist daher ausreichende Kapazitäten bereit zu halten.

a)

- Keine verpflichtenden Maßnahmen vorgesehen

b)

- Die Kapazitäten der eigenen Infrastruktur und an Austauschpunkten müssen ausreichend dimensioniert sein um die Verfügbarkeit des Gesamtnetzes im Falle eines DDoS-Angriffes mit kleiner und mittlerer Stärke individuell zu gewährleisten

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

ENTWURF

2.2 Mitigation

Viele DDoS-Angriffe ähneln in ihren Symptomen Lastspitzen. Eine einfache Art kleinen und mittleren DDoS-Angriffen erfolgreich zu widerstehen ist daher ausreichende Kapazitäten bereit zu halten.

a)

- Keine verpflichtenden Maßnahmen vorgesehen

b)

- Zum Schutz der eigenen Infrastruktur sowie der angeschlossenen Kunden muss eine Möglichkeit zur Filterung/Bereinigung des Angriffsverkehrs bestehen

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

2.3 Absicherung ausnutzbarer Systeme

Viele Internetdienste lassen sich für DDoS-Angriffe missbrauchen. Typische Beispiele sind etwa Domain Name System (DNS)- und Network Time Protocol (NTP)-Server, bei denen die Antworten oft um ein Vielfaches größer sind als die Anfragen. Somit lassen sich diese Internetdienste als Verstärker in DDoS-Angriffen ausnutzen.

a)

- Nicht benötigte Dienste müssen deaktiviert werden
- In Ergänzung zu Kapitel 4.4.3 des Sicherheitskatalogs: Der Zugang zu Systemen, die sich prinzipiell als Reflektoren für DDoS-Angriffe nutzen lassen (beispielsweise DNS-Resolver oder NTP-Server), muss auf die angedachten Nutzer eingeschränkt werden
- Systeme, die sich prinzipiell als Reflektoren für DDoS-Angriffe nutzen lassen, müssen derart konfiguriert werden, dass der Verstärkungsfaktor möglichst gering ausfällt (beispielsweise keine Unterstützung „monlist“ bei NTP oder ein kleiner Apex der DNS-Zone)

b)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

ENTWURF

3. Inter-Domain-Routing

Der Austausch von IP-Routing-Informationen ist die Voraussetzung für den Betreiber-übergreifenden Datenfluss. Dieser Austausch erfolgt im Internet über das exterior Border Gateway Protocol (eBGP, im Folgenden BGP).

3.1 Schutz der BGP-Session

Bestehende BGP-Sessions sind die Voraussetzung für den Austausch von Routing-Informationen. Daher kommt dem Schutz der BGP-Sessions eine zentrale Bedeutung zu.

a)

- BGP-Sessions sollten nach gängiger Best-Practice (etwa TCP-AO, GTSM) geschützt werden
- Die einer BGP-Session zugrundeliegende TCP-Session sollte ebenfalls mit den gängigen Best-Practices (etwa ACLs) gegen Angriffe geschützt werden

b)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

ENTWURF

3.2 Bereitstellung von Routing-Informationen

Um falsche Routing-Informationen zu filtern (siehe Anhang, Kapitel 3.3), müssen die eigenen Routing-Informationen dokumentiert werden.

a)

- authentisierte und autorisierte Routing-Informationen müssen in standardisierter Form bereitgestellt werden (beispielsweise mittels ROAs in RPKI)

b)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

3.3 Verhinderung der Weitergabe falscher Routing-Informationen

Die Verbreitung falscher Routing-Informationen kann zu Störungen führen und Angriffe begünstigen.

a)

- Es muss sichergestellt werden, dass ausschließlich diejenigen IP-Präfixe originär in BGP annonciert werden, für die sie als Routen-Ursprung autorisiert sind
- Ein- und ausgehende Routing Annoncierungen der BGP-Nachbarn (außer die Annoncierungen der Transit-Provider) müssen gegen eine authentisierte Quelle (beispielsweise RPKI) geprüft und gefiltert werden [MANRS] [RFC7454]

b)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

3.4 Verhindern von Datenverkehr mit gefälschten Quell-IP-Adressen

Basis für viele Vorfälle und Angriffe ist die Verwendung gefälschter IP-Adressen. Dies lässt sich über die Einrichtung entsprechender Filter eindämmen oder sogar verhindern.

a)

ENTWURF

- Netzwerkbetreiber müssen für ihre Infrastruktur, ihre Endkunden sowie Kundennetze (genauer single-homed stub networks) ein System zur Validierung von Quell-IP-Adressen (source address validation) implementieren und Pakete mit gefälschter Quell-IP-Adresse filtern. [MANRS] [RFC2827] [RFC8704]

b)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

3.5 Bereitstellung aktueller Kontaktinformationen

Die folgenden Anforderungen dienen Netzbetreibern der gegenseitigen Kontaktaufnahme bei Vorfällen:

a)

- Verpflichtete sollten in einer Datenbank (etwa bei der zugehörigen RIR/NIR oder PeeringDB) aktuelle Kontaktinformationen pflegen [MANRS]

b)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

ENTWURF

4. Domain Name System – Resolver

Zur Bereitstellung von interpersonellen Kommunikationsdienstleistungen ist der Betrieb von Systemen zur Namensauflösung (Domain Name System) zwingend notwendig. Weiterhin ist die Bereitstellung von DNS-Resolvern eine zentrale Dienstleistung vieler TK-Betreiber und Diensteanbieter im Internet. Im Internet geht nahezu jedem Kommunikationsvorgang eine Anfrage an das DNS voraus, deshalb ist eine sichere Konfiguration des DNS-Resolvers unerlässlich.

4.1 Technische Voraussetzungen

Für die korrekte Funktion des DNS-Resolvers sind unter anderem folgende technische Voraussetzungen erforderlich:

a)

- DNS-Resolver müssen sich über die Transportprotokolle TCP und UDP ansprechen lassen
- DNS-Resolver müssen EDNS(0) unterstützen [RFC 6891]
- DNS-Resolver müssen die Größe von DNS-Antwortpaketen über UDP auf 1232 Byte begrenzen[75]

b)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

ENTWURF

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

4.2 DNSSEC

Die Sicherheitserweiterung Domain Name System Security Extensions (DNSSEC) ermöglicht es Domaininhabern, DNS-Einträge kryptografisch zu signieren, und DNS-Resolvern diese Signaturen zu validieren. Auf diese Weise lassen sich Integrität und Authentizität der DNS-Einträge sicherstellen.

a)

- DNS-Resolver müssen DNSSEC validieren, sofern die angefragte Domain eine DNSSEC-Konfiguration hat
- DNS-Resolver müssen neben RSA auch die aktuellen kryptografische Verfahren (etwa ECDSA und EdDSA) unterstützen [RFC 9364]

b)

[75] https://www.bsi.bund.de/dok/frag-dns

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

4.3 Cache-Poisoning

Typischerweise speichern DNS-Resolver die Ergebnisse von Anfragen zwischen (caching), um erneute Anfragen schneller direkt aus dem Zwischenspeicher beantworten zu können. Angriffe zur Manipulation bestehender Einträge oder zur Einbringung falscher Einträge in diesem Zwischenspeicher werden als Cache-Poisoning bezeichnet. Zur Erschwerung solcher Angriffe haben sich eine Reihe von Maßnahmen etabliert, die vom DNS-Resolver unterstützt werden müssen.

a)

- DNS-Resolver müssen die Randomisierung des Source Ports unterstützen
- Es sollte sich am DNS-Resolver eine Obergrenze für die Dauer der Zwischenspeicherung (Time to Live, TTL) festlegen lassen
- DNS-Resolver sollten Domain-bezogen die vorzeitige Entfernung von Cache-Einträgen unterstützen (Flushing)

ENTWURF

b)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

4.4 Privacy

DNS-Anfragen können sensible Informationen beinhalten. Zum Schutz dieser Informationen haben sich verschiedene Methoden etabliert:

a)

- DNS-Resolver müssen QNAME Minimization [RFC 9156] unterstützen

b)

- DNS-Resolver sollten eine Möglichkeit für den verschlüsselten Transport unterstützen (beispielsweise DNS-over-QUIC [RFC 9250])

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

ENTWURF

5. Domain Name System - Autoritative DNS-Server

Der für eine bestimmte Domain zuständige Nameserver wird als autoritativer DNS-Server bezeichnet. Er stellt Informationen über den Domainnamen in Form einer DNS-Zone bereit.

5.1 Technische Voraussetzungen

Für die korrekte Funktion des autoritativen DNS-Servers sind unter anderem folgende technische Voraussetzungen erforderlich:

a)

- Autoritative DNS-Server müssen sich über die Transportprotokolle TCP und UDP ansprechen lassen
- Autoritative DNS-Server müssen EDNS(0) unterstützen [RFC 6891]
- Autoritative DNS-Server müssen die Größe von DNS-Antwortpaketen über UDP auf 1232 Byte begrenzen

b)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

ENTWURF

5.2 Schutz vor Ausnutzung

Autoritative DNS-Server können als Werkzeug für DDoS-Angriffe missbraucht werden. Mit den folgenden Maßnahmen lässt sich die Nutzung des DNS-Servers reglementieren.

a)

- Am autoritativen DNS-Server müssen Maßnahmen gegen die Ausnutzung für Amplification-/Reflection-Angriffe getroffen werden, beispielsweise Response Rate Limiting und die Vermeidung fragmentierter Antwortpakete

b)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

5.3 DNSSEC

Die Signierung einer DNS-Zone ermöglicht die Überprüfung der Integrität und Authentizität der bereitgestellten Informationen durch den Empfänger. Dadurch lassen sich Angriffe erkennen und ggf. verhindern. Des Weiteren ist DNSSEC eine zwingende Voraussetzung für weitere Sicherheitsmechanismen (beispielsweise DNS-based Authentication of Named Entities (DANE)).

a)

- Keine verpflichtenden Maßnahmen vorgesehen

b)

- Die Zonen des autoritativen DNS-Servers sollten mit DNSSEC signiert werden. Dies gilt insbesondere für Zonen mit Mail Exchange Resource Records (MX-Records), die auf E-Mail-Server zeigen, sowie die Zonen der E-Mail-Server selbst.
- Autoritative DNS-Server sollten aktuelle kryptografische Verfahren, wie Elliptic Curve Digital Signature Algorithm (ECDSA), implementieren [RFC 9364]
- Betreiber autoritativer DNS-Server sollten die Entwicklung der DNS- und DNSSEC-bezogenen Internetstandards beachten

ENTWURF

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

6. E-Mail-Sicherheit

E-Mail-Diensteanbieter haben zum Schutz sowohl der eigenen als auch anderer E-Mail-Nutzender organisatorische und technische Maßnahmen zum Schutz vor Schadprogrammen, Phishing und Spam umzusetzen.

6.1 Maßnahmen zum Schutz vor Malware und zur Abwehr von Spam und Phishing

Ein wirksamer Schutz vor den verschiedenen Bedrohungen im Kontext von E-Mails lässt sich durch eine Kombination verschiedener Maßnahmen realisieren. Dazu gehört das Scannen ein- und ausgehender E-Mails, verschiedene Methoden der E-Mail-Authentisierung und verschiedene Verfahren der Inhalts-Filterung.

6.1.1 Scan von E-Mails auf Malware (Viren, Würmer, Trojaner) und zu Hinweisen auf Spam oder Phishing

Um die Gefahren von E-Mails mit Schadsoftware und die Auswirkungen von SPAM/Phishing für die Nutzer zu minimieren, sind wirksame Schutzmaßnahmen zu etablieren.

a)

- Scannen von ein- und ausgehenden E-Mails mit einem Virenschutzprogramm
- Prüfen eingehender E-Mails durch:
  - (Reverse-) MX-Records
  - Sender Policy Framework (SPF) und Sender ID
  - Domain Keys Identified Mail (DKIM)

b)

- Domain-based Message Authentication, Reporting and Conformance (DMARC) ist zu nutzen

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

6.1.2 Prüfung eingehender E-Mails mit einem Spam-Filter

Um die Vertrauenswürdigkeit einer E-Mail bzw. eines MTA zu bewerten, sind SPF- und DKIM-Prüfungen nicht hinreichend. Die Prüfung muss daher um Verfahren ergänzt werden, die neben der Authentizität auch die Vertrauenswürdigkeit der Absender prüft.

a)

- Einsatz grundlegender Prüfverfahren (Vertrauenswürdigkeit des Absenders):
  - Allowlisting: E-Mails von bekannten vertrauenswürdigen MTAs werden immer akzeptiert

ENTWURF

- Denylisting: E-Mails von bekannten nicht vertrauenswürdigen MTAs werden immer abgewiesen
- Frequenzanalyse: Versendet ein MTA plötzlich eine große Zahl von E-Mails mit gleichartigen Eigenschaften (z. B. gleiche Größe) deutet dies auf Spam hin. Wird solches Verhalten beobachtet, sind E-Mails des betreffenden MTA zeitlich begrenzt abzuweisen (temporäres Denylisting)
- Suspicious- bzw. Grey-Listing: E-Mails von unbekannten MTAs werden zunächst abgewiesen und erst beim zweiten Zustellversuch akzeptiert (nutzt die Tatsache aus, dass Spam-Systeme i. d. R. keinen zweiten Zustellversuch unternehmen, wenn der Erste abgewiesen wurde)

b)

- Einsatz weiterer Prüfverfahren (automatisierte und datenschutzkonforme Prüfung bestimmter Merkmale des E-Mail-Inhalts):
  - Prüfsummenvergleich: Der Inhalt der E-Mail, z.B. charakteristische Textsequenzen, werden gehasht und mit bekannten Spam-Signaturen verglichen
  - Heuristische Inhaltsanalyse: Der Filter „lernt“ Spam an Hand charakteristischer Textsequenzen (z. B. Begriffe und Schreibweisen usw.) zu erkennen
  - Statistische Inhaltsanalyse: Der Filter erkennt Spam aufgrund der statistischen Verteilung gewisser Stichwörter (Tokens)
  - Provider-/User-Reports: Filterung von Spam, der bereits von anderen TK-Diensteanbietern oder eigenen Usern als solcher erkannt und gemeldet wurde

  Für die Bewertung des Risikos einer potentiellen Spam-E-Mail eignet sich ein Kriteriensystem, welches der E-Mail nach jedem Prüfschritt eine gewisse Punktzahl zuordnet. Überschreitet die Gesamtpunktzahl am Ende einen bestimmten Schwellenwert, so ist die E-Mail als Spam oder Phishing zu bewerten.

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

6.1.3 Maßnahmen gegen Spam-Verbreitung durch Kunden

Um zu verhindern, dass die Rechner von Kunden – z. B. weil sie unwissentlich zum Teil eines Botnetzes geworden sind – unkontrolliert Spam oder Schadsoftware verbreiten, ist die Umsetzung folgender Maßnahmen empfehlenswert:

a)

- E-Mail-Versand nur durch gegenüber dem Mailserver authentisierten Clients
- Wird über Port 25 Spam versendet, ist der Port temporär zu sperren und der Kunde zu informieren

ENTWURF

b)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

6.1.4 Umgang mit verdächtigen Emails

Verdächtige E-Mails können sofort abgelehnt werden oder zunächst in einen dafür vorgesehenen Ordner verschoben werden, sofern der Kunde zugestimmt hat oder entsprechend über die Vorgehensweise informiert wird (siehe Anhang, 6.1.5). Abhängig von der vermuteten Bedrohung und dem Grad der Sicherheit der Bewertung (Confidence) sind angemessene Schutzmaßnahmen zu ergreifen.

a)

- Sicherstellen, dass erkannter Schadcode nicht die Empfänger erreichen z. B. durch folgende Maßnahmen:
- eingehende infizierte E-Mails bereits am Relay abweisen (Echtzeitfilterung)
- eingehende infizierten E-Mails basierend auf den Einstellungen des Kunden isolieren (z.B. durch Verschiebung in einen separaten Ordner)
- bei einer hohen Anzahl von verdächtigen E-Mails aus einer bestimmten Quelle, ist die Verbindung zu dieser Quelle geeignet einzuschränken
- bei einer hohen Anzahl von ausgehenden infizierten E-Mails, ist der Mailversand der betreffenden Accounts vorübergehend zu unterbinden

b)

- Erkannte Spam und Phishing-Versuche sind dem Empfänger geeignet kenntlich zu machen z.B. durch Modifikation des Betreffs und/oder Ablegen in einem gesonderten Ordner

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

6.1.5 Kundenbenachrichtigung

a)

ENTWURF

- Information des Empfängers (respektive bei ausgehenden E-Mails der Sender) darüber, wie mit einer verdächtigen E-Mail verfahren wurde, die nicht bereits am Relay abgewiesen wurde.[76] Darüber hinaus soll der Kunde bereits im Rahmen des Vertragsabschlusses auf diese Vorgehensweise hingewiesen werden.

b)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

ENTWURF

[76] Bei am Relay abgewiesenen E-Mails wird der Absender automatisch informiert und kann dann im Falle eines „false positive“ auch den vorgesehenen Empfänger informieren

6.2 Vertraulichkeit des E-Mail-Verkehrs

Jeglicher Kommunikationsvorgang im Kontext von E-Mails ist, wenn technisch möglich und wirtschaftlich zumutbar, zu verschlüsseln. Dabei ist die Technische Richtlinie TR-02102-2 des BSI anzuwenden.

Im Folgenden ist mit dem Begriff „moderne Transportverschlüsselung“ die Nutzung kryptographischer Verfahren im Sinne der Technischen Richtlinie TR-02102 des BSI[77] gemeint.

a)

- Eingehende Verbindungen MTA zu MTA:
  - Der Anbieter muss anderen Anbietern den Aufbau von Verbindungen über TLS-Verbindungen über STARTTLS ermöglichen. Dabei müssen Algorithmen, die Perfect Forward Secrecy unterstützen, bevorzugt werden
- Ausgehende Verbindungen MTA zu MTA:
  - Für ausgehende Verbindungen zu anderen Anbietern muss der Anbieter selbst STARTTLS nutzen, wenn auch der empfangende Anbieter STARTLS unterstützt. Dabei sollten Algorithmen, die Perfect Forward Secrecy unterstützen, bevorzugt werden.
- Ein- und ausgehende Verbindungen MTA zu Client:
  - Nutzung moderner Transportverschlüsselung zum Senden und Empfangen von E-Mails
  - Nutzung moderner Transportverschlüsselung für alle andere Kommunikation im Rahmen in diesem Kontext (z. B. die Übermittlung der Zugangsdaten).
  - Zugriff auf E-Mails über STARTTLS
- Web-Mail
  - Nutzung moderner Transportverschlüsselung zur Anmeldung und während der Sitzung
  - Das Server-Zertifikat muss die Mindestanforderungen des CA/Browser Forums erfüllen (und somit in den Stammzertifikatsspeichern der Browser enthalten sein)
- Die Zugangsdaten müssen auf dem Server gesichert, aber keinesfalls im Klartext gespeichert werden. Hierzu ist ein entsprechend dem aktuellen Stand der Technik geeignetes Verfahren zu verwenden (z. B. rundenbasiertes Hashverfahren: PBKDF2 und Salt)
- Für den Kunden sollte die Option bestehen, für seine E-Mails selbst eine Ende-zu-Ende-Verschlüsselung vorzunehmen. Da in diesem Fall eine Virenprüfung durch den TK-Diensteanbieter

ENTWURF

[77] https://www.bsi.bund.de/dok/TR-02102

nicht möglich ist, sollten diese Mails beim Empfänger – soweit technisch möglich (z. B bei Web-Mail) – entsprechend gekennzeichnet werden, um ihn darauf aufmerksam zu machen, dass er für die Virenprüfung selbst verantwortlich ist.

- Genutzte Zertifikate
  - Alle vom Anbieter zur Kommunikation mit anderen Anbietern genutzten Zertifikate (z. B. MTA zu MTA mittels STARTTLS) müssen von einer anerkannten Certification Authority (CA) ausgestellt sein.

b)

- Eingehende Verbindungen
  - Einsatz von DNSSEC für alle vom Anbieter genutzten Domains
  - Veröffentlichen der Informationen über sein Zertifikat durch DANE/TLSA
  - Ergänzend sollte der Anbieter durch die Nutzung von MTA-STS [IETF RFC 8461] Informationen über sein Zertifikat veröffentlichen
  - Information des Senders über fehlgeschlagene verschlüsselte Übertragungen mittels Veröffentlichung einer TLS-Report-Policy (TLSRP-Policy) in der DNS-Zone der „Public Domain“ sowie Versand von TLSRP-Reports per SMTP (nicht HTTPS)[78]. Versendung des TLSRP-Reports sollte unverschlüsselt und möglichst fehlertolerant erfolgen, damit dessen Zustellung nicht an den gleichen Gründen scheitert wie die verschlüsselte Übertragung der ursprünglichen Nachricht.
- Ausgehende Verbindungen
  - Prüfung aller Verbindungen zu anderen Anbietern unter Nutzung von DNSSEC, ob Informationen über die Nutzung von DANE/TLSA in den DNS-Records der empfangenden Anbieter veröffentlicht sind
  - Prüfung aller Verbindungen zu anderen Anbietern, ob Informationen zur Nutzung von MTA-STS veröffentlicht sind
  - Sind diese Informationen vorhanden, muss die Authentizität der Verbindung auf deren Grundlage verifiziert werden
  - Falls die Informationen im Zertifikat nicht mit den kryptographischen Informationen übereinstimmen, die der empfangende Anbieter übermittelt, oder falls überhaupt keine bzw. eine weniger sichere Transportverschlüsselung vom Empfänger angeboten wird, als in der Policy im

ENTWURF

[78] um die Identität des Absenders verifizieren zu können

DNS-Record bzw. MTA-STS angegeben, so muss die Verbindung abgebrochen werden, da in diesem Fall von einer Kompromittierung der Übertragungstrecke auszugehen ist.

- Prüfen, ob in den in DNS-Zonen der Empfänger-Domains, zu denen er erfolgreich oder nicht erfolgreich verschlüsselte E-Mails überträgt, TLSRP-Policies veröffentlicht sind und ob diese TLSRP-Reports anfordern. Ist dies der Fall, muss der Anbieter TLSRP-Reports erstellen und versuchen, diese zu übermitteln.

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

ENTWURF

7. Bewusstsein für Bedrohungen (Awareness)

In Kapitel 4.10 des Sicherheitskataloges werden Sicherheitsziele im Zusammenhang mit der Aufklärung von Bedrohungen und dem Kontakt zu Endnutzern formuliert. Entsprechende Informationen über die wichtigsten Bedrohungen für die Sicherheit von Netzen und Diensten sind von den Verpflichteten an ihre Kunden weiterzugeben. Diese im Sicherheitskatalog zunächst abstrakt umrissenen Sicherheitsziele werden durch die im Folgenden aufgeführten Maßnahmen für Internet-TK-Netzbetreiber und TK-Diensteanbieter im Internet weiter konkretisiert.

Um die Sicherheit von Netzen und Diensten stets auf dem aktuellen Stand der Technik zu halten, sollte ein systematisches Wissensmanagement aufgebaut werden. Ziel hierbei ist es, möglichst umfassende Informationen über neue Bedrohungen und Abwehrmechanischen aus Quellen wie Hersteller- oder Computer Emergency Response Team (CERT)-Mitteilungen zu sammeln und sich über den sicherheitstechnischen „State oft the ART“ auch mit anderen TK-Anbietern auszutauschen.

Weiterhin sollten Informationen über Gefährdungen, die insbesondere die Kunden betreffen, an diese weitergegeben werden, zusammen mit Hinweisen, wie ein wirksamer Schutz vor diesen Gefahren möglich ist.

7.1 Etablieren eines Schwachstellen-Managements

Für den sicheren IT-Betrieb ist ein Schwachstellen-Management zu etablieren, um Lücken in Software, Komponenten, Protokollen und Außenschnittstellen der Umgebung zu identifizieren sowie die sich daraus ergebenden erforderlichen Handlungen abzuleiten, zu bewerten und umzusetzen.

ENTWURF

7.1.1 Systematisches Sammeln und Auswerten der Schwachstellenmeldungen von Herstellern und CERTs

a)

- Warnungen und Schwachstellenmeldungen von Herstellern bzgl. der im eigenen Netz eingesetzten Produkte sind zu beachten, auszuwerten und die sich daraus ergebenden Sicherheitsmaßnahmen sind umzusetzen

b)

- Ergänzend zu den Mitteilungen der Hersteller sind darüber hinaus auch Meldungen und Warnungen einschlägiger CERTs und sonstiger Quellen (Öffentliche Berichterstattung, Sicherheitshinweise von Dritten, MISP, Honeypot Analysen, etc.) entsprechend auszuwerten und die sich daraus als notwendig ergebenden Sicherheitsmaßnahmen für die eigenen Systeme umzusetzen

- Weiterhin sind auch selbst regelmäßig organisatorische und technische Audits der eigenen Systeme zur Schwachstellenanalyse durchzuführen

c)

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

7.1.2 Informationsaustausch und Zusammenarbeit mit anderen Anbietern und Betreibern

a)

- Keine verpflichtenden Maßnahmen vorgesehen

Hinweis: Es steht Anbietern und Betreibern der Kategorie a) offen, sich den in b) spezifizierten Kooperationen anzuschließen.

b)

- Erkenntnisse über aktuelle Angriffsverfahren und -arten (z.B. hinsichtlich DDOS, DNS-Reflection usw.) sowie passende Abwehrtechniken (z. B. Filterregeln) sollten anbieterübergreifend regelmäßig untereinander ausgetauscht werden
- Um im Bedarfsfall eine schnelle Handlungsfähigkeit anbieterübergreifend sicherzustellen, sollten Ansprechpartner, Erreichbarkeiten und Notfallnummern untereinander ausgetauscht werden
- Die anbieterübergreifende Zusammenarbeit sollte durch regelmäßige Übungen optimiert werden
- Für Krisenfälle sollte ein gemeinsames Lagezentrum betrieben werden

c)

ENTWURF

- Für diesen Punkt sind keine darüberhinausgehenden Maßnahmen verpflichtend

Begriffsbestimmungen für Anhang (Technische Spezifikation)

Apex der DNS-Zone
Ein "Apex Domain" (auch als "Root Domain" bezeichnet) ist die höchste Ebene einer Domain im DNS. Sie umfasst den Domainnamen ohne Subdomains und endet in der Regel mit einer Top-Level-Domain (TLD) wie .com, .org oder .de.

Dienste im Sinne des TKG
Gemäß §3 Nr. 1 TKG ist „Anbieter von Telekommunikationsdiensten“ jeder, der Telekommunikationsdienste erbringt.
Demnach definiert das TKG den Begriff „Dienst“ im Sinne einer Dienstleistung, die von einem Anbieter erbracht wird.

Dienste im technischen Sinne
Ein „Internetdienst“ im technischen Sinne bezeichnet im Gegensatz zum TKG keine Dienstleistung eines „Anbieters“, sondern eine Anwendung, die das Internet dem Nutzer über seine Infrastruktur zur Verfügung stellt. Beispiele für solche Dienste bzw. Anwendungen sind z.B.:

- Das World Wide Web (WWW)
- E-Mail
- (VoIP-)Telefonie
- Chat
- ...

ENTWURF

Eine weitere Spezialisierung erfährt der Begriff „Dienst“ im technischen Bereich in Bezug auf eine bestimmte Betriebssystem- oder Server-Ebene.

So stellt ein Betriebssystem wie Unix, Linux, Windows usw. Dienste wie:

- Nutzerverwaltung
- Dateisystemverwaltung
- Konfiguration der Hardware
- Druckerfreigabe

in Form von „Dienstprogrammen“ zur Verfügung.

Dienste wie:

- HTTP, HTTPS
- FTP, SFTP
- SMTP, IMAP, POP
- SQL

- ...

werden hingegen von Servern den „Clients“ (d.h. Client-Anwendungen bzw. Client-Programmen) bzw. deren Nutzern zur Erfüllung ihrer Aufgaben zur Verfügung gestellt.

Transit-Provider
Endkunden greifen auf Inhalte und Anwendungen zu, die von CAPs (Content and Application Providern) bereitgestellt werden. Damit diese Inhalte und Anwendungen zum Endnutzer gelangen, müssen sich die beteiligten Netze zusammenschalten. Dies erfolgt im Internet über Transit bzw. Peering. Durch Transitvereinbarungen bietet ein Netzbetreiber (Transit Provider) anderen Netzbetreibern gegen Entgelt Konnektivität zum ganzen Internet. Beim Peering tauschen Netzbetreiber Verkehr nur untereinander aus, zumeist ohne Entgeltzahlungen.

https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/Schutz/PeeringTransitmaerkte/start.html

ENTWURF

Abkürzungsverzeichnis

ACL	Access Control List
BGB	Border Gateway Protocol
- eBGP	- exterior Border Gateway Protocol
CERT	Computer Emergency Response Team
DANE	DNS-based Authentication of Named Entities
DDoS	Distributed Denial of Service
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Name System
- DNSSEC	- Domain Name System Security Extensions
- EDNS(0)	- Extension Mechanisms for DNS (gem. RFC 6891)
- DNS-over-QUIC	- DNS over Quick UDP Internet Connections
DSA	Digital Signature Algorithm
- ECDSA	- Elliptic Curve Digital Signature Algorithm
- EdDSA	- Edwards-curve Digital Signature Algorithm
DV	Datenverarbeitung
GTSM	Generalized TTL Security Mechanism
IMAP	Internet Message Access Protocol
MANRS	Mutually Agreed Norms for Routing Security
MTA	Mail Transfer Agent
MX-Record	Mail Exchange Resource Record
NTP	Network Time Protocol
PeeringDB	Peering Data Base
QNAME Minimization	DNS Query Name Minimisation to Improve Privacy (gem. RFC 9156)

ENTWURF

RIR/NIR	Regional Internet registry / National Internet registry
ROAs in RPKI	Route Origin Authorizations in Resource Public Key Infrastructure
RSA	Rivest–Shamir–Adleman (asymmetrisches kryptographisches Verfahren)
Sender-ID	Sender Identification
SPF	Sender Policy Framework
TCP	Transmission Control Protocol
- TCP-AO	- TCP Authentication Option
TK	Telekommunikation
TLS	Transport Layer Security
- STARTTLS	- Verfahren zum Einleiten einer TLS-Verbindung
- TTL	- Time to Live
UDP	User Datagram Protocol

ENTWURF

ENTWURF

II Konsultation

Im Rahmen der aktuellen Überarbeitung des Sicherheitskataloges wurden bereits die sich abzeichnenden Änderungen der nationalen Gesetzeslage durch die Umsetzung der NIS2- und CER-Richtlinie berücksichtigt. Die Maßnahmen orientieren sich somit an den derzeit gültigen Vorgaben des EU-Rechts. Vor Verfügung der endgültigen Fassung werden die Verweise auf Rechtsnormen an die dann geltende Rechtslage angepasst.

ENTWURF

Die Bundesnetzagentur ersucht um Stellungnahmen zum vorliegenden Entwurf des Katalogs von Sicherheitsanforderungen bis zum 19.12.2025. Nähere Informationen finden Sie auf den Webseiten der Bundesnetzagentur.

ENTWURF

Verzeichnisse

ENTWURF

Abbildungsverzeichnis

Abbildung 1: Liste der festgelegten kritischen Funktionen, § 167 Abs. 1 Nr. 2 TKG 80

Abbildung 2: Normen, Standards und Guidelines 109

ENTWURF

Impressum

Herausgeber

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Tulpenfeld 4

53113 Bonn

Ansprechpartner

Referat 217

An der Trift 40

66123 Saarbrücken

217.Postfach@bnetza.de

www.bundesnetzagentur.de

Tel. +49 228 14-0

Fax +49 681 9330-734

Stand

Oktober 2025

ENTWURF

Druck

[Bundesnetzagentur oder Druckerei]

Bildnachweis

[Auflistung der Fotografien in alphabetischer Reihenfolge]

Fotograf A: Seite 5

Text

Referat 217