Anlage 2

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

Liste der kritischen Funktionen nach § 109 Abs. 6 Satz 1 Nr. 2 TKG für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial

Stand: 18.08.2021

Anlage 2

1 Einleitung

Die Bundesnetzagentur (BNetzA) legt gemäß § 109 Abs. 6 S. 1 Nr. 2 des Telekommunikationsgesetzes (TKG) im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) durch Verfügung in einem Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten fest, welche Funktionen kritische Funktionen im Sinne von § 2 Abs. 13 S. 1 Nr. 3 b des BSI-Gesetzes (BSIG) sind, die von kritischen Komponenten im Sinne von § 2 Abs. 13 BSIG realisiert werden.

2 Kritische Funktionen und Komponenten

§ 2 Abs. 13 S. 1 BSIG definiert kritische Komponenten als IT-Produkte,

1. die in Kritischen Infrastrukturen eingesetzt werden,
2. bei denen Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit Kritischer Infrastrukturen oder zu Gefährdungen für die öffentliche Sicherheit führen können und
3. die eine auf Grund eines Gesetzes unter Verweis auf diese Vorschrift als kritisch bestimmte Funktion realisieren (§ 2 Abs. 13 S. 1 Nr. 3b BSIG).

Die Gefährdungslage einer Funktion wird wesentlich auch vom aktuellen Stand der Technik beeinflusst. Weder der Stand der Technik noch eine Gefährdungslage sind statische Befunde, sondern unterliegen der weiteren zukünftigen technischen Entwicklung und der Einsatzmöglichkeiten der Komponenten und deren Funktionen. Daher muss auch bei etwaigen Veränderungen die Kritikalität einer Funktion erneut beurteilt werden.

Für den Betreiber eines Telekommunikationsnetzes wird sich vor dem Hintergrund dieser abstrakten Auslegungsüberlegungen bei im Einzelfall betriebenen Telekommunikationsnetzen oder -diensten die Frage nach der Ermittlung und der Bewertung von kritischen Funktionen stellen. Hierbei benennt die nachfolgende Liste die gegenwärtig bereits als kritisch oder grundsätzlich als kritisch bewerteten Funktionen in Tabelle 1 und stellt eine mögliche Vorgehensweise bei der Ermittlung der kritischen Komponenten dar.

Anlage 2

3 Liste der kritischen Funktionen

Eine Bewertung und Einordnung von Funktionen als kritisch erfolgt gemäß § 109 Abs. 6 S. 1 Nr. 2 TKG durch die BNetzA im Einvernehmen mit dem BSI und der oder dem BfDI auf der Grundlage einer gemeinsamen Gefährdungsanalyse und des jeweils aktuellen Stands der Technik. Die Bewertung und Einordung kann u.a. unter Rückgriff auf bereits vorliegende geeignete Untersuchungen erfolgen.

Geeignete Untersuchungen in diesem Sinn sind nach Auffassung der BNetzA, des BSI und der oder dem BfDI die EU-Risikoanalyse (CG Publication 02/2019 – „Risk assessment of 5G networks“ v. 9.10.2019) sowie die Implementierungsempfehlungen der EU-Toolbox (CG Publication 01/2020 – „Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures“ v. 29.01.2020).

Die nachfolgende Liste in Tabelle 1 listet insofern kritische Funktionen für öffentliche Mobilfunknetze der 5. Generation auf. Nur bei diesen handelt es sich derzeit um öffentliche Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial.

Die erfolgte Bewertung und Einordnung der Funktion überträgt sich auch auf die jeweilige Komponente, welche die Funktion ganz oder teilweise umsetzt.

Im Ergebnis dieser derzeitigen Bewertung werden die Komponenten, die die Funktionen der Kategorien a) und b) in der nachfolgenden Tabelle ausführen, als kritisch bewertet. Bei den Komponenten, die grundsätzlich als kritisch zu bewertende Funktionen aus den Kategorien c) bis f) in der nachfolgenden Tabelle ausführen, kann jedoch von der Bewertung der konkreten Funktion als kritisch im konkreten Einzelfall abgewichen werden, wenn der Netzbetreiber plausibel und begründet darlegen kann, dass im Einzelfall keine Kritikalität von der Funktion ausgeht.

Ein Ausschluss der mit der Kritikalität einhergehenden Gefahrenlage kann unter Umständen dann vorliegen, wenn die jeweilige Funktion aufgrund ihrer Zweckverwendung oder der für sie vorgesehenen Einsatzumgebung bereits nicht das Potenzial für eine Realisierung der Gefahrenlage hat, aber die Funktion in geeigneter Form sicher von der Gefahrenlage isoliert wurde.

Ein Ausschluss der Gefahrenlage für eine Funktion kann im Einzelfall dazu führen, dass die jeweilige Komponente, die diese Funktion ausführt, in diesem Fall nicht kritisch ist. Allerdings ist eine Komponente in jedem Fall kritisch, wenn diese zusätzlich auch eine Funktion nach a) oder b) oder eine andere Funktion nach c) bis f), die ihrerseits nicht im Einzelfall unkritisch ist, erfüllt. Kommt der verpflichtete Netzbetreiber bei der Bewertung zu dem Ergebnis, dass im vorliegenden Einzelfall keine Kritikalität gegeben ist, so muss der Ausschluss der Gefahrenlage begründet werden und sein. Die zugrundeliegenden Gegebenheiten hat der Verpflichtete im Sicherheitskonzept zu vermerken und der Bundesnetzagentur vorzulegen, § 109 Abs. 4 S. 6 TKG.

Wird ein Ausschluss der Gefahrenlage bei einer hier als kritisch bewerteten Funktion geltend gemacht, so wird bei Netzen mit erhöhtem Gefährdungspotenzial im Rahmen einer Überprüfung durch eine qualifizierte unabhängige Stelle oder eine zuständige nationale Behörde gemäß § 109 Abs. 7 S. 1 TKG festgestellt, ob der Ausschluss der Gefahrenlage zurecht angenommen wurde und die Anforderungen des § 109 Abs. 1 bis 3 TKG erfüllt sind.

Anlage 2

Tabelle 1: Liste der kritischen Funktionen für das 5G Netz

Kategorie	Funktionalitäten
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 Kernnetzwerkfunktionen gegenüber externen Anwendungen - Zuordnung von Endgeräte zu Netzwerk-Slices
b) NFV management and network orchestration (MANO)	- Management und Orchestrierung virtualisierter Netzwerkfunktionen
c) Management systems and supporting services	- Sicherheitsfunktionen des Management-Systems
d) Radio Access Network (RAN)	- 5G-RAN Management
e) Transport and transmission functions	- Sprach- und Datentransportfunktionen mit erhöhter Relevanz
f) Internetwork exchanges	- IP-Netzwerk außerhalb der MNO-Räumlichkeiten (Netzwerkdienste von Dritten)

Die in der Tabelle aufgeführten Funktionen werden in den Implementierungsempfehlungen der EU-Toolbox (CG Publication 01/2020 –

[1] unabhängig vom Ort der Realisierung innerhalb des 5G-Netzes (z.B. eine Realisierung im RAN oder MEC)

„Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures“ v. 29.01.2020) im Annex 2 beschrieben.

4 Prozess zur Identifikation von kritischen Komponenten im konkret betriebenen Netz oder erbrachten Dienst

Betreiber öffentlicher Telekommunikationsnetze und Erbringer öffentlich zugänglicher Telekommunikationsdienste sollten einen Prozess für die Identifikation von kritischen Komponenten einführen und umsetzen.

Zur Identifikation 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.

In Abbildung 1 wird der Prozess zur Identifizierung kritischer Komponenten dargestellt. Der Prozess integriert sich in den Gesamtprozess zur Erstellung eines Sicherheitskonzeptes gemäß § 109 Abs. 4 TKG (vgl. Katalog von Sicherheitsanforderungen, Kapitel 5).

Anlage 2

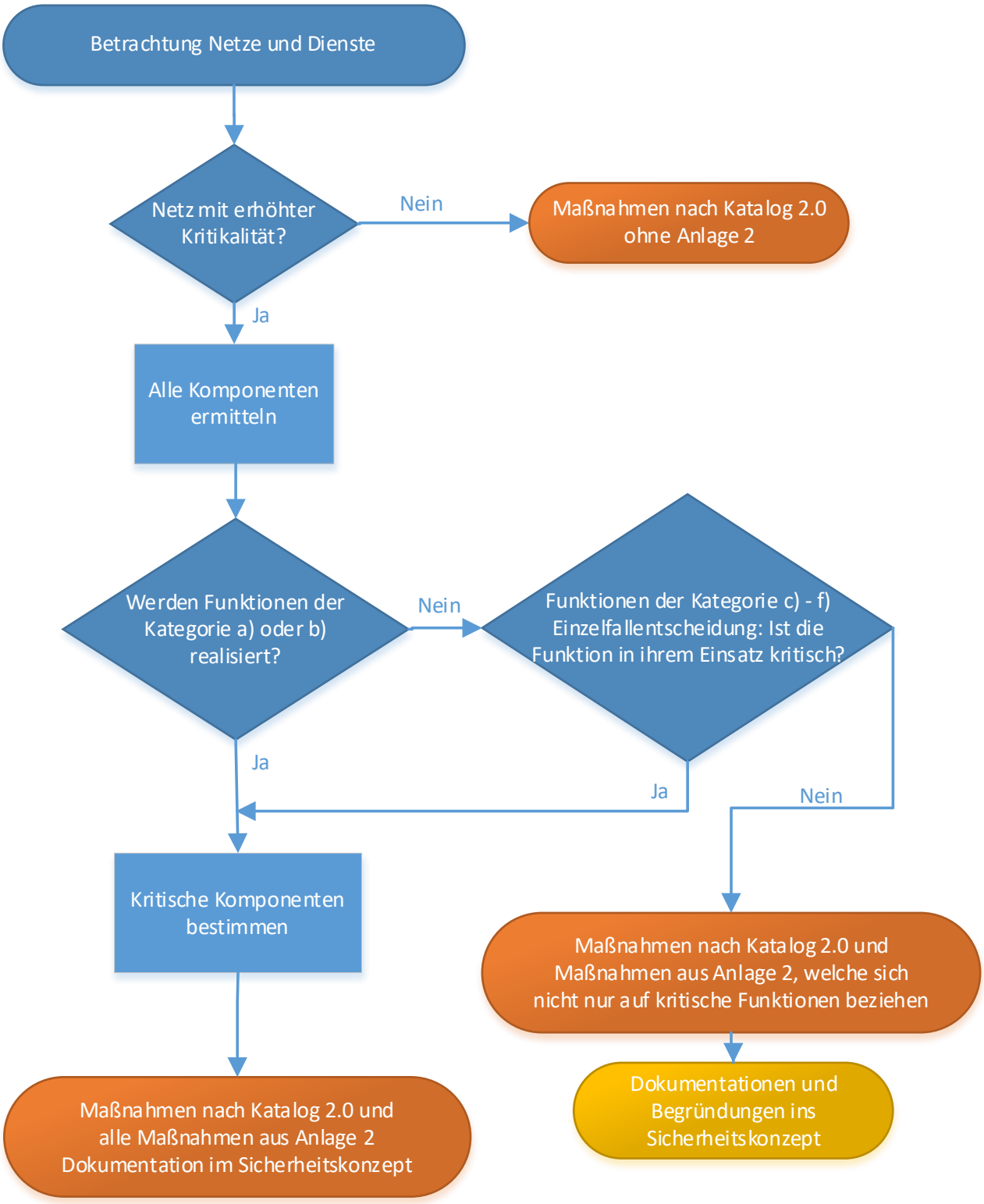

Abbildung 1 Identifikationsprozess kritischer Komponenten

Anlage 2

Nachfolgend werden die einzelnen Schritte zur Identifizierung kritischer Komponenten beschrieben:

Schritt 1: Identifikation und Abgrenzung der Komponenten des Netzes
Nach Beschreibung des Netzes oder des Dienstes, der Gefährdungsanalyse einschließlich der Festlegung der Kritikalität gemäß Kapitel 5 des Kataloges von Sicherheitsanforderungen sind für die Netze und Dienste, welche nicht unter die erhöhte Kritikalität fallen, die erforderlichen technischen Vorkehrungen und sonstigen Maßnahmen festzulegen und zu beschreiben.

Für Netze mit erhöhtem Gefährdungspotenzial werden alle Komponenten ermittelt.
Die Identifikation und Abgrenzung der Komponenten des 5G-Netzes erfolgt durch den Netzbetreiber. Dieser Schritt erlaubt dem Netzbetreiber eine Anpassung auf dessen individuelle Netzarchitektur vorzunehmen.
Es sind grundsätzlich alle Komponenten zu betrachten, unabhängig davon, ob kritische Funktionen gemäß den Ausführungen in Tabelle 1 realisiert sind oder nicht.

Der Netzbetreiber hat eine detaillierte Beschreibung über alle identifizierten Komponenten seines Netzes zu erstellen und dem Sicherheitskonzept beizufügen.

Schritt 2: Identifikation von kritischen Komponenten mittels kritischer Funktionen
Nachdem alle relevanten Komponenten des Netzes identifiziert wurden, können anhand der Ausführungen in Tabelle 1 die Komponenten identifiziert werden, die kritische Funktionen ganz oder teilweise realisieren. Wenn eine Komponente eine kritische Funktion teilweise oder in vollem Umfang realisiert, so ist diese Komponente grundsätzlich als kritische Komponente zu bewerten.

Sind Funktionen der Kategorien c) – f) im Einzelfall nach Risikoeinschätzung des Netzbetreibers nicht kritisch, so ist dies unter Darlegung von Gründen und Umständen im neu vorzulegenden Sicherheitskonzept zu dokumentieren und zu belegen, § 109 Abs. 4 TKG.

Für Komponenten, die keine kritischen Funktionen erfüllen, müssen die erforderlichen technischen Vorkehrungen und sonstigen Maßnahmen festgelegt und beschrieben werden, sowie ergänzende Sicherheitsanforderungen nach Anlage 2 des Kataloges von Sicherheitsanforderungen, welche sich nicht ausschließlich auf kritische Komponenten beziehen, umgesetzt werden.

Schritt 3: Umgang mit identifizierten kritischen Komponenten
Kritische Komponenten im Sinne von § 2 Absatz 13 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, § 109 Abs. 2 S. 4 TKG. Kritische Komponenten unterliegen daher unter anderem der Zertifizierung gemäß der Technischen Richtlinie TR-03163 "Sicherheit in TK-Infrastrukturen“ des BSI.
Im Übrigen unterliegen identifizierte kritische Komponenten den Anforderungen des Kataloges von Sicherheitsanforderungen einschließlich dessen Anlagen.