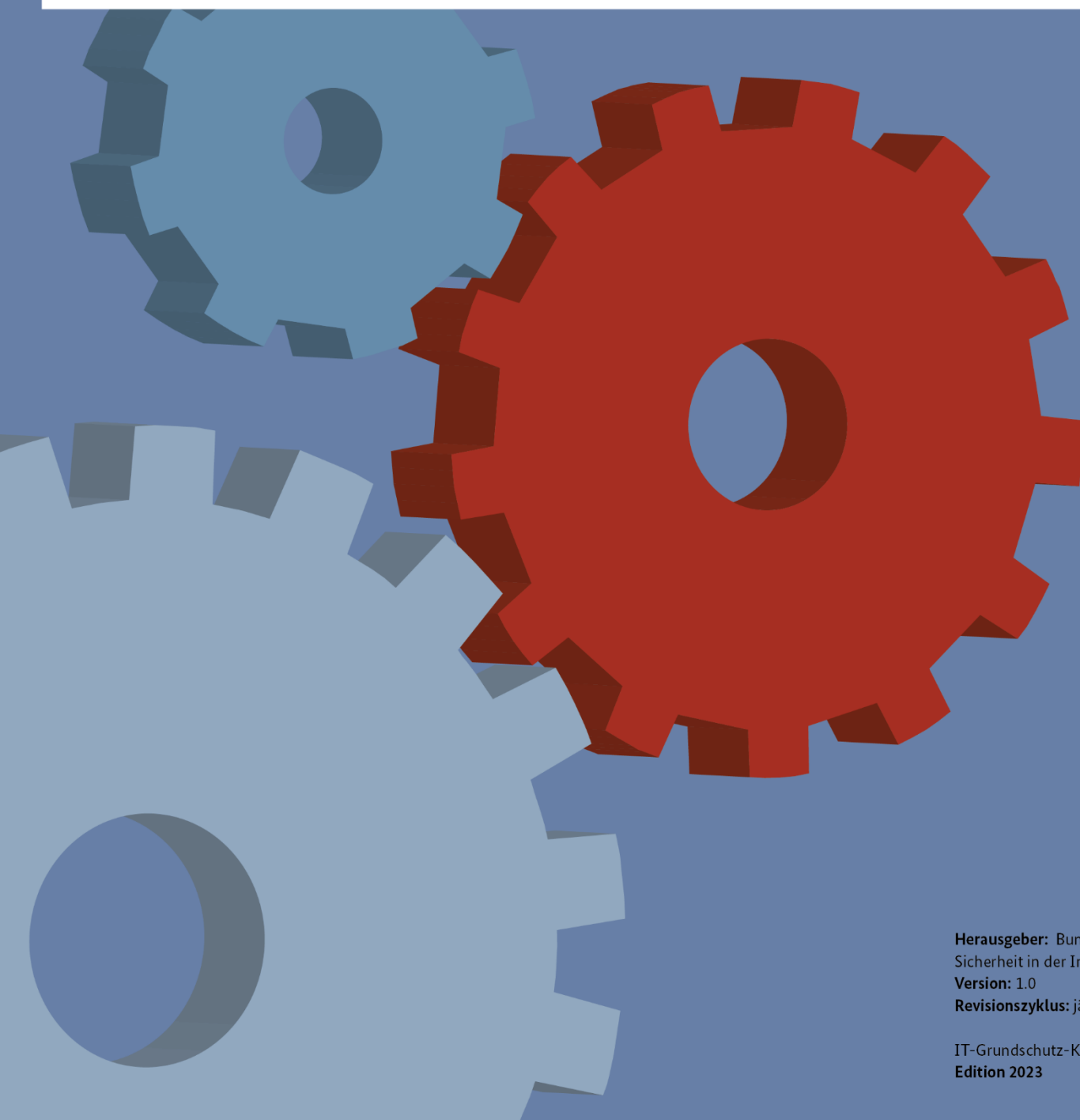




Bundesamt  
für Sicherheit in der  
Informationstechnik

# IT-Grundschutz-Profil zur Absicherung von 5G-Campusnetzen

5G-Campusnetz im Eigenbetrieb



**Herausgeber:** Bundesamt für  
Sicherheit in der Informationstechnik  
**Version:** 1.0  
**Revisionszyklus:** jährlich

IT-Grundschutz-Kompodium  
Edition 2023

# Inhaltsverzeichnis

1	Einleitung .....	4
1.1	Formale Aspekte .....	6
1.2	Haftungsausschluss.....	6
2	Management Summary .....	7
2.1	Zielgruppe .....	7
2.2	Zielsetzung .....	7
3	Festlegung des Geltungsbereichs .....	8
3.1	Zielgruppe .....	8
3.2	Beschreibung des Schutzbedarfs.....	8
3.3	IT-Grundschutz Vorgehensweise .....	8
3.4	Kompatibilität zu anderen Standards.....	9
3.5	Berücksichtigte Rahmenbedingungen.....	9
4	Abgrenzung Informationsverbund.....	10
4.1	Bestandteile des Informationsverbundes .....	10
4.2	Nicht berücksichtigte Teile .....	11
5	Referenzarchitektur.....	12
5.1	Anwendungen.....	14
5.2	IT-Systeme .....	15
5.3	Netze und Netzkomponenten.....	16
5.4	Infrastruktur .....	18
5.5	Umgang mit Abweichungen.....	19
6	Feststellung des Schutzbedarfes.....	20
7	Zu erfüllende Anforderungen und umzusetzende Maßnahmen.....	23
7.1	Auswahl relevanter Bausteine .....	23
7.2	Anforderungen aus den IT-Grundschutz-Bausteinen.....	24
7.3	Anforderungen an spezifische Zielobjekte .....	26
8	Risiko.....	27
9	Anwendungshinweise.....	34
10	Unterstützende Informationen.....	35

# Versionshistorie

Datum	Version	Änderung	Bearbeiter
August 2023	Draft 0.1	Initiale Erstellung	
Oktober 2023	CD 1.0	Comunity Draft	
Februar 2024	1.0	Finale Veröffentlichung	

# 1 Einleitung

Mit dem Einsatz von 5G-Campusnetzen ergeben sich aufgrund der Bedeutung der eingesetzten Technologie für die nutzenden Institutionen wesentliche Fragen hinsichtlich der Informations- und IT-Sicherheit.

Die Anwendenden von 5G-Campusnetzen verfolgen meist das Ziel, verlässlich hohe Bandbreiten bei hohen Übertragungsgeschwindigkeiten sowie zuverlässig geringen Latenzen bei der drahtlosen Kommunikation zur Verfügung zu haben. Dabei werden oft schützenswerte Daten übertragen, sodass Sicherheitsaspekten eine besondere Bedeutung zukommt. Gleichzeitig ist die Verbreitung des entsprechenden Fach- und IT-Knowhows noch sehr begrenzt und entsprechende Hilfestellungen schwer zu finden.

Dieses IT-Grundschutz-Profil bietet den Anwenderinnen und Anwendern eine Anleitung, sich mit dem Thema Informations- und IT-Sicherheit im Zusammenhang mit 5G-Campusnetzen vertraut zu machen, und damit verbundene Risiken transparent darstellen zu können. Detaillierte Betrachtungen zu Angriffsszenarien und anderweitigen Bedrohungen sind im Kapitel 8 Risiko beschrieben.

Der Begriff „5G-Campusnetz“ bezeichnet dabei ein lokal betriebenes, nicht öffentliches 5G-Mobilfunknetz. Solch ein Netz hat gewöhnlich keine Anbindung an das öffentliche Mobilfunknetz (engl.: Public Land Mobile Network (PLMN)). Dieses Profil legt die aktuellen Standards ab Release 15 der 3GPP und den Betrieb als 5G-Standalone (SA) Netz zu Grunde. 5G-Standalone Netze nutzen ausschließlich 5G-Komponenten, auch im Kernnetz. Sogenannte 5G-Non-Standalone (5G-NSA) Netze nutzen zwar 5G-Mobilfunkbasisstationen, jedoch basiert das Kernnetz auf LTE-Technik.

Das 5G-Campusnetz verfügt, wie alle anderen 5G-Netze auch, über mindestens eine Basisstation, den gNodeB, über deren angeschlossene Radio Unit (Antenne) sich die mobilen Endgeräte mit dem Kernnetz (engl. Core Network), im Weiteren auch als 5G-Core bezeichnet, verbinden. Die Radio Unit, der gNodeB und der 5G-Core bilden die Kernkomponenten des 5G-Campusnetzes. Die Radio Unit bildet mit dem gNodeB das Radio Access Network (RAN). Das Netz kann für eine größere Reichweite und Ausleuchtung über weitere eingesetzte gNodeB und Radio Units (RU) verteilt werden. Der 5G-Core ist die zentrale Einheit des 5G-Campusnetzes. Dieser besteht aus mehreren IT-Systemen und Netzkomponenten. Er stellt die Verbindung von den Endgeräten zum Netz her und bietet Zugang zu den Diensten.

In einem solchen Netz können verschiedene Arten von Sensorik und Aktorik eingesetzt werden, die beispielsweise in autonomen Plattformen wie fahrerlosen Transportsystemen verbaut sein können. Diverse IoT-Geräte können ebenfalls über solch ein Netz drahtlos miteinander vernetzt werden. Als Endgeräte kommen häufig Smartphones, Tablets, Notebooks und Modems zum Einsatz. Innerhalb des Kernnetzes können verschiedene Netz-Dienste bereitgestellt werden. Die im Netz eingesetzten Geräte und IT-Systeme müssen über SIM-Karten verfügen. In diesem IT-Grundschutz-Profil wird der Einsatz physischer SIM-Karten betrachtet.

Für den Betrieb eines 5G-Campusnetzes müssen Betreibende bei der Bundesnetzagentur (BNetzA) Lizenzen zur lokalen Nutzung der erforderlichen Frequenzen beantragen. Die Lizenzen und damit der Betrieb des Netzes ist somit ortsgebunden.

Das IT-Grundschutz-Profil wurde im Auftrag des BSI, zusammen mit Fachexpertinnen und -experten aus dem Bereich von 5G-Campusnetzen sowie aus dem Bereich der IT-Grundschutz-Profile erstellt. Das Ergebnis ist dieses Muster-Sicherheitskonzept, das als Schablone für die Beachtung und Implementierung sogenannter „Best Practices“ dienen soll.

Das vorliegende „IT-Grundschutz-Profil für 5G-Campusnetze“ zeigt Wege auf, wie Anwendenden das Thema IT- und Informationssicherheit zielgerichtet angehen und umsetzen können. In der vorliegenden Version bildet das Dokument 5G-Campusnetze als reine „Insellösungen“ ab, ohne unmittelbare Anbindung an öffentliche Netze,

wie das öffentliche Mobilfunknetz oder das Internet. Alle Komponenten des 5G-Campusnetzes befinden sich beim Anwendenden vor Ort.

Anwendende des 5G-Campusnetzes sind in der vorliegenden Version gleichzeitig Betreibende.

Auch beschränken sich die Empfehlungen in diesem Dokument auf die Nutzung eines privaten 5G-Netzes mit nur einer Quality-of-Service Klasse, ohne jegliche Priorisierung von Verkehr. Durch die Fokussierung auf diesen grundlegenden Netzaufbau, steht das IT-Grundschutz-Profil vielen Anwendenden zur Verfügung und kann bei Bedarf erweitert werden. Dieses IT-Grundschutz-Profil bildet damit die Basis, um das 5G-Campusnetz sicher in ein Firmennetz zu integrieren und zu betreiben.

Für alle darüber hinaus gehenden Anforderungen sind weitere Bausteine aus dem IT-Grundschutz-Kompendium zu berücksichtigen und gegebenenfalls zusätzliche Sicherungsmaßnahmen zu treffen.

Sicherheitsanforderungen an das 5G-Campusnetz werden in diesem IT-Grundschutz-Profil aus der Perspektive von Anwendenden, die gleichzeitig Betreibende sind, abgebildet. Die Kernkomponenten können in die bereits bestehende Netzinfrastruktur integriert werden, sodass einzelne Bestandteile, wie bestehende Kabelverbindungen oder Switches genutzt werden können.

Die Anwendenden des 5G-Campusnetzes können für die Durchführung oder Unterstützung bei unterschiedlichen Aufgaben, die im Zusammenhang mit der Implementierung und dem Betrieb eines 5G-Campusnetzes stehen, externe Dienstleistende beauftragen. Die in diesem IT-Grundschutz-Profil beschriebenen Anforderungen müssen dann durch den jeweiligen Dienstleistenden umgesetzt werden.

## 1.1 Formale Aspekte

Aspekt	Beschreibung
Titel:	IT-Grundschutz-Profil für 5G-Campusnetze
Autorenschaft:	Jennifer Gabriel, Thomas Lundström und Richard Fritzsche Softed Systems GmbH
Reviewer:	Rolf Siekmeyer und Daniel Günzel blackned GmbH, Christian Mondry GuardStack GmbH
Herausgeber:	Bundesamt für Sicherheit in der Informationstechnik
Versionsstand:	1.0
IT-Grundschutz- Kompendium	2023
Revisionszyklus:	Jährlich

Tabelle 1: Formale Aspekte.

## 1.2 Haftungsausschluss

Dieses Dokument wurde mit größter Sorgfalt erstellt, erhebt aber keinen Anspruch auf Vollständigkeit und Richtigkeit. Die Autorenschaft hat keinen Einfluss auf die Nutzung dieses IT-Grundschutz-Profiles durch Anwendende und kennen auch nicht die individuellen Anforderungen an ihre Sicherheitskonzepte, sodass sie naturgemäß für die Auswirkungen auf die Rechtsposition der Parteien keine Haftung übernehmen können.

# 2 Management Summary

## 2.1 Zielgruppe

Das IT-Grundschutz-Profil für 5G-Campusnetze richtet sich an alle Institutionen, die ein rein lokales 5G-Campusnetz bereits nutzen oder dies vor haben und eine Absicherung in Bezug auf die Informations- und IT-Sicherheit nach dem Stand der Technik erreichen wollen.

In diesem Profil wird dabei ein Szenario beschrieben, in dem die Anwendenden eines 5G-Campusnetzes selbst auch die Betreibenden sind. Für den Betrieb kann zur Unterstützung und der Umsetzung einzelner Aufgaben ein externes Dienstleistungsunternehmen einbezogen werden. Solche Aufgaben können die Bereitstellung der erforderlichen Hardware, die Konfiguration der eingesetzten Hard- und Software bis zu deren Wartung umfassen. Dies betrifft auch die Bereitstellung, Provisionierung und Deaktivierung der SIM-Karten, die in den im 5G-Campusnetz genutzten Endgeräten eingesetzt werden. Das IT-Grundschutz-Profil für 5G-Campusnetze richtet sich an die verantwortlichen Entscheidungsträger für Informationstechnik und jene Fachbereiche, in denen 5G-Campusnetze zum Einsatz kommen und in den Betrieb eines solchen Netzes involviert sind.

## 2.2 Zielsetzung

Dieses IT-Grundschutz-Profil soll Anwendende von 5G-Campusnetzen bei der Umsetzung einer geeigneten Sicherheitskonzeption unterstützen. Dieses IT-Grundschutz-Profil betrachtet ein rein lokal eingesetztes 5G-Campusnetz. Die grundlegende Verantwortung für den Betrieb des 5G-Campusnetzes liegt bei den Anwendenden. Dies gilt ebenso, wenn Anwendende für einzelne oder auch mehrere Aufgaben im Betrieb des 5G-Campusnetzes ein externes Dienstleistungsunternehmen beauftragen. Es soll als Schablone dienen, den IT-Grundschutz des BSI in geeigneter Weise zu implementieren. Es unterstützt die sichere Integration von 5G-Campusnetzen durch die übersichtliche Zusammenstellung der, für diesen Anwendungsfall wichtigen, IT-Grundschutz-Bausteine.

# 3 Festlegung des Geltungsbereichs

## 3.1 Zielgruppe

Das IT-Grundschutz-Profil für 5G-Campusnetze richtet sich an die Verantwortlichen für Informationssicherheit und Fachbereiche, in denen die 5G-Campusnetz-Technik zum Einsatz kommt und die in den Betrieb eines solchen Netzes involviert sind.

## 3.2 Beschreibung des Schutzbedarfs

Der Einsatz der 5G-Technik in 5G-Campusnetzen erfolgt in der Regel mit dem Ziel zuverlässig geringe Latenzen oder hohen Bandbreiten zu erreichen. Dabei wird erwartet, dass in äußerst niedrigen Reaktionszeiten die richtigen Daten zuverlässig das Ziel erreichen, um eine korrekte Verarbeitung sicherzustellen. Der 5G Technologien beschreibende Standard der 3GPP beschreibt dazu unterschiedliche Nutzungsprofile um ein Bündel von Konfigurationen festzulegen, die für unterschiedliche Einsatzzwecke bestmöglich geeignet sind. Fragen der IT-Sicherheit – insbesondere die genutzten Verschlüsselungsalgorithmen unterscheiden sich nicht.

Die Luftschnittstelle in Funknetzen ist grundsätzlich leicht zu detektieren und abzuhören. Aus diesem Grund wurde mit 5G eine verbesserte Abhörsicherheit eingeführt, die in 5G-Standalone Campusnetzen standardmäßig angewandt wird. Dazu beigetragen haben eine Veränderung der Authentisierung am Netz, wodurch nun die Langzeitidentitäten verschlüsselt übertragen werden können. Entsprechend werden die Integrität und Vertraulichkeit in einem höheren Maß ermöglicht und die Verfügbarkeit verbessert. Zudem kann das Sicherheitsniveau individuell höheren Anforderungen angepasst werden.

In einigen Anwendungsgebieten, insbesondere im industriellen und medizinischen Umfeld, in denen 5G-Campusnetze unter anderem zum Einsatz kommen, wird dem Schutz der transportierten Informationen ein besonderer Stellenwert beigemessen, beispielsweise um Wirtschaftsspionage zu verhindern oder dem Patientenschutz zu dienen.

Daher wird empfohlen kritisch zu prüfen, ob der Schutz der Grundwerte der Informationssicherheit Vertraulichkeit, Verfügbarkeit und Integrität über den normalen Schutzbedarf hinaus erreicht werden soll. Infolgedessen wird in diesem IT-Grundschutz-Profil der Betrachtung eines erhöhten Schutzniveaus Rechnung getragen. Liegt im betrachteten Informationsverbund erhöhter Schutzbedarf vor, so ist für alle betreffenden Zielobjekte eine Risikoanalyse durchzuführen.

Der Schutzbedarf der verarbeiteten Informationen und der im Netz befindlichen Systeme kann auch Auswirkungen auf den Umfang der Beteiligung von externen Dienstleistenden bei der Betriebsunterstützung eines solchen Netzes haben.

## 3.3 IT-Grundschutz Vorgehensweise

Der IT-Grundschutz des BSI bietet die Vorgehensweisen Basis-, Standard- oder Kern-Absicherung an. Abhängig von der gewählten Vorgehensweise müssen die in den Bausteinen des IT-Grundschutz-Kompends beschriebenen Anforderungen umgesetzt werden. Die beschriebenen Anforderungen in diesem IT-Grundschutz-Profil entsprechen mindestens der Standard-Absicherung des BSI-Standards 200-2. Zudem wird empfohlen, bei Bedarf Anforderungen aus dem erhöhten Schutzbedarf umzusetzen.



### 3.4 Kompatibilität zu anderen Standards

Durch eine Umsetzung der Standard-Absicherung besteht Kompatibilität zur ISO 27001.<sup>1</sup>

### 3.5 Berücksichtigte Rahmenbedingungen

Bei der Anwendung des IT-Grundschutz-Profiles ist darauf zu achten, dass gesetzliche Anforderungen sowie branchen- oder anwendungsspezifische Rahmenbedingungen (beispielsweise DS-GVO oder BSI-Gesetz) zusätzlich zu berücksichtigen sind.

Insbesondere Institutionen, die Betreibende einer Kritischen Infrastruktur gemäß dem BSI-Gesetz sind und den IT-Grundschutz anwenden, müssen bei der Absicherung ihres 5G-Campusnetzes sektorspezifische Anforderungen berücksichtigen. Diese Anforderungen können sich aus dem BSI-Gesetz und, für einzelne Sektoren und Branchen, aus anzuwendenden spezifischen Standards ergeben.

Weiterhin berücksichtigt der IT-Grundschutz keine Anforderungen, die sich aus dem Geheimschutz und der Verschlusssachenanweisung (VSA) ergeben. Diese sind zusätzlich zu den in diesem IT-Grundschutz-Profil beschriebenen Anforderungen zu berücksichtigen.

Das IT-Grundschutz-Profil berücksichtigt die Anwendung der 3GPP-Standards ab Release 15 in den Kernkomponenten eines 5G-Campusnetzes.

---

<sup>1</sup> [ISO/IEC 27001 - 2022-10 - Beuth.de](https://www.iso.org/standard/72431.html) (aufgerufen am. 09.11.2023)

# 4 Abgrenzung Informationsverbund

Die zusammenhängenden Komponenten einer Institution oder eines speziellen Anwendungsbereichs werden als Informationsverbund bezeichnet. Im nächsten Abschnitt werden die für das IT-Grundschutz-Profil relevanten Bestandteile des Informationsverbundes 5G-Campusnetze definiert. Anschließend werden die Teile des Informationsverbundes aufgeführt, die in diesem IT-Grundschutz-Profil nicht berücksichtigt werden. Der skizzierte Informationsverbund stellt den gemeinsamen Nenner verschiedener Nutzungsszenarien dar.

## 4.1 Bestandteile des Informationsverbundes

Im Informationsverbund werden die Bestandteile beschrieben, die Prozesse und Verfahren in einem lokalen 5G-Campusnetz unterstützen. Das IT-Grundschutz-Profil beschreibt eine Sicherheitskonzeption für die Komponenten, die zur Nutzung eines 5G-Campusnetzes zwingend erforderlich sind.

Die Kernkomponenten des 5G-Campusnetzes werden in der Strukturanalyse so weit in seine Bestandteile separiert, wie es aus der Sicherheitsbetrachtung erforderlich ist, um die auf die Zielobjekte zu modellierenden Bausteine zu identifizieren und die erforderlichen Anforderungen zu beschreiben.

Darüber hinaus erfolgt eine exemplarische Beschreibung der Sicherheitskonzeption für zusätzliche Objekte, die in verschiedenen Anwendungsfällen im 5G-Campusnetz zum Einsatz kommen.

Weiterhin werden alle Objekte im Informationsverbund betrachtet, die zum Netzmanagement und dessen Monitoring und Detektion dienen. Üblicherweise liegen diese in einem eigenen Netzbereich, der sowohl vom restlichen Firmennetz als auch vom eigentlichen 5G-Campusnetz separiert ist. Hier werden die bereits zur Überwachung aller anderen Netzbereiche eingesetzten Systeme genutzt.

Einzelne Aufgaben die im Zusammenhang mit dem Aufbau und dem Betrieb eines 5G-Campusnetzes stehen können an externe Dienstleistungsunternehmen vergeben werden. Das üblich im Rahmen von Dienstleistungen zu erbringende Liefern und Aufbauen und Warten von technischen Komponenten, das Einspielen von Updates und ähnliche Tätigkeiten sind kein Outsourcing im Sinne des IT-Grundschutzes.

Daher werden Aspekte des Outsourcings in diesem IT-Grundschutz-Profil nicht betrachtet.

Handelt es sich bei den extern erbrachten Dienstleistungen um Outsourcing im Sinne des Kapitel 1.3 des Bausteines OPS.2.3 Nutzung von Outsourcing, so muss dieser berücksichtigt werden. Das Dienstleistungsunternehmen muss den Baustein OPS.3.2 Anbieten von Outsourcing für den Informationsverbund bereitstellen. Die Anforderungen an die Nutzung von Outsourcing sind im IT-Grundschutz-Profil "5G-Campusnetz Betrieb durch einen externen Dienstleister" beschrieben.

In der nachfolgend dargestellten Tabelle sind die Schichten des Informationsverbundes aufgeführt. Die in den Schichten abgebildete Referenzarchitektur bilden die fachlichen und technischen Komponenten des Informationsverbundes für die eine exemplarische Sicherheitskonzeption erstellt wird. Die Referenzarchitektur ist detailliert im Abschnitt 5 dargestellt.

Identifikator	Objekt des Informationsverbundes
IV1	Prozesse
IV2	Anwendungen
IV3	IT-Systeme
IV4	Netze und Netzkomponenten
IV5	Infrastruktur

*Tabelle 2: Bestandteile des Informationsverbundes in einem 5G-Campusnetz.*

## 4.2 Nicht berücksichtigte Teile

Aus dem 5G-Campusnetz des betrachteten Informationsverbundes besteht keine direkte Verbindung zum öffentlichen Mobilfunknetz. Soll dies für Geräte ermöglicht werden, die im 5G-Campusnetz eingesetzt werden, müssen die sich daraus ergebenden Risiken zusätzlich betrachtet werden.

Einzelne Komponenten oder Funktionen des 5G-Campusnetzes, wie z. B. der 5G-Core oder der gNodeB, können in der Cloud betrieben werden. Diese Fälle werden in diesem IT-Grundschatz-Profil nicht betrachtet. Bei der Nutzung solcher Dienste sind neben den Auswirkungen auf die Latenzen beim Datentransfer zusätzliche Risiken und sich daraus ergebende Sicherheitsanforderungen im individuellen Informationsverbund zu betrachten. Die Anforderungen zur Nutzung von Cloud-Diensten sind im IT-Grundschatz Baustein OPS.2.2 Cloud-Nutzung beschrieben.

Die im 5G-Campusnetz eingesetzten Endgeräte können je nach individueller Regelung auch im Firmennetz (Intranet) benutzt werden. Dies wird in diesem Profil jedoch nicht betrachtet. Die sich aus dem Einsatz im Firmennetz zusätzlich ergebenden Risiken und Anforderungen müssen im individuellen Informationsverbund zusätzlich betrachtet werden.

Eine Verbindung des 5G-Core über herkömmliche Techniken wie TCP/IP und IPSec zu anderen Netzen ist möglich, wird in diesem IT-Grundschatz-Profil jedoch nicht berücksichtigt.

Voraussetzung zur Nutzung von Mobilfunk ist das Vorhandensein einer SIM-Karte im jeweiligen Gerät. Hierüber registriert sich das Gerät im Netz und es wird verifiziert, ob es im Netz teilnehmen darf. Im vorliegenden IT-Grundschatz-Profil werden für die Authentisierung am Netz lediglich physische SIM-Karten, die in das jeweilige Gerät eingelegt werden, berücksichtigt.

Sogenannte eSIM sind bisher nur wenig verbreitet. Um eSIM nutzen zu können, muss eine direkte Internetanbindung zum Endgerät im 5G-Netz bestehen, andernfalls ist eine Registrierung am Netz nicht möglich. Grund ist, dass die Server zur Verwaltung von eSIM üblicherweise in der Cloud stehen. Die Nutzung von eSIM wird daher in diesem IT-Grundschatz-Profil nicht betrachtet.

Weitere Formen der SIM-Karten, wie beispielsweise iSIM (integrated SIM) werden in diesem Profil ebenfalls nicht betrachtet.

# 5 Referenzarchitektur

Der vom IT-Grundschutz-Profil betrachtete Informationsverbund fokussiert auf die Kernkomponenten eines 5G-Campusnetzes sowie auf Objekte, die für den Betrieb und die Verwaltung des 5G-Campusnetzes zum Einsatz kommen. Objekte, die zur Erledigung der Fachprozesse oder -aufgaben zum Einsatz kommen wie beispielsweise Maschinen oder mobile Endgeräte, werden insofern betrachtet, dass für diese im IT-Grundschutz Sicherheitsanforderungen beschrieben sind.

Die Kernkomponenten des 5G-Campusnetzes werden in diesem IT-Grundschutz-Profil, soweit es für die Sicherheitsbetrachtung erforderlich ist, in seine einzelnen Bestandteile separiert.

Die tatsächlich im Informationsverbund der Anwendenden zum Einsatz kommenden Geschäftsprozesse und Zielobjekte sind im Rahmen der Strukturanalyse zu ermitteln. Die nachfolgend dargestellte Referenzarchitektur dient hierfür als Schablone.

5G-Campusnetze können in vielfältigen Nutzungsszenarien unterschiedlichster Institutionen in verschiedenen Branchen zum Einsatz kommen. In allen Szenarien unterstützt der Einsatz eines 5G-Campusnetzes bei der Abwicklung von Geschäftsprozessen, beispielsweise in der Erprobung, Fertigung und Logistik.

Die grundlegenden Sicherheitsanforderungen an die Nutzung und den Betrieb eines 5G-Campusnetzes sind in der Regel vergleichbar.

Die Provisionierung der SIM-Karten ist dem Betrieb zuzuordnen. Häufig werden die SIM-Karten bereits fertig provisioniert eingekauft. Dennoch wird in diesem IT-Grundschutz-Profil die eigene Provisionierung der SIM-Karten betrachtet.

In diesem IT-Grundschutz-Profil werden die Prozesse

- P1: 5G-Campusnetz nutzen
- P2: 5G-Campusnetz betreiben

stellvertretend für viele Nutzungsszenarien verwendet. Denkbar sind in nachfolgender Tabelle aufgeführte Teilprozesse, die bestimmte Aufgaben innerhalb des 5G-Campusnetzes ausführen.

Prozess	Teilprozess	Beschreibung (beispielhaft)
P1	Verbinden	Verbinden der im 5G-Campusnetz eingesetzten Endgeräte, Sensoren, Aktoren und weiterer Komponenten miteinander und dem 5G-Core
	Sammeln	Einsammeln von Daten beispielsweise mobiler und stationärer Sensoren
	Analysieren	Protokollieren, Bewerten und Auswerten der gesammelten Daten
	Umsetzen	Übertragen von Steuersignalen an Aktoren
P2	Planen	<p>Anforderungen aufstellen und deren Umsetzungsmöglichkeit prüfen und ausplanen hinsichtlich Netzgröße, benötigte Komponenten, Ausleuchtung, benötigte SIM-Karten etc.</p> <p>Häufig ist Unterstützung von Dienstleistenden notwendig. Bei großen Netzen sollte auf den Planungs-Knowhow von Dienstleistungsunternehmen zurückgegriffen werden</p>
	Bereitstellen	Komponenten des 5G-Campusnetz einkaufen, mieten, implementieren usw. Netz in Betrieb nehmen
	Monitoring	Netz hinsichtlich festgelegter Leistungsparameter, dessen Nutzung und deren Zielerreichung überwachen
	Service-Wartung	Allgemeine Wartungsarbeiten, wie Updates, Fehlerbeseitigung, Konfigurationsanpassungen oder Services, wie die Bereitstellung eines Service-Desk. Bei Einsatz eines externen Dienstleistungsunternehmens können Wartungsarbeiten via Fernwartung erfolgen.
	Service-SIM-Kartenverwaltung	<p>Beschaffung von SIM-Karten bei entsprechenden Anbietenden.</p> <p>SIM-Karten können dabei fertig provisioniert sein und sind in den Geräten damit voll einsatzfähig (Zuweisung von speziellen SIM-Karten-IDs (ICCID), IMSI-Nummern (International Mobile Subscriber Identity), Authentisierungsdaten und anderen erforderlichen Konfigurationen).</p> <p>Die Provisionierung der SIM-Karten kann durch die Betreibenden selbst erfolgen. Die SIM-Karten werden als „Rohlinge“ eingekauft. Die Provisionierung wird über eine SIM-Kartenmanagementlösung selbst vorgenommen. Die SIM-Karten werden mit den erforderlichen Konfigurationseinstellungen versehen, wie z. B. Netzeinstellungen, APN, Authentisierungsinformationen und anderer Parameter.</p> <p>Alle SIM-Karten müssen im Netz registriert und aktiviert sowie den Geräten zugeordnet werden und können dann in diesen eingesetzt werden. Sollten SIM-Karten nicht mehr zum Einsatz kommen, werden diese gesperrt und gegebenenfalls eingelagert oder vernichtet.</p> <p>Die SIM-Kartenverwaltung stellt eine nachvollziehbare Dokumentation sicher.</p>
	Aussondern	Geordnete Außerbetriebnahme und Entsorgung oder Rückgabe von Komponenten des 5G-Campusnetzes.

Tabelle 3: Mögliche Teilprozesse der P1: 5G-Campusnetz nutzen und P2: 5G-Campusnetz betreiben

Weiterhin findet eine Kommunikation zwischen unterschiedlichsten Endgeräten statt, wie beispielsweise Kameras, Smartphones, Laptops oder Tablets mit 5G-Modem. Die Sicherheitsanforderungen sind in jeder Institution individuell zu prüfen. Im vorliegenden IT-Grundschutz-Profil wird von erhöhtem Schutzbedarf bei einem Teil der Prozesse ausgegangen.

## 5.1 Anwendungen

Zum Informationsverbund gehören neben den Prozessen auch die Anwendungen. Innerhalb des 5G-Campusnetzes können verschiedene Fachanwendungen zur Unterstützung der zu erledigenden Aufgaben zum Einsatz kommen (beispielsweise Sensordaten erheben und weiterleiten). Darüber hinaus ist es möglich individuell entwickelte Software zum Einsatz zu bringen. All diese Anwendungen sollten entsprechend der IT-Grundschutz-Anforderungen abgesichert werden.

Insbesondere auf den in einem 5G-Campusnetz eingesetzten mobilen Endgeräten wird unterschiedliche, spezifische Software eingesetzt. In diesem IT-Grundschutz-Profil wird die für den genannten Prozess mit seinen Teilprozessen notwendige Software beschrieben. Dies können Anwendungen sein, um erfasste Daten zu visualisieren oder Befehle an Aktoren zu generieren. Darüberhinausgehende Software, beispielsweise diverse auf den Endgeräten vorinstallierte Apps, sind nicht Bestandteil dieses IT-Grundschutz-Profiles.

In der nachfolgenden Tabelle sind Anwendungen aufgeführt, die je nach Einsatz mit konkreten Softwarelösungen ausgestaltet werden.

Identifikator	Anwendungen des Informationsverbundes	Erläuternde Beispiele	Unterstützte Prozesse
A1	Datengenerierung (Sensor-Daten = Input)	Ermittlung von Messdaten (beispielsweise Temperatur oder Bewegungsdaten)	P1
A2	Reaktion auf (Sensor-)Daten (Aktorik = Output)	Übermittlung von Daten an Aktoren, wie zur Bewegungssteuerung von Robotern	P1
A3	Datenverarbeitung (Compute)	Auswertung ermittelter Sensordaten	P1
A4	Netzmanagementlösung	Lösung für die Netz- und Gerätekonfiguration, Sicherheits- und Leistungsmanagement und Fehlerbehebung	P2
A5	Monitoring	kontinuierliche Überwachung des 5G-Campusnetzes, um die geforderten Leistungsparameter und Sicherheit sowie die Verfügbarkeit der Komponenten zu gewährleisten, Detektion von Abweichungen und deren Meldung	P2
A6	SIM-Karten-managementlösung	Verwaltung der SIM-Karten, gegebenenfalls inklusive Provisionierung	P2
A7	5G-Core Funktionen	Diese Funktionen können direkt auf dem Server laufen oder auf der virtualisierten Umgebung  beispielsweise AF-Server (Authentication Funktion)	P2

Tabelle 4: Anwendungen des Informationsverbundes, die im 5G-Campusnetz verwendet werden.

## 5.2 IT-Systeme

Im Informationsverbund werden neben den Prozessen und Anwendungen auch die IT-Systeme betrachtet. In der Anwendung des IT-Grundschutz-Profiles ist zusätzlich noch das konkrete Betriebssystem der verwendeten IT-Systeme zu erfassen und mit den dazugehörigen Bausteinen zu modellieren. Aus Gründen der Übersichtlichkeit wird hier zunächst darauf verzichtet.

Die im 5G-Campusnetz eingesetzten Endgeräte können auch im Firmennetz (Intranet) benutzt werden. Dies wird in diesem Profil jedoch nicht betrachtet. Die sich aus dem Einsatz im Firmennetz zusätzlich ergebenden Risiken und Anforderungen müssen im individuellen Informationsverbund zusätzlich betrachtet werden.

Identifikator	IT-Systeme des Informationsverbundes	Abhängige Anwendungen bzw. IT-Systeme
S1	Smartphone, Tablet	A1, A2
S2	Laptop	A1, A2
S3	Mobiltelefon	A1, A2
S4	Kamera	A1
S5	5G-Core	A3, A7, A8
S6	gNodeB (Basisstation) mit den Funktionen <ul style="list-style-type: none"><li>• RU Radio Unit (Funkeinheit inkl. Antenne)</li><li>• CU Centralized Unit (dezentrale Aggregation für die umliegenden Funkeinheiten)</li><li>• DU Distributed Unit (zentrale Verarbeitung von Signalisierung und Nutzdaten)</li></ul>	S5
S7	Server zur Zeitsynchronisation (über Satellitenzeitsignal in der Regel Precision Time Protocol PTP)	S5, S6
S8	Management-Server	A4, A5, A6
S9	Endgerätenetzmanagement, um auf Anwendung zur SIM-Kartenverwaltung, Netzmanagement und dem Monitoring zugreifen zu können	A4, A5, A6
S10	Administrations-Laptop für lokale Konfiguration (5G-Core, Zeitsynchronisation, gNodeB)	A7, A8

Tabelle 5: IT-Systeme des Informationsverbundes

In einem 5G-Campusnetz können, je nach Einsatzzweck, Systeme zur Steuerung von Maschinen, Geräten und Fahrzeugen bzw. zur Verarbeitung von Daten zum Einsatz kommen. Diese Geräte sind grundsätzlich wie IT-Systeme zu behandeln. In nachfolgender Tabelle werden mögliche industrielle Komponenten aufgeführt.

Identifikator	Industrielle IT-Komponenten des Informationsverbundes	Abhängige Objekte
IN1	Prozessleittechnik	A1, A2
IN2	Produktionsmaschine	IN1
IN3	Sensor / Aktor	A1, A2

Identifikator	Industrielle IT-Komponenten des Informationsverbundes	Abhängige Objekte
IN4	Robotik	A1, A2

Tabelle 6: Industrielle IT-Systeme bzw. Komponenten des Informationsverbundes

### 5.3 Netze und Netzkomponenten

Bestandteil dieses IT-Grundschutz-Profiles ist ein lokales 5G-Campusnetz. Es verbindet via Funkzugangsnetz (RAN) verschiedene Anwendungen und Endgeräte mit dem 5G-Core. Die Radio Unit, der gNodeB und der 5G-Core bilden die Hauptkomponenten im 5G-Campusnetz.

Vom 5G-Core aus können anfallende Daten über die Schnittstelle der „User Plane Function“ (UPF) auf einem Datenspeicher außerhalb des 5G-Campusnetzes in das interne Firmennetz bereitgestellt werden. Ein unvollständiger Schutz des 5G-Campusnetz (Boundary Protection) gegenüber internen Zonen (Intranet) könnte zum Abfluss schützenswerter Informationen führen.

Im Firmennetz befindliche Netzkomponenten und IT-Systeme, die zum Betrieb des 5G-Campusnetzes erforderlich sind, werden als Teil des Informationsverbundes betrachtet. Alle weiteren IT-Komponenten und Komponenten des Firmennetzes liegen außerhalb des beschriebenen Informationsverbundes und müssen entsprechen zusätzlich betrachtet werden.

Eine direkte Anbindung des 5G-Campusnetzes an öffentliche Netze, wie das Internet oder das öffentliche Mobilfunknetz, besteht in dieser Betrachtung nicht. Der Fernzugang zu den Komponenten des 5G-Campusnetzes, beispielsweise durch Dienstleistende für die Wartung, kann nur über das interne Firmennetz des Anwendenden erfolgen. Somit gibt es keine verdeckte direkte Anbindung an ein öffentliches Netz, über die Dritte unkontrolliert auf das 5G-Campusnetz zugreifen können.

Aufgrund der aktuell noch selten eingesetzten Technologie Non-3GPP Access, wie beispielsweise WLAN-Sidelink, wird diese Anbindung im aktuell vorliegenden Profil nicht betrachtet. Alle Endgeräte in einem 5G-Campusnetz kommunizieren über das 5G-Netz. Dazu hat jedes Gerät mindestens eine Kennung, ähnlich der Telefonnummer. Eine Direktverbindung zwischen den Geräten ist ebenso unmöglich wie Broadcasts.

Ein beispielhafter schematischer Netzaufbau ist in Abbildung 1 zu sehen. Darin wird auch dargestellt, wie sich das 5G-Campusnetz in ein bestehendes Firmennetz integrieren lässt. Die in der Abbildung dargestellten Endgeräte sind exemplarisch zu sehen. In vielen Endgeräten, wie beispielsweise Fahrzeugen oder Drohnen befinden sich Sensoren, die über das 5G-Campusnetz Daten liefern.

Identifikator	Objekt des Informationsverbundes	Erläuterungen	Abhängige Objekte
NE1	Antenne (Radio Head)	Sende- und Empfangsantenne mit Radio Unit	S1, S2, S3, S4, S6, IN1, IN2, IN3
NE2	Ethernet Verbindungen	Kabelverbindung (Ethernet) zwischen den Netzkomponenten und IT-Systemen im 5G-Campusnetz sowie zu restlichen Netzbereichen einer Institution	S5, NE3, NE6, S7, S8
NE3	Switch-Architektur	Die Integration der 5G-Campusnetz-Komponenten kann über die im Firmennetz bestehenden Switches und Netzkomponenten erfolgen	NE2
NE4	5G-Campusnetz	Gesamtheit des 5G-Campusnetz inkl. eingebundener Komponenten	NE1, NE2, NE3



Identifikator	Objekt des Informationsverbundes	Erläuterungen	Abhängige Objekte
NE5	Managementnetz	Im allgemeinen Firmennetz bereits bestehendes Managementnetz, Nutzung zur Administration und Netzmanagement des 5G-Campusnetzes	
NE6	Firewall Managementnetz	Schnittstelle zwischen Managementnetz und Firmennetz	NE6, NE2, NE4
NE7	Firewall Außenanbindung	Schnittstelle vom Firmennetz zum öffentlichen Internet	NE2

*Tabelle 7: Netzkomponenten und Netze des Informationsverbundes.*

## Netzplan

Die nachfolgende Abbildung beinhaltet einen vereinfachten Netzplan für ein exemplarisch dargestelltes 5G-Campusnetz. In diesem Netzplan sind die Schichten der IT-Systeme und des Netzes abgebildet. Aus Gründen der Übersichtlichkeit wurde auf die Darstellung weiterer Schichten aus dem Informationsverbund verzichtet.

Im Informationsverbund werden nur Teile aus dem bestehenden Firmennetz berücksichtigt, die zwingend für den Betrieb eines 5G-Campusnetzes erforderlich sind. Diese Komponenten können entsprechend genutzt werden.

Anwendenden und Betreibenden eines 5G-Campusnetzes steht es frei, abweichend von der nachfolgenden Darstellung, parallel für den Betrieb eine eigene Infrastruktur aufzubauen. Diese kann durch eine weitere Firewall vom restlichen Netz getrennt sein.

Das Netzsegment und die IT-Systeme, die nicht im Informationsverbund berücksichtigt werden, sind zur vollständige Darstellung informativ aufgeführt und eigens gekennzeichnet.

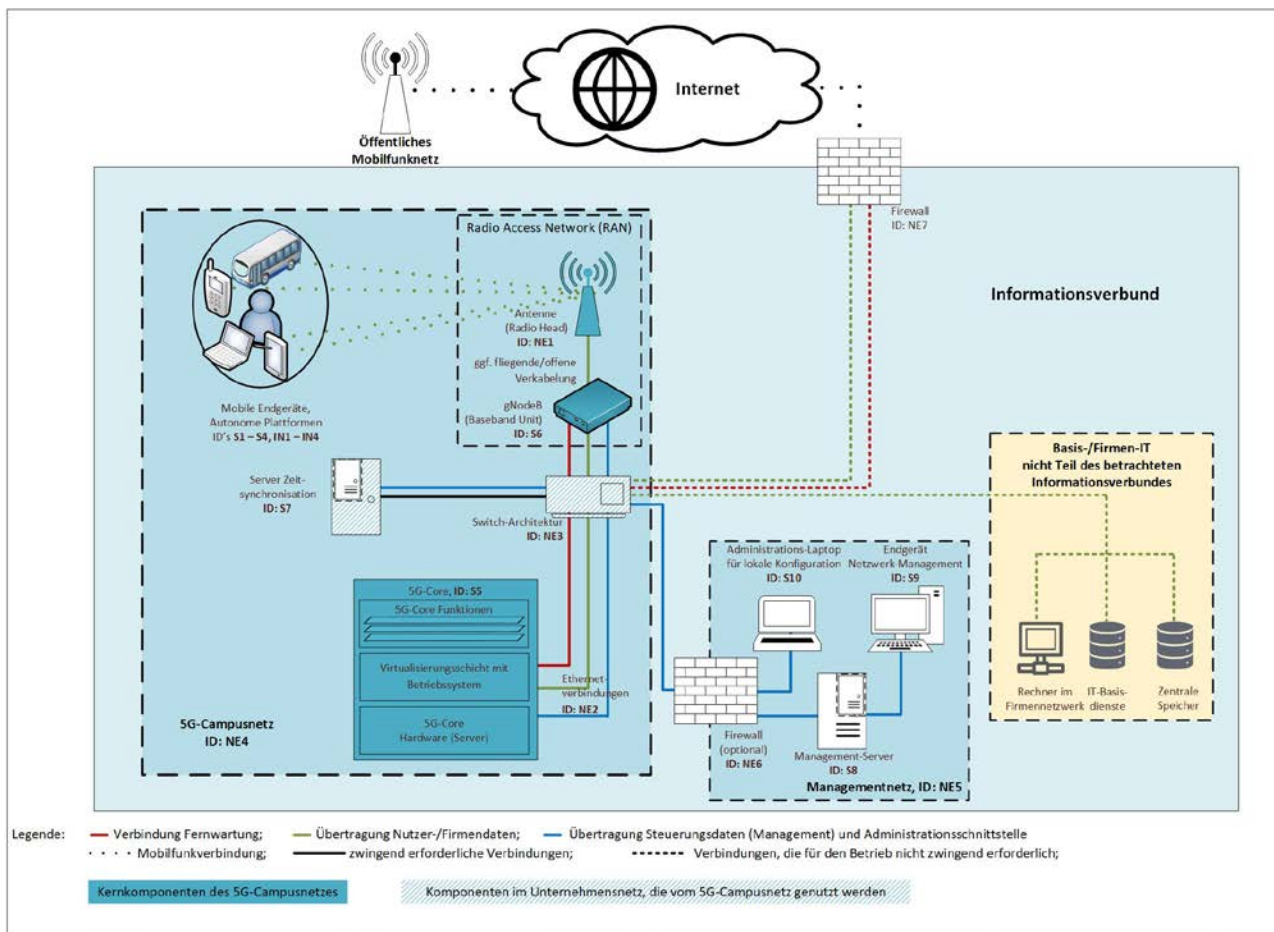


Abbildung 1: Muster-Netzplan für ein 5G-Campusnetz, der Grundlage dieses IT-Grundschutz-Profiles ist. Es handelt sich um eine Darstellung, die auf generische Art verschiedenste Nutzungsszenarien berücksichtigt.

## 5.4 Infrastruktur

Der 5G-Core und häufig auch der gNodeB befinden sich entweder in einem Serverraum oder in einer ortsveränderlichen Einhausung. Die Einhausung kann unterschiedlichste Größen annehmen.

Im Weiteren werden alle Unterbringungsmöglichkeiten des 5G-Core unter dem Begriff „Raum oder Einhausung mit 5G-Core“ zusammengefasst.

Der Betrieb eines 5G-Campusnetzes ist nur innerhalb des von der Bundesnetzagentur lokal lizenzierten Bereiches und der genehmigten Frequenzbänder zulässig. Befindet sich ein 5G-Campusnetz außerhalb des lokalen Bereiches, muss es abgeschaltet werden.

In nachfolgender Tabelle sind die notwendigen Infrastrukturkomponenten in einem 5G-Campusnetz aufgeführt.

Identifikator	Räume des Informationsverbundes	In den Räumen installierte IT-Systeme
R1	Raum oder Einhausung mit 5G-Core	S5, S6, NE1
R2	Stromversorgung	S5, S6, NE1
R3	Gebäude inklusive Außenbereiche der Institution	NE2, NE3
R4	Verkabelung in Einhausung	R1, R2, S5

Identifikator	Räume des Informationsverbundes	In den Räumen installierte IT-Systeme
R5	Verkabelung zwischen 5G-Core und angeschlossenen Komponenten und dem allgemeinen Firmennetz	R3, S5, S6

*Tabelle 8: Räume des Informationsverbundes*

## 5.5 Umgang mit Abweichungen

Weicht der zu schützende Informationsverbund von der hier dargestellten Referenzarchitektur ab, müssen die zusätzlich vorhandenen Zielobjekte im Rahmen der Strukturanalyse dokumentiert werden. Die Objekte sollten passenden Komponenten des IT-Grundschutz-Kompendium zugeordnet werden. Die abgeleiteten Anforderungen müssen an den jeweiligen Schutzbedarf angepasst werden.

Zielobjekte aus diesem IT-Grundschutz-Profil, die im zu schützenden Informationsverbund nicht vorkommen, brauchen entsprechend nicht berücksichtigt werden.

# 6 Feststellung des Schutzbedarfes

Für die im Rahmen der Strukturanalyse ermittelten Prozesse, Anwendungen, IT-Systeme und Kommunikationsverbindungen sowie Infrastrukturkomponenten muss zunächst der Schutzbedarf festgelegt werden.

Grundlegend dafür sind die Auswirkungen, die eine Verletzung der Grundwerte der Informationssicherheit Vertraulichkeit, Integrität oder Verfügbarkeit hätten. Geeignete Ansprechpartner und Ansprechpartnerinnen für die Schutzbedarfsfeststellung der Prozesse sind beispielsweise Prozessverantwortliche oder Data Owner der im jeweiligen Prozess verarbeiteten Daten.

Der Schutzbedarf vererbt sich grundsätzlich nach dem Maximumprinzip aus den ermittelten Prozessen auf die darin verwendeten Zielobjekte. Die Vererbungsprinzipien des Schutzbedarfes sind im BSI-Standard 200-2 näher erläutert.

Der BSI IT-Grundschatz benennt verschiedene Szenarien, auf die sich ein Schaden beziehen kann. Diese sind in nachfolgender Tabelle aufgeführt.

Identifikator	Schadensszenario
SZ1	Verstöße gegen Gesetze, Vorschriften oder Verträge
SZ2	Beeinträchtigungen des informationellen Selbstbestimmungsrechts
SZ3	Beeinträchtigungen der persönlichen Unversehrtheit
SZ4	Beeinträchtigungen der Aufgabenerfüllung
SZ5	negative Innen- oder Außenwirkung
SZ6	finanzielle Auswirkungen

*Tabelle 9: Potenzielle Schadensszenarien*

Da dieses IT-Grundschatz-Profil nicht auf individuelle Informationsverbünde eingehen kann, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt.

Die konkreten Auswirkungen und damit möglichen Schadensszenarien können je nach Anwendungsfall bzw. Einsatzgebiet des 5G-Campusnetzes variieren. Daher sollte die Einschätzung der Schadensszenarien und deren Auswirkungen auf die Grundwerte durch jeden Anwendenden eines 5G-Campusnetzes sorgfältig durchgeführt werden. In nachfolgender Tabelle sind mögliche Beispiele zu den Schadensszenarien aufgeführt:

Identifikator	Schadensszenario
SZ1	Eine unvollständige und langsame Übertragung sowie Übertragung schädlich veränderter Daten führt zu Schäden an Produkten, Beeinträchtigungen von Prozessen und Dienstleistungen und damit zu Vertragsverletzung, gegebenenfalls wird dadurch gegen gesetzliche oder regulatorische Vorschriften verstoßen.
SZ2	Personenbezogene Daten von Kunden werden ohne Autorisierung öffentlich zugänglich und dadurch für jedermann einsehbar. Es kann zu Verstößen gegen gesetzliche Vorschriften kommen.  Unternehmenskritische bzw. -vertrauliche Daten werden ohne Autorisierung öffentlich zugänglich. Dies kann zu finanziellen Nachteilen führen.
SZ3	Eine unvollständige Datenübertragung oder die Übertragung von schädlich veränderten Daten führt zu Fehlsteuerung von Maschinen oder Geräten, bzw. führen zu falschen Entscheidungen im Prozessablauf in deren Folge es zu Unfällen mit Personenschäden kommen kann.
SZ4	Eine unvollständige und langsame Datenübertragung führt zur Einschränkung oder zum Ausfall der Aufgabenerfüllung.
SZ5	Eine unvollständige und langsame Übertragung sowie Übertragung schädlich veränderter Daten führen zu Imageschäden.
SZ6	Eine unvollständige und langsame Übertragung sowie Übertragung schädlich veränderter Daten führen zu Produktions-, Dienstleistungs- oder Prozessausfällen bzw. Einschränkungen sowie Schäden an Geräten und Maschinen, die zu zusätzlichen Kosten führen.

Tabelle 10: Beispiele für potenzielle Schadensszenarien

Die Schadensauswirkung kann dabei im Voraus normalerweise nicht detailgenau festgelegt werden. Daher empfiehlt die IT-Grundschutz-Methodik des BSI drei Kategorien zu nutzen, um den Schutzbedarf zu bestimmen. Die drei Kategorien sind *normal*, *hoch* oder *sehr hoch*. Die nachstehende Tabelle führt die Kategorien, ergänzt um die Schadensauswirkungen auf. Die Schadensauswirkung wird dabei auf den Informationsverbund bezogen. Schäden, die im Informationsverbund auftreten, können sich auf die Institution selbst oder Dritte auswirken.

Der normale Schutzbedarf deckt dabei ein Standard-Sicherheitsniveau ab und kann ausreichend durch die Umsetzung der Anforderungen aus dem IT-Grundschutz abgedeckt werden. Für normalen Schutzbedarf ist die Risikoanalyse implizit und wird in den Basis – und Standard-Anforderungen hinreichend berücksichtigt.

Der Zusammenhang zwischen Schutzbedarf, der Auswahl der IT-Grundschutz-Anforderungen sowie der Risikoanalyse wird in nachfolgenden Kapiteln erläutert.

Kategorie	Schadensauswirkung
Normal	Die Schadensauswirkungen sind begrenzt und überschaubar.
Hoch	Die Schadensauswirkungen können beträchtlich sein.
Sehr hoch	Die Schadensauswirkungen können ein existenziell- oder lebensbedrohliches Ausmaß erreichen.

Tabelle 11: Vom BSI empfohlene Schutzbedarfskategorien.

Nachfolgend wird das Vorgehen in der Schutzbedarfsfeststellung beispielhaft für die Anwendenden eines 5G-Campusnetzes erläutert.

Werden in einem Geschäftsprozess Daten zur Überwachung der Abläufe erhoben und verarbeitet, sind potenzielle Schadensauswirkungen in jedem der vorab definierten Schadensszenarien zu ermitteln, wenn die Daten nicht zur

Verfügung (Verfügbarkeit) stehen oder nicht korrekt zur Verfügung (Integrität) gestellt werden. Im Ergebnis könnten beispielsweise Verschleißgrenzen, Temperaturanomalien oder Abweichungen von vorgegeben Fahrwegen nicht (rechtzeitig) erkannt werden, sodass es in der Folge zu Defekten oder schwerwiegenden Unfällen kommt. In diesen Fällen können finanzielle Schäden sowie Personenschäden entstehen und zusätzlich die Aufgabenerfüllung des Prozesses eingeschränkt sein. Der Schutzbedarf hinsichtlich Vertraulichkeit ist gleichfalls zu ermitteln.

Werden in einem Geschäftsprozess Daten zur Steuerung von Maschinen oder anderen Geräten benötigt, beispielsweise für die Herstellung von Produkten oder den Transport von Gütern, so sind die Schadensauswirkungen nach dem gleichen Vorgehen zu bewerten und der Schutzbedarf für die Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität festzustellen. Mögliche Auswirkungen könnten sein, dass beispielsweise vertraglich vereinbarte Qualitätsmerkmale durch Produktionsfehler nicht eingehalten werden können, oder eine Fehlsteuerung von Transportmitteln zu Unfällen führen kann.

Werden in einem der Schadensszenarien beträchtliche oder auch existenzbedrohende bzw. lebensbedrohliche Auswirkungen festgestellt, so ist der betroffene Grundwert im Schutzbedarf mit hoch oder sehr hoch einzustufen, in allen anderen Fällen mit normal.

Im Weiteren wird der ermittelte Schutzbedarf je Grundwert auf die Schicht der Anwendungen vererbt, beispielsweise auf die Software, die zur Datengewinnung und deren Auswertung verwendet wird. Anschließend erfolgt die Weitervererbung auf die IT-Systeme, welche die Software benötigen bzw. auch auf die IT-Systeme bzw. industriellen Komponenten, die durch die Software bedient werden.

Aus der Schicht der IT-Systeme vererbt sich der Schutzbedarf weiter auf die Netze und die Räumlichkeiten bzw. Infrastrukturobjekte, in denen sich die IT-Systeme befinden.

Darüber wird sichergestellt, dass alle einem Geschäftsprozess zur Erfüllung dienenden Zielobjekte das erforderliche Schutzniveau erreichen. Darüber hinaus kann aber auch vermieden werden, unangemessene und überbeuerte Schutzmaßnahmen umzusetzen.

In diesem IT-Grundschutz-Profil wird angenommen, dass ein 5G-Campusnetz insbesondere in Bereichen bzw. Prozessen zum Einsatz kommt, in denen erhöhte Anforderungen an die Verfügbarkeit und Integrität von Daten bestehen.

Entsprechend werden bei der Auswahl der Anforderungen in den Bausteinen des IT-Grundschutz-Kompendiums auch Anforderungen an erhöhten Schutzbedarf ermittelt, die der Absicherung eines 5G-Campusnetzes dienen.

Anwendenden kann in der Schutzbedarfsfeststellung zu einem abweichenden Ergebnis kommen, und diesen mit „normal“ in allen Grundwerten einstufen. Dann ist die Anwendung der Basis- und Standard-Anforderungen aus dem IT-Grundschutz-Kompendium ausreichend.

# 7 Zu erfüllende Anforderungen und umzusetzende Maßnahmen

Das IT-Grundschutz-Kompendium des BSI stellt Bausteine bereit, die anwendungsbezogene Anforderungen zur Umsetzung des IT-Grundschutzes geben.

Nachdem der Schutzbedarf für die Zielobjekte im Informationsverbund bestimmt wurde, werden im Rahmen der Modellierung die für die Abbildung des Informationsverbundes relevanten Bausteine aus dem IT-Grundschutz-Kompendium identifiziert. Alle in den Bausteinen aufgeführten Basis- und Standard-Anforderungen müssen umgesetzt werden. Können in Ausnahmefällen Anforderungen nicht umgesetzt werden, ist dies zu begründen.

Liegt erhöhter Schutzbedarf vor, so ist bei den Anforderungen für erhöhten Schutzbedarf zu prüfen, ob diese umgesetzt werden können. Im Rahmen einer Risikoanalyse sind dann darüber hinaus erweiterte Sicherheitsmaßnahmen zu definieren.

Auf Basis der Anforderungen müssen an den Informationsverbund angepasste Maßnahmen definiert und anschließend umgesetzt werden.

In diesem IT-Grundschutz-Profil werden spezifische Hinweise zu ausgewählten Anforderungen, die auf ein 5G-Campusnetz wirken, gegeben.

Die Auswahl der relevanten Bausteine und die Beschreibung der zu erfüllenden Anforderungen sind in einer separaten dem Dokument beigefügten Exceltabelle zu finden. Diese umfasst folgende Tabellenblätter:

- Anlage 1: Kap. 7.1 Auswahl Prozessbausteine
- Anlage 2: Kap. 7.1 Auswahl Systembausteine
- Anlage 3: Kap. 7.2 Anforderungen Prozessbausteine
- Anlage 4: Kap. 7.3 Anforderungen spezifischer Systembausteine

## 7.1 Auswahl relevanter Bausteine

Auf Basis der festgelegten Referenzarchitektur mit den relevanten Zielobjekten wird nun der Informationsverbund mit den Bausteinen aus dem IT-Grundschutz-Kompendium nachgebildet. In diesem IT-Grundschutz-Profil werden diejenigen Bausteine modelliert, die zur Absicherung der Zielobjekte eines 5G-Campusnetzes anzuwenden sind.

Mit dieser Vorgehensweise fokussiert sich dieses IT-Grundschutz-Profil auf die wesentlichen und wiederverwendbaren Aspekte. Unabhängig davon, muss von jeder Institution, die ein 5G-Campusnetz einsetzt, untersucht werden, inwiefern der eigene Informationsverbund vom IT-Grundschutz-Profil abweicht. Um eine vollständige Standard-Absicherung umzusetzen, sind weitere Bausteine aus dem IT-Grundschutz-Kompendium zu berücksichtigen.

Die im IT-Grundschutz-Kompendium auszuwählenden Bausteine unterteilen sich in die Prozess-Bausteine sowie System-Bausteine.

### Auswahl der Prozessbausteine

Auf jeden Informationsverbund sind die übergreifenden Prozess-Bausteine anzuwenden. Diese behandeln Sicherheitsaspekte, die für große Teile des Informationsverbundes gleichermaßen gelten. In diesem Dokument werden die Prozess-Bausteine daraufhin geprüft, ob diese auf den vorliegenden Informationsverbund

anzuwenden sind. Die Auswahl der relevanten Prozessbausteine (Bezeichnung in Spalten B und C) ist in Anlage 1 Kap. 7.1 Prozessbausteine (Excel-Tabelle) dargestellt. Sind im IT-Grundschutz-Kompendium vorliegende Bausteine für den abgebildeten Informationsverbund nicht relevant, so wird dies in Spalte E begründet.

Ein geringer Teil der Prozessbausteine wird in den meisten Anwendungsfällen nicht modelliert werden. Beispielsweise ist der Baustein „CON.7 Informationssicherheit auf Auslandsreisen“ nur dann anzuwenden wenn tatsächlich Teile des Informationsverbundes auch im Ausland eingesetzt werden sollen.

## **Auswahl der System-Bausteine**

In diesem Abschnitt werden die System-Bausteine auf ihre Relevanz hin eingeschätzt. Hier ist entscheidend, ob der Baustein für eine spezifische, in Abschnitt 5 bestimmte, Komponente relevant ist. Die Auswahl der relevanten System-Bausteine (Bezeichnung in Spalten B und C) ist in Anlage 1 Kap. 7.1 Prozessbausteine (Excel-Tabelle) dargestellt. Sind im IT-Grundschutz-Kompendium vorliegende Bausteine für den abgebildeten Informationsverbund nicht relevant, so wird dies in Spalte F begründet.

Weicht der Informationsverbund des Anwendenden von diesem IT-Grundschutz-Profil ab, bzw. umfasst der Informationsverbund weitere in diesem IT-Grundschutz-Profil nicht beschriebene Zielobjekte, sind weitere System-Bausteine zusätzlich auf den Informationsverbund anzuwenden.

Die System-Bausteine sind direkt auf die im Informationsverbund eingesetzten Zielobjekte anzuwenden. Die Zuordnung der Zielobjekte zu den aufgeführten Bausteinen ist in Spalte E aufgeführt.

Folgende Hinweise gelten für die Bausteine der jeweiligen Schichten aus dem IT-Grundschutz Kompendium:

### **APP: Anwendungen**

Werden im betrachteten Informationsverbund Fachanwendungen eingesetzt, so sind zusätzlich die passenden Bausteine aus dem IT-Grundschutz-Kompendium anzuwenden.

### **SYS: IT-Systeme**

Ja\* -In Abhängigkeit der im 5G-Campusnetz eingesetzten IT-Systeme müssen diese Bausteine angewendet werden. Gegebenenfalls sind die zum genutzten Betriebssystem zugehörigen Bausteine zusätzlich zu den allgemeinen Bausteinen für die Komponenten zu modellieren.

### **IND: Industrielle IT**

Die in dieser Schicht aufgeführten Bausteine kommen auch in Nutzungsszenarien außerhalb der Industrie vor, beispielsweise Logistik und medizinische Nutzungsszenarien.

### **NET: Netze und Kommunikation**

Einige IT-Grundschutz Bausteine aus der Schicht Netze- und Kommunikation werden auf IT-Systeme angewendet.

### **INF: Infrastruktur**

Die in diesem Profil benötigten Bausteine enthalten neben den Anforderungen für die Gebäude- und Rauminfrastruktur auch Anforderungen zur physischen Verkabelung.

## **7.2 Anforderungen aus den IT-Grundschutz-Bausteinen**

In der Modellierung wurden die IT-Grundschutz-Bausteine den Zielobjekten zugeordnet. In den IT-Grundschutz-Bausteinen sind Anforderungen enthalten, die zur Absicherung des Informationsverbundes umgesetzt werden sollen. Die Anforderungen unterteilen sich in Basis- und Standard-Anforderungen, sowie Anforderungen bei erhöhtem Schutzbedarf.



Die Basis-Anforderungen in relevanten Bausteinen müssen immer umgesetzt werden und sind auf geeignete Weise zu erfüllen. Mit deren Erfüllung wird ein grundlegendes Sicherheitsniveau erreicht. Werden Basis-Anforderungen nicht umgesetzt, kann das zu erheblichen Sicherheitslücken und sehr hohen Risiken führen.

Basis-Anforderungen werden in der Regel durch die Nominalverben MUSS oder MÜSSEN und DARF NICHT oder DÜRFEN NICHT beschrieben.

Standard-Anforderungen sind ebenfalls grundsätzlich auf geeignete Weise zu erfüllen. Eine Nichtumsetzung ist nur in begründeten Einzelfällen zulässig. In einem solchen Fall müssen die sich aus der Nichtumsetzung ergebenden Risiken der Institutionsleitung transparent gemacht werden. Mit der Umsetzung der Standard-Anforderungen wird ein sogenanntes Standard-Sicherheitsniveau erreicht. Mit der Umsetzung dieser Anforderungen kann davon ausgegangen werden, dass in Bereichen, die einem normalen Schutzbedarf unterliegen, alle Risiken ausreichend behandelt sind. Es wird ein akzeptables Risikoniveau erreicht.

Standard-Anforderungen werden in der Regel mit den Nominalverben SOLLTE oder SOLLTEN und SOLLTE NICHT oder SOLLTEN nicht beschrieben. Entgegen der allgemeinen Verwendung der o. g. Nominalverben ist hier zu beachten, dass die hier genutzte Definition auf [RFC2119] sowie DIN 820-2:2012, Anhang H basiert.

Der BSI Standard 200-2 führt dazu aus:

SOLLTE: Dieser Ausdruck bedeutet, dass eine Anforderung normalerweise erfüllt werden muss, es aber Gründe geben kann, dies doch nicht zu tun. Dies muss aber sorgfältig abgewogen und stichhaltig begründet werden.

Die Anforderungen bei erhöhtem Schutzbedarf sind zusätzlich zu beachten, wenn für das betreffende Zielobjekt in einem der Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit ein hoher oder sehr hoher Schutzbedarf festgelegt wurde. Da in diesen Fällen zwingend eine Risikoanalyse durch den Anwendenden durchzuführen ist und hier gegebenenfalls erweiterte Sicherheitsmaßnahmen umzusetzen sind, haben diese Anforderungen empfehlenden Charakter.

Diese Anforderungen werden ebenfalls mit den SOLLTE oder SOLLTEN und SOLLTE NICHT oder SOLLTEN nicht beschrieben.

Die zu erfüllenden Anforderungen sind in den beigefügten Anlagen beschrieben. Zu einigen Anforderungen sind spezifische Hinweise beschrieben, die speziell im Kontext zur Absicherung eines 5G-Campusnetzes stehen. Ist das Umsetzen spezifischer Maßnahmen zur Erfüllung der Anforderungen erforderlich, werden diese zusätzlich beschrieben.

## **Anforderungen übergreifend gültiger Prozess-Bausteine**

Die Prozess-Bausteine beschreiben Anforderungen, die übergreifend auf den Informationsverbund wirken. Es handelt sich dabei in den meisten Fällen um umzusetzende prozessuale, organisatorische und personelle Vorgaben oder übergreifend wirkende Konzepte, die über mehrere Systeme hinweg wirken.

Die zu erfüllenden Anforderungen der Prozess-Bausteine sind mit den entsprechenden Hinweisen in der beigefügten Exceltabelle im Reiter Anl. 3 Kap. 7. 2 Anf. Prozessbausteine beschrieben. Liegt im Informationsverbund erhöhter Schutzbedarf vor, ist bei den Prozess-Bausteinen zu prüfen, ob zusätzlich zu den Basis- und Standard-Anforderungen die Anforderungen bei erhöhtem Schutzbedarf relevant sind. Dann sollten diese umgesetzt werden. Anforderungen, welche den erhöhten Schutzbedarf adressieren und einen konkreten Bezug zur Nutzung eines 5G-Campusnetzes aufweisen, werden in der Exceltabelle explizit benannt.

## **Anforderungen spezifisch gültiger System-Bausteine**

Die System-Bausteine beschreiben systemspezifische Sicherheitsanforderungen und werden auf die in der Referenzarchitektur aufgeführten Zielobjekte angewendet.

In der beigefügten Exceltabelle werden die relevanten Bausteine aufgeführt. Es werden auch hier zu einzelnen Anforderungen spezifische Hinweise mit Bezug zum 5G-Campusnetz gegeben.

Sind bei einzelnen Bausteinen zusätzlich zu den Basis- und Standard-Anforderungen, die Anforderungen bei erhöhtem Schutzbedarf je nach vorliegender individueller Schutzbedarfsfeststellung relevant, werden diese extra benannt.

Die zu erfüllenden Anforderungen der System-Bausteine sind mit den entsprechenden Hinweisen in der beigefügten Exceltabelle im Reiter Anl. 3 Kap. 7.2 Anf. Systembausteine beschrieben.

### 7.3 Anforderungen an spezifische Zielobjekte

Nicht alle im betrachteten Informationsverbund eingesetzten Zielobjekte können mit den im IT-Grundschutz-Kompendium vorhandenen Bausteinen ausreichend nachgebildet werden. Für solche Zielobjekte ist eine Risikoanalyse obligatorisch durchzuführen und die entsprechenden Anforderungen sind zu definieren.

Die Anforderungen können in einem eigenen Baustein abgebildet werden. Ein eigener Baustein ist vor allem dann zweckmäßig, wenn die betroffenen Geräte mehrfach eingesetzt werden. Dann verkürzt sich der Aufwand der Risikoanalyse. Benutzerdefinierte Bausteine können auch bereits von Dritten bereitgestellt werden. Um diese von den im Kompendium enthaltenen Bausteinen abzugrenzen, werden diese Bausteine unabhängig von der Quelle so benannt.

In diesem Baustein sind folgende Aspekte zu behandeln:

- Abgrenzung zu vorhandenen Bausteinen,
- Spezifische Gefährdungslage,
- Anforderung für unterschiedliche Schutzbedarfe,
- Verweis auf einschlägige Normen und Veröffentlichungen,
- Kreuzreferenztafel für Risikoanalyse.

Ein 5G-Campusnetz wird im Wesentlichen aus dem 5G-Core, gNodeB und der Radio Unit bereitgestellt. Grundsätzlich lassen sich diese Komponenten mit den im IT-Grundschutz-Kompendium vorhandenen Bausteinen abbilden.

Spezifische Anforderungen an den Betrieb eines 5G-Campusnetzes und die darin notwendigen Antennen werden im benutzerdefinierten Baustein *NET.bd.2.3 Betrieb privater Mobilfunknetze (5G-Campus)* beschrieben.

Da im privaten Mobilfunk der Einsatz von SIM-Karten und deren sichere Verwaltung eine wesentliche Rolle spielen, werden die damit in Verbindung stehenden Sicherheitsanforderungen in einem eigenen benutzerdefinierten Baustein *CON.bd.1 Verwaltung von SIM-Karten* beschrieben.

Der 5G-Core und der gNodeB können sich in einer abgeschlossenen ortsveränderlichen Einhausung befinden, insbesondere dann, wenn das Netz an unterschiedlichen Orten zum Einsatz kommen soll. Um die spezifischen mit der Ortsveränderlichkeit verbundenen Anforderungen an eine solche Einhausung abzubilden, wurde ein benutzerdefinierter Baustein *INF.bd.1 Ortsveränderliche Einhausung für IT-Systeme* erarbeitet. Dieser steht für die Modellierung im Informationsverbund zur Verfügung.

Darüber hinaus können innerhalb eines 5G-Campusnetzes je nach Einsatzgebiet spezifische Objekte zum Einsatz kommen, die mit den vorhandenen Bausteinen des IT-Grundschutz nicht hinreichend modelliert werden. Diese müssen ebenfalls gesondert betrachtet und einer Risikoanalyse unterzogen werden. Daraus sind dann gemäß der IT-Grundschutzmethode Anforderungen abzuleiten, um das angestrebte Schutzniveau zu erreichen.

# 8 Risiko

Auch bei der Umsetzung aller Anforderungen verbleiben Risiken, die zu betrachten sind. Dies muss sowohl den Anwendenden des IT-Grundschutz-Profils als auch den Entscheidungsträgern bewusst sein. Das Restrisiko wird ermittelt, transparent gemacht und kommuniziert.

In einigen Fällen ist es zwingend erforderlich eine Risikoanalyse zu erstellen. Dies ist insbesondere der Fall, wenn:

- in einem Geschäftsprozess und damit für die darin benötigten Zielobjekte erhöhter Schutzbedarf festgestellt wurde, oder
- es für ein Zielobjekt keinen passenden Baustein im IT-Grundschutz-Kompendium gibt.

Für den Schutzbedarf „normal“ sind nach der IT-Grundschutzmethodik die Risiken mit der Erfüllung der Basis- und Standard-Anforderungen bereits ausreichend behandelt. Der Nachweis über die berücksichtigten spezifischen Gefährdungen und damit der Durchführung der Risikoanalyse ist mit dem Kapitel 2 im IT-Grundschutz-Baustein erbracht.

Bei erhöhtem Schutzbedarf decken die Anforderungen möglicherweise die tatsächlichen Risiken nicht ausreichend ab, sodass hier zwingend die Risikoanalyse durchgeführt werden muss.

In nachfolgender Tabelle wird der Zusammenhang zwischen dem ermittelten Schutzbedarf, der Auswahl der IT-Grundschutz-Anforderungen und der Risikoanalyse dargestellt.

IT-Grundschutz-Anforderungen	Beschreibung Schutzbedarf	Risikoanalyse
Basis	Decken ein Mindestsicherheitsniveau ab. Diese müssen daher immer umgesetzt werden, sofern der Baustein relevant ist.	Die Risikoanalyse wurde durch das BSI für die Basis- und Standard-Anforderungen implizit durchgeführt. Daher wird mit der Erfüllung der Basis- und Standard-Anforderungen der normale Schutzbedarf ausreichend abgedeckt und weitere Risikoanalysen sind im Regelfall nicht erforderlich. Zum Nachweis der betrachteten Gefährdungslage wird in jedem Baustein das Kapitel 2 genutzt.
Standard	In Verbindung mit den Basis-Anforderungen sind die Standard-Anforderungen des IT-Grundschutzes ausreichend und angemessen, um dem normalen Schutzbedarf gerecht zu werden. Mit deren Erfüllung wird ein Standard-Sicherheitsniveau erreicht.	
Bei erhöhten Schutzbedarf	Die Erfüllung der Basis- und Standard-Anforderungen ist unter Umständen nicht ausreichend. Die im IT-Grundschutz beschriebenen Anforderungen für erhöhten Schutzbedarf (hoch und sehr hoch) können das erforderliche Schutzniveau abdecken.	Für die Zielobjekte mit erhöhten Schutzbedarf, muss eine Risikoanalyse explizit durchgeführt werden, da mit Erfüllung der Standard-Anforderungen die Risiken nicht ausreichend abdeckt sind.

Tabelle 12: Zusammenhang zwischen Schutzbedarf, IT-Grundschutz-Anforderungen und der Risikoanalyse

Sowohl der Betrieb eines 5G-Campusnetzes, als auch der Einsatz von SIM-Karten in einem solchen Mobilfunknetz sowie die Unterbringung der Kernkomponenten in transportablen Einhausungen außerhalb fester Gebäude ist bisher nicht durch das IT-Grundschutz Kompendium vollständig abgedeckt.

Es können sich daher für den Informationsverbund und die entsprechenden Zielobjekte zusätzliche Gefährdungen ergeben. In diesen Fällen müssen jeweils Risikoanalysen durchgeführt werden.

Es empfiehlt sich daher die in den drei zugehörigen benutzerdefinierten Bausteinen (siehe Kapitel 7.4 Anforderungen an spezifische Zielobjekte)

- Betrieb 5G-Campus
- SIM-Karte
- Transportable Einhausung

berücksichtigten elementaren Gefährdungen konsolidiert zu betrachten und gegebenenfalls um zusätzliche spezifische Gefährdungen zu erweitern.

Für alle drei Fälle wurden benutzerdefinierte Bausteine erstellt (siehe Kapitel 7.4 Anforderungen an spezifische Zielobjekte). In diesem Zusammenhang wurden exemplarische Risikoanalysen durchgeführt und dabei sowohl zutreffende elementare Gefährdungen ermittelt als auch sich daraus ergebende spezifische Gefährdungen beschrieben. Die ermittelten elementaren Gefährdungen sind in der jeweiligen Kreuzreferenztabelle zum Baustein abgebildet. Die spezifischen Gefährdungen werden im Kapitel 2 des jeweiligen Bausteins beschrieben.

Diese können als Grundlage für eine Risikoanalyse dienen, jedoch sollte für den individuellen Informationsverbund analysiert werden, ob es weitere zu betrachtende Gefährdungen gibt.

Im Weiteren wird das Vorgehen der Risikoanalyse nach dem BSI-Standards 200-3 empfohlen. In diesem BSI-Standard werden bereits 47 elementare Gefährdungen aufgeführt, die im IT-Grundschutz-Kompendium näher erläutert werden. Diese Gefährdungen sollten dabei Ausgangspunkt für die Erstellung der Gefährdungsübersicht sein und sollten bei Bedarf jedoch ergänzt werden.

Besondere Restrisiken, wie beispielsweise Überspannung durch Blitzschlag, Sabotage und Zerstörung durch Angreifende, können sich insbesondere aus dem Umstand ergeben, dass die Infrastruktur von 5G-Campusnetzen außerhalb fester Gebäude und Räumlichkeiten unter freiem Himmel aufgebaut werden kann.

Die im Rahmen einer Risikoanalyse auf Basis des BSI-Standard 200-3 zu durchlaufenden Schritte werden in den nachfolgenden Abschnitten erläutert.

## **Schritt 1: Erstellung einer Gefährdungsübersicht:**

Grundsätzlich werden nach dem BSI-Standard 200-3 die Risikoanalysen auf Ebene der Zielobjekte durchgeführt und damit auch die auf das jeweilige Zielobjekt wirkenden Gefährdungen dokumentiert. Um jedoch einen effizienten Einstieg zu finden, sollte überlegt werden, welche der zutreffenden Gefährdungen bereits auf den gesamten Informationsverbund als eigenes Zielobjekt wirken. Dies ermöglicht es Maßnahmen zu finden, die Risikoübergreifend (Behandlung mehrere Risiken gleichzeitig) und im Ergebnis in der Breite wirken. Grundsätzlich empfiehlt es sich von Zielobjekten mit übergreifender Wirkung (beispielsweise Netz) zu den Zielobjekten mit sehr spezifischen Wirkungen (einzelne Anwendung) vorzugehen. Dabei ist zu empfehlen je Zielobjekt die Wirkung der Gefährdung konkret zu beschreiben und bereits etwaige umgesetzte Maßnahmen oder existierende Schwachstellen mit aufzuführen.

Für die Zielobjekte, die sich vollständig mit IT-Grundschutz Bausteinen modellieren lassen, bietet es sich an als Ausgangspunkt für die Erstellung der Gefährdungsübersicht auf die jeweils zugehörigen Kreuzreferenztabelle zurückzugreifen. In denen sind die als für das zutreffende Zielobjekt relevant eingestuften elementaren Gefährdung bereits aufgeführt.

Jedoch muss für jedes Zielobjekt noch ermittelt werden, ob es zusätzliche spezifische Gefährdungen gibt. Eine spezifische Gefährdung, insbesondere für die Antennen im Außenbereich ist der Einschlag eines Blitzes.

Diese Gefährdungen werden mit einem vorangestellten e als eigene Gefährdung abgegrenzt. Wir verwenden nachfolgend die eG.1 „Blitzschlag und Überspannung“.

Zusammenfassend wird die Gefährdungsübersicht in folgenden Schritten erstellt:

- Ermittlung der relevanten elementaren Gefährdungen gemäß Gefährdungsübersicht nach BSI-Standard 200-3 Kapitel 3
- Zuordnung der elementaren Gefährdungen zu den Zielobjekten, wobei übergreifend wirkende Gefährdungen dem Zielobjekt Informationsverbund zugeordnet werden
- Ermittlung weiterer spezifischer Gefährdungen (siehe auch Kapitel 2 in den jeweiligen IT-Grundschutz Bausteinen)

Im Weiteren ist zu prüfen, ob die ermittelten Gefährdungen,

- direkt relevant, d. h. sie wirken direkt auf das betreffende Zielobjekt,
- indirekt relevant, d. h. deren potentielle Wirkung geht nicht über die anderer allgemeiner Gefährdungen hinaus, die beispielsweise bereits auf den Informationsverbund als Ganzes wirken,
- nicht relevant, d. h. die Gefährdung kann nicht auf das Zielobjekt wirken, und wird daher nicht weiter betrachtet,

sind.

In nachfolgender Tabelle sind für die drei Zielobjekte, die bei der Erstellung des jeweiligen benutzerdefinierten Baustein ermittelten elementaren Gefährdungen konsolidiert aufgeführt.

Gefährdung	transportable Einhausung	SIM-Karte	Betrieb 5G-Campusnetz	CIA-Wert
eG.1 Blitzschlag und Überspannung	X		X	A
G 0.1 Feuer	X			A
G 0.2 Ungünstige klimatische Bedingungen	X	X		I, A
G 0.3 Wasser	X			I, A
G 0.4 Verschmutzung Staub Korrosion	X	X		I, A
G 0.5 Naturkatastrophen	X			A
G 0.08 Ausfall oder Störung der Stromversorgung	X	X		I, A
G 0.9 Ausfall oder Störung von Kommunikationsnetzen			X	I, A
G 0.10 Ausfall oder Störung von Versorgungsnetzen	X			A
G 0.12 Elektromagnetische Störstrahlung	X	X		I, A
G 0.13 Abfangen kompromittierender Strahlung	X			C
G 0.15 Abhören			X	C

Gefährdung	transportable Einhausung	SIM-Karte	Betrieb 5G- Campusnetz	CIA-Wert
G 0.16 Diebstahl von Geräten Datenträgern oder Dokumenten	X	X	X	C, A
G 0.17 Verlust von Geräten, Datenträgern und Dokumenten		X		C, A
G 0.18 Fehlplanung oder fehlende Anpassung	X	X	X	C, I, A
G 0.20 Informationen und Produkte aus unzuverlässiger Quelle		X		C, I, A
G 0.21 Manipulation von Hard- und Software	X	X		C, I, A
G 0.23 Unbefugtes Eindringen in IT- Systeme			X	C, I
G 0.24 Zerstörung von Geräten oder Datenträgern	X	X	X	A
G 0.25 Ausfall von Geräten und Systemen		X	X	A
G 0.26 Fehlfunktion von Geräten oder Systemen		X	X	C, I, A
G 0.27 Ressourcenmangel			X	A
G 0.29 Verstoß gegen Gesetze oder Regelungen			X	C, I, A
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen		X	X	C, I, A
G 0.32 Missbrauch von Berechtigungen	X		X	C, I, A
G 0.34 Anschlag	X			C, I, A
G 0.41 Sabotage	X		X	A
G 0.43 Einspielen von Nachrichten			X	C, I,
G 0.46 Integritätsverlust schützenswerter Informationen		X		I

Tabelle 13: Konsolidierte Betrachtung der elementaren und spezifischen Gefährdungen für spezifische Zielobjekte

In der durchzuführenden Risikoanalyse sind alle weiteren Zielobjekte, die einem erhöhten Schutzbedarf unterliegen oder sich nicht mit IT-Grundschutz Bausteinen modellieren lassen, zu berücksichtigen und die zutreffenden Gefährdungen zu ermitteln.

## Schritt 2. Risikoeinschätzung vornehmen

### Voraussetzungen:

Bevor eine Risikoeinschätzung vorgenommen werden kann, müssen im Vorfeld die Risikokategorien und -klassen für die Institution festgelegt werden. Darüber hinaus sollten die relevanten Schadensszenarien bestimmt werden, welche bei der Risikoeinschätzung betrachtet werden sollten.

Existiert in der Institution bereits ein Verfahren und Vorgaben zur Durchführung der Risikoanalyse, können diese bei Geeignetheit übernommen werden.

### Durchführung

In diesem Schritt wird für die ermittelten Gefährdungen je Zielobjekt die Eintrittshäufigkeit (gegebenenfalls in Verbindung mit Eintrittswahrscheinlichkeit) und die erwarteten Schadensauswirkungen bei Eintritt des Risikos ermittelt. Bei der Ermittlung der entsprechenden Risikoparameter sollten sowohl bestehende Sicherheitsmaßnahmen als auch existierende Schwachstellen berücksichtigt werden. Es sollte ein durchschnittlich zu erwartender Schaden ermittelt werden.

In den nachfolgenden Tabellen werden die Risikoparameter beispielhaft nach dem BSI Standard 200-3 aufgeführt. Es bietet sich an die Beschreibung der jeweiligen Kategorien der Risikoparameter an die Bedürfnisse der Institution anzupassen. Bei der Schadenauswirkung ist es sinnvoll bei der Betrachtung der finanziellen Auswirkungen passende Schwellwerte vorzugeben.

Eintrittshäufigkeit	Beschreibung
Selten	Ereignis könnte nach heutigem Kenntnisstand höchstens alle fünf Jahre eintreten.
Mittel	Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.
Häufig	Ereignis tritt einmal im Jahr bis einmal pro Monat ein.
sehr häufig	Ereignis tritt mehrmals im Monat ein.

Tabelle 14: Beschreibung der Kategorien der Eintrittshäufigkeit

Schadensauswirkung	Beschreibung
vernachlässigbar	Die Schadensauswirkungen sind gering und können vernachlässigt werden.
Begrenzt	Die Schadensauswirkungen sind begrenzt und überschaubar.
beträchtlich	Die Schadensauswirkungen können beträchtlich sein.
existenzbedrohend	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Tabelle 15: Beschreibung der Kategorien der Schadensauswirkung

## Schritt 3: Risikobewertung vornehmen

Die Risikoermittlung kann nach dem im BSI-Standard 200-3 genutzten Matrix-Ansatz durchgeführt werden. Aus den zuvor ermittelten Kategorien für die Schadensauswirkungen und der Eintrittshäufigkeit ergibt sich eine Risikokategorie.

Im Ergebnis ist bekannt, ob das jeweilige Risiko akzeptabel ist und keine weiterführenden Sicherheitsmaßnahmen umgesetzt werden müssen, oder tatsächlich eine weitere Behandlung der Risiken erforderlich ist.

In der nachfolgenden Abbildung ist eine Risikomatrix nach dem BSI-Standard 200-3 dargestellt.

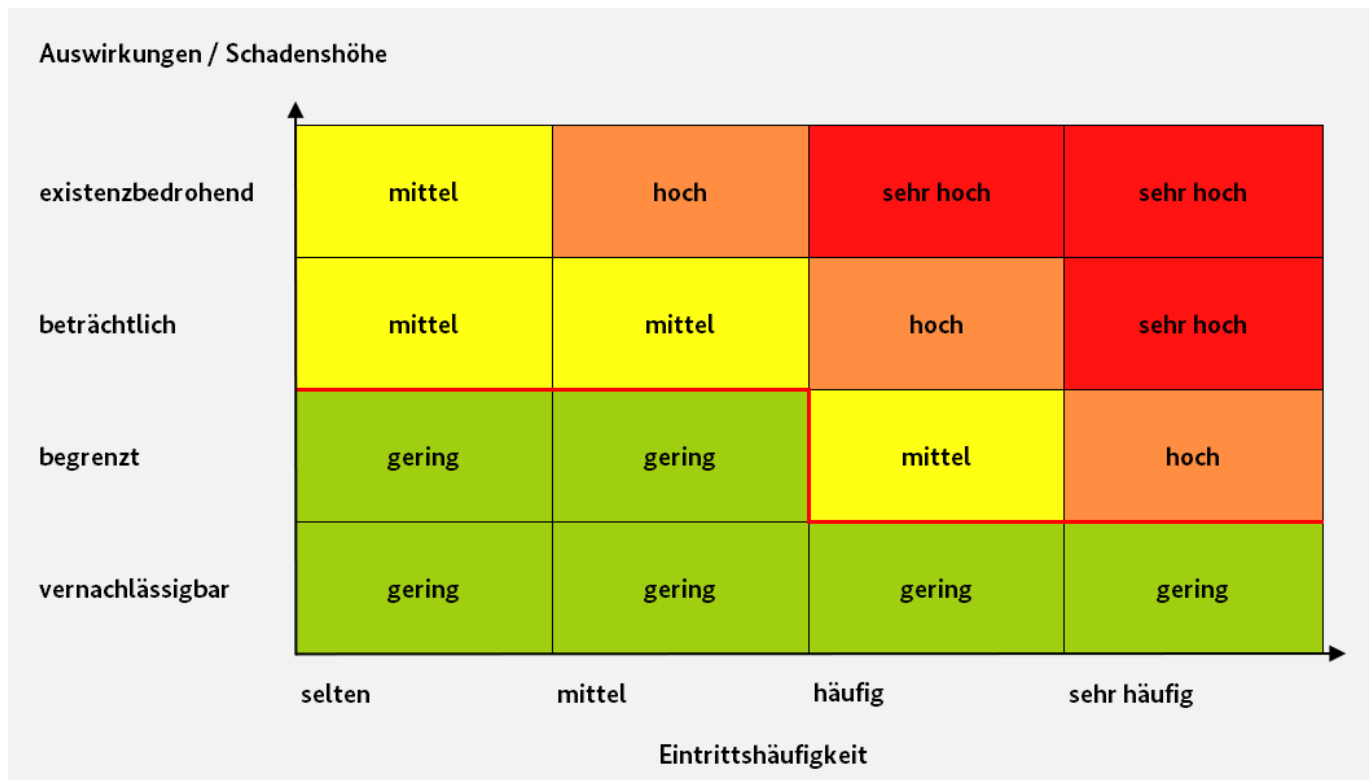


Abbildung 2: Matrix zur Einstufung von Risiken nach BSI-Standard 200-3

Die in der Matrix beispielhaft eingezeichnete rote Linie kennzeichnet das Risikoakzeptanzniveau. Die Risiken, welche als gering eingestuft werden und in diesem Beispiel damit unter der Linie liegen, bedürfen keiner weiteren Behandlung und können akzeptiert werden.

Alle Risiken die als mittel oder höher eingestuft werden bedürfen einer weiteren Behandlung.

Die Risikokategorien sind nach BSI-Standard 200-3 wie folgt definiert:

Risikokategorie	Beschreibung
Gering	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten einen ausreichenden Schutz. In der Praxis ist es üblich, geringe Risiken zu akzeptieren und die Gefährdung dennoch zu beobachten.
Mittel	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen reichen möglicherweise nicht aus.
Hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung.
sehr hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung. In der Praxis werden sehr hohe Risiken selten akzeptiert.

Tabelle 16: Definition von Risikokategorien

## Schritt 4: Risikobehandlung vornehmen

Risiken, die nicht vom Risikoakzeptanzniveau abgedeckt sind, müssen durch weiterführende Sicherheitsmaßnahmen soweit behandelt werden, dass die verbleibenden Restrisiken für die Institution tragbar



sind. Daher ist eine Entscheidung zu treffen, wie mit den verbleibenden Risiken umzugehen ist. Es wird eine der nachfolgend aufgeführten Risikobehandlungsoptionen gewählt:

- Vermeiden von Risiken, durch beispielsweise Ausschluss der Risikoursache
- Reduzieren von Risiken, durch das Modifizieren von Rahmenbedingungen, die zur Risikoeinstufung geführt haben
- Transferieren von Risiken, durch das Übertragen eines Risikos auf eine andere Partei
- Akzeptieren von Risiken, wenn es beispielsweise keine sinnvollen Maßnahmen zur Behandlung gibt, oder mit dem Risiko einhergehende Chancen wahrgenommen werden sollen.

Im Ergebnis werden weiterführende Maßnahmen auf Basis einer der Behandlungsoptionen gewählt. Beispielsweise könnte das für die Gefährdung G 0.19 Offenlegung schützenswerter Informationen im 5G-Campusnetz mit der Wahl der Behandlungsoption „Risikoreduzierung“, die Implementierung einer zusätzlichen Firewall am Netzübergang zwischen 5G-Campusnetz und Firmenintranet sein.

### **Schritt 5: Konsolidierung der erweiterten Sicherheitsmaßnahmen und Überführung in den Sicherheitsprozess.**

In der Konsolidierung wird noch einmal überprüft inwieweit die definierten Sicherheitsmaßnahmen

- geeignet sind, die Gefährdungen abzuwehren,
- sinnvoll zusammenwirken,
- nutzerfreundlich sind,
- gleiche Ziele verfolgen und dadurch sich gegenseitig ersetzen können
- sich gegenseitig in der Wirkung behindern
- vor dem Hinblick entstehender Kosten nutzenbringend sind
- technisch umsetzbar sind

Die definierten Maßnahmen werden mit dem bisher bestehenden Sicherheitskonzept konsolidiert. Damit kann ermittelt werden, wie die definierten Maßnahmen auf Anforderungen wirken, die nicht in der Risikoanalyse betrachtet wurden.

# 9 Anwendungshinweise

Die ermittelten Anforderungen sind in das Gesamtsicherheitskonzept zu integrieren und im Zuge der geplanten Realisierung umzusetzen.

Das vorliegende IT-Grundschutz-Profil ist generisch beschrieben. Bei der Nutzung des IT-Grundschutz-Profiles sollte das eigene Anwendungsszenario zugrunde gelegt werden, um die tatsächlich anzuwenden Bausteine mit den für das eigene Einsatzszenario relevanten Anforderungen zu identifizieren.

Für einige Bausteine und den darin enthaltenen Anforderungen aus dem IT-Grundschutz-Kompendium werden durch das BSI sogenannten Umsetzungshinweise bereitgestellt. Diese können zur Erfüllung der Anforderungen herangezogen werden.

# 10 Unterstützende Informationen

Detailliertere Informationen zu den einzelnen Anforderungen finden sich in den Umsetzungshinweisen der einzelnen Bausteine des IT-Grundschutzes. Die Umsetzungshinweise sind auf den Webseiten des BSI unter: [\*\*www.bsi.bund.de\*\*](http://www.bsi.bund.de).

Als weiterführende Informationen wird auf die Normierungen der 3GPP verwiesen.