5G.NRW
Competence Center

Fokusgruppe 5G und IT-Sicherheit

31. Januar 2023

Henning Horn
Bergische Universität Wuppertal (TMDT)

BERGISCHE
UNIVERSITÄT
WUPPERTAL

Institute for TMDT
Technologies and Management of Digital Transformation

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Absicherung von 5G-Campusnetzen mit dem IT-Grundschutz

Dresden, 31.01.2023

IT-Grundschutz im Kontext von 5G-Sicherheit

Jo-Ann Scharkoff, Referentin SZ32 Vorgaben und Auditierung für Telekommunikationsnetze, 5G

Jennifer Gabriel, PhD Researcher am Lehrstuhl von Herrn Prof. Dr.-Ing. Dr. h.c. Frank Fitzek und Chief Security Officer (CSO) bei Campus Genius

1. **Warum** brauchen wir Absicherung von 5G-Campusnetzen?

2. **Wie** lassen sich 5G-Campusnetze absichern?

3. **Was** kommt danach?

BSI und 5G-Security

- Cyber-Security-Behörde Deutschlands
- Wissensträger und Multiplikator für technische 5G/6G Sicherheitsbelange
- Schnittstelle zu anderen Beteiligten (u.a. Bundesnetzagentur, Zertifizierungsstellen, Mobilfunknetzbetreibern und Hersteller)

Warum brauchen wir Absicherung von 5G-Campusnetzen?

Gesetzliche Rahmenbedingungen

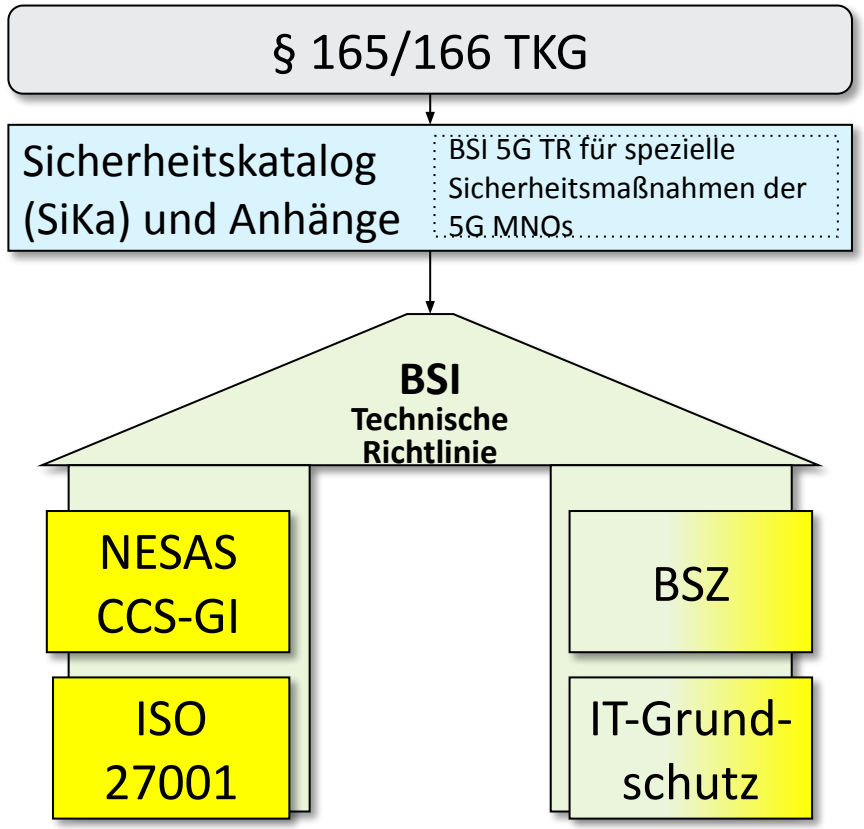
- Nicht ausreichend für ganzheitliche Absicherung

Öffentliche Mobilfunknetze

- Mobile Network Operator setzen Sicherheitsanforderungen durch Sicherheitskonzepte um
- Fokus auf resistente Netze

Campusnetze

- Keine gesetzliche Regulierung vorhanden
- Standardisierte Werkzeuge zur Einführung von IT-Sicherheit durch Campusnetzbetreiber nötig



Wie lassen sich 5G-Campusnetze absichern?

- Entwicklung gemeinsam mit Experten und Anwendern aus der Wirtschaft
- Hilfe für Unternehmen und Behörden ein 5G-Campusnetz sicher aufzubauen, zu betreiben und in das Firmennetz zu integrieren.

IT-Grundschutz-Profil zur Absicherung von 5G-Campusnetzen	INF.bd.1 Ortsveränderliche Einhausung für IT-Systeme

Diese sollen Unternehmen und Behörden dabei helfen ein 5G-Campusnetz sicher aufzubauen, zu betreiben und in den Unternehmensverbund zu integrieren.

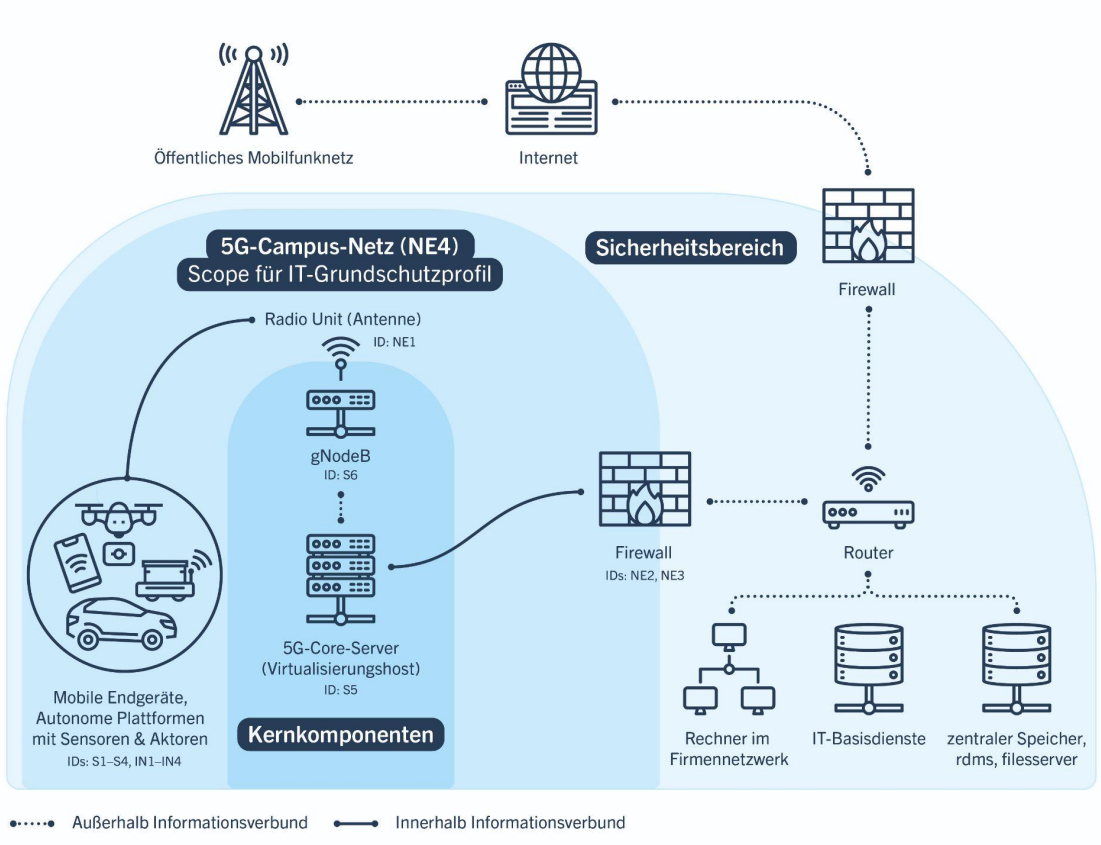
Bundesamt für Sicherheit in der Informationstechnik

Campus Genius

ComNets
Deutsche Telekom Chair of Communication Networks

Deutschland Digital•Sicher•BSI•

Netzplan



Bundesamt für Sicherheit in der Informationstechnik

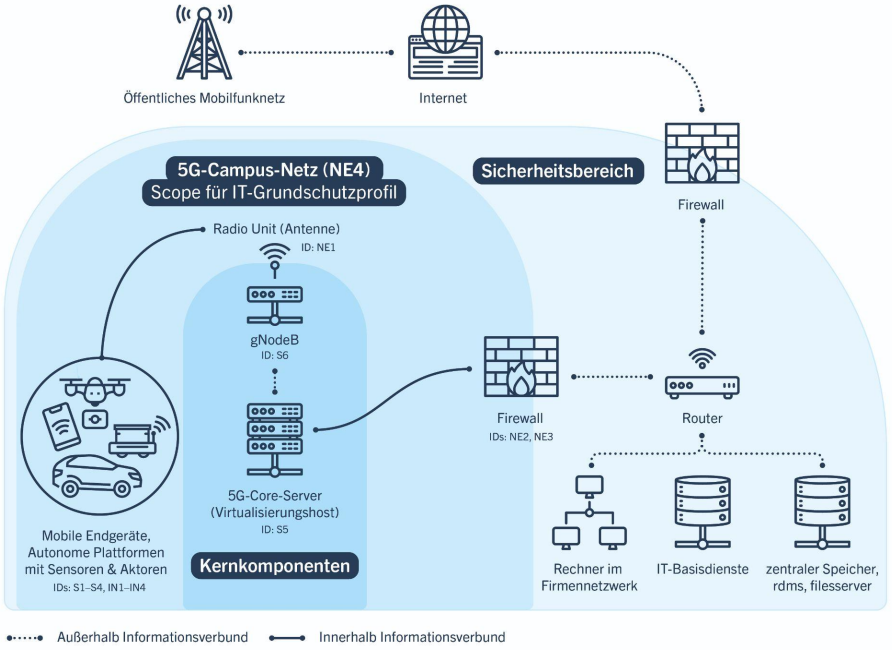
Campus Genius

ComNets
Deutsche Telekom Chair of Communication Networks

Deutschland Digital•Sicher•BSI•

Prozesse im 5G-Campusnetz

Teilprozess	Beschreibung (beispielhaft)
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	Übertragung von Steuersignalen an Aktoren

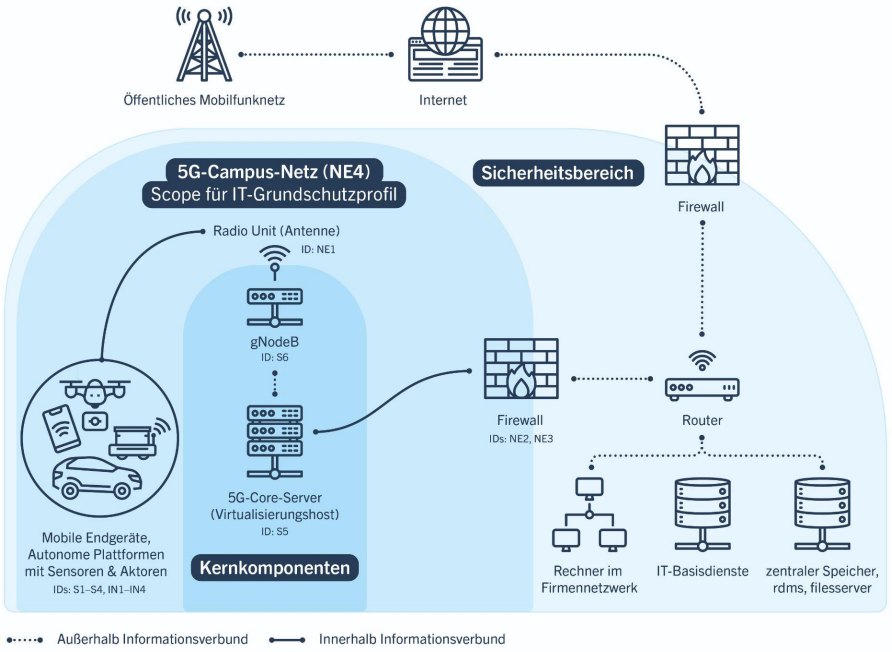


Schutzbedarfsfeststellung

Schadensszenarien (beispielhaft)
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.
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.
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.

IT-Systeme im Informationsverbund

Smartphones, Tablets
Laptop
Mobiltelefon
Kamera
5G-Core
gNodeB - Basisstation
Prozessleittechnik
Produktionsmaschine
Sensoren / Aktoren
Robotik



ISMS: Sicherheitsmangement

ID	Baustein
ISMS.1	Sicherheitsmanagement

ORP: Organisation und Personal

ID	Baustein
ORP.1	Organisation
ORP.2	Personal
ORP.3	Sensibilisierung und Schulung zur Informationssicherheit
ORP.4	Identitäts- und Berechtigungsmanagement
ORP.5	Compliance Management (Anforderungsmanagement)

CON: Konzeption und Vorgehensweise

ID	Baustein
CON.1	Kryptokonzept
CON.2	Datenschutz
CON.3	Datensicherungskonzept
CON.6	Löschen und Vernichten
CON.9	Informationsaustausch

OPS: Betrieb

ID	Baustein
OPS.1.1.2	Ordnungsgemäße IT-Administration
OPS.1.1.3	Patch- und Änderungsmanagement
OPS.1.1.4	Schutz vor Schadprogrammen
OPS.1.1.5	Protokollierung
OPS.1.1.6	Software-Tests und Freigaben
OPS.1.2.5	Fernwartung

DER: Detektion und Reaktion

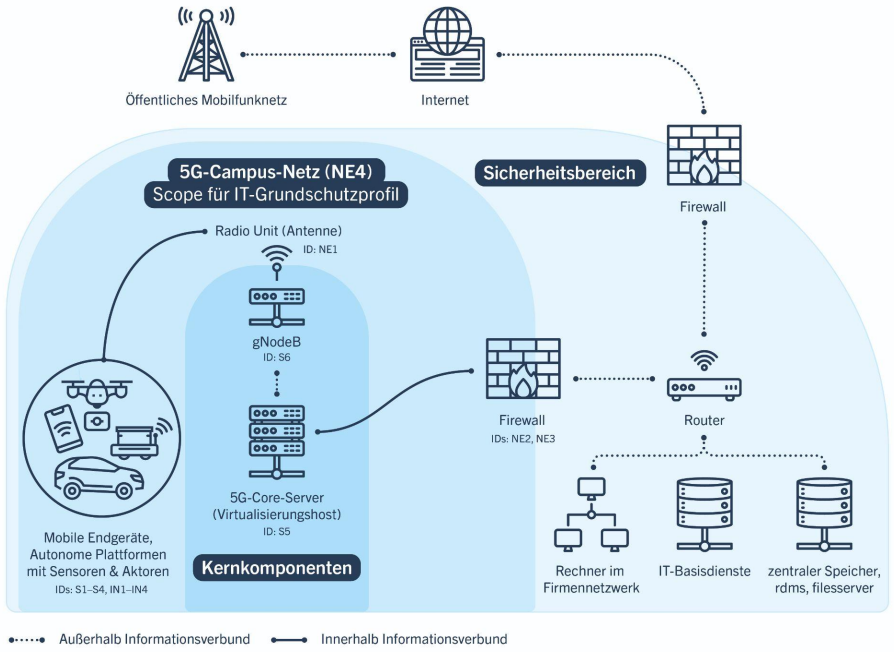
ID	Baustein
DER.1	Detektion von sicherheitsrelevanten Ereignissen
DER.2.1	Behandlung von Sicherheitsvorfällen
DER.2.2	Vorsorge für die IT-Forensik
DER.2.3	Bereinigung weitreichender Sicherheitsvorfälle
DER.3.1	Audits und Revisionen
DER.4	Notfallmanagement

APP: Anwendungen

ID	Baustein
APP.1.2	Web-Browser
APP.6	Allgemeine Software

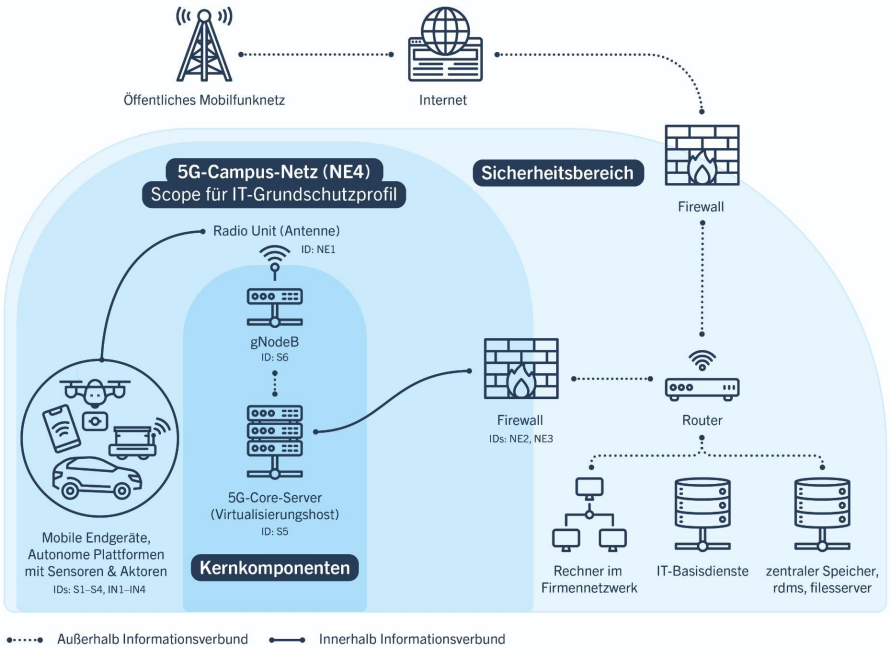
SYS: IT-Systeme

ID	Baustein
SYS.2.1	Allgemeiner Client (+ Bausteine für Clients mit unterschiedlichen Betreibssystemen)
SYS.3.1	Laptops
SYS.3.2.1	Allgemeine Smartphones und Tablets (+ Bausteine für iOS und Android)
SYS.3.3	Mobiltelefon
SYS.4.3	Eingebettete Systeme
SYS.4.4	Allgemeines IoT-Gerät



IND: Industrielle IT

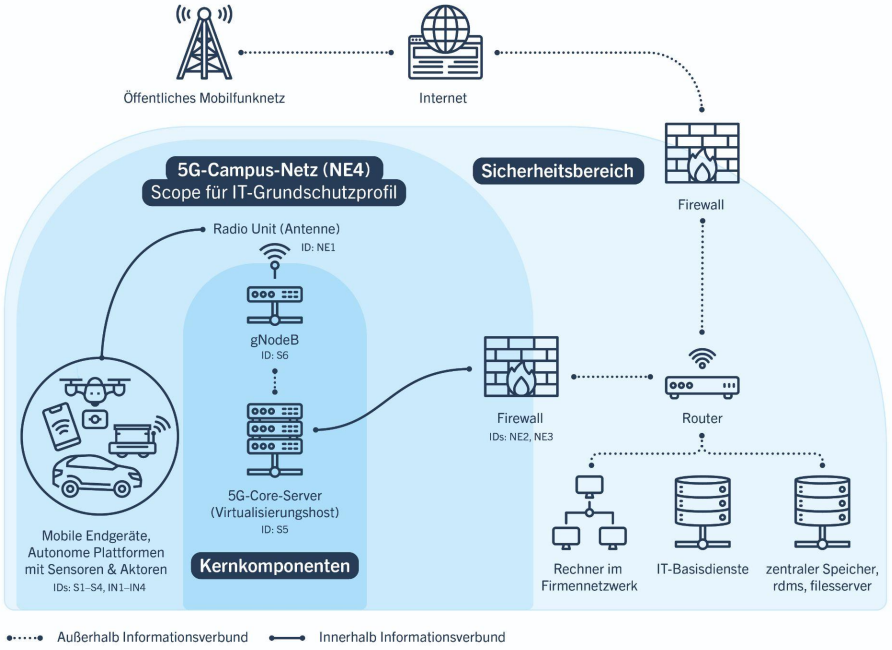
ID	Baustein
IND.1	Prozessleit- und Automatisierungstechnik
IND.2.1	Allgemeine ICS-Komponente
IND.2.2	Speicherprogrammierbare Steuerung (SPS)
IND.2.3	Sensoren und Aktoren
IND.2.4	Maschine
IND.2.7	Safety Instrumented Systems
IND.3.2	Fernwartung im industriellen Umfeld



BSI IT-Grundschutz Bausteine

NET: Netze und Kommunikation

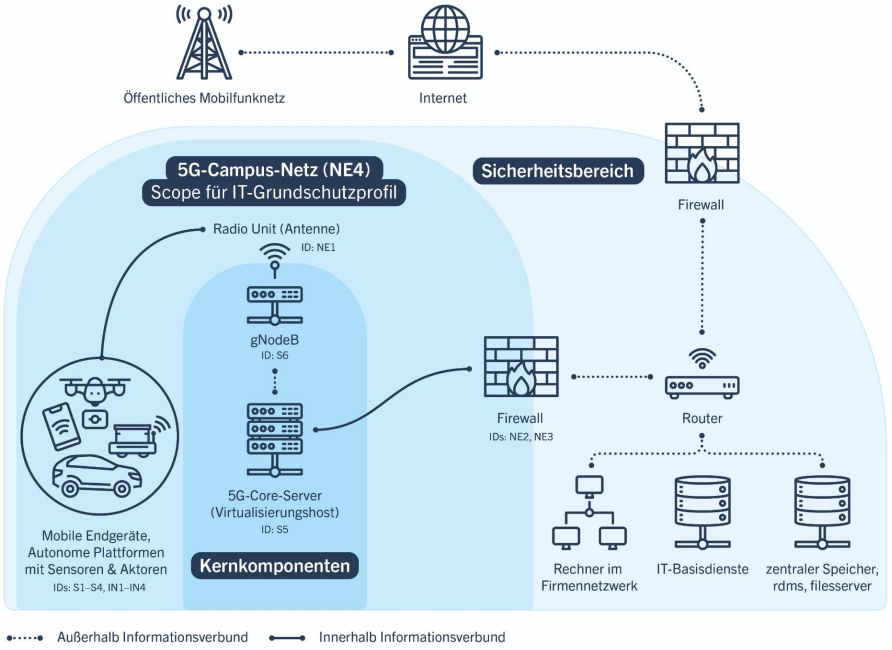
ID	Baustein
NET.1.1	Netzarchitektur und -design
NET.1.2	Netzmanagement
NET.3.2	Firewall
NET.3.3	VPN



BSI IT-Grundschutz Bausteine

INF: Infrastrukutr

ID	Baustein
INF.1	Allgemeines Gebäude
INF.2	Rechenzentrum sowie Serverraum
INF.5	Raum sowie Schrank für technische Infrastruktur
INF.12	Verkabelung
INF.bd.1	Ortsveränderliche Einhausung für IT-Systeme



INF.bd.1 Ortsveränderliche Einhausung für IT-Systeme

- z. B. 5G-Campusnetz Installationen in Containern, Autos und Rucksäcken
- Ortsveränderlich, jedoch nur bedingt mobil (Frequenzspektrum)
- Hinweise zur Auswahl des Aufbauorts, dem sicheren Transport sowie Schutz vor Vandalismus

Was kommt danach?

- Anwender Workshop mit Betreibern und Dienstleistern von 5G Campusnetzen
- Erweiterung der IT-Grundschutz-Profilfamilie
  - IT-Grundschutz-Profil zur Absicherung von 5G Campusnetzen im Eigenbetrieb
- Jährliche Überarbeitung der vorhandenen IT-Grundschutz-Profile und benutzerdefinierter Bausteine

IEEE 6G Summit 09.-10-05-2023, Dresden

Bundesamt für Sicherheit in der Informationstechnik

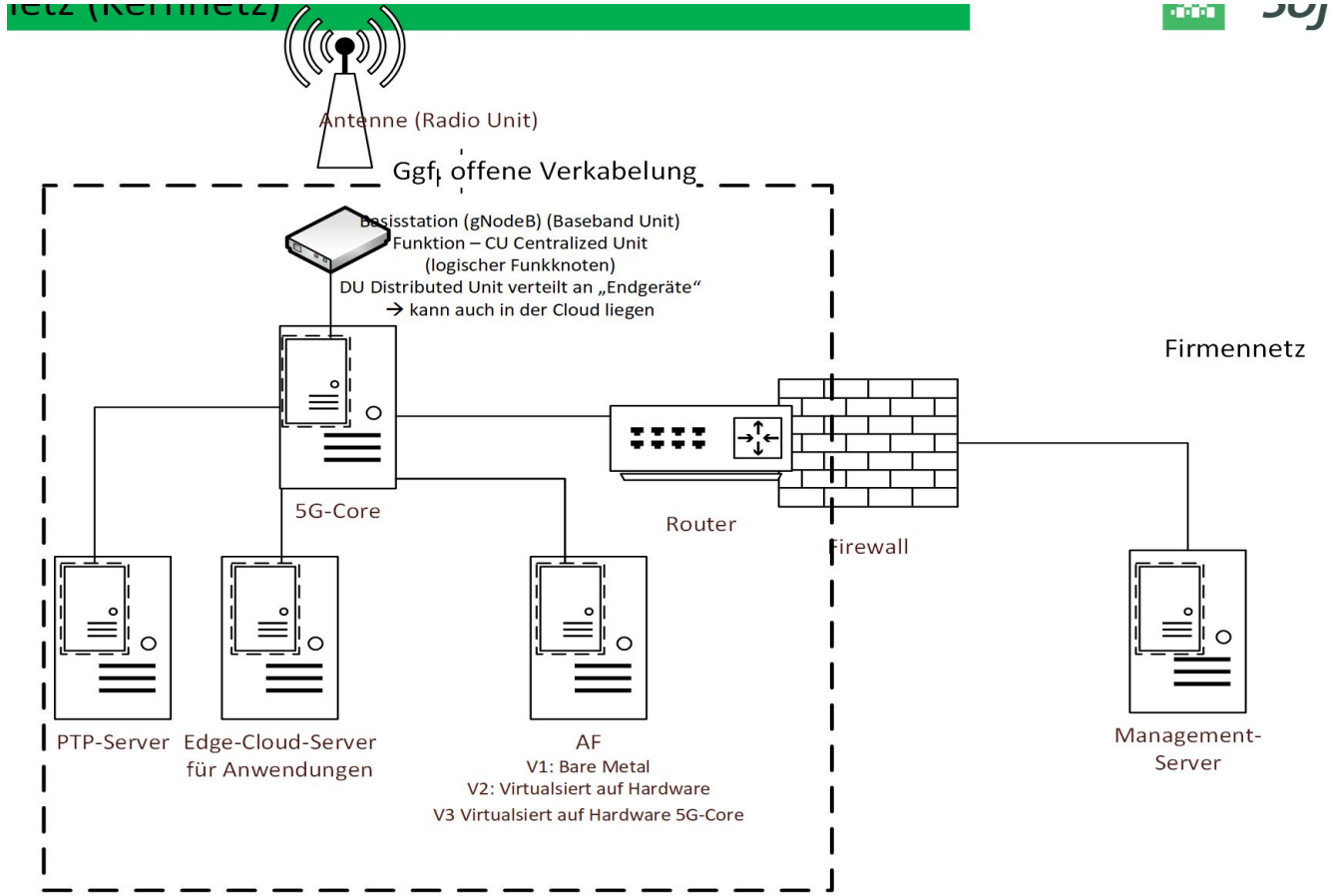
Campus Genius

ComNets
Deutsche Telekom Chair of Communication Networks

Deutschland Digital•Sicher•BSI•

Was kommt danach?

- Erweiterung der IT-Grundschutz-Profilfamilie
  - IT-Grundschutz-Profil zur Absicherung von 5G Campusnetzen im Eigenbetrieb



Vielen Dank für Ihre Aufmerksamkeit!

Deutschland
Digital•Sicher•BSI•

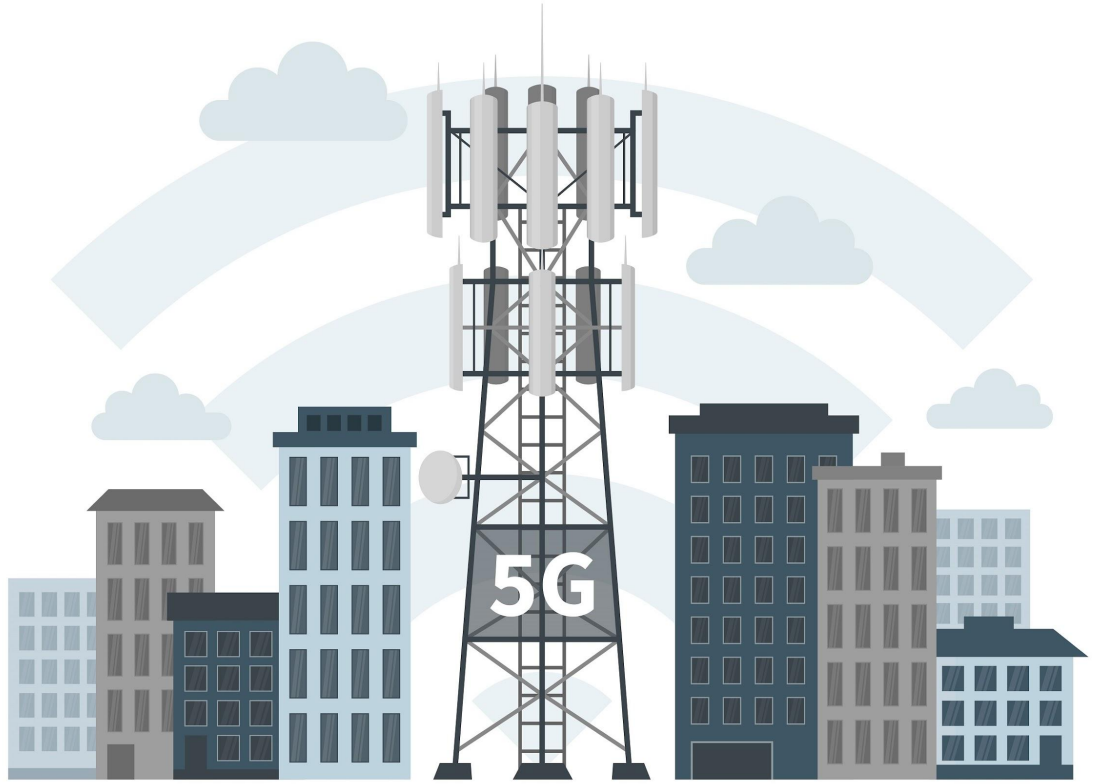
Vortragende:

Jo-Ann Scharkoff
Referat SZ 32 - Vorgaben und Auditierung für Telekommunikationsnetze, 5G
Bundesamt für Sicherheit in der Informationstechnik

E-Mail: jo-ann.scharkoff@bsi.bund.de

Jennifer Gabriel
CampusGenius GmbH &&
Technische Universität Dresden
Deutsche Telekom Professur für Kommunikationsnetze

E-Mail: jennifer.gabriel@tu-dresden.de
jennifer.gabriel@campusgenius.com



Bundesamt
für Sicherheit in der
Informationstechnik

Schrittmacher der Innovation in NRW

5G.NRW Competence Center

Kontakt:
Henning Horn
Bergische University of Wuppertal
Institute for Technologies and Management of Digital Transformation
T: 0049 202 439 1035
@: hhorn@uni-wuppertal.de

Gefördert durch:

Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen