Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

Handreichung "5G-Campusnetze"

2024

Danksagung

Diese Publikation wurde von einer Autorengruppe in der TeleTrusT-AG "Smart Grids/Industrial Security" erarbeitet. TeleTrusT bedankt sich bei den nachstehenden Personen für ihre Mitwirkung sowie für die aktive Mitgestaltung dieser Handreichung.

Autorenliste

Fritsch, Sebastian - secuvera (Koordinierung)
Kretschmar, Kay - BSI
Kus, Mehmet, OTARIS
Scharkoff, Jo-Ann - BSI
Schmierer, Marc - ads-tec

Redaktion

Mühlbauer, Dr. Holger - Bundesverband IT-Sicherheit e.V. (TeleTrusT)

In dieser Publikation werden Anglizismen und Abkürzungen verwendet, die sich in der zugrundeliegenden Fachdiskussion branchentypisch verfestigt haben.

Impressum

Herausgeber:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4306
Fax: +49 30 4005 4311
E-Mail: info@teletrust.de
https://www.teletrust.de

V 1_2024-03

Inhalt

1 Motivation

Der Mobilfunkstandard 5G ist eine Schüsseltechnologie, die sich zum größten Infrastrukturvorhaben des kommenden Jahrzehnts entwickelt und die Digitalisierung von Staat, Wirtschaft und Gesellschaft auf eine vollkommen neue Basis stellt. Öffentliche Mobilfunknetze der 5. Generation unterliegen gesetzlichen Regularien, an deren Erarbeitung und Fortschreibung das Bundesamt für Sicherheit in der Informationstechnik (BSI) beteiligt ist. Details regelt die BSI TR-03163 "Sicherheit in TK-Infrastrukturen". Private 5G-Netze, auch 5G-Campusnetze genannt sind im Vergleich zu öffentlichen Mobilfunknetzen der 5. Generation nicht durch das BSI-Gesetz (BSIG) oder das Telekommunikationsgesetz (TKG) reguliert. Schlussfolgernd sind Unternehmen oder Behörden, die 5G-Campusnetze nutzen oder eine zukünftige Nutzung anstreben, nicht zur Umsetzung von technischen Richtlinien oder an Zertifizierungspflichten gebunden.

Unternehmen aller Branchen und Größen verfügen über schützenswertes Wissen und sind auf den störungsfreien Betrieb ihrer Informationstechnik angewiesen - das rückt sie in den Fokus von Cyber-Angriffen. Um Daten zu schützen und die Verfügbarkeit des 5G-Campusnetzes zu gewährleisten, müssen sich Anwendende von 5G-Campusnetzen selbst um deren Absicherung kümmern.

Diese Handreichung richtet sich an alle interessierten Unternehmen, Institutionen und Organisationen die bereits private 5G-Netze produktiv oder als Testkonzept betreiben. Konkret wird die Ebene der IT-Administration und IT-Leitung angesprochen.

Neben einem Überblick zu Betriebsmodellen, Einsatz- und Bedrohungsszenarien ist dieser Handreichung ergänzend eine Arbeitsmappe beigefügt. Diese listet wichtige Fragen auf, die beim Aufbau sowie Betrieb eines 5G-Campusnetzes gestellt werden sollten, um bei der Auswahl der Technologie, des Anbieters und des Betriebsmodells ebenfalls die IT-Sicherheit zu berücksichtigen. Für die praktische Umsetzung von Informationssicherheit in 5G-Campusnetzen können konkrete Sicherheitsmaßnahmen im IT-Grundschutz des BSI herangezogen werden. Die IT-Grundschutz-Profile betrachten die verschiedenen Betriebsmodelle dieser Handreichung und geben konkrete Empfehlungen, um ein adäquates Sicherheitsniveau zu erreichen.

2 Einsatz von 5G-Campusnetzen

5G-Campusnetze sind insbesondere als Alternative oder Ergänzung für vorhandene Kommunikationsinfrastrukturen (z.B. WLAN-Netze) interessant, denn Mobilfunktechnik hat sich in den letzten Jahren als sehr zuverlässig für stabile und weiträumige Netzanbindungen herausgestellt. Beispielsweise ist der Zugriff von Endgeräten auf Antennen nicht mehr zufallsgesteuert (wie bei WLAN), sondern fest (mit Bandbreite, Datendurchsatz) vorgegeben und garantiert. Mittels Network Slicing können darüber hinaus im Netz befindliche Endgeräte unterschiedliche Qualitätsparameter wie z.B. Latenz, Übertragungsgeschwindigkeit und Bandbreiten zugesichert werden. Das ermöglicht auch zeitkritische Anwendungen über ein 5G-Campusnetz durchzuführen.

Eine vertrauliche und nicht repräsentative Erhebung der TeleTrusT-AG "Smart Grids/Industrial Security" hat gezeigt, dass nach einer ersten Phase von 5G-Campusnetzen für Forschungszwecke mittlerweile erste kommerzielle Netze entstanden sind. Aktuell werden 5G-Campusnetze zum Beispiel in der Logistik für die Steuerung von führerlosen Transportsystemen, für die Vernetzung von Internet-of-Things (IoT)-Geräten in der Gebäudeautomation oder beim Produktionsprozess im industriellen Umfeld zur Steuerung und Überwachung von Maschinen und Robotern in Echtzeit verwendet. Aber auch im medizinischen oder landwirtschaftlichen Bereich finden 5G-Campusnetze bereits Anwendung.

Um ein 5G-Campusnetz betreiben zu dürfen, ist die Beantragung einer Lizenz zur Nutzung der entsprechenden Frequenzen bei der Bundesnetzagentur (BNetzA) notwendig. Da diese Lizenz nur zur Nutzung der Frequenzen an einem bestimmten Ort ausgestellt wird, muss das 5G-Campusnetz immer ortsfest betrieben werden. Soll das 5G-Campusnetz an unterschiedlichen Orten zum Einsatz kommen, muss für jeden dieser Einsatzorte eine gesonderte Lizenz bei der BNetzA beantragt werden.

Für 5G-Campusnetze gibt es verschiedene Betriebsmodelle. Grob lassen sich diese Betriebsmodelle in Eigen- und Fremdbetrieb unterteilen.

Beim Eigenbetrieb ist der Anwender des 5G-Campusnetzes auch gleichzeitig der Betreiber. Die eingesetzte Hard- und Software wird entweder über einen Dienstleister bezogen oder direkt beim Hersteller erworben. Jegliche Konfiguration sowie der Aufbau des Netzes liegt in der Verantwortung des Anwenders und kann durch einen Dienstleister unterstützt werden. Der Antrag auf Nutzung der entsprechenden Frequenzen wird von der nutzenden Institution direkt bei der BNetzA gestellt. Der Anwender hat die Netzhoheit. Die Provisionierung der SIM-Karten (physisch oder eSIM) wird zumeist von Dienstleistern vorgenommen, kann aber auch durch den Betreiber selbst durchgeführt werden.

Beim Fremdbetrieb übernimmt ein Dienstleister den Betrieb und die Wartung des 5G-Campusnetzes vollständig. Entsprechende Dienstleister sind oft auf 5G-Campusnetze spezialisiert. Der Dienstleister übernimmt die Rolle des Netzbetreibers und verfügt demnach über die Netzhoheit. Die genutzten Frequenzen werden in der Regel weiterhin vom Anwender bei der BNetzA beantragt. Bei der Nutzung

eines gemeinsamen Zugangsnetzes kann es auch vorkommen, dass der Dienstleister diese bereitstellt und somit eine Beantragung bei der BNetzA entfällt. Jegliche Konfigurationen sowie die Provisionierung der SIM-Karten und die Verteilung der Radio Units werden vom Dienstleister durchgeführt. Auch einige öffentliche Mobilfunknetzanbieter stellen 5G-Campusnetze bereit und betreiben diese für deren Kunden. Den Anwendern werden lediglich Konnektivitätsdienste zur Verfügung gestellt. Bei der Erhebung der TeleTrusT-AG konnte festgestellt werden, dass Unternehmen diesem Betriebsmodell skeptisch gegenüberstehen. Ein Kernargument für Industriekunden sich mit 5G als Access-Technologie und Campusnetzen selbst zu beschäftigen, ist es dadurch unabhängig von öffentlichen Netzen zu werden.

5G-Campusnetze werden typischerweise als Stand-alone-Netze aufgebaut. Dies bedeutet, dass das Netz eine eigenständige Implementierung der 5G-Netzwerkarchitektur, einschließlich aller Kernnetzfunktionen, bietet. In einem Stand-alone-Netz können 5G-Geräte direkt auf 5G-Frequenzen zugreifen und alle Vorteile von 5G vollständig nutzen.

Im Gegensatz zu "Stand alone" gibt es auch noch die Möglichkeit, das Netz als Non-"Stand alone"-Variante aufzubauen. Diese Zwischenlösung baut auf bestehender 4G-Infrastruktur auf und ergänzt sie um bestimmte 5G-Komponenten. In einem Non-"Stand alone"-Netzwerk ist zum Beispiel 5G bei der Datenübertragung auf die 4G-Netze angewiesen, insbesondere für den Internetzugriff oder die Kernnetzfunktionen. Diese Art der Architektur ermöglicht also, dass sowohl 4G- als auch 5G-Frequenzen verwendet werden können.

Auch die wik-Befragung [1] aus dem Jahr 2021 hatte bereits festgestellt, dass ein Großteil der Anwender von 5G-Campusnetzen diese vollständig eigenständig betreiben möchten. Dies beinhaltet den Betrieb des gesamten Netzes auf dem Campus selbst. Im Vergleich zu WLAN-Netzen ist häufig der Platzbedarf für den zentralen Teil eines 5G-Campusnetzes, der sogenannte 5G-Core, immens. Nicht selten ist hierfür ein ganzes Rack vorzusehen. Es gibt bereits erste Hersteller, die versuchen, das Management eines 5G-Campusnetzes analog zur Administration einer WLAN-Umgebung bereitzustellen. Umgekehrt wurde der TeleTrusT-AG in der Befragung berichtet, dass die klassischen Netzequipment-Anbieter oft nicht die Größenordnung und den Umfang des Bedarfs von 5G-Campusnetzbetreibern anbieten. Die angebotenen Campusnetze sind häufig deutlich geringer als bei öffentlichen 5G-Netzen.

3 Bedrohungen für 5G-Campusnetze

5G-Campusnetze sind in der Regel komplex in Bezug auf ihre Architektur und die große Anzahl unterstützter Gerätetypen (IoT-Geräte). Dies kann potentiell eine Reihe von Angriffsvektoren eröffnen. In 5G-Netzen kommt verstärkt auch Virtualisierung zum Einsatz, die Flexibilität und Effizienz ermöglicht. Aber dies bringt auch neue Sicherheitsrisiken durch Schwachstellen in Virtualisierungstechnologien mit sich, z.B. nicht wirksame Separierung von Gastsystemen. Die Hardwarekomponenten eines 5G-Campusnetzes benötigen darüber hinaus einen adäquaten Schutz vor physischen Zugriffen.

Der Blick in die Praxis zeigt einige Angriffs- und Bedrohungsszenarien im Bereich der 5G-Campusnetze. Beispielsweise könnten Angreifer sich Zugang zum Netz verschaffen, in dem eine SIM-Karte aus einem Gerät entwendet oder von einem Mitarbeitenden gestohlen wird. Das kann verhindert werden, indem eine bestimmte SIM-Karte an ein bestimmtes Gerät gebunden wird (IMEI/IMSI-Binding) - wobei sich auch da immer noch Angriffe ergeben können (IMEI spoofing).

Desweiteren kann ein falsch konfiguriertes 5G-Campusnetz Einfallstor für Industriespionage oder sogar Sabotage sein. Neben dem Abgreifen von firmeninternen oder produktionsrelevanten Daten oder dem Lahmlegen des gesamten Netzes (z.B. durch einen Denial-of-Service-Angriff), könnte sich auch eine Art schleichender Ertrag/Qualitätsminderung durch marginale Manipulationen von Messdaten ergeben. Ein gutes IT-Sicherheitskonzept kann vielen dieser Probleme begegnen und Risiken minimieren.

4 Absicherung von 5G-Campusnetzen

Zur Eindämmung potentieller Bedrohungen müssen auch in 5G-Campusnetzen geeignete IT-Sicherheitsmaßnahmen umgesetzt werden. Dazu gehören unter anderem starke Authentifizierungs- und Verschlüsselungsverfahren, regelmäßige Überwachung des Netzwerkverkehrs, Netzwerksegmentierung und regelmäßige Sicherheitsupdates. Die vorliegende Handreichung dient hierbei als Orientierungshilfe.

Um den Betrieb sowie die Integration von unterschiedlich gearteten 5G-Campuslösungen so sicher wie möglich zu gestalten, hat das BSI zusammen mit Fachleuten und Anwendenden aus der Wirtschaft, Industrie und Verwaltung bereits zwei IT-Grundschutz-Profile entwickelt. Diese sollen dabei helfen, ein 5G-Campusnetz sicher aufzubauen, zu betreiben und in das vorhandene Firmennetz zu integrieren. Die beiden IT-Grundschutz-Profile [2] betrachten dabei zwei Betriebsmodelle, die in nachfolgender Abbildung dargestellt sind. Zum einen gibt es die Möglichkeit, das 5G-Campusnetz durch ein externes Dienstleistungsunternehmen betreiben zu lassen. In Anlehnung an die wik-Befragung [1] betrachtet das zweite IT-Grundschutz-Profil die Möglichkeit des Eigenbetriebs. Hier besitzt die betreibende Institution die Netzhoheit und übernimmt das Management selbst. Auch bei diesem Betriebsmodell sind Cloudlösungen, sowie Core-as-a-Service möglich.

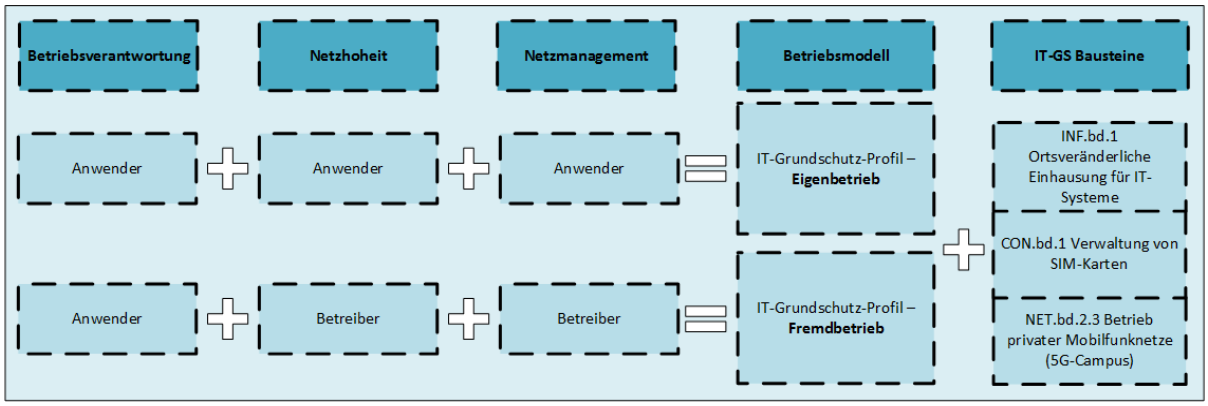

Abbildung 1: Zuordnung der Betriebsmodelle zu IT-Grundschutz-Profilen und benutzerdefinierten IT-Grundschutz-Bausteinen

Die IT-Grundschutz-Profile stehen auf der BSI-Webseite als Download zur Verfügung:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/5-G/Absicherung-5G-Campusnetze/IT-Grundschutz/IT-Grundschutz-Absicherung-5G-Campusnetze_node.html

Die nachfolgende Abbildung zeigt einen logischen Netzplan für ein exemplarisch dargestelltes 5G-Campusnetz. Die Grenzen des Informationsverbundes werden durch den Bereich "5G-Campusnetz" abgebildet. Alle weiteren Bestandteile in der Abbildung dienen der Verdeutlichung, dass ausschließlich eine Netzanbindung zum internen Firmennetz besteht. Im 5G-Campusnetz eingesetzte Geräte kommunizieren ausschließlich über den 5G-Core mit dem internen Firmennetz. Der gelb markierte Bereich

skizziert die bereits vorhandene Basis- und Firmen-IT die für alle Prozesse der Leistungserbringung des Unternehmens unabhängig vom 5G-Campusnetz genutzt wird. Davon separiert ist das Managementnetz, welches durch eine Firewall getrennt die Administration des 5G-Campusnetzes übernimmt. Im 5G-Campusnetz selbst befinden sich der 5G-Core mit allen zugehörigen Funktionen, die Antenne mit gNodeB, ein Server für die Zeitsynchronisation und die IoT-Geräte. Zudem wird für die Datenübertragung in das und aus dem 5G-Campusnetz ein Switch eingesetzt. Da es sich hier um ein exemplarisches Beispiel eines 5G-Campusnetzes handelt, das von der Organisation selbst betrieben wird, können auch Netze mit einer anderen Architektur den Umsetzungshinweisen der IT-Grundschutz-Profile folgen.

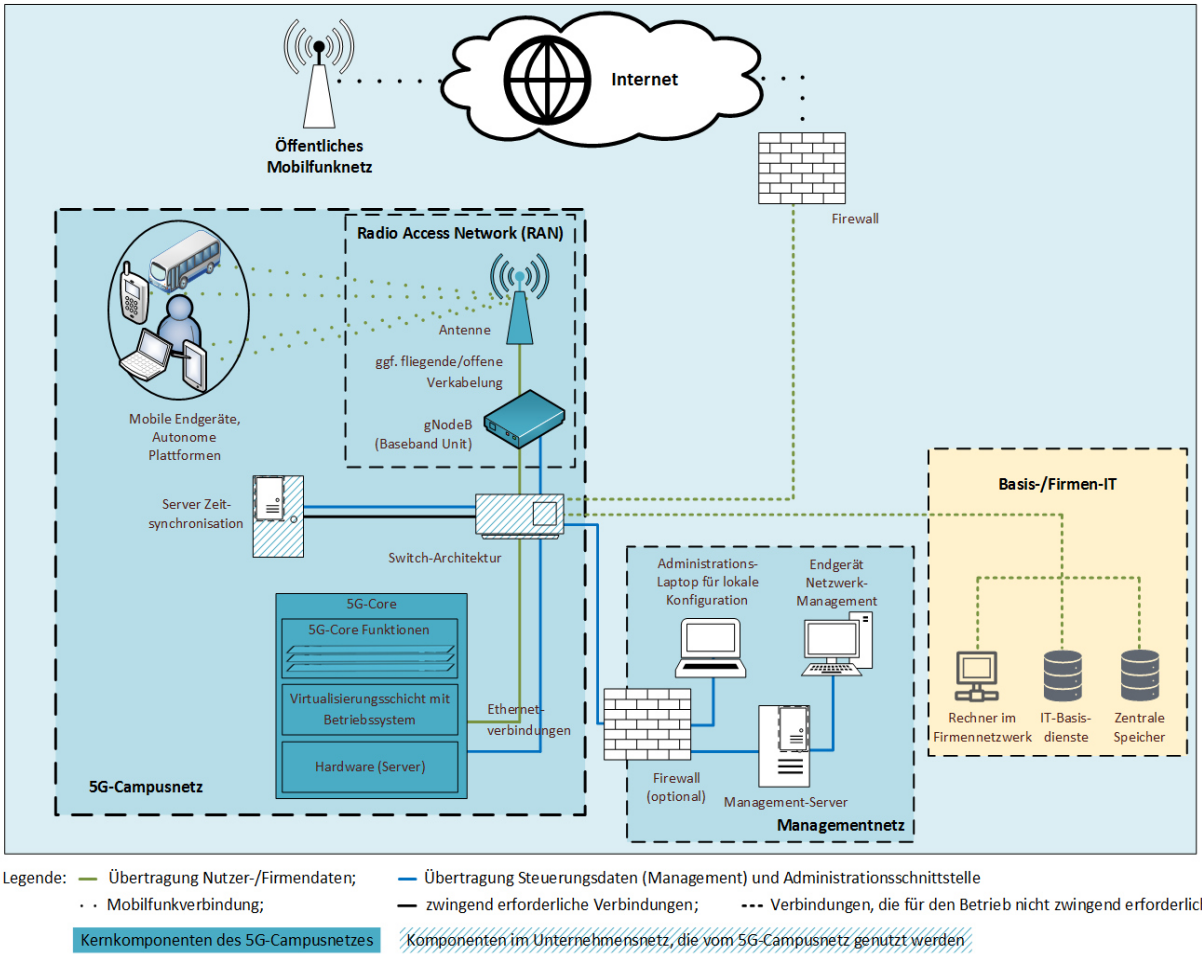

Abbildung 2: Exemplarische Einbettung eines 5G-Campusnetzes in ein Unternehmensnetz

Für die Ebene des Netzwerkequipments existiert mit NESAS [3] (Network Equipment Security Assurance Scheme) ein durch die GSMA (Groupe Speciale Mobile Association) bereitgestelltes freiwilliges Überprüfungsschema. Dieses basiert auf definierten IT-Sicherheitstestfällen und einem Ökosystem qualifizierter Prüfer, welches Netzbetreibern helfen soll eine unabhängige sicherheitstechnische Bewertung von Mobilfunk Netzwerkequipment zu erhalten. Inwieweit dieses Angebot der GSMA im Markt der 5G-Campusnetze angenommen wird, ist aktuell offen.

5 Stand der IT-Sicherheit

Die Erhebung der TeleTrusT-AG fokussiert insbesondere die IT-Sicherheit von 5G-Campusnetzen. Die Erhebung diente einer Sachstandsabfrage: Wie ist der Stand der IT-Sicherheit von 5G-Campusnetzen und was ist noch zu tun?

Bei der Beschaffung von 5G-Campusnetztechnik war IT-Sicherheit häufig noch kein Entscheidungsaspekt. Fast keine befragte Institution hatte im Rahmen der Beschaffung explizit IT-Sicherheitsaspekte in die Beschaffungskriterien aufgenommen. Security bei den Netzkomponenten hatte daher keine hohe Relevanz. Im Aufbau der Netze sind Firewalls und Netzwerkmonitoring allerdings bereits relevante Aspekte.

Auch im Betrieb wurde eine gewisse Relevanz von Security festgestellt. Anwender lassen sich typischerweise von einem Dienstleister oder Integrator das 5G-Campusnetz errichten und konfigurieren. Zudem wird auf den Integrator wieder bei Betriebsproblemen oder zur Fehlerbehebung zurückgegriffen. Auch das Einspielen von Updates wird durch Integratoren vorgenommen. Ein ausgefeiltes Berechtigungsmanagement scheint noch nicht ausreichend priorisiert zu sein. Dies liegt auch an flachen Administrationskonzepten der Forschungsnetze.

Physische Zutrittskontrolle zu den Technik- oder Netzwerkräumen ist oft gegeben. Teilweise ist dies auf sehr hohe Investitionskosten der 5G-Technik zurückzuführen.

Ob die Verfügbarkeit der Cloudsysteme einen Einfluss auf die Verfügbarkeit der 5G-Campusnetze hat, wurde bisher nicht ermittelt.

6 Fragenkatalog/Hilfestellung

Von TeleTrusT wird ein Fragenkatalog zu IT-Sicherheitsthemen bereitgestellt, der während der Beschaffung, der Realisierung und dem Betrieb eines 5G-Campusnetzes dem Anwender als Hilfestellung dienen sollen. Auch die Themen Security by Design, sichere Lieferkette und Software Bill Of Material (SBOM) werden dabei adressiert.

Der Fragenkatalog ist in Verbindung mit dieser Publikation über die TeleTrusT-Webseite als Download verfügbar.

7 Ausblick

Die TeleTrusT-AG "Smart Grids/Industrial Security" hofft mit dieser Handreichung der wachsenden Anzahl an Anwendern von 5G-Campusnetzen eine Hilfestellung zur IT-Sicherheit geben zu können. Es ist geplant, diese Handreichung fortzuschreiben, um Erkenntnisse aus dem Markt erneut zu spiegeln.

Die IT-Grundschutz-Profile zur Absicherung von 5G-Campusnetzen sind kompatibel zum ISO-Standard 27001 und berücksichtigt die Empfehlungen der anderen ISO-Standards wie beispielsweise die Risikoanalyse der ISO 27005.

Um eine Plattform zur Vernetzung und zum Erfahrungsaustausch für 5G-Campusnetzbetreiber und Unternehmen und Organisationen in der Planungsphase zu bieten, plant das BSI den Aufbau eines Erfahrungskreises für 5G im Rahmen der Allianz für Cyber-Sicherheit. Mit der 2012 gegründeten Allianz für Cyber-Sicherheit verfolgt das BSI das Ziel, die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu stärken.

8 Quellen

[1] Entwicklung von 5G-Campusnetzen in Deutschland und Europa, Abschlusspräsentation, wik GmbH, 14.10.2021

[2] IT-Grundschutz-Profile zur Absicherung von 5G-Campusnetzen im Eigen- und Fremdbetrieb https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/5-G/Absicherung-5G-Campusnetze/IT-Grundschutz/IT-Grundschutz-Absicherung-5G-Campusnetze_node.html

[3] NESAS-Schema der GSMA https://www.gsma.com/security/network-equipment-security-assurance-scheme/

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Fachleute, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Personenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie der Vertrauenszeichen "IT Security made in Germany" und "IT Security made in EU". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kontakt:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Telefon: +49 30 4005 4306
E-Mail: holger.muehlbauer@teletrust.de
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.


TeleTrusT
Pioneers in IT security.