

PRESSEMITTEILUNG

IT-Sicherheit in 5G-Campusnetzen

Bundesverband IT-Sicherheit e.V. (TeleTrust) veröffentlicht Handreichung

Berlin, 27.03.2024 - Der Mobilfunkstandard 5G ist eine Schlüsseltechnologie, die sich zum größten Infrastrukturvorhaben des kommenden Jahrzehnts entwickelt und die Digitalisierung von Staat, Wirtschaft und Gesellschaft auf eine vollkommen neue Basis stellt. Um Daten zu schützen und die Verfügbarkeit von sog. 5G-Campusnetzen zu gewährleisten, müssen sich die Anwender selbst um deren Absicherung kümmern. Eine jetzt veröffentlichte Handreichung des Bundesverbandes IT-Sicherheit e.V. (TeleTrust) richtet sich an alle interessierten Unternehmen, Institutionen und Organisationen, die bereits 5G-Netze produktiv oder als Testkonzept betreiben. Konkret wird die Ebene der IT-Administration und IT-Leitung angesprochen.

www.teletrust.de/publikationen/broschueren/5g-campusnetze/

5G-Technik hat das Potential, der Digitalisierung in den kommenden Jahren einen deutlichen Schub zu geben. Um dies erfolgreich zu realisieren, muss die IT-Sicherheit ausreichend berücksichtigt werden. Die Sicherheit von öffentlichen 5G-Netzen soll in Deutschland durch Regulierung erreicht werden. Die IT-Sicherheit privater 5G-Netze ist dagegen freiwillig und liegt in der Verantwortung der Betreiber. Betreiber sogenannter 5G-Campusnetze müssen nur eine Nutzungslizenz für die Frequenzen bei der Bundesnetzagentur beantragen, weitere Auflagen an die Auswahl der Technik und minimaler IT-Sicherheitsmaßnahmen gibt es dagegen nicht.

Aktuell werden 5G-Campusnetze unter anderem 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.

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.

Zur Eindämmung potentieller Bedrohungen müssen 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 jetzt publizierte TeleTrust-Handreichung dient hierbei als Orientierungshilfe. Neben einem Überblick zu Betriebsmodellen, Einsatz- und Bedrohungsszenarien ist der TeleTrust-Handreichung ein ergänzender Fragenkatalog beigelegt. Dieser listet wichtige Fragen auf, die beim Aufbau und Betrieb eines 5G-Campusnetzes gestellt werden sollten, um bei der Auswahl der Technologie, des Anbieters und des Betriebsmodells auch die IT-Sicherheit zu berücksichtigen.

Die Publikation wurde in der TeleTrust-AG "Smart Grids/Industrial Security" erarbeitet.

Sebastian Fritsch (secuvera GmbH), der die Erarbeitung koordinierte, stellt fest: "Neue 5G-Netzbetreiber erhalten mit der Handreichung eine praktische Fragenliste, um mit Anbietern neben funktionalen Aspekten auch die IT-Sicherheit noch vor der Beschaffung zu diskutieren."

Die Autorengruppe führte Workshops mit Anwendern und Anbietern von 5G-Campusnetzen durch und erstellte einen niederschweligen Einstieg in das Thema. Die Handreichung richtet sich primär an die IT-Verantwortlichen und Administratoren in Organisationen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterstützte das Projekt. Uwe Hoppenz, BSI-Fachbereichsleiter SZ3 (Cyber-Sicherheit in mobilen Infrastrukturen und Chiptechnologie), kommt zu dem Fazit: "Die bereitgestellte Handreichung dient als Hilfsmittel für Institutionen und Unternehmen, um die IT-Sicherheit ihrer privaten 5G-Netze von der Planungs- bis hin zur Betriebsphase zu gewährleisten."

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 Mitgliedschaft 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.