5G Risikoanalyse

Bundesamt
für Sicherheit in der
Informationstechnik

Das BSI als die **Cybersicherheitsbehörde des Bundes**
gestaltet Informationssicherheit in der Digitalisierung
durch Prävention, Detektion und Reaktion
für Staat, Wirtschaft und Gesellschaft.

Kompetenzzentrum 5G/6G

- Vorgaben zur Sicherheit von 5G-Netzen
- Untersuchung und Bewertung von Bedrohungen und Angriffstechniken im ***5G/6G Security Labor***
- Fachliche Mitarbeit in europäischen und internationalen Gremien im Rahmen der ***Standardisierung*** und ***Zertifizierung*** (u.a. ENISA, 3GPP, ETSI, GSMA)
- Kooperation mit F&E sowie Herstellern und Betreibern von Mobilfunknetzen

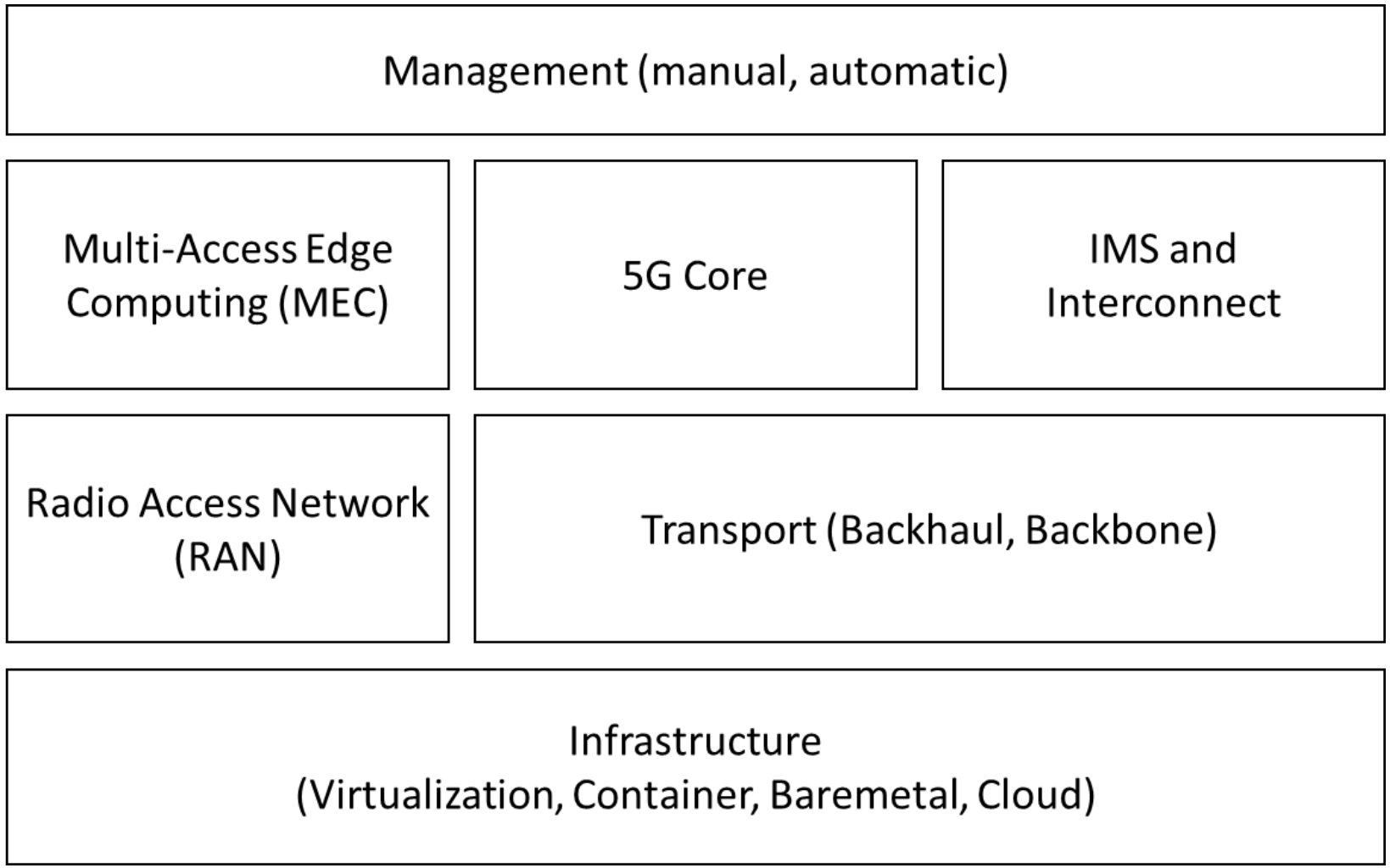
Inhalt

1. Überblick über das Projekt
2. Methodik: Risikoszenarien und Risk Score
3. Ausgewählte Beispiele aus den Studien
4. Gesamtergebnisse

Ziele des Projekts 5G Risikoanalyse

Bestimmung der abstrakten Kritikalität von Teilsystemen oder Funktionen/Komponenten in 5G-Netzen

- Wissensaufbau zum Thema Sicherheitsrisiken und –analysen in Mobilfunknetzen
- Fokussierung auf relevante Sicherheitsaspekte für Szenarien mit bezifferbarem Schadenspotential
- Annahme: Existenz parallel verfügbarer Netze (weitere MNOs, 4G/2G)
- Grundlage der Risikoanalyse: Modellhaftes 5G-System inkl. nicht-standardisierter Elemente


Management (manual, automatic)
Multi-Access Edge Computing (MEC)
5G Core
IMS and Interconnect
Radio Access Network (RAN)
Transport (Backhaul, Backbone)
Infrastructure
(Virtualization, Container, Baremetal, Cloud)

Projektphasen

I	Erste Materialsammlung zu Risikoanalysen Ausarbeitung der Methodik Entwurf der Risikoszenarien und des Rahmendokuments	05/22 – 05/23
II	Detailanalysen: Radio Access Network, Transport Networks, Core Network	05/23 – 07/24
III	Detailanalysen: IMS und Interconnect Network, Infrastructure, Management, Multi-Access Edge Computing	06/24 – 10/24
IV	Finalisierung der Detailanalysen (Qualitätsmanagement, Konsistenzcheck, Barrierefreiheit) Veröffentlichung	06/24 – 05/25

Methodik

Risiko = Schadenspotential x Eintrittswahrscheinlichkeit

Risikoszenarien

Risk Perspective	Risk Scenario	CIA	Beschreibung
Public Mobile Network Operator (MNO)	Emergency Call	A	§164 TKG (Notruf)
	Cell Broadcast	A	§164a TKG (Öffentliche Warnungen)
	Telecommunications Secrecy	C	§3 TTDSG (Fernmeldegeheimnis)
	Emergency Preparedness	A	§184 TKG (Notfallvorsorge)
	Regional Network Failure	A	
	Multi-Regional Network Failure	A	
	Failure of Mobile Service	A	
	Fraud	I	
	Subscriber Data Leak	C	
User Perspective	Urgent Telephone Calls Not Possible	A	
	Authenticity of the Receiver of a Call	I	
	Integrity of Transmitted Data	I	
	User Identity	I	
	Eavesdropping of a Communication	C	
	Slowing Down/Restricting the Connection	A	
	Connection Failure	A	
	Tapping or Altering of the Geographical Position	C	
Private 5G Network Operator	Network Failure	A	
	Degraded Services/Connections	A	
	Information Disclosure	C	
	User Identities	I	

Schadenspotential

6.1.1 Emergency Call (TKG § 164)

Emergency calls have the highest priority on the network. It is necessary to ensure that emergency calls are transmitted to the correct public safety answering point (PSAP) and that the data necessary to determine the location is transmitted.

If it is not possible to make emergency calls in general, there may be significant personal or economic damage. In the case that the PSAP transmission is incorrect, there is a risk that rescue measures might be delayed, which can lead to significant personal or economic damage.

Example: In a private home a fire could break out. If is not possible to make an emergency call the fire could spread unhindered by firefighters and cause significant economic damage (estimated value of a private home 350,000 EUR) or even loss of life (at least one fatality). The fire is likely to spread and could harm neighboring residents and other persons nearby.

Causative subsystems: Emergency call routing is performed in the Core and the IMS. Emergency call routing may be configurable from the management layer.

Impact Category	Impact Value	Impact Level
EUR (private user)	> 350,000 EUR	High
Personal injury	at least one fatality	High

Schadenspotential

Table 3: Impact Categories and Impact Levels

Categories	German term	Impact level		
		Low	Medium	High
User hours	Teilnehmerstunden	< 1,000,000	1,000,000 – 10,000,000	> 10,000,000
EUR (Network operator)	EUR (Netzbetreiber)	< 0.4% of the annual turnover	between 0.4% and 4% of the annual turnover	> 4% of the annual turnover
EUR (enterprise user)	EUR (kommerzieller Nutzer)			
EUR (private user)	EUR (privater Nutzer)	< 1,000 EUR	between 1,000 EUR and 10,000 EUR	> 10,000 EUR
Personal injury	Personenschaden	at most one lightly injured person (Unfall-kategorie 3 or higher)	at least one seriously injured person but no fatalities (Unfall-kategorie 2)	at least one fatality (Unfall-kategorie 1)

Eintrittswahrscheinlichkeit

5.3.3 Integrity of Transmitted Data

The 5G core network is a relevant attack domain for the risk scenario of the integrity of transmitted data due to its centralized role in data routing and control. It serves as the hub for processing and managing all types of data transmitted across the network, making it a critical point for ensuring data integrity. Failures can lead to widespread corruption, as the Core network is responsible for the application of security protocols that maintain the integrity of data between endpoints.

Attack Path Category	Attack Path ID	Probability Description	Probability Level
Misconfiguration	Integrity (AP1-I)	The probability of integrity compromise due to misconfigurations is ranked as **MEDIUM** and specifically addresses the risk scenario of integrity in transmitted data within the 5G core network. The relevance of this scenario is heightened by the Core network's role in managing a variety of transmission protocols that, if misconfigured, could lead to unauthorized data manipulation. The potential for attackers to exploit improperly configured TLS and mTLS protocols could allow for the alteration of control and user plane data, directly impacting the integrity of the data being transmitted. This is particularly concerning for interfaces N1 through N4, which are essential for the secure and accurate exchange of data within the network. The mandatory implementation of security protocols, albeit their optional use, introduces a risk variable that could be critical in the event of misconfiguration [DRU19, THE23]. Ensuring the integrity of transmitted data hinges on the robustness of these configurations, making this a focal point for safeguarding the network against integrity attacks.	Medium
Insufficient Access Controls	Integrity (AP2-I)	Integrity compromise in the 5G core network due to insufficient access controls is rated as **MEDIUM** and considers the multiple avenues for unauthorized data manipulation. Critical data alterations can occur from overly privileged cloud workloads and weak MFA, providing attackers with opportunities to disrupt the integrity of data transmission [DAT23]. The longevity of certain credentials can also facilitate extended unauthorized access, further endangering data integrity. High-level access via compromised management interfaces could allow for significant unauthorized modifications, impacting the network's integrity.	Medium

Eintrittswahrscheinlichkeit

Attack Path Category	Attack Path ID	Probability Description	Probability Level
Implementation Flaw or Quality of the Product	Integrity (AP3-I)	The threat to the integrity of transmitted data due to implementation flaws in the 5G core network is assessed as **MEDIUM**. This risk encompasses potential vulnerabilities in the implementation of 3GPP protocols and other critical software components that could be exploited, leading to data manipulation [SSI23, MTE21]. Notably, the exploitation of these flaws could directly impact the integrity of the data being transmitted across the network, which allows for the injection and alteration of network traffic. The complexities inherent in the telecommunications software and the reliance on various open-source components further increase the risk of such integrity breaches. Mitigation provided by certification schemes like NESAS CCS-GI reduce the risk to LOW. However, until these become mandatory, the network remains exposed to these threats, underlining the importance of robust and secure software implementation practices.	Medium
Specification Weakness	Integrity (AP4-I)	In the context of ensuring the integrity of transmitted data within the 5G core network, the risk of integrity compromise due to specification weaknesses is assessed as **LOW**, highlighting the sophisticated design of 5G security protocols. Historical issues have largely been addressed, still the integration of advanced algorithms underscores the need for precise configuration to maintain the integrity of data [ETS06, ETS11]. Potential weaknesses could lead to scenarios where attackers exploit specification gaps, leading to the alteration or fabrication of data being transmitted. This risk is especially relevant in the context of non-3GPP protocol vulnerabilities. These components are crucial for ensuring the secure and authentic exchange of data across the network, and any compromise could directly impact the network's ability to preserve the integrity of data transmissions. The rating reflects confidence in the existing security measures while acknowledging the continuous effort needed to adapt to evolving threats within the 5G ecosystem.	Low
Failure of Power Supply	Integrity (AP5-I)	No specific attack path or risk source could be identified during this analysis.	Low
Failure of Hardware Components or Unavailability of Spare Parts	Integrity (AP6-I)	No specific attack path or risk source could be identified during this analysis.	Low

Risiko = Schadenspotential x Eintrittswahrscheinlichkeit

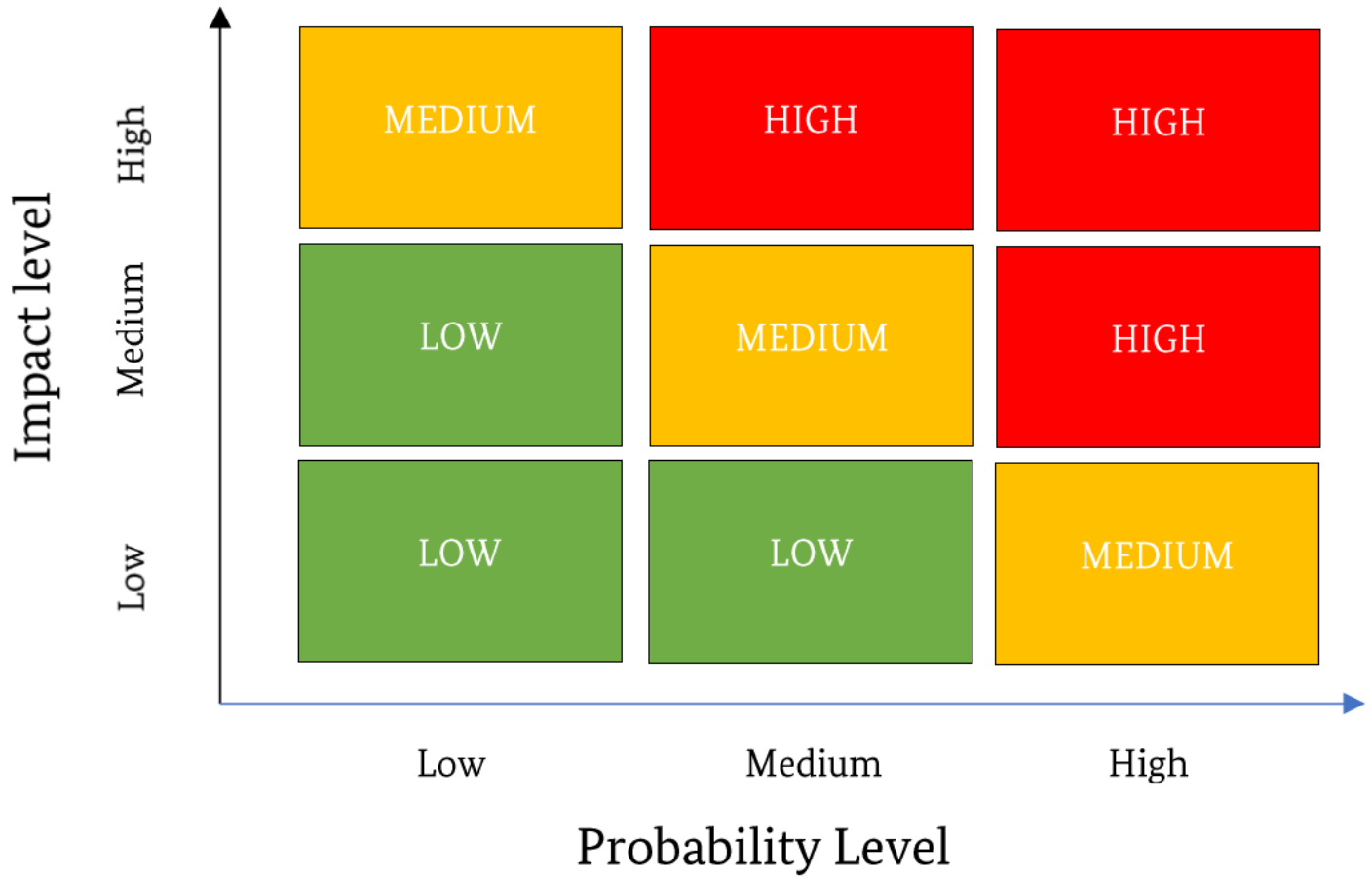


Figure 8: Risk score matrix

Beispiel 1: Core Network

Integrity of Transmitted Data (User)

Definition des Schadenspotentials

- In this scenario, the participants of an established connection can‘t be sure that the data received is the very same data that was sent
- Example:
  - This scenario, most likely, occurs due to a targeted attack → only one person or business affected
  - Since this scenario affects all kind of transmitted data, the consequences might be very severe.
  - Business is affected with a damage value of over 4% of the annual turnover. For a private person, the damage could reach several thousands of euros, for example if the attacker manages to manipulate transmitted banking data.

Impact Category	Impact Value	Impact Level
EUR (enterprise user)	> 4% of the annual turnover	High
EUR (private user)	> 10,000 EUR	High

Analyse der Eintrittswahrscheinlichkeit (Core als „Ursache“)

Attack Path Category	Probability Description	Probability Level
Misconfiguration	Core manages a variety of transmission protocols Attackers could exploit improperly configured TLS and mTLS protocols to alter control and user plane data	Medium
Insufficient Access Controls	Data alterations can occur from overly privileged cloud workloads and weak MFA	Medium
Implementation Flaw (Quality of the Product)	Telco software is complex → potential vulnerabilities in implementation of 3GPP protocols Certification (NESAS CCS-GI) could reduce probability	Medium
Specification Weakness	Design of 5G security architecture and protocols is sophisticated	Low
Failure of Power Supply	No specific attack path or risk source could be identified during this analysis	Low
Failure of Hardware Components	No specific attack path or risk source could be identified during this analysis	Low

Berechnung des Risikos: Probability x Impact = Risk Score

6.2.3	Integrity of Transmitted Data	Core	Medium		High
		RAN	Medium	High	High
		Transport	Medium		High
		IMS and Interconnect	Medium		High
		Infrastructure	Medium		High
		Management	Medium		High
		MEC	Medium		High

Einordnung des Beispiels in das Gesamtprojekt

7 Detailanalysen (Core, RAN, Transport, IMS und Interconnect, Infrastructure, MEC, Management)

21 Risikoszenarien

→ Insgesamt betrachtet: Eintrittswahrscheinlichkeit für **107 Szenarien** analysiert

→ Beispiel zeigt ca. 1% der Wahrscheinlichkeitsanalyse

Beispiel 2: RAN

Information Disclosure (Private 5G Network Operator)

Definition des Schadenspotentials

6.3.3 Information Disclosure

The 5G transport layer is capable of securing the transmission of data if the configuration is set properly according to the 3GPP specifications. Applications on higher software layers could rely on the proper configuration of the transport layer security. This could lead to an information disclosure, if the transmission encryption of the transport layer is not properly working by accident or with a malicious intent.

Example: In a hospital scenario different kind of medical devices are connected to the private 5G network. A medical device could assume the transport network is secure and does not implement transport security. In these cases, transport security of the 5G network is essential. Misconfiguration of communication parameters might lead to unencrypted connections that could be eavesdropped. Finally, personal identifiable information (PII) could be disclosed like ECG, pulse, blood pressure, the patient's name, data about the treated disease/injury, prescribed medication, treatment plans etc. This could lead to severe penalty fee of several tens of thousands of euros, or up to 4% of the organization's yearly turnover according to GDPR.

Causative subsystems: All subsystems of a private 5G network with external interfaces play a dominant role in providing secure transmission of data. While Infrastructure is therefore excluded, an information disclosure may also be caused by configurations via the Management layer.

Impact Category	Impact Value	Impact Level
EUR (network operator)	< 4% of the annual turnover	Medium

Analyse der Eintrittswahrscheinlichkeit (RAN als „Ursache“)

Attack Path Category	Probability Description	Probability Level
Misconfiguration	Configuration of encryption heavily depends on the security concepts of the corresponding company → encryption might not be enforced or could be bypassed	Medium
Insufficient Access Controls	Extractions of sensitive information can occur from overly privileged cloud components and weak MFA Radio sites of private networks are often well protected. In contrast, deployments at public places such as stations or hospitals ease the physical access to radio sites → Probability depends on the security measures installed	Medium
Implementation Flaw (Quality of the Product)	Telco software is complex → potential vulnerabilities in implementation of 3GPP protocols and open source software	Medium
Specification Weakness	Traffic of user priority groups is transmitted without encryption on air interface → Tracking and exploitation of user priority groups is associated with medium effort	Low
Failure of Power Supply	The failure of power supply appears unrelated to information disclosure	Low
Failure of Hardware Components	Hardware failures appear unrelated to information disclosure	Low
Radio Interference	Attacks utilizing radio interference appear unrelated to information disclosure	Low

Berechnung des Risikos: Probability x Impact = Risk Score

6.3.3	Information Disclosure	Core	Medium		Medium
		RAN	Medium		Medium
		Transport	Medium	Medium	Medium
		IMS and Interconnect			
		Infrastructure			
		Management	Medium		Medium
		MEC	Medium		Medium

Ergebnisse der 7 Detailanalysen

Core, RAN, Transport

IMS & Interconnect

Infrastructure

MEC

Management

Core

Netzfunktionen im Core kritisch für Szenarien mit großflächigen Auswirkungen

Relevante Vorfälle:

- → Datenleck bei SK Telecom durch HSS-Hack
- → Kompromittierung von US-Telcos durch Salt Typhoon
- → Landesweiter Ausfall (14 h) von Mobilfunknetz in Australien durch Software-Upgrade

Perspective	Risk Scenario	Impact	Probability	Risk Score
Public MNO	Emergency Call (TKG § 164)	High	Medium	High
	Cell Broadcast (TKG § 164a)	High	Medium	High
	Telecommunications Secrecy (TTDSG § 3)	Medium	Medium	Medium
	Emergency Preparedness (TKG § 184)	High	Medium	High
	Regional Network Failure	Medium	Medium	Medium
	Multi-Regional Network Failure	High	Medium	High
	Failure of Mobile Service	Medium	Medium	Medium
	Fraud	Low	Medium	Low
	Subscriber-Data Leak	Medium	Medium	Medium
User	Urgent Telephone Calls Not Possible	Low	Medium	Low
	Authenticity of the Receiver of a Call	Medium	Medium	Medium
	Integrity of Transmitted Data	High	Medium	High
	User's Identity	High	Medium	High
	Eavesdropping of a Communication	Medium	Medium	Medium
	Slowing Down/Restricting the Connection	Low	Medium	Low
	Connection Failure	Low	Medium	Low
	Tapping or Altering of the Geographical Position	High	Medium	High
Private 5G Network Operator	Network Failure	Medium	Medium	Medium
	Degraded Services/Connections	Medium	Medium	Medium
	Information Disclosure	Medium	Medium	Medium
	User Identities (Authenticity/ Integrity)	Medium	Medium	Medium

RAN

RAN-Komponenten sind kritisch bei Szenarien mit regional begrenzten Auswirkungen

Problematisch: Integritätsschutz auf der Luftschnittstelle wird von MNOs oft nicht aktiviert

Perspective	Risk Scenario	Impact	Probability	Risk Score
Public MNO	Emergency Call (TKG § 164)	High		
	Cell Broadcast (TKG § 164a)	High	High	High
	Telecommunications Secrecy (TTDSG § 3)	Medium	Medium	Medium
	Emergency Preparedness (TKG § 184)	High	Medium	High
	Regional Network Failure	Medium	High	High
	Multi-Regional Network Failure	High		
	Failure of Mobile Service	Medium		
	Fraud	Low		
	Subscriber-Data Leak	Medium	Medium	Medium
User	Urgent Telephone Calls Not Possible	Low	Medium	Low
	Authenticity of the Receiver of a Call	Medium		
	Integrity of Transmitted Data	High	Medium	High
	User's Identity	High	Low	Medium
	Eavesdropping of a Communication	Medium	Medium	Medium
	Slowing Down/Restricting the Connection	Low	Medium	Low
	Connection Failure	Low	Medium	Low
	Tapping or Altering of the Geographical Position	High	Medium	High
Private 5G Network Operator	Network Failure	Medium	High	High
	Degraded Services/Connections	Medium	High	High
	Information Disclosure	Medium	Medium	Medium
	User Identities (Authenticity/ Integrity)	Medium	Medium	Medium

Transport

Nachteil der abstrakten Betrachtung der Risikoanalyse wird bei dieser Analyse deutlich → keine Aussage zu einzelnen Komponenten(gruppen) möglich

Anzahl an neu entdeckten Schwachstellen bei Netzwerkprodukten sehr hoch
→ aktive Ausnutzung durch APT-Hackergruppierungen, z.B. Salt Typhoon

Perspective	Risk Scenario	Impact	Probability	Risk Score
Public MNO	Emergency Call (TKG § 164)	High	Medium	High
	Cell Broadcast (TKG § 164a)	High	Medium	High
	Telecommunications Secrecy (TTDSG § 3)	Medium	Medium	Medium
	Emergency Preparedness (TKG § 184)	High	Medium	High
	Regional Network Failure	Medium	Medium	Medium
	Multi-Regional Network Failure	High	Medium	High
	Failure of Mobile Service	Medium	Medium	Medium
	Fraud	Low		
	Subscriber-Data Leak	Medium	Medium	Medium
User	Urgent Telephone Calls Not Possible	Low	Medium	Low
	Authenticity of the Receiver of a Call	Medium		
	Integrity of Transmitted Data	High	Medium	High
	User's Identity	High		
	Eavesdropping of a Communication	Medium	Medium	Medium
	Slowing Down/Restricting the Connection	Low	Medium	Low
	Connection Failure	Low	Medium	Low
	Tapping or Altering of the Geographical Position	High		
Private 5G Network Operator	Network Failure	Medium	High	High
	Degraded Services/Connections	Medium	High	High
	Information Disclosure	Medium	Medium	Medium
	User Identities (Authenticity/ Integrity)	Medium		

IMS & Interconnect

Abgrenzung der beiden Teilbereiche ist anhand des Risikowerts nicht eindeutig
→ im Fließtext besser unterscheidbar

Aktuell noch kein realer Betrieb des SEPP
→ Analyse sehr theoretisch

Campusnetzbetreiber könnten zukünftig IMS integrieren → Risikoanalyse trifft Annahme, dass Probability analog zu Public MNO ist

Perspective	Risk Scenario	Impact	Probability	Risk Score
Public MNO	Emergency Call (TKG § 164)	High	Medium	High
	Cell Broadcast (TKG § 164a)	High		
	Telecommunications Secrecy (TTDSG § 3)	Medium	High	High
	Emergency Preparedness (TKG § 184)	High	High	High
	Regional Network Failure	Medium		
	Multi-Regional Network Failure	High		
	Failure of Mobile Service	Medium	Medium	Medium
	Fraud	Low	High	Medium
	Subscriber-Data Leak	Medium	High	High
User	Urgent Telephone Calls Not Possible	Low	Medium	Low
	Authenticity of the Receiver of a Call	Medium	Low	Low
	Integrity of Transmitted Data	High	Medium	High
	User's Identity	High	Medium	High
	Eavesdropping of a Communication	Medium	Medium	Medium
	Slowing Down/Restricting the Connection	Low	High	Medium
	Connection Failure	Low	High	Medium
	Tapping or Altering of the Geographical Position	High	Medium	High
Private 5G Network Operator	Network Failure	Medium		
	Degraded Services/Connections	Medium		
	Information Disclosure	Medium		
	User Identities (Authenticity/ Integrity)	Medium		

Infrastructure

Im Prinzip Erweiterung/Ergänzung der MANO-Studie auf abstrakterem Level

Ergebnisse verstärken den Eindruck, dass virtualisierte Infrastrukturelemente sehr kritisch sein können, vor allem für Integrität und Vertraulichkeit von Userdaten

Perspective	Risk Scenario	Impact	Probability	Risk Score
Public MNO	Emergency Call (TKG § 164)	High		
	Cell Broadcast (TKG § 164a)	High		
	Telecommunications Secrecy (TTDSG § 3)	Medium	High	High
	Emergency Preparedness (TKG § 184)	High		
	Regional Network Failure	Medium		
	Multi-Regional Network Failure	High	Medium	High
	Failure of Mobile Service	Medium		
	Fraud	Low		
	Subscriber-Data Leak	Medium	High	High
User	Urgent Telephone Calls Not Possible	Low		
	Authenticity of the Receiver of a Call	Medium		
	Integrity of Transmitted Data	High	Medium	High
	User's Identity	High	High	High
	Eavesdropping of a Communication	Medium	Medium	Medium
	Slowing Down/Restricting the Connection	Low		
	Connection Failure	Low		
	Tapping or Altering of the Geographical Position	High		
Private 5G Network Operator	Network Failure	Medium	Medium	Medium
	Degraded Services/Connections	Medium	High	High
	Information Disclosure	Medium		
	User Identities (Authenticity/ Integrity)	Medium		

MEC

Bisher wenig Erfahrung (Theorie & Praxis) und Berührungspunkte mit MEC

MEC wird in öffentlichen Netzen wahrscheinlich erst relevant, wenn Slicing an Bedeutung gewinnt

Bei Campusnetzen spielt MEC jetzt schon eine große Rolle

Perspective	Risk Scenario	Impact	Probability	Risk Score
Public MNO	Emergency Call (TKG § 164)	High		
	Cell Broadcast (TKG § 164a)	High		
	Telecommunications Secrecy (TTDSG § 3)	Medium	Medium	Medium
	Emergency Preparedness (TKG § 184)	High		
	Regional Network Failure	Medium		
	Multi-Regional Network Failure	High		
	Failure of Mobile Service	Medium	High	High
	Fraud	Low		
	Subscriber-Data Leak	Medium		
User	Urgent Telephone Calls Not Possible	Low		
	Authenticity of the Receiver of a Call	Medium		
	Integrity of Transmitted Data	High	Medium	High
	User's Identity	High	Medium	High
	Eavesdropping of a Communication	Medium	Medium	Medium
	Slowing Down/Restricting the Connection	Low	High	Medium
	Connection Failure	Low		
	Tapping or Altering of the Geographical Position	High	Low	Medium
Private 5G Network Operator	Network Failure	Medium	Medium	Medium
	Degraded Services/Connections	Medium	Medium	Medium
	Information Disclosure	Medium	Medium	Medium
	User Identities (Authenticity/ Integrity)	Medium	Medium	Medium

Management

Initial isolierte Betrachtung der Management-Ebene ohne direkte Auswirkungen auf andere Teilbereiche des 5G-Netzes → Zuerst viele Low-Ergebnisse

Anpassung der Ergebnisse: Integration der Misconfiguration-Ergebnisse aus allen anderen Teilbereichen

Am meisten High-Ergebnisse aus allen Analysen → Management-Systeme sind sehr kritisch und haben Einfluss auf alle Teilbereiche

Perspective	Risk Scenario	Impact	Probability	Risk Score
Public MNO	Emergency Call (TKG § 164)	High	Medium	High
	Cell Broadcast (TKG § 164a)	High	Low	Medium
	Telecommunications Secrecy (TTDSG § 3)	Medium	High	High
	Emergency Preparedness (TKG § 184)	High	High	High
	Regional Network Failure	Medium	Medium	Medium
	Multi-Regional Network Failure	High	Medium	High
	Failure of Mobile Service	Medium	High	High
	Fraud	Low	High	Medium
	Subscriber-Data Leak	Medium	High	High
User	Urgent Telephone Calls Not Possible	Low	Medium	Low
	Authenticity of the Receiver of a Call	Medium	Medium	Medium
	Integrity of Transmitted Data	High	Medium	High
	User's Identity	High	High	High
	Eavesdropping of a Communication	Medium	Medium	Medium
	Slowing Down/Restricting the Connection	Low	High	Medium
	Connection Failure	Low	High	Medium
	Tapping or Altering of the Geographical Position	High	Medium	High
Private 5G Network Operator	Network Failure	Medium	Medium	Medium
	Degraded Services/Connections	Medium	High	High
	Information Disclosure	Medium	Medium	Medium
	User Identities (Authenticity/ Integrity)	Medium	Medium	Medium

Perspektivwechsel

Public MNO

User

Private 5G Network Operator

Public MNO

9 Szenarien

Section	Risk Scenario	5G Subsystem	Probability Level	Impact Level	Risk Score
6.1.1	Emergency Call (TKG § 164)	Core	Medium	High	High
		RAN			
		Transport	Medium		High
		IMS and Interconnect	Medium		High
		Infrastructure			
		Management	Medium		High
		MEC			
6.1.2	Cell Broadcast (TKG § 164a)	Core	Medium	High	High
		RAN	High		High
		Transport	Medium		High
		IMS and Interconnect			
		Infrastructure			
		Management	Low		Medium
		MEC			
6.1.3	Telecommunications Secrecy (TTDSG § 3)	Core	Medium	Medium	Medium
		RAN	Medium		Medium
		Transport	Medium		Medium
		IMS and Interconnect	High		High
		Infrastructure	High		High
		Management	High		High
		MEC	Medium		Medium
6.1.4	Emergency Preparedness (TKG § 184)	Core	Medium	High	High
		RAN	Medium		High
		Transport	Medium		High
		IMS and Interconnect	High		High
		Infrastructure			
		Management	High		High
		MEC			
6.1.5	Regional Network Failure	Core	Medium	Medium	Medium
		RAN	High		High
		Transport	Medium		Medium
		IMS and Interconnect			
		Infrastructure			
		Management	Medium		Medium
		MEC			
6.1.6	Multi-Regional Network Failure	Core	Medium	High	High
		RAN			
		Transport	Medium		High
		IMS and Interconnect			
		Infrastructure	Medium		High
		Management	Medium		High
		MEC			
6.1.7	Failure of Mobile Service	Core	Medium	Medium	Medium
		RAN			
		Transport	Medium		Medium
		IMS and Interconnect	Medium		Medium
		Infrastructure			
		Management	High		High
		MEC	High		High

6.1.8	Fraud	Core	Medium	Low	Low
		RAN			
		Transport			
		IMS and Interconnect	High		Medium
		Infrastructure			
		Management	High		Medium
		MEC			
6.1.9	Subscriber-Data Leak	Core	Medium	Medium	Medium
		RAN	Medium		Medium
		Transport	Medium		Medium
		IMS and Interconnect	High		High
		Infrastructure	High		High
		Management	High		High
		MEC			

User

8 Szenarien

Section	Risk Scenario	5G Subsystem	Probability Level	Impact Level	Risk Score
6.2.1	Urgent Telephone Calls Not Possible	Core	Medium	Low	Low
		RAN	Medium		Low
		Transport	Medium		Low
		IMS and Interconnect	Medium		Low
		Infrastructure			
		Management	Medium		Low
		MEC			
6.2.2	Authenticity of the Receiver of a Call	Core	Medium	Medium	Medium
		RAN			
		Transport			
		IMS and Interconnect	Low		Low
		Infrastructure			
		Management	Medium		Medium
		MEC			
6.2.3	Integrity of Transmitted Data	Core	Medium	High	High
		RAN	Medium		High
		Transport	Medium		High
		IMS and Interconnect	Medium		High
		Infrastructure	Medium		High
		Management	Medium		High
		MEC	Medium		High
6.2.4	User's Identity	Core	Medium	High	High
		RAN	Low		Medium
		Transport			
		IMS and Interconnect	Medium		High
		Infrastructure	High		High
		Management	High		High
		MEC	Medium		High
6.2.5	Eavesdropping of a Communication	Core	Medium	Medium	Medium
		RAN	Medium		Medium
		Transport	Medium		Medium
		IMS and Interconnect	Medium		Medium
		Infrastructure	Medium		Medium
		Management	Medium		Medium
		MEC	Medium		Medium
6.2.6	Slowing Down/Restricting the Connection	Core	Medium	Low	Low
		RAN	Medium		Low
		Transport	Medium		Low
		IMS and Interconnect	High		Medium
		Infrastructure			
		Management	High		Medium
		MEC	High		Medium
6.2.7	Connection Failure	Core	Medium	Low	Low
		RAN	Medium		Low
		Transport	Medium		Low
		IMS and Interconnect	High		Medium
		Infrastructure			
		Management	High		Medium
		MEC			
6.2.8	Tapping or Altering of the Geographical Position	Core	Medium	High	High
		RAN	Medium		High
		Transport			
		IMS and Interconnect	Medium		High
		Infrastructure			
		Management	Medium		High
		MEC	Low		Medium

Private 5G Network Operator

4 Szenarien

Section	Risk Scenario	5G Subsystem	Probability Level	Impact Level	Risk Score
6.3.1	Network Failure	Core	Medium	Medium	Medium
		RAN	High		High
		Transport	High		High
		IMS and Interconnect			
		Infrastructure	Medium		Medium
		Management	Medium		Medium
		MEC	Medium		Medium
6.3.2	Degraded Services/Connections	Core	Medium	Medium	Medium
		RAN	High		High
		Transport	High		High
		IMS and Interconnect			
		Infrastructure	High		High
		Management	High		High
		MEC	Medium		Medium
6.3.3	Information Disclosure	Core	Medium	Medium	Medium
		RAN	Medium		Medium
		Transport	Medium		Medium
		IMS and Interconnect			
		Infrastructure			
		Management	Medium		Medium
		MEC	Medium		Medium
6.3.4	User Identities (Authenticity/ Integrity)	Core	Medium	Medium	Medium
		RAN	Medium		Medium
		Transport			
		IMS and Interconnect			
		Infrastructure			
		Management	Medium		Medium
		MEC	Medium		Medium

Gesamtergebnis

Perspective	Risk Scenario	Risk Score (Low/Medium/High)						
		Core	RAN	Transport	IMS and Inter-connect	Infra-structure	Manage-ment	MEC
Public MNO	Emergency Call (TKG § 164)							
	Cell Broadcast (TKG § 164a)							
	Telecommunications Secrecy (TTDSG § 3)							
	Emergency Preparedness (TKG § 184)							
	Regional Network Failure							
	Multi-Regional Network Failure							
	Failure of Mobile Service							
	Fraud							
	Subscriber-Data Leak							
User	Urgent Telephone Calls Not Possible							
	Authenticity of the Receiver of a Call							
	Integrity of Transmitted Data							
	User's Identity							
	Eavesdropping of a Communication							
	Slowing Down/Restricting the Connection							
	Connection Failure							
	Tapping or Altering of the Geographical Position							
Private 5G Network Operator	Network Failure							
	Degraded Services / Connections							
	Information Disclosure							
	User Identities (Authenticity/Integrity)							

Fazit

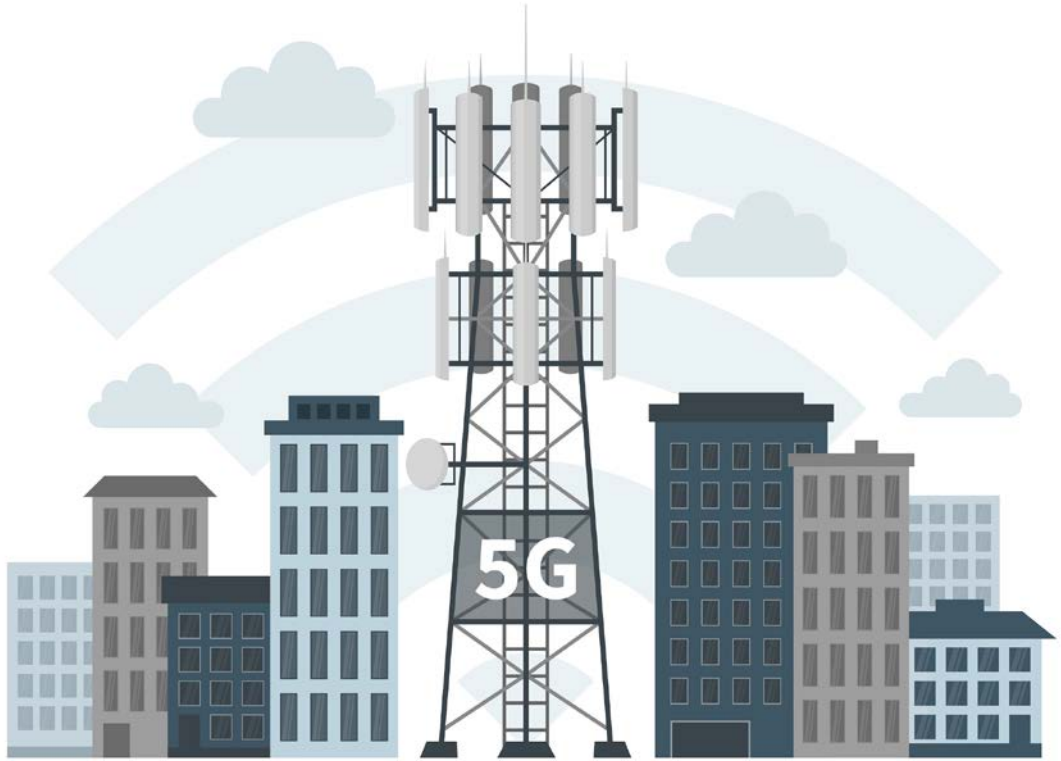
Medium- und High-Bewertung der abstrakten Kritikalität überwiegen

→ Maßnahmen des BSI:

- Vorgaben und Richtlinien für MNO, z.B. Beteiligung an der Überarbeitung des Sicherheitskatalogs
- Veröffentlichung von Grundschutzprofilen zur Absicherung von 5G-Campusnetzen
- Entwicklung und Umsetzung des nationalen Zertifizierungsschemas NESAS CCS-GI
- Beteiligung an Standardisierungsgremien (3GPP, ETSI, GSMA)

Deutschland
Digital•Sicher•BSI•

Vielen Dank für Ihre Aufmerksamkeit!



Kontakt

Referat S 31 – Sicherheit der Infrastruktur für 5G/6G
referat-s31@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Hüttenstr. 14
01705 Freital
www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik