Horst Görtz Institut
für IT-Sicherheit

0 1 0 1
0 1 0 1
0 1 0 1

Whitepaper – Mit *Sicherheit* 5G

Was bedeutet die „fünfte Generation“ des Mobilfunkstandards für die IT-Sicherheit?

Einleitung

5G – die „fünfte Generation“ des mobilen Internets und Telefonie – soll ab 2020 flächendeckend in Deutschland verfügbar sein. Anders als beim Vorgänger 4G ist hiermit aber nicht nur der Funkstandard (LTE) gemeint, sondern der Begriff umfasst vielmehr die gesamte Netzinfrastruktur und schließt diverse Kommunikationstechnologien mit ein. Damit wird 5G zum Synonym für die vollständige Vernetzung von Wirtschaft und Gesellschaft mit dem Internet – egal wo. Die Übertragung von Daten in Echtzeit und enorme Netzkapazitäten ermöglichen zahlreiche Anwendungsmöglichkeiten wie etwa in der Produktion, der Logistik, dem autonomen Fahren, Smart Cities oder dem Internet der Dinge, die bislang noch undenkbar sind.

Deutschland möchte im Bereich 5G international eine Vorreiterrolle einnehmen. Als Basis für diesen Ausbau wurden im Frühjahr 2019 von der Bundesnetzagentur Lizenzen für insgesamt 6,55 Milliarden Euro versteigert. Der Ausbau des Netzes kann nun beginnen, aber was ist 5G eigentlich? Welche Akteure sind an dieser Innovation beteiligt und welchen Beitrag kann die IT-Sicherheitsforschung leisten, den Herausforderungen von 5G passgenau zu begegnen?

Dieses Whitepaper widmet sich diesen Fragen und argumentiert, dass 5G untrennbar mit dem Thema IT-Sicherheit verbunden ist. Wenn wir künftig die Vorteile von 5G nutzen wollen – egal ob privat oder in der Industrie – darf die Sicherheit dieser neuen Technologien nicht nur randständig berücksichtigt werden, sondern muss eine zentrale Rolle spielen.

In a nutshell: Was ist 5G?

Unter dem Sammelbegriff 5G sind diverse Schlüsseltechnologien zusammengefasst. Die Basis bilden die Zugangsnetze. Die bestehenden 4G/ LTE Netze mit der 5G *(New Radio)* Technologie werden erweitert. Die höhere Geschwindigkeit der Datenübertragung kann damit kürzere Latenzen, sprich Reaktionszeiten, erreichen.

Im zweiten Schritt wird ein „eigenes“ 5G-Kernnetz realisiert. Neben Mast- und Dachstandorten werden auch kleine Funkzellen *(small cells)* und größere Mehrantennensysteme (MIMO – Multiple Input, multiple output) zum Einsatz kommen und durch *Beamforming* – sprich der variablen und damit gezielten Ausrichtung von Signalen auf Endgeräte – abgerundet. Auf Basis der Zugangsnetze bildet die Virtualisierung von

Netzwerken ein neues Element von 5G. Hierbei erhält das lokale Netzwerk eine virtuelle Ebene und ermöglicht so eine ortsunabhängige Steuerung von Dienstangeboten und der Zuweisung von Ressourcen. Ein innovatives Element von 5G ist seine *„cloud Basis"*. Durch *slicing* können die Netzwerkbetreiber je nach Anwendung ihren Kunden z. B. diverse Übertragungsraten und Reaktionszeiten „portioniert" zur Verfügung stellen und ermöglichen hierdurch eine höhere Effizienz und Flexibilität. Im Gegensatz zu traditionellen Datennetzwerken ergibt sich hieraus ein enges Zusammenspiel zwischen Hard- und Software und die Konfigurierung und Inbetriebnahme erfolgt weitgehend softwarebasiert. Erst durch die Kombination der diversen Lösungen werden alle Vorteile von 5G nutzbar sein (siehe Kasten).

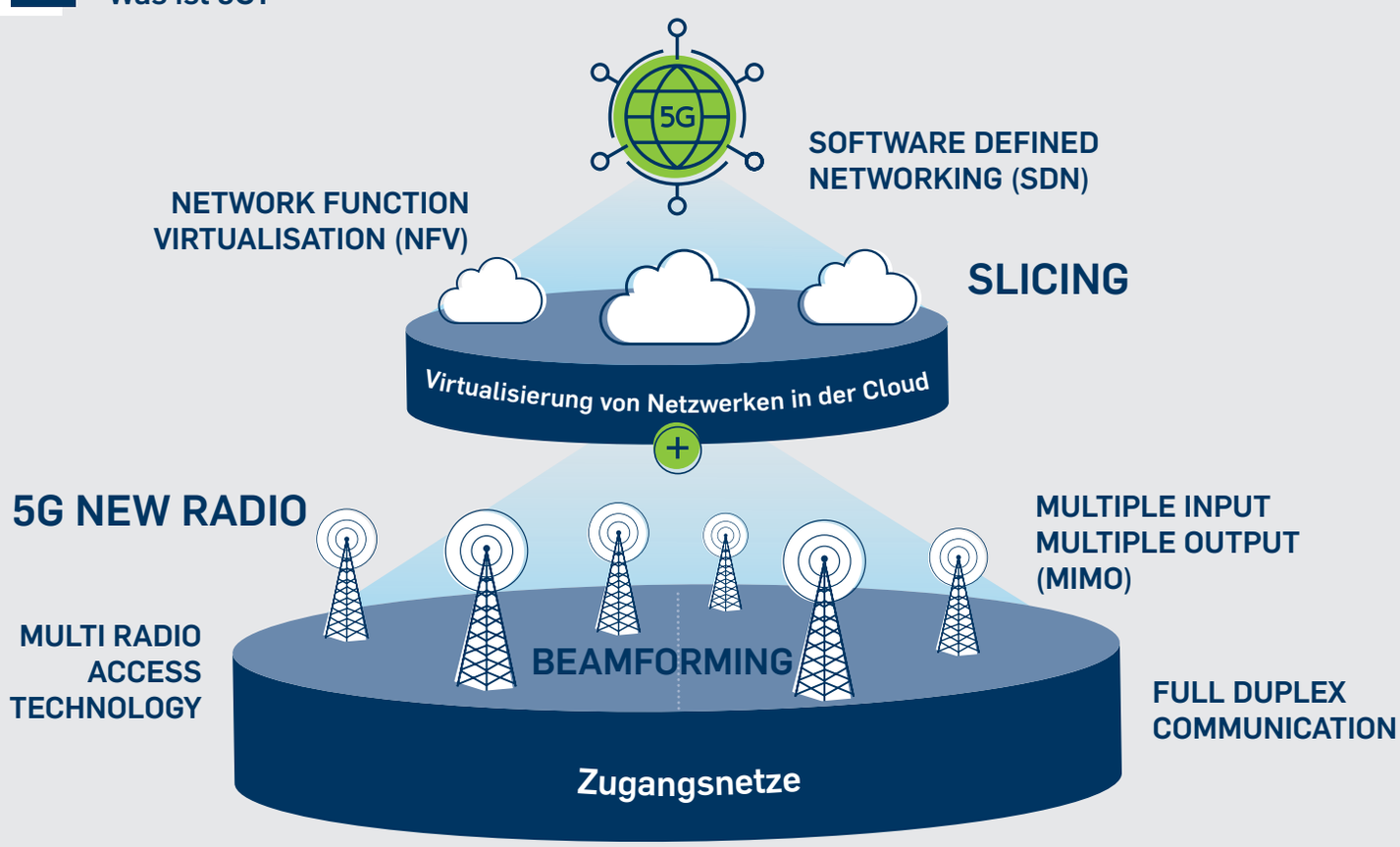
!

Die Vorteile von 5G im Überblick

- → *Schnelligkeit – mit Datenraten von bis zu 10.000 Mbit/s wäre 5G 100 Mal schneller als 4G*
- → *Kapazitäten* – die Netzkapazitäten könnten LTE um ein 1.000-faches übersteigen
- → *Niedrigere Latenzzeiten,* sprich jene Zeitspanne für eine Aktivität von einem Endgerät auf ein anderes. Dieser könnte künftig in Bruchteilen von Millisekunden, also quasi in Echtzeit erfolgen
- → Eine *Senkung der Energiekosten* von 90 % pro Mobildienst im Vergleich zum jetzigen Verbrauch.

?

Was ist 5G?



Glossar

- → ***Full Duplex Communication*** (Vollduplex) ist das gleichzeitige Empfangen und Senden von Informationen
- → ***MIMO – Multiple Input, multiple output*** ermöglicht Datenströme über mehrere Antennen gleichzeitig zu senden und zu empfangen. Hierdurch kann die Übertragungsgeschwindigkeit gesteigert werden.
- → ***Multi Radio Access Technology*** (RAT) ist ein Sammelbegriff für die diversen physikalischen Verbindungsverfahren für funkbasierte Kommunikationsnetzwerke.
- → ***network function virtualisation*** (NFV) umfasst diverse Cloud- und Virtualisierungstechnologien und ermöglicht die Steuerung von Netzwerkfunktionen durch Software.
- → ***New Radio*** ist ein Überbegriff für die Zugangstechnologien, die beim Netzausbau für 5G angewendet werden; wird teilweise auch als Luftschnittstelle bezeichnet.
- → ***Software Defined Networking*** entkoppelt Hard- und Software in einem Netzwerk voneinander und erleichtert so die Administration von Netzwerken.

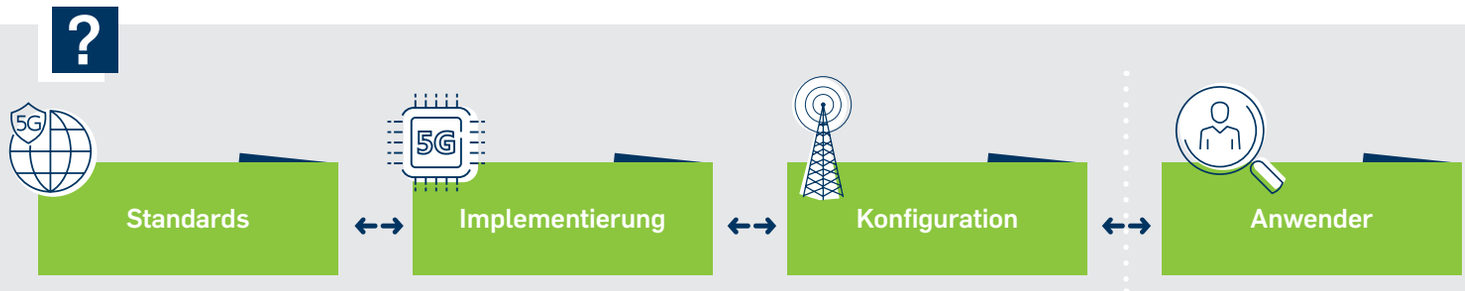
Nicht nur die technische Umsetzung ist sehr komplex, auch die an 5G beteiligten Akteure. Um die Anforderungen der Sicherheit der IT nachvollziehen zu können, sollte man nicht nur die technische Komponente betrachten, sondern auch die beteiligten Akteure. Es lassen sich grob vier Gruppen von Akteuren definieren, die an der Umsetzung von 5G beteiligt sind:

Zunächst müssen die technischen **Standards** und Spezifikationen definiert werden. Das 3rd Generation Partnership Project (3GPP) ist eine weltweite Kooperation von Standardisierungsgremien, die dieses Ziel verfolgt und 2019 mit dem *Release 15* und *Release 16* die Spezifikationen veröffentlicht hat. Bei 3GPP sind international Mobilfunknetzbetreiber, Hersteller, Regulierungsbehörden, Regierungen, Interessenvertreter und Dachverbände involviert.

Bei der **Implementierung** werden die Netzwerkbetreiber zunächst Milliarden in neue Funktechnik investieren. Allerdings gibt es nur wenige Hersteller, die das 5G Equipment produzieren. Viele Hersteller kaufen 99% der verarbeiteten Teile ein; dadurch ergibt sich eine relativ komplexe und fragmentierte Lieferkette. Hersteller sind beispielsweise Huawei, Ericson, Nokia, ZTE, Samsung und Qualcomm.

Wenn die Zugangsnetze ausgebaut wurden, kann der Netzbetrieb von 5G beginnen. In der **Konfiguration** müssen die Netzwerkbetreiber die technischen Standards umsetzen und den reibungslosen Netzbetrieb sicherstellen. Dazu gehört neben der Standortpflege auch die Inbetriebnahme und Steuerung in der Cloud. Die relevanten Netzwerkbetreiber in Deutschland sind die Deutsche Telekom, Vodafone, Telefonica und 1&1 Drilisch.

Im letzten Schritt erfolgt dann erst die tatsächliche Anwendung von 5G. Diese **Operationalisierung** ermöglicht wie angedeutet eine Vielzahl von Anwendungsmöglichkeiten wie etwa in der industriellen Fertigung und Logistik, beim autonomen Fahren, der Medizin, bei Smart Cities und allgemein im Bereich der Internet der Dinge. Die Nutzer können Klein- und Mittelständische Unternehmen, Großkonzerne, Start-Ups, Kommunen, aber auch private Nutzer sein.



Welche Herausforderungen ergeben sich für die (IT-)Sicherheit? Was sind Forschungsfragen der Zukunft?

Die Sicherheit von mobilen Netzwerken hängt von dem Zusammenspiel der verschiedenen Ebenen ab und wird durch 5G hinsichtlich der beteiligten Akteure als auch der technischen Fragmentierung komplexer und damit anfälliger für Sicherheitslücken.

Die Anforderungen an IT-Sicherheit vergrößern sich durch 5G auf allen Ebenen – beginnend bei der Standardisierung über die Implementierung und Konfiguration als auch der Operationalisierung. In der öffentlichen Debatte wird der Fokus jedoch stark auf die Implementierung und die Frage der Abhängigkeit von (meist ausländischen) Herstellern gerichtet. Diese Debatte zur „Politisierung der Lieferkette" ist berechtigt, aber greift zu kurz: Bei der Frage nach der Sicherheit der Systeme und Netze sollte die Debatte nicht auf einzelne Hersteller gerichtet werden, sondern das Zusammenspiel der verschiedenen Akteure gleichermaßen berücksichtigt werden. So sind die Standardisierung und ihre Umsetzung bei der Konfigurierung und Implementierung ebenso relevant wie die Risikominimierung auf Betreiberebene. Die Orchestrierung von 5G-Netzen über die Cloud verstärkt besonders die Rolle von Software (Sicherheit).

Im folgenden Schaukasten werden exemplarisch einzelne Herausforderungen und Forschungsfragen für die Bereiche **Standardisierung, Implementierung** und **Konfiguration** aufgeführt, die aus Sicht des Horst Görtz Instituts für IT-Sicherheit relevant sind. Die Auflistung erhebt keinen Anspruch auf Vollständigkeit, sondern soll vielmehr für die Komplexität und Abstraktion der Thematik sensibilisieren.

Ebenso wird hier die tatsächliche **Anwendung** von 5G schemenhaft angerissen. Insgesamt erhöht die Einführung von

Cyber Physical Systems (CPS)-Komponenten – sprich der Verbindung von mechanischen Komponenten mit Software – die Empfindlichkeit für Angriffe von außen. Für Unternehmen muss daher sichergestellt werden, dass geistiges Eigentum bestmöglich geschützt wird. Die Anwendungsfelder von 5G sind so vielfältig, dass sich auch hier nur andeuten lässt, welche Herausforderungen/Fragen noch ungelöst sind.

Forschungsfragen der Zukunft

Standards

Herausforderungen

- Die Vielzahl an beteiligten Akteuren (und Interessenten?) bei den Verhandlungen führt oft dazu, dass man sich nur auf den kleinsten gemeinsamen Nenner einigen kann. Für den Bereich der IT-Sicherheit bedeutet das meist Abstriche (Bsp. die Verschlüsselung von Funkverbindungen ist aus diesem Grund noch immer optional).
- Außerdem gibt es einen Interessengegensatz zwischen Sicherheitsanforderungen einerseits (z.B. durch Ende-zu-Ende-Verschlüsselung) und der rechtmäßigen Strafverfolgung durch Polizei und Justiz andererseits

Noch offen

- Wie sicher und robust sind die 5G-Standards (3GPP) für diverse gesellschaftliche Anwendungsfälle?
- Wie kann sichergestellt werden, dass der 5G-Standard keine absichtlichen oder unabsichtlichen Schwachstellen enthält?
- Wie müssen die staatlichen Rahmenbedingungen ausgestaltet sein, damit die Sicherheitsanforderungen eingehalten werden?

Implementierung

Herausforderungen

- Auslegung der komplexen Standards ist oft nicht eindeutig und lässt viel Interpretationsraum zu
- Lieferkette komplex und fragmentiert; diese hohe Interdependenz macht Vertrauenswürdigkeit entlang der gesamten Lieferkette schwierig aber zwingend erforderlich.
- *Pentests* oder *„security assessments"* helfen, aber es lässt sich nie zweifelsfrei beweisen, ob bösartige Software oder Hintertüren in vernetzten Systemen vorhanden sind

Noch offen

- Wie kann ein Hersteller sicherstellen, dass die zugelieferte Hard- oder Software keine Schwachstellen enthält?
- Wie kann man Algorithmen für die Verschlüsselung und den Integritätsschutz performant implementieren und den Datenraten von 5G gerecht werden?
- Wie kann man testen, ob das Equipment bei der Implementierung dem Standard entspricht und keine absichtlichen oder unabsichtlichen Fehler enthält?
- Die Forschung muss (standardisierte) Verfahren entwickeln, die Hintertüren entdeckt und verhindert.

Konfiguration

Herausforderungen

- Auslegung der komplexen Standards ist auch bei der Konfiguration nicht eindeutig und lässt viel Interpretationsraum zu.
- Den Betreibern kommt hinsichtlich der Kontroll- und Sicherungsfunktion eine stärkere Rolle als bisher zu.
- Durch die neuen Technologien muss jeder Hersteller konstant Softwareupdates installieren; die Pflege der Software erfordert die Schulung von qualifizierten Mitarbeitern).
- Im Bereich der Justiz/Strafverfolgung wird eine Einschränkung durch 5G befürchtet, da z.B. IMSI (International Mobile Subscriber Identity)-Catcher für die Polizei künftig wirkungslos wird. Diese können durch starke Funkzellen erkennen, welche Mobilfunkgeräte sich zu einem bestimmten Zeitpunkt an einem (Tat-)Ort befunden haben.

Noch offen

- Wie kann Sicherheit bei der Komplexität der Netze und Systeme bereitgestellt werden?
- Wie setzen die Betreiber spezifische Konfiguration des Netzwerkequipments um?
- Wie kann man die permanente Sicherheit eines komplexen Systems sicherstellen?
- Wie viel (IT-)Sicherheit wird von staatlicher Seite gewünscht?

Anwender

Herausforderungen

- Durch die stärkere digitale Vernetzung wird die Verwundbarkeit von Daten und Prozesse erhöht
- Die erhöhten Anforderungen an die Sicherheit der IT müssen/ können nicht nur auf Betreiberseite abgedeckt werden, sondern müssen auch in die internen Prozesse und Strukturen integriert werden

Noch offen

- Wie kann Vertraulichkeit, Integrität und Verfügbarkeit der Systeme – egal ob bei eingebetteten -oder softwarebasierten Systemen – sichergestellt werden?
- Wie kann „Security by Design" und „Privacy by Design" – die initiale Integration von Sicherheits- und Privatsspähremechanismen in den verwendeten Softwarekomponenten – sinnvoll in diesem dynamischen Umfeld umgesetzt werden?

Wie ein roter Faden spielt der **Faktor Mensch** auf allen skizzierten Ebenen eine zentrale Rolle und sollte in der Forschung dezidiert betrachtet werden. „Der Mensch" setzt die Standards, fungiert sowohl als Entwickler, IT-Integrator oder Systemadministrator der Technologien und Sicherheitsmechanismen aber auch als Nutzer in der Anwendung. Somit stellt sich grundlegend die Frage:

Wie können Sicherheitsmechanismen auf allen Ebenen der Wertschöpfungskette so gestaltet werden, dass sie für die betreffenden Personenkreise auch effektiv anwendbar sind?

Fazit

5G ermöglicht durch ein Zusammenspiel an diversen Technologien Schnelligkeit, höhere Kapazitäten und niedrige Latenzzeiten bei gleichzeitiger Senkung der Energiekosten im mobilen Internet und Telefonie. Sowohl die technische Implementierung und Konfiguration als auch die tatsächlichen Anwendungsfelder sind so spannend wie zukunftsweisend.

Der Ausbau von 5G sollte unbedingt vorangetrieben werden und ist für die technologische und wirtschaftliche Entwicklung Deutschlands hoch relevant. Dabei ist zu berücksichtigen, dass durch 5G gleichzeitig auch die Verwundbarkeit von Wirtschaft und Gesellschaft zunehmen wird – ganz unabhängig davon, welche konkreten Hersteller, Betreiber oder Anwender letztendlich involviert sein werden. Das Zusammenspiel von Standardisierung, Konfigurierung und Implementierung muss für einen sicheren Ausbau und Umsetzung von 5G sinnvoll gestaltet werden, so dass die Anwender die positiven Effekte der Technologien nutzen können.

Noch offen ist ein politischer und gesellschaftlicher Diskurs über die Frage wie viel (IT-)Sicherheit im Zusammenhang mit 5G gewünscht ist. Im Juni 2019 legten die Justizminister der Länder einen Beschlussvorschlag vor in dem sie auf die Gefährdung der Überwachungsmöglichkeiten für die Strafverfolgung in diesem Zusammenhang hinweisen (z. B. werden Einschränkungen durch End-zu-End Verschlüsselung oder Wirkungslosigkeit von IMSI-Catchern vermutet, siehe „Forschungsfragen der Zukunft"). Dies verdeutlicht, dass das Thema 5G nicht nur technisch betrachtet werden muss, sondern unbedingt durch rechts- und sozialwissenschaftliche Gesichtspunkte ergänzt werden sollte.

Aus unserer Sicht ist die Sicherheit der IT entlang der gesamten Kette ist zentrale Voraussetzung für den positiven Nutzen der neuen Schlüsseltechnologien. Aus diesem Grund ist die enge Zusammenarbeit zwischen Forschung, Industrie und Politik notwendig, um Risiken zu minimieren und Potentiale voll auszuschöpfen. An die skizzierten Forschungsfragen werden sich zahlreiche weitere essentielle Fragen anschließen. Es ist daher unbedingt notwendig, die neuen Herausforderungen in einem iterativen Prozess unter Beteiligung aller relevanten Akteure zu begleiten, der von der Forschung flankiert wird.

!

Über das HGI

Das Horst Görtz Institut für IT-Sicherheit (HGI), Research Department der Ruhr-Universität Bochum (RUB), wurde 2001 gegründet, um den europaweiten Defiziten in der IT-Sicherheitsforschung zu begegnen.

Am HGI forschen aktuell 26 Professorinnen und Professoren mit ihren Arbeitsgruppen aus der Elektro- und Informationstechnik, Mathematik und Informatik sowie den Geistes- und Gesellschaftswissenschaften. In diesem interdisziplinären Umfeld werden nahezu alle Aspekte der IT-Sicherheit abgedeckt. Mit rund 200 Wissenschaftlerinnen und Wissenschaftlern gehört es zu den europaweit größten und renommiertesten Hochschuleinrichtungen im Bereich IT-Sicherheit.

www.hgi.rub.de | www.casa.rub.de

Für weitere Informationen siehe

→ **On Security Research Towards Future Mobile Network Generations, David Rupprecht, Adrian Dabrowski, Thorsten Holz, Edgar Weippl, Chris-tina Pöpper, IEEE Communications Surveys and Tutorials, Volume: 20, Issue:3, 2018**

Haben Sie Fragen?

Ruhr-Universität Bochum | Horst Görtz Institut für IT-Sicherheit
Universitätsstrasse 150 | Raum ID 2/141 | 44780 Bochum

Friederike Schneider, M.A.
Referentin Research Department IT-Sicherheit
T (+49) (0) 234 - 32 29975 | friederike.schneider@rub.de