SOLUTION BRIEF

Schutz von 4G- und 5G-Infrastrukturen und -Diensten mit Fortinet

Zusammenfassung

Die technologische Weiterentwicklung von Mobilfunknetzen zum 4G-Standard und die Einführung von 5G eröffnen neue Zielmärkte und Einnahmequellen für die Mobilfunkbetreiber, die den Umfang und Nutzen ihres Leistungsangebots grundlegend verändern. Diese neuen Funktionen und Dienstleistungen sind für Innovationen in allen Branchen entscheidend – von der Fertigung, Energiewirtschaft und Logistik bis hin zum Transport- und Gesundheitswesen. Doch so vielversprechend die Aussichten auch sein mögen: Die Erwartungen an 5G werden sich nur erfüllen, wenn Infrastrukturen und Dienste richtig geschützt sind.

Bei digitalen Innovationen in Mobilfunknetzen kommt der Security eine Doppelrolle zu: einmal bei der internen mobilen Infrastruktur, zum anderen bei externen Anwendungsfällen und der Monetarisierung. Fortinet ist ideal positioniert, um Wirtschaft und Industrie dabei zu helfen, die Vorteile von 4G und 5G durch eine umfassende sicherheitsorientierte Netzwerk-Strategie und die richtige Unterstützung von robusten Diensten und Nutzererfahrungen zu realisieren.

Interne Security der mobilen Infrastruktur

Bei früheren Mobiltechnologie-Generationen war das Privatkundengeschäft der wichtigste Zielmarkt, in dem wenige Dienste – hauptsächlich Sprach-, Messaging- und Internet-Verbindungen – einen Mehrwert (und damit den Umsatz) generierten. Wert und Content wurden dabei größtenteils von Drittanbietern geliefert, nicht vom Mobilfunkbetreiber.

Diese Faktoren führten zu einer begrenzten Security-Implementierung für typische Angriffspunkte mobiler Infrastrukturen – wie nicht vertrauenswürdige PDNs (Public Data Networks), das RAN-Kernnetz (Radio Access Network = Funkzugangsnetz) und Roaming-Verbindungen –, um die Dienstkontinuität sicherzustellen. Da sich mobile Infrastrukturen und Technologien inzwischen weiterentwickelt haben, muss nun auch die Sicherheitsinfrastruktur nachziehen. 5G wird somit zur Nagelprobe für Mobilfunknetze, ob sich Sicherheit und ein erstklassiges Teilnehmererlebnis erfolgreich miteinander vereinbaren lassen.

Security für externe Anwendungsfälle und Monetarisierung

Durch die Einführung und Implementierung neuer Technologien in 4G- und 5G-Netzen können Mobilfunkbetreiber Mehrwertdienste anbieten, die weit über die mobile Konnektivität hinausgehen. Aus diesem Mix an Funktionen lassen sich Dienste entwickeln, mit denen Mobilfunkbetreiber neue Marktsegmente erschließen und deren sich entwickelnde Anforderungen erfüllen können.

Security als Teil einer speziellen Branchenlösung ist aus folgenden Gründen wichtig:

- Die Akzeptanz und Umsetzung von branchenspezifischen Anwendungsfällen hängt davon ab, ob der Mobilfunkbetreiber die Erfüllung der entsprechenden Service-Vereinbarungen (SLA, Security Service Level Agreements) gewährleisten kann.
- Bei Branchenlösungen stellen Mobilfunkbetreiber Mehrwertdienste bereit, die über eine reine Konnektivität hinausgehen (z. B. Anwendungen, Plattformen, Partner-Ökosysteme). Wie gut die Security für diese Komponenten funktioniert, ist ein kritischer Faktor für erfolgreich umgesetzte Anwendungsfälle.
- Transparenz und Kontrolle bei der Sicherheit eröffnen neue Einnahmequellen und Wachstumschancen durch Managed Security Services, die der Mobilfunkbetreiber Kunden anbieten kann.

Mehr innovative mobile Dienste und Anwendungsfälle – und damit auch Kunden, die diese nutzen – sind jedoch auch für Bedrohungsakteure „interessant“: Diese Anwendungsfälle können als Angriffsvektoren oder sogar Angriffsziele missbraucht werden. Mobilfunkbetreiber sollten daher auch diesen Aspekt bei ihrer grundlegenden Security-Strategie berücksichtigen.

Fortinet Security-Infrastruktur für Mobilfunkbetreiber: Innovationen schützen und Wachstum ermöglichen

Fortinet bietet umfassende Sicherheitslösungen und -Tools, die eine durchgängige Security-Transparenz und -Kontrolle für die mobile 4G- und 5G-Infrastruktur schaffen und zugleich den Schutz und die gewinnbringende Umsetzung industrieller Anwendungsfälle ermöglichen. Dieser Ansatz erleichtert nicht nur die Integration und das Onboarding, sondern minimiert zugleich den Betriebs- und

Management-Aufwand. Zu diesen Produkten und Diensten gehören die FortiGate Next Generation Firewall (NGFW) und die FortiWeb Web Application Firewall (WAF). Mobilfunkbetreiber können durch eine Kombination aus NGFW und WAF innovative Technologien, Leistungsangebote und Anwendungsfälle für Privat- und Geschäftskunden gleichermaßen sicher ausbauen.

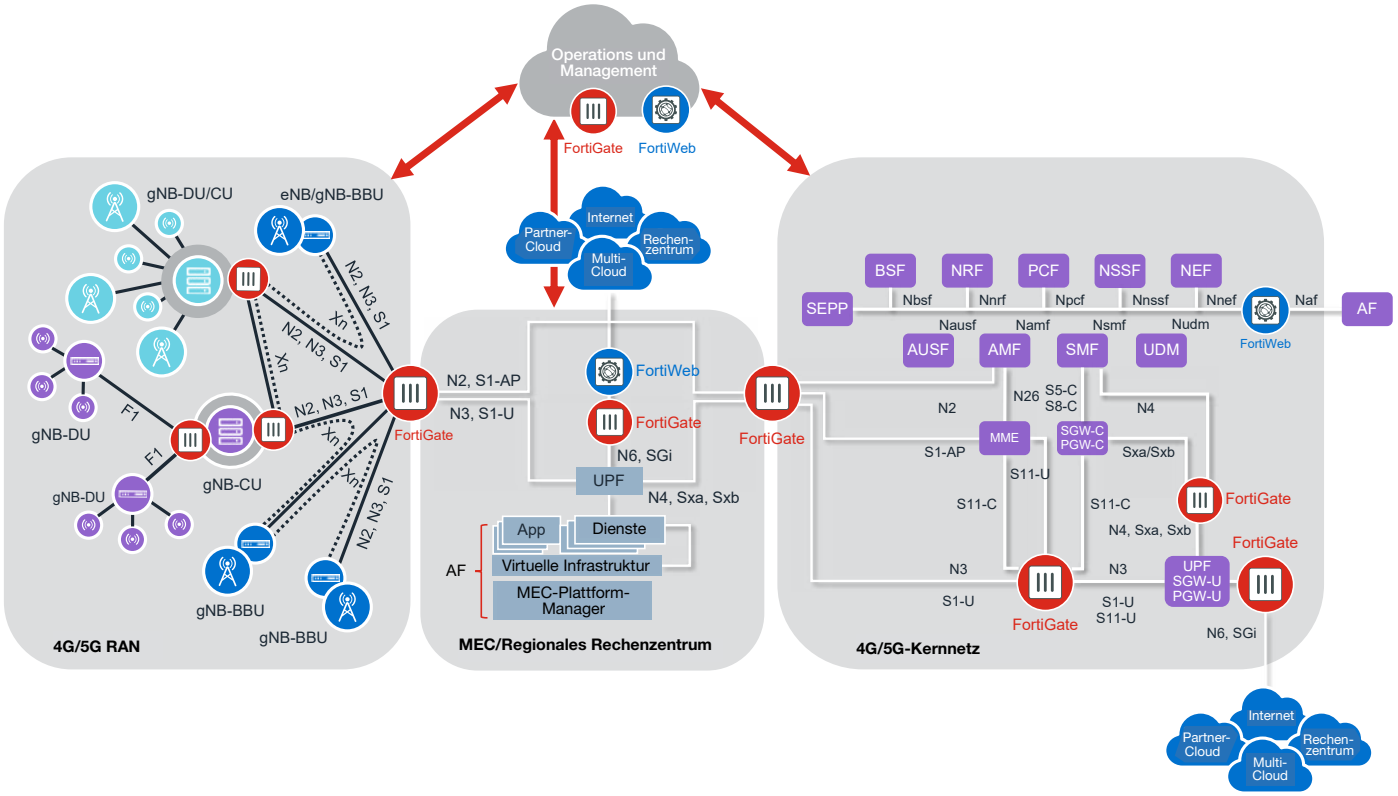

Abbildung 1: Security für das Ökosystem des Mobilfunkbetreibers

Agile, leistungsstarke interne Security für mobile Infrastrukturen und Dienste

Das folgende Diagramm zeigt die Fortinet-Lösung zum Schutz der Mobilfunkbetreiber-Infrastruktur vor Bedrohungen sowie zur Gewährleistung der Dienstverfügbarkeit und -kontinuität.

Security für Funkzugangsnetze (RAN)

Der Schutz eines vielseitigen, hybriden und hochskalierbaren 4G- und 5G-Funkzugangsnetzes ist wichtiger denn je, da sich Funktechnologien und Anwendungsfälle ständig weiterentwickeln. Für die RAN-Sicherheit ist eine neuartige Security-Gateway-Infrastruktur (SecGW) notwendig, die nicht nur agil und hybrid ist, sondern auch die gemischten Architekturen und die unterschiedlichen Anforderungen an Leistung, Skalierbarkeit und Dienstgüte (QoS) von vorhandenen LTE-A- und 5G-Netzen unterstützt. Die physischen und virtuellen Netzwerk-Funktionen (PNF/VNF) der Fortinet FortiGate bieten eine gemeinsame, flexible SecGW-Hyperscale-Plattform, die bereits weltweit bei führenden Tier-1-Mobilfunkbetreibern eingesetzt wird. Funktionalität und Leistungsstärke der FortiGate SecGW- und NGFW-Funktionalität sind in der Branche einzigartig: Mobilfunkbetreiber erhalten damit eine Plattform für das Management von RAN IPsec VPNs sowie zum Schutz von Benutzer- und Steuerungsebenen mit sicheren S1-, N2-, N3- und Xn-Schnittstellen.

Sicherheit für Multi-Access Edge Computing (MEC)

Durch die Implementierung von MEC-Standorten mit Netzwerk-, Speicher- und Computer-Ressourcen können Mobilfunkbetreiber extrem geringe Latenzzeiten für Anwendungen und Anwendungsfälle realisieren. Diese lassen sich vollständig am MEC-Standort hosten oder in einem größeren Ökosystem aus Telekommunikations- und Partner-Clouds bzw. Public Clouds implementieren. Dabei muss die Terminierung der Benutzerebenen-Daten mit lokalen Benutzerebenen-Funktionen (User Plane Function, UPF) und lokalem PDN-Breakout für die IP- und API-Konnektivität zu Anwendungen und Ökosystem-Partnern möglich sein.

Die FortiGate VNF/PNF-Plattform bietet ein Carrier-Grade-NAT (CGNAT) sowie eine NGFW für umfassende Security-Transparenz und -Kontrolle auf Layer 3 bis 7. So wird sowohl der Datenverkehr auf Steuerungs- und Benutzerebene als auch die PDN-Konnektivität beim MEC geschützt. Die FortiGate-Plattform eröffnet zudem neue Einnahmequellen durch zusätzliche Sicherheitsleistungen wie

Managed Security Services für die IoT-Security (Internet der Dinge), Application Control und Botnetz-Schutz.

Die FortiWeb-Plattform mit PNF, VNF oder CNF (Cloud-Native Network Function) bietet eine KI-gestützte Anwendungs- und API-Sicherheit für lokal gehostete MEC-Anwendungen sowie die Integration und Bereitstellung von Anwendungen und Diensten aus Partner-Clouds.

Security für Nicht-3GPP-Zugänge

Nicht-3GPP-Zugangstechnologien wie WLAN (Wireless Local Area Network) können auf verschiedene Weise mit dem 3GPP-Kernnetz wie dem EPC (Evolved Packet Core) verbunden werden, basierend auf den Geschäftsmodellen und Architekturpräferenzen des Betreibers. Bei einem ungesicherten Nicht-3GPP-Zugang stellt das Endgerät zuerst eine Verbindung zur Nicht-3GPP-Interworking-Funktion (N3IWF) und dann zur Access- und Mobility-Management-Funktion (AMF) bzw. zur UPF für den 3GPP-Zugang her.

Die FortiGate-Plattform bietet ein SCTP-Firewalling (Stream Control Transmission Protocol) für die N3IWF-N2-Steuerungsebene sowie L4-L7-NGFW-Dienste für den N3-Datenverkehr auf Benutzerebene. So wird sichergestellt, dass der nicht vertrauenswürdige Zugang auf beiden Ebenen geschützt wird.

Security für das Mobilfunk-Kernnetz

Das Mobilfunk-Kernnetz und das Funkzugangsnetz (RAN) ermöglichen gemeinsam eine breite Palette von Basis- und Zusatzdiensten für Privat- und Geschäftskunden. Diese Entwicklung sowie verschiedene technologische Neuerungen – wie die Trennung der Steuerungs- und Benutzerebenen bei 4G und 5G (Control and User Separation, CUPS), Virtualisierung, PDN-Konnektivität, Verbindungen zu Roaming-Partnern, RAN-Konnektivität, dienstbasierte Architekturen (Service-based Architecture, SBA) oder die Offenlegung von Anwendungsfunktionen – tragen dazu bei, dass das Mobilfunk-Kernnetz für Bedrohungsakteure an „Attraktivität gewinnt“.

Das Mobilfunk-Kernnetz lässt sich mit den gleichen Tools wie RAN und MEC schützen, was für Mobilfunkbetreiber einen großen Vorteil hat: Sie erhalten umfassende Transparenz und Kontrolle über die gesamte Security der mobilen Infrastruktur – von End-to-End.

Das bietet die FortiGate PNF/VNF-Plattform:

- 4G/5G PDN L4-L7 NGFW-Security- und CGNAT-Dienste mit einem Höchstmaß an Skalierbarkeit und extrem geringer Latenz bei SGi- und N6-Verbindungen
- Schutz auf Datenebene mit GTP-U-Firewalling und Deep Content Inspection auf N3 und S1-U
- Security-Gateway (SecGW) zwischen Kernnetz und Funkzugangsnetz mit massiver VPN-Skalierbarkeit und hohem Durchsatz
- Schutz der Steuerungs- und Datenebene auf Sxa/Sxb und N4

Die SBA-Funktionen von 5G verwenden API-Aufrufe über HTTP V2 für Übertragungen auf Steuerungsebene. Die FortiWeb-Plattform schützt vor Angriffen auf HTTP- und Anwendungsebene. Zudem bietet sie ein API-Schema, die Durchsetzung von API-Werten sowie API-Gateway-Funktionalitäten für die SBA-Exposure-Funktion.

Security für private 4G- und 5G-Netze

Ob Konnektivität, Dienstgüte (QoS), Security, Verfügbarkeit oder Latenz: Private Mobilfunknetze bieten notwendige Funktionen für geschäftskritische Anwendungsfälle, die sich auf individuelle Anforderungen abstimmen lassen.

Bereitstellung und Management privater Mobilfunknetze hängen von deren Architektur, Diensten, Funktionen und Komplexität sowie den Unternehmensanforderungen ab. Private Netzwerke lassen sich z. B. als vollkommen private, enggefasste Umgebungen am Unternehmensstandort (mit RAN, MEC und Kernnetz), als gemeinsame Umgebungen von Unternehmen und Mobilfunkbetreiber (RAN und Steuerungsebene werden gemeinsam genutzt) oder als End-to-End-Network-Slice bereitstellen.

Ungeachtet der Architektur und gewählten Lösung muss die Security an verschiedenen Stellen in die implementierte Architektur integriert werden, um die Dienstverfügbarkeit und Datenintegrität der Benutzerebene sicherzustellen. Die FortiGate und die FortiWeb-Plattform bieten diese gemeinsame Security-Transparenz und -Kontrolle – unabhängig von der Architektur und den Diensten des Privatnetzes, einschließlich RAN SecGW, CGNAT, L4-L7 NGFW sowie API-Schutz und Anwendungssicherheit.

Security-Anwendungsfälle für die Industrie und Monetarisierung

Die in FortiGate- und FortiWeb-Plattformen integrierten Security-Dienste eignen sich nicht nur zum Schutz der mobilen Infrastruktur, sondern auch für branchenspezifische Anwendungsfälle. So lassen sich z. B. mit maßgeschneiderten Managed Security Services neue Einnahmequellen erschließen.

Ein Beispiel dafür ist eine intelligente, vernetzte Fertigungsanlage – Stichwort „Connect Smart Factory“. Hier könnte die im MEC-Standort oder nächstgelegenen Rechenzentrum implementierte FortiGate den Schutz vor IoT-Angriffen, Signalstürmen und Fehlfunktionen mitübernehmen und gleichzeitig Security-Dienste für die Anlage selbst bereitstellen, wie einen Malware-Schutz, Botnetz-Schutz, Application Control und URL-Filter. FortiWeb ergänzt dies mit einem Schutz der Anwendungs- und API-Ebene von Industrie-Anwendungen, die im MEC-Standort gehostet werden, sowie deren Integration mit externen Anwendungen. Mit denselben FortiGate- und FortiWeb-Plattformen, die für das Funkzugangsnetz, im MEC-Standort und im Kernnetz verwendet werden, lässt sich auch das Onboarding und die Security neuer Anwendungsfälle sowie die Bereitstellung von Security-Diensten für Unternehmenskunden schnell und kosteneffizient realisieren.

Fazit

Durch die Verwendung von zwei Plattformen der Carrier-Klasse – FortiGate und FortiWeb – können Mobilfunkbetreiber mit Fortinet ihre 4G- und 5G-Infrastruktur schützen, Unternehmen eine Security für unterschiedlichste innovative Anwendungsfälle bereitstellen, Security-Dienste in private Netze einbetten und dank der Investition in eine Fortinet-Sicherheitslösung neue Einnahmequellen erschließen.

Die Verwendung gemeinsamer Security-Tools bietet Mobilfunkbetreibern entscheidende Vorteile: Sie können so bietet Mobilfunkbetreibern entscheidende Vorteile: Sie können so das gesamte Security-Onboarding sowie operative Aspekte für die mobile Infrastruktur und mobile Dienste optimieren, Kosten senken, Qualifikationslücken bei Security-Teams schließen und ihre Agilität und Fähigkeit grundlegend verbessern. So lässt sich ein Mehrwert schaffen, der das Kundenvertrauen stärkt und eine bessere Akzeptanz bei Kunden fördert.

18. Februar 2021, 20:21 Uhr

734139-0-1-DE