White Paper

Ansätze und Überlegungen zur Sicherung von 5G Netzen

verizon

Der dramatische Anstieg der Zahl der IoT-Geräte – von derzeit 31 Milliarden auf geschätzte 75 Milliarden im Jahr 2025[1] – ist einer der Gründe dafür, dass die in Unternehmen gespeicherten Datenmengen exponentiell wachsen. Im Zuge dieser Entwicklung müssen IT-Experten nicht nur höhere Netzwerkanforderungen und Gerätedichten unterstützen, sondern auch effektive Maßnahmen zur Verbesserung der Datensicherheit und -verwaltung ergreifen. Dabei gilt es zu beachten, dass 90 % aller Sicherheitsverletzungen nach Angaben des diesjährigen Data Breach Investigations Report (DBIR) von Verizon auf finanzielle Motive[2] zurückzuführen sind und dass der Umstieg auf 5G neue Sicherheitsherausforderungen mit sich bringt.

Das vorliegende White Paper wirft ein Schlaglicht auf die aktuelle Bedrohungslage und benennt die Chancen und Risiken, die sich aus der Implementierung neuartiger 5G Funknetze ergeben.

Die aktuelle Bedrohungslage

Neue Zahlen zur Netzwerksicherheit geben über die Bedrohungen Aufschluss, mit denen moderne Unternehmen während des Umstiegs auf 5G konfrontiert sind. So geht aus dem DBIR 2020 hervor, dass 45 % der im Beobachtungszeitraum registrierten Sicherheitsverletzungen auf Hackerangriffe zurückzuführen waren, während 22 % aus manuellen Bedienfehlern der Nutzer oder Fehlkonfigurationen resultierten. Dabei wurden drei Viertel der Vorfälle von externen Akteuren verursacht (55 % von kriminellen Organisationen).

Zugleich belegt der DBIR, dass die durchschnittlich zur Eindämmung akuter Sicherheitsverletzungen benötigte Zeit geschrumpft ist und in den meisten Fällen nicht mehr als wenige Tage beträgt. Trotzdem ist die von Hackern und anderen Bedrohungen ausgehende Gefahr weiterhin nicht zu unterschätzen, da sich 72 % der erfassten Angriffe gegen Großunternehmen richteten und bei mehr als der Hälfte der Opfer personenbezogene Daten erbeutet wurden. Außerdem ist festzustellen, dass Cyber-Kriminalität offensichtlich weiterhin ein einträgliches Geschäft ist, da nach Angaben des Berichts 86 % der beobachteten Vorfälle finanziell motiviert und 27 % aller Malware-Infektionen mit einer Lösegeldforderung verbunden waren.

Parallel dazu wächst die Angriffsfläche der Unternehmen, deren Infrastrukturen nun neben konventionellen Endpunkten auch immer mehr Sensoren, IoT-Geräte und M2M-Systeme umfassen. Prognosen zufolge wird die Zahl der mit IP-Netzwerken verbundenen M2M-Geräte im Jahr 2023 bei knapp 15 Milliarden liegen[3] – und somit mehr als das Dreifache der Gesamtheit der menschlichen Nutzer betragen. Das bedeutet ein wachsendes Risiko, zumal viele vernetzte Geräte mit einfachen vorkonfigurierten Passwörtern ausgeliefert werden, die für versierte Hacker leicht zu knacken sind.

5G: Einfallstor oder Bollwerk?

Bei der Analyse und Minimierung des mit der flächendeckenden Implementierung von 5G Diensten verbundenen Sicherheitsrisikos sind verschiedene wichtige Aspekte zu beachten.

Einerseits handelt es sich bei 5G nicht um einen neuartigen Angriffsvektor, sondern lediglich um eine leistungsstarke Netzwerktechnologie, die latenzarme Drahtlosverbindungen zur schnelleren und effizienteren Übertragung von IP-Traffic bereitstellt. Andererseits sind 5G Netze neben den bereits aus 4G Netzwerken bekannten Bedrohungen auch neuen Gefahren ausgesetzt, weil sie Hackern zusätzliche Möglichkeiten für schädliche Aktivitäten bieten.

Daher ist bei der Ablösung und Erweiterung kabelgebundener Netzwerke durch 5G Netze erhöhte Wachsamkeit geboten. So können beispielsweise ausgedehnte IoT-Infrastrukturen mit vielschichtigen M2M-Interaktionen und datengestützten Funktionen als Einfallstor für finanziell motivierte Cyber-Spione dienen, die zunächst eines der zahlreichen vernetzten Endgeräte infiltrieren und von dort aus in weitere Bereiche des Unternehmensnetzwerks eindringen, um wertvolle Informationen und Daten in ihren Besitz zu bringen.

Aus diesem Grund bieten 5G Netze neben den bewährten 4G Sicherheitsfunktionen weitere innovative Features zur Abwehr unbekannter Bedrohungen und zur Stärkung des Vertrauens der Nutzer.[4] Dazu zählen unter anderem:

- Lückenlose Verschlüsselung von Datenverkehr und Steuersignalen zum Schutz vor Lauschangriffen. Außerdem muss bei jedem Zugriffsversuch auf das unternehmensintern oder von einem externen Anbieter bereitgestellte Netzwerk die Identität des Teilnehmers überprüft und verifiziert werden.
- Identische Netzwerkverifizierungsmechanismen für 5G und WLAN-Verbindungen, die unautorisierte Basisstationen wie beispielsweise IMSI-Catcher enttarnen.
- Netzwerkübergreifende Authentifizierungs-Frameworks, die nicht nur eine bessere Kontrolle des internen Netzwerks ermöglichen, sondern auch die Ausspähung von Zugangsdaten erschweren.
- Secure Edge Protection Proxys (SEPP), die die Ausbreitung von in schwach gesicherten Netzwerken zirkulierenden Bedrohungen auf angebundene 5G Netze verhindern.
- Network Slicing – ein Mechanismus zur logischen Unterteilung der physischen Netzwerkinfrastruktur in verschiedene virtuelle Teilnetze, die jeweils verschiedene Funktionen bereitstellen und voneinander isoliert werden können. Bisher war eine derartige funktionelle Differenzierung nur auf der Basis separater physischer Netzwerke möglich. Doch mit 5G Network Slicing können Netzbetreiber die bereitgestellten Dienste genau auf die Anforderungen ihrer Anwendungen abstimmen und den Datenverkehr geschäftskritischer Apps in speziellen Netzwerksegmenten isolieren, um sie gegen störende Einflüsse anderer Systeme abzuschirmen.

Die erforderlichen Maßnahmen zur Sicherung von Basisstationen, Antennen und Kernnetzen sowie andere Sicherheitsstandards für 5G werden durch die Partner des 3GPP (3rd Generation Partnership Project) auf der Grundlage der Sicherheitsprotokolle von Organisationen wie der Internet Engineering Task Force (IETF) und dem National Institute of Standards and Technology (NIST) festgelegt. Mit diesen Designvorgaben sollen Schwachstellen in 5G Netzen vermieden werden.

Best Practices zur Sicherung von 5G

Starke Datensicherheit ist nur mit effektiven Abwehrmechanismen zu erreichen. Deshalb sollten Sie bei der Planung einer 5G Infrastruktur unbedingt die folgenden Gesichtspunkte berücksichtigen:

Erstens ist es empfehlenswert, ein bewährtes Cyber-Sicherheits-Framework als Grundlage für die Gestaltung der Sicherheitsarchitektur zu nutzen, um ein optimales Zusammenspiel aller Komponenten zu gewährleisten. Hier bietet sich vor allem das NIST-Framework an, das nicht nur auf gängigen Standards basiert und speziell zur Risikominimierung in kritischen Infrastrukturen wie 5G Netzen entwickelt wurde, sondern außerdem umfassende Informationen zu von außen zugänglichen Schnittstellen und unzähligen weiteren Aspekten der Netzwerkarchitektur enthält. Es liefert den Verantwortlichen in den Unternehmen eine Vorlage zur Einrichtung einer ersten Verteidigungslinie für alle Komponenten, Schnittstellen, Übergangspunkte und anderen Angriffsvektoren, über die sich Angreifer potenziell Zugriff verschaffen könnten.

Zweitens sollten Sie unbedingt flächendeckend Verschlüsselungsmechanismen implementieren. Denn auch wenn 5G die lückenlose Verschlüsselung der Steuersignale und des nutzerspezifischen Datenverkehrs unterstützt, muss dieses Feature doch eigens eingerichtet und aktiviert werden. Nur durch entsprechende Konfigurationseinstellungen können Sie dafür sorgen, dass sowohl der Nutzkanal als auch die Signalisierung standardmäßig verschlüsselt sind. Begleitend sollten Sie flächendeckend das Zero-Trust-Prinzip implementieren, das jede einzelne Transaktion erst nach vorheriger Authentifizierung gestattet – und zwar unabhängig davon, ob es sich um Daten- oder Voice-Übertragungen beziehungsweise um vertrauliche oder weniger sensible Informationen handelt. Die Sicherheit wird also gestärkt, indem der klassische Perimeterschutz durch ein System abgelöst wird, das jeden Vorgang und jeden Benutzer als potenziell verdächtig einstuft und überprüft. Damit wird Zero Trust den komplexen Architekturen moderner Netzwerke eher gerecht als ein auf scharfen Vertrauensgrenzen basierender Ansatz.

Drittens ist neben der Einhaltung der einschlägigen Standards auch eine detaillierte Prüfung der 5G Lieferkette nötig. Zum einen sollte die 5G Hardware – bis hinunter zu den einzelnen Chips – nur von vertrauenswürdigen Herstellern bezogen werden, deren Produkte nachweislich keine Backdoor-Zugriffsmechanismen aufweisen. Zum anderen müssen die Verantwortlichen sicher sein können, dass ihre 5G Firmware und Software strengsten Sicherheitsanforderungen genügt und beispielsweise keine Malware aus Code-Repositorys auf die eigenen Geräte herunterlädt oder in das Kernnetz des gewählten Anbieters einschleust.

Abgesehen davon sollte sich jedes verantwortungsbewusste Unternehmen an den Branchenführern orientieren und die folgenden Best Practices umsetzen:

Aufgabentrennung: Durch diese einfache Maßnahme lässt sich verhindern, dass eine einzelne Person sämtliche Sicherheitsprozesse außer Kraft setzen kann.

Rollenbasierte Zugangskontrollen: Der Zugriff auf Daten und Ressourcen sollte durch die Definition von Nutzerrollen auf befugte Mitarbeiter und Anwendungen beschränkt werden.

Minimierung der Zugriffsrechte: Jeder Nutzer sollte nur die Zugangsberechtigungen besitzen, die für die Erledigung seiner Arbeitsaufgaben erforderlich sind.

Multifaktor-Authentifizierung: Wo immer dies möglich ist, sollten Remote-Anmeldeprozesse durch zwei oder mehr Authentifizierungsverfahren abgesichert werden.

Modernisierungsmaßnahmen: Veraltende, nicht vom eigenen Unternehmen verwaltete Netzwerkressourcen benötigen möglicherweise ein Upgrade. Denn unzureichend gesicherte Altgeräte oder Sensoren erweisen sich in einer ansonsten gut geschützten Netzwerkinfrastruktur als attraktive Einfallstore.

Governance: Angesichts der wachsenden Zahl vernetzter medizinischer Geräte und anderer Wearables ist davon auszugehen, dass künftig auch 5G Netze für die Einhaltung von gesetzlichen Vorgaben und Branchenstandards wie HIPAA und PCI ausgelegt werden müssen. Deshalb können die Unternehmen nur durch eine enge Zusammenarbeit mit ihren Hardware-, Software- und Netzwerkanbietern sicherstellen, dass ihre Netzwerkkomponenten nicht zum schwachen Glied in ihrer Sicherheitskette werden.

Kompetente Unterstützung von Verizon

Als einer der Wegbereiter von 5G bietet Verizon vielfältige Lösungen an, die modernen Unternehmen jeder Branche und Größe den Umstieg auf 5G Netze erleichtern. Dabei kommt unseren Experten ihre Erfahrung beim Aufbau sicherer 5G Infrastrukturen unter Einhaltung von Compliance-Vorgaben wie PCI und HIPAA in unseren eigenen über 2000 US-amerikanischen Ladengeschäften zugute. Dieser reiche Erfahrungsschatz erweist sich bei der Weiterentwicklung unseres weltweiten Dienstleistungs- und Produktangebots als äußerst nützlich.

Außerdem fließt unsere geballte Expertise in den Aufbau eines ganz auf Sicherheit ausgerichteten 5G Partnernetzwerks ein. Denn um neben unserer Produktpalette auch unsere physischen und digitalen Lieferketten rigoros abzusichern, unterziehen wir jeden Anbieter und jedes Produkt einem strengen Auswahlprozess, bei dem nicht nur die Eignung für einen bestimmten Zweck, sondern auch native Sicherheitskontrollen geprüft werden. Dadurch können wir unter anderem sicherstellen, dass von uns bereitgestellte Updates und Patches sicher, effektiv und frei von Schwachstellen sind.

Parallel dazu leisten wir in verschiedenen branchenübergreifenden Kooperationen und Sicherheitsorganisationen richtungsweisende Grundlagenarbeit: Zum einen zählt Verizon zu den Gründungsmitgliedern des Council to Secure the Digital Economy und der O-RAN Alliance und ist damit gleich an zwei Gremien beteiligt, die bei der Koordination der weltweiten Anstrengungen zur Sicherung des IoT und zur flächendeckenden Einführung von auf offenen Standards basierenden virtuellen 5G Basisstationen und Antennen eine führende Rolle spielen. Zum anderen kooperieren wir mit dem Communications Information Sharing and Analysis Center (Communications ISAC)4 des U.S. Department of Homeland Security, um gemeinsam mit anderen Mobilfunkanbietern und der US-Regierung zum Schutz der nationalen Kommunikationsinfrastrukturen und -dienste beizutragen.

So ist es zu erklären, dass die von Verizon propagierte Sicherheitsarchitektur sowohl auf den 3PGG-Standards als auch auf Empfehlungen der IETF und des NIST basiert und beispielsweise Mechanismen zur wechselseitigen Authentifizierung von Endgeräten und Basisstationen, zur Abwehr von Lauschangriffen und zur Vereitelung des Diebstahls von Anmeldedaten umfasst.

Zusätzlich müssen die Smartphones und sonstigen 5G Appliances aus unserem Sortiment unseren eigenen strengen Sicherheitsanforderungen und -prozessen genügen, die unter anderem die Verwendung einer speziell gegen den Diebstahl von Authentifizierungs- und Zugangsdaten gesicherten UMTS-SIM-Karte4 vorschreiben.

Um dies sicherzustellen und jedes neu eingerichtete 5G Netz optimal zu schützen, setzen wir automatisierte Testpipelines und standardisierte Konfigurationen für alle Netzwerkgeräte, Telefone und Router ein. Auf diese Weise sorgen wir dafür, dass jede Komponente sowohl den gängigen Branchenstandards als auch unseren internen Anforderungen an 5G Geräte entspricht.

Ergänzend bieten wir zukunftsweisende 5G Dienste an, die auf einer neuen softwaredefinierten Architektur basieren und Kundenunternehmen dadurch in die Lage versetzen, den Traffic verschiedener Anwendungen in unterschiedlichen Netzwerksegmenten zu isolieren – ähnlich wie in VPN-Infrastrukturen, jedoch mit einfacheren Mechanismen zur Einrichtung und Ressourcenzuweisung. Das ermöglicht unter anderem den Schutz geschäftskritischer Systeme, wenn diese zum Ziel von DDoS-Angriffen über unzureichend gesicherte IoT-Geräte werden.

Kurz: Wir von Verizon verfügen über jahrzehntelange Erfahrung im Bereich Netzwerkmanagement und lassen die Erkenntnisse aus unseren bisherigen Einsätzen in die Bereitstellung zukunftsweisender 5G Netze und Geräte einfließen. Mit unseren Tools, Produkten und Fachleuten unterstützen wir unsere Partner und Endkunden bei der Analyse und Modernisierung ihrer Sicherheitsmaßnahmen im Zuge des Umstiegs auf 5G.

Nächste Schritte

Als Anbieter des ersten kommerziellen 5G Dienstes ist Verizon bestens aufgestellt, um Ihrem Unternehmen zu einer sicheren 5G Infrastruktur zu verhelfen. Wenn Sie mehr über die starken Schutzfunktionen von Verizon 5G erfahren möchten, wenden Sie sich bitte an Ihren Business Account Manager.

verizon

1 „The Future of IoT Miniguide: The Burgeoning IoT Market Continues“, Cisco, 19. Juli 2019.

2 „Data Breach Investigations Report 2020“, Verizon, 2020.

3 „Cisco Annual Internet Report (2018–2023)“, Cisco, 9. März 2020.

4 „First Principles for Securing 5G“, Verizon, Dezember 2019.