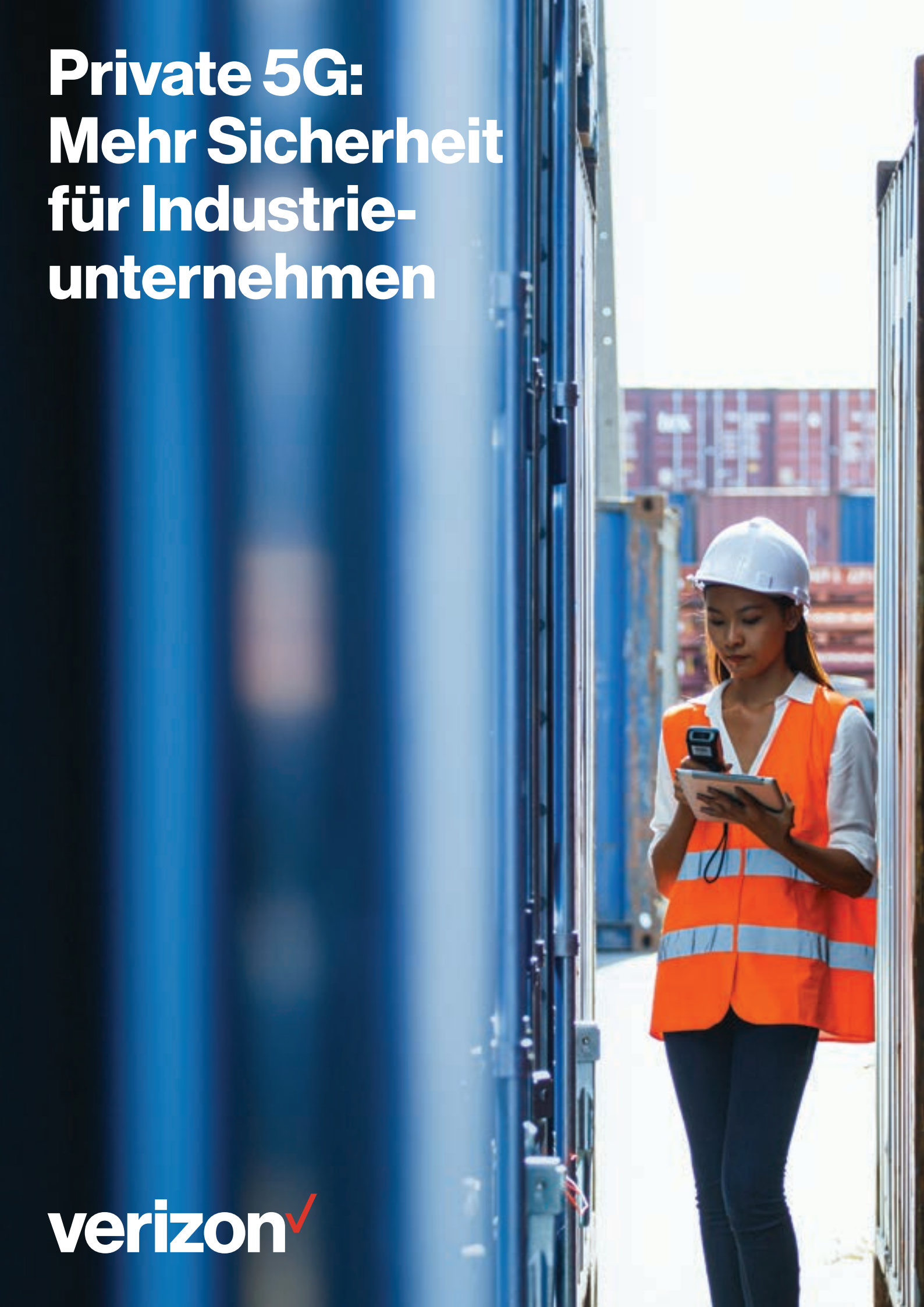
Private 5G: Mehr Sicherheit für Industrie-unternehmen



verizon

Inhalt

Warum Sie dieses Whitepaper lesen sollten

5G hat den Schritt von der aufkommenden zur einsatzbereiten Technologie schnell genommen und viele Unternehmen profitieren bereits von privaten 5G Netzwerken. Zukunftsorientierte Firmen – insbesondere in der Fertigung und anderen industriellen Branchen – entwickeln schon seit einigen Jahren Anwendungsszenarien, die ihren Betrieb gründlich modernisieren sollen. Jetzt tragen diese Anstrengungen Früchte – in Werkhallen, Labors und im Außendienst. Das Versprechen einer „vierten industriellen Revolution" wird zur Wirklichkeit.

Doch wie immer gibt die Sicherheit Grund zur Sorge.

Bei der Entwicklung von 5G wurde zwar auf stärkere Sicherheitsvorkehrungen zum besseren Schutz sensibler Daten und Systeme geachtet, doch die Technologie allein reicht nicht aus, um tief sitzende Lücken im Sicherheitsprogramm eines Unternehmens zu schließen, die es möglicherweise schon seit längerer Zeit gibt. Wenn es dem Sicherheitsteam eines Unternehmens bisher schwer gefallen ist, Technologien wie Clouds, Mobilgeräte und das industrielle Internet der Dinge (IIoT) unter Kontrolle zu bekommen, nachdem sie auf Betreiben der Geschäftsbereiche schnellstmöglich eingesetzt wurden, wird das bei 5G wohl nicht anders sein.

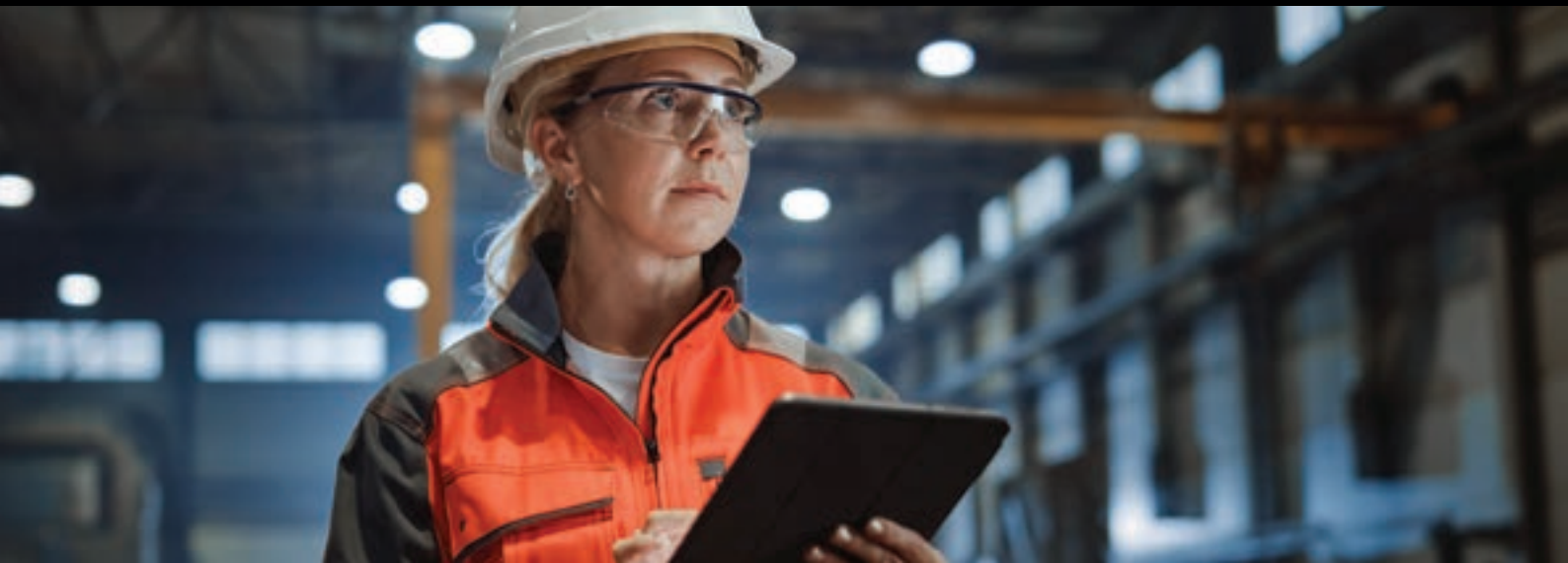
Das soll jedoch nicht heißen, dass es unmöglich ist, mit 5G für stärkere Sicherheit zu sorgen – im Gegenteil.

Das NIST CSF (National Institute of Standard and Technology Cybersecurity Framework) des US-amerikanischen Department of Commerce enthält Empfehlungen und Anleitungen für Unternehmen, die die Sicherheit ihrer gesamten IT-Infrastruktur stärken und die Risiken mindern können, die mit bestimmten 5G Anwendungsszenarien einhergehen. Dieses Framework gilt als globaler Standard, an dem sich die Verfasser anderer Standards, wie ISO 27110, orientieren.

Dieses Whitepaper:
- beschreibt die Unterschiede zwischen öffentlichen und privaten 5G Netzwerken
- untersucht die Nutzung von Private 5G in Industriebetrieben – und die Sicherheitsaspekte, die dabei berücksichtigt werden müssen
- beschreibt, wie das NIST CSF zur Stärkung der Sicherheit beitragen kann, wenn Unternehmen 5G und Industrie 4.0 nutzen

Sicherheits-, IT- und Netzwerkteams müssen miteinander und mit Managern aus IT-fremden Geschäftsbereichen zusammenarbeiten, um sicher und im vollen Umfang von den Vorteilen von 5G zu profitieren.

Mit diesem Whitepaper möchten wir ihnen einen gemeinsamen Referenzrahmen für diese Kollaboration anbieten.



Ein schönes Problem: Viel Auswahl für moderne Konnektivität

In vielen Branchen – darunter Fertigung, Logistik, Bergbau und Energieerzeugung – werden durch die Eigenschaften und Kapazitäten modernster Netzwerke Anwendungsfälle möglich, die alle Aspekte des Geschäftsbetriebs modernisieren.

Machine-to-Machine-Kommunikation macht etablierte Betriebsprozeduren hinfällig und das IIoT generiert riesige Datenmengen, die sich in bares Geld ummünzen lassen, wenn sie in Echtzeit analysiert werden. Auch neu aufkommende Anwendungsfälle wie autonom-gesteuerte Fahrzeuge (Autonomous Guided Vehicles, AGV), die zeitkritische WLAN-Verbindungen benötigen, oder vernetzte Videokameras, Augmented/Virtual Reality und andere Anwendungen mit großem Bandbreitebedarf erfordern ein solides Netzwerk als Basis.

Doch welche Netzwerktechnologie ist am besten geeignet, um diese Basis bereitzustellen und die spezifischen Anforderungen Ihres Unternehmens zu erfüllen? Ein privates 5G Netz? Ein öffentliches 5G Netz? WLAN 5 oder WLAN 6?

Und welche Sicherheitsaspekte müssen dabei jeweils berücksichtigt werden?

5G und WLAN im Vergleich

Die Nutzung von 5G für kritische Netzwerke hat, insbesondere für große Industrieunternehmen, eine Reihe von Vorteilen, mit denen WLAN 6 und andere nicht mobilfunkbasierte Technologien nicht aufwarten können. Beide Technologien werden derzeit mit Hochdruck weiterentwickelt, um neue Anwendungsbereiche und Anforderungen rund um Industrie 4.0 zu unterstützen.

5G stellt in vielerlei Hinsicht einen großen Fortschritt dar, beispielsweise bezüglich der Durchsatzsteigerung, Servicebereitstellung, Latenzverkürzung, Zuverlässigkeit und der Fähigkeit, mit großen Datenvolumen fertig zu werden. 5G ist eine verbesserte Weiterentwicklung der Mobilfunktechnologie 4G. Unter anderem veröffentlichte das Standardisierungsgremium 3GPP (3rd Generation Partnership Project) Hinweise zu Best Practices für die Sicherheit für 5G Anbieter. Das heißt, dass 5G Netzwerke, dank der Authentifizierung und Autorisierung von Nutzergeräten, einer lückenlosen Verschlüsselung, diverser Datenschutzfunktionen, einer Zero-Trust-Architektur und anderer von Anfang an integrierter Sicherheitsfeatures von Haus aus sicher sind. Dadurch ist mit 5G eine nativ sichere Netzwerkkommunikation möglich.

Darüber hinaus nutzt 5G lizenzierte Frequenzbereiche, wodurch die Interferenz mit anderen drahtlosen Geräten reduziert und das Network-Slicing (und damit eine bessere Servicequalität) möglich werden. Zudem bietet 5G mehr Flexibilität für die Servicebereitstellung, da es eine Reihe cloudbasierter Technologien nutzt und von Haus aus stark auf Virtualisierung basiert. Infolgedessen kann 5G Mobile Edge Computing (und somit unter anderem kosteneffiziente Methoden zur Latenzverkürzung) unterstützen. Außerdem unterstützt 5G standortunabhängigen Zugriff, flexible Roadmaps und sowohl WAN- als auch LAN-Technologie.

Im Gegensatz dazu nutzt WLAN 6 nur nicht lizenzierte Frequenzbereiche. In Umgebungen mit zahlreichen drahtlosen Geräten gibt es daher oft Interferenzprobleme, die sich nur schwer beheben oder vermeiden lassen. Da WLAN hauptsächlich in Heim- und Büro-LANs eingesetzt wird, wurden die meisten WLAN-Geräte für diese Art von Umgebung entwickelt. Als Mobilfunktechnologie ist 5G hingegen für mobile und ortsgebundene, Außen- und Innenbereiche geeignet.

Trotz dieser Nachteile wird WLAN in Verbraucher- und Büro-LANs voraussichtlich weiterhin eine wichtige Rolle spielen, insbesondere da WLAN 6 einige Verbesserungen gegenüber WLAN 5 aufweist, zum Beispiel bessere Werte für die Spitzenlast, Latenz, Gerätedichte und Energieeffizienz.

Die Authentifizierung und Autorisierung von Nutzergeräten, eine lückenlose Verschlüsselung, diverse Datenschutzfunktionen, eine Zero-Trust-Architektur und andere Features stärken die Sicherheit, sodass mit 5G eine nativ sichere Netzwerkkommunikation möglich ist.

5G – aber wie: öffentlich oder privat?

Bei Mobilfunktechnologien gibt es zwei Optionen: öffentlich oder privat. Ein Merkmal privater Netzwerke ist, dass sie oft für sehr spezifische, auf einen Ort beschränkte Anwendungsszenarien eingerichtet werden, deren Anforderungen sich von denen eines Verbrauchernetzwerks unterscheiden. Beispiele hierfür sind die Verwaltung von Produktionslinien oder autonom-gesteuerte Fahrzeuge (AGVs).

Private 5G nutzt zwar die gleiche Technologie, bietet aber ein Netzwerk, das ausschließlich dem Kunden zur Verfügung steht und dessen Bandbreite dem Bedarf des Unternehmens entspricht. Dieser Kunde hat auch mehr Kontrolle über seine Daten und sein Netzwerk, da die Daten nicht mit externen Nutzern geteilt werden können. Aufgrund dieser Eigenschaften eignen sich private 5G Netzwerke für IoT-Geräte wie Sensoren oder Kameras, die fest auf einem Firmengelände installiert sind und keine Roaming-Funktion benötigen.

Private 5G Netzwerke bieten sich auch an, wo es Sicherheitsbedenken gibt. Sie sind zwar denselben Cyber-Bedrohungen ausgesetzt wie öffentliche 5G Netzwerke, doch die Tatsache, dass sie nur in einem begrenzten Gebiet genutzt werden, das von einem Unternehmen kontrolliert und geschützt wird, wirkt wie eine zusätzliche Sicherheitsebene. Um beispielsweise einen Signal-Jamming-Angriff durchzuführen, müsste sich der Angreifer auf dem Unternehmensgelände befinden. Er müsste sich also am Sicherheitspersonal vorbeimogeln und dann unbemerkt bleiben. Sie sollten jedoch nicht vergessen, dass eine mehrschichtige Sicherheitsinfrastruktur aus physischen und logischen Ebenen besteht.

Hauptmerkmale der verschiedenen 5G Netzwerkarten

Öffentliche Netzwerke ...

- nutzen die Expertise und Lösungen eines Mobilfunkbetreibers und ein breites Frequenzspektrum.
- werden von einem öffentlichen Netzwerk aus bereitgestellt, mit dem sie kompatibel sind.
- erfordern Verbesserungen hinsichtlich der Servicequalität, wenn der Datenverkehr von und zu kritischen Geräten und Anwendungen bevorzugt behandelt werden soll.
- unterstützen das Edge Computing im öffentlichen Netzwerk mit der Option eines Gateways vor Ort, das für kürzere Latenzzeiten und lokale Datenspeicherung und -verarbeitung sorgt.

Private Netzwerke ...

- sind dedizierte Netzwerke, in denen ein hohes Datensicherheits- und Datenschutzniveau erreicht werden kann.
- sind nicht mit dem öffentlichen Mobilfunknetz verbunden.
- bieten dem Kunden volle Kontrolle über das Design, die Termine für die Bereitstellung und den Betrieb.
- bieten dem Kunden volle Kontrolle über die SLAs.
- unterstützen das Edge Computing für kürzere Latenzzeiten und lokale Datenspeicherung und -verarbeitung.
- können vom Kunden selbst oder von Outsourcing-Partnern entworfen, eingerichtet und verwaltet werden.
- übertragen dem Kunden die Verantwortung für den Erwerb und die Nutzung eines Frequenzspektrums.

Bearbeitete Wiedergabe von: https://www.gsma.com/iot/wp-content/uploads/2020/10/2020-10-GSMA-5G-IoT-Private-and-Dedicated-Networks-for-Industry-4.0.pdf

verizon

5G und die wichtigsten Sicherheitsaspekte in der Industrie

In Unternehmen mit komplexen, geschäftskritischen Umgebungen, die stark auf ICS (industrielle Steuerungssysteme) und OT (Operational Technology) angewiesen sind, sollte die Nutzung von Private 5G erwogen werden. In einer vollen Fabrikhalle oder einem weitläufigen Hafengelände könnte die Konnektivität beispielsweise sehr leicht unter Interferenz leiden, wenn sie durch physische Strukturen oder andere drahtlos übertragene Signale gestört wird. Private Netzwerke eignen sich in diesen Situationen besonders gut, da sie zuverlässige, vorhersehbare Geschwindigkeiten und niedrige Latenz bieten und so das Risiko einer Verbindungsunterbrechung minimieren.

Wie jeder Sicherheitsprofi weiß, gehört die Verfügbarkeit (ebenso wie die System- und Datenintegrität und der Schutz vertraulicher Daten) zu den wichtigsten Zielen der Cyber-Sicherheit.

Eine riesige, 5G-fähige IoT-Umgebung benötigt ein Sicherheitsprogramm, das mit der Anzahl der Geräte skalierbar ist, ihre Schwachstellen unter Kontrolle behält und für die sichere Übertragung der Daten zu den Analyseplattformen sorgt. Ein kontinuierliches Monitoring der IoT-Geräte mit Funktionen zur umgehenden Angriffserkennung und -abwehr sind unverzichtbar. In der jüngeren Vergangenheit haben groß angelegte DDoS-Angriffe, bei denen gekaperte IoT-Geräte missbraucht wurden, wiederholt Schlagzeilen gemacht. Cyber-Angriffe auf 5G-basierte Anwendungen (wie Malware- und Ransomware-Angriffe) können Produktionsprozesse in der Fertigung erheblich stören und so den Kundendienst und den Umsatz gefährden. In manchen Fällen können auch Vertragsstrafen, Sanktionen durch Regulierungsbehörden und Reputationsverlust zu den Konsequenzen gehören. Wenn Daten bei der Übertragung nicht ausreichend geschützt sind, kann dies dem Diebstahl geistigen Eigentums und vertraulicher Kundendaten Vorschub leisten.

In einigen Anwendungsbereichen sind sogar Menschenleben in Gefahr, wenn der Sicherheit beim Entwurf und der Umsetzung nicht genug Aufmerksamkeit gezollt wird. Ein oft genanntes Beispiel ist ein 5G-fähiges autonomes Fahrzeug: Wer möchte als Passagier in einem selbstfahrenden Auto sitzen, dass nicht umfassend vor Cyber-Autoentführern geschützt ist?

Auch Angriffe auf kritische Infrastrukturen wie Kraftwerke und Wasseraufbereitungsanlagen können katastrophale Folgen haben. Das ist keine bloße Panikmache – solche Angriffe hat es bereits gegeben. Im Jahr 2014 wurde ein Hochofen eines deutschen Stahlwerks bei einem Cyber-Angriff stark beschädigt.[1] Und Anfang 2021 versuchten Hacker, in das industrielle Steuerungssystem der Grundwasseraufbereitungsanlage einer Stadt in Florida einzudringen, um das Trinkwasser zu vergiften.[2]

Wie NIST CSF zum Schutz Ihres privaten 5G Netzwerks beitragen kann

NIST CSF bietet einen bewährten Ansatz für die Entwicklung von Cyber-Sicherheitsprogrammen, mit denen sich die inhärenten Risiken der Netzwerknutzung erheblich reduzieren lassen. Dieser Ansatz ist auch auf private 5G Netzwerke und die Apps anwendbar, die durch diese Netzwerke möglich werden. Im NIST CSF werden fünf Kapazitäten hervorgehoben, die sich Unternehmen unbedingt aneignen sollten:

Identifizieren
Sie müssen wissen, welche internen und externen Bedrohungen für ihre Anlagegüter und ihr Unternehmen relevant sind.

Schützen
Sie müssen kritische Infrastrukturen, Anlagegüter und Daten in allen Umgebungen schützen, von der Cloud über Mobilgeräte bis zum IoT.

Erkennen
Sie müssen infizierte Systeme und Daten schneller und besser erkennen.

Reagieren
Sie müssen einen Plan für die schnelle und effektive Reaktion auf Sicherheitsverstöße entwickeln und fortlaufend aktualisieren.

Wiederherstellen
Sie müssen ihre Infrastrukturen robust gestalten, um die Systemverfügbarkeit zu maximieren und teure Geschäftsstörungen auf ein Minimum zu reduzieren.

[1] https://www.heise.de/security/meldung/BSI-Sicherheitsbericht-Erfolgreiche-Cyber-Attacke-auf-deutsches-Stahlwerk-2498990.html
[2] https://www.heise.de/news/Hackerangriff-auf-das-Trinkwasser-5049266.html

Das branchenweite Framework umfasst drei Hauptkomponenten:

Framework-Kern | Implementationsstufen | Profile

Der Kern besteht aus drei Teilen:

Funktionen | Kategorien | Unterkategorien

und fünf Hauptfunktionen:

Identifizieren | Schützen | Erkennen | Reagieren | Wiederherstellen

Die Hauptfunktionen sind wie folgt in 23 Kategorien aufgeteilt:

Funktion	Kategorie
Identifizieren	Ressourcenverwaltung Geschäftsumfeld Governance Risikobewertung Risikomanagementstrategie Risikomanagement für die Lieferkette
Schützen	Identitätsmanagement und Zugangskontrollen Sensibilisierung und Weiterbildung Datensicherheit Datenschutzprozesse und -prozeduren Wartung Schutztechnologie
Erkennen	Anomalien und Ereignisse Ununterbrochenes Sicherheitsmonitoring Erkennungsprozesse
Reagieren	Reaktionsplanung Kommunikation Schadensbegrenzung Verbesserungen
Wiederherstellen	Planung der Wiederherstellung Verbesserungen Kommunikation

[1] https://www.heise.de/security/meldung/BSI-Sicherheitsbericht-Erfolgreiche-Cyber-Attacke-auf-deutsches-Stahlwerk-2498990.html
[2] https://www.heise.de/news/Hackerangriff-auf-das-Trinkwasser-5049266.html

NIST CSF im Detail

Identifizieren

Als Ausgangsbasis zur Entwicklung eines Sicherheitsprogramms sollten Sie sämtliche Geräte in Ihrem Unternehmensnetzwerk identifizieren und ermitteln, welche Daten auf jedem dieser Geräte gespeichert sind. Schließlich können Sie nur die Anlagewerte schützen, deren Existenz Ihnen bekannt ist. Im Rahmen dieser Übung sollten Sie auch Ihre „Kronjuwelen" identifizieren, also die Ressourcen, ohne die Ihr Geschäftsbetrieb schwer beeinträchtigt oder unmöglich wäre und die daher auf keinen Fall kompromittiert werden oder ausfallen dürfen.

Kurz gesagt sollten Sie sich einen umfassenden Überblick über Ihre Infrastruktur verschaffen. Um zu ermitteln, welche Auswirkungen das Hinzufügen eines privaten 5G Netzwerks auf Ihr bereits bestehendes Unternehmensnetzwerk hätte, müssen Sie zudem wissen, was genau Sie hinzufügen. Neben dem privaten 5G Netzwerk und dessen Hardware- und Softwarekomponenten werden Sie vermutlich einige weitere Elemente installieren müssen, um die anvisierten Anwendungsszenarien der neuen Technologie zu unterstützen.

Außerdem sollten Sie sich unbedingt im Klaren darüber sein, wo die erfassten und verarbeiteten Daten gespeichert und für den zukünftigen Zugriff bereitgestellt werden sollen. Darüber hinaus benötigen Sie eine nach Priorität geordnete Liste der Anwendungsszenarien. Bei der Priorisierung der Anwendungsfälle sollten Sie sowohl deren potenziellen Beitrag zum Unternehmenserfolg als auch die jeweils erforderliche Kombination aus Technologie und Daten berücksichtigen.

Die andere Schlüsselaufgabe in diesem Schritt ist das Ermitteln des Risikoprofils Ihres Unternehmens. Moderne Unternehmen bestehen möglicherweise aus mehreren Geschäftsbereichen mit unterschiedlichen Arbeitsweisen. Viele haben zudem Tochterfirmen in anderen Branchen. All das verkompliziert das Erstellen eines Sicherheitsprogramms, da Daten zu verschiedenen Netzwerken erfasst und in den richtigen Kontext gesetzt werden müssen, um das jeweilige Risikoprofil zu ermitteln.

Wir haben bereits einige Punkte erwähnt, die bei der Risikobewertung für ein geplantes privates 5G Netzwerk berücksichtigt werden sollten, insbesondere bei Anwendungsszenarien in Industriebetrieben. Zudem müssen die auf proprietärer Technologie basierenden, von spezialisierten IT- und OT-Anbietern bereitgestellten Prozesse und ihre Auswirkungen auf die Wiederherstellung nach einem Vorfall in das Risikoprofil des Unternehmens aufgenommen werden.

Dasselbe gilt für die älteren proprietären Technologien, die in vielen Unternehmen noch immer genutzt werden und aus Sicherheitsgründen in einem eigenen privaten Netzwerk isoliert sind. Viele typische Anwendungsszenarien für Private 5G erfordern jedoch Zugang zu öffentlichen Clouds.

Die resultierenden Änderungen an der Netzwerkarchitektur wirken sich auf das Risikoprofil des Unternehmens aus und müssen daher sorgfältig geplant werden. Zudem müssen die aktuell vorhandenen Sicherheitstechnologien und -prozesse regelmäßig katalogisiert und bewertet werden, um etwaige Lücken zeitnah aufzudecken und zu schließen. Es muss auch festgelegt werden, welcher Mitarbeiter welche Sicherheitsfreigaben hat. Dies geschieht in der Regel bei jährlichen unabhängigen Beurteilungen. Das gemeinsame Ziel all dieser Aktivitäten sollte das angestrebte Sicherheitsniveau des Unternehmens (einschließlich des anvisierten Maßes an Risikominimierung, Compliance und Datenschutz) sein.

Schützen

Sicherheitstechnologien sind die Basis jedes Sicherheitsprogramms. Die Konfiguration dieser Technologien muss mit der Unternehmensstruktur Schritt halten. Für ein modernes, hybrides Unternehmensnetzwerk mit virtualisierten Komponenten, On-Premises- und Cloud-Umgebungen, Software-as-a-Service-Anwendungen und einer steigenden Anzahl mobiler Nutzer ist ein nur auf den Netzwerkrand fixierter Sicherheitsansatz ebenso überholt wie eine Burg mit Burggraben.

Die Sicherheitsvorkehrungen müssen dem Netzwerkmodell entsprechen. Die von Haus aus in 5G Netzwerke integrierten Sicherheitsmaßnahmen, wie die Verschlüsselung und die eingebauten Zero-Trust-Prinzipien, bieten ein hohes Maß an Schutz. Nutzer sollten sich daher auf den Schutz der verschiedenen Elemente der auf 5G Netzwerke aufbauenden Anwendungsfälle konzentrieren.

Dafür kommen mehrere Technologien infrage. Durch Network-Slicing können Sie beispielsweise die Netzwerkkapazitäten für verschiedene Anwendungsfälle und deren Daten voneinander und vom restlichen Datenverkehr im Netzwerk trennen und damit eine zusätzliche Sicherheitsebene einfügen.

Ein weiterer wichtiger Aspekt ist der Endpunktschutz. Während Laptops, Mobilgeräte und ähnliche Endpunkte Sicherheitssensoren unterstützen, erfordert der Schutz von IoT-Geräten spezielle, auf ihre jeweilige Größe und Kapazität abgestimmte Technologien.

Auch die Anwendungen und die Datenverarbeitung in 5G Anwendungsszenarien müssen geschützt werden. Wie und in welchem Umfang das geschieht, hängt von der genutzten Technologie, den darin integrierten Sicherheitsmaßnahmen und davon ab, ob öffentliche Clouds genutzt werden und welche Risiken das mit sich bringt. Angesichts der steigenden Raffinesse und Vielfalt der Cyber-Angriffe und Cyber-Angreifer – und der Notwendigkeit, die „Kronjuwelen“ des Unternehmens zu schützen – ist und bleibt Zero Trust unverzichtbar für die Umsetzung der Funktion „Schützen“ des NIST CSF.

Abschließend soll erwähnt werden, dass Unternehmen ihre Mitarbeiter mit Schulungs- und Sensibilisierungsmaßnahmen über alle neuen Bedrohungen, Technologien und Prozesse informieren sollten, die für sie relevant werden könnten. Dies ist umso wichtiger, da die Mitarbeiter zunehmend als „vorderste Verteidigungslinie“ ihres Unternehmens betrachtet werden.

Erkennen

Das Mantra der Cyber-Sicherheit ist heutzutage: „Die Frage lautet nicht, ob Sie angegriffen werden, sondern, wann.“. Wenn das geschieht, kommt es auf jede Sekunde an. Doch aus dem Data Breach Investigations Report 2021 von Verizon geht hervor, dass fast 20 Prozent der Angreifer monatelang oder sogar noch länger unbemerkt bleiben, nachdem sie sich Zugang zur anvisierten Umgebung verschafft haben.

Angesichts der weiter oben erwähnten Risiken für Unternehmen (bis hin zur Lebensgefahr für Nutzer) ist es unglaublich wichtig, Angriffe so schnell wie möglich aufzudecken. Daher spielt Detection Technology in jedem Sicherheitsprogramm eine Schlüsselrolle. Wenn Unternehmen mit der Implementierung von Private 5G und der darauf aufbauenden Anwendungsfälle beginnen, sollten sie daher unbedingt erwägen, wie sie ihre Detection Technology aufstocken müssen, um mit den vorgenommenen Änderungen am Netzwerk, den Anwendungen und der Datenspeicherung Schritt zu halten.

Eine potenzielle Herausforderung, besonders für Unternehmen mit sehr industriellen Umgebungen, ist, ob und wie die in vielen Fällen herstellerspezifischen Logdaten in die bereits genutzte Detection Technology eingespeist werden können. Selbst wenn dies möglich ist, muss außerdem sichergestellt werden, dass Detection Technology die genutzten Datentypen sinnvoll verarbeitet werden können. Möglicherweise wird auch Technologie zur Netzwerkanalyse benötigt, um den Netzwerkverkehr nach Hinweisen auf Datenausschleusung und andere verdächtige Aktivitäten zu durchsuchen.

Reagieren

Eine wichtige Komponente dieser Funktion ist die (für den Erfolg aller Sicherheitsmaßnahmen ausschlaggebende) Planung. In diesem Fall bedeutet das regelmäßige Tests und Planübungen, um die Reaktion auf verschiedene Bedrohungen zu trainieren. Unabhängige Begutachtungen der Sicherheitsinfrastruktur sind ebenfalls sehr empfehlenswert.

Unternehmen sollten branchenspezifisch planen, da sie anders auf Vorfälle reagieren müssen als Unternehmen in anderen Branchen. Deshalb sollten auch ihre Technologiepartner die industrielle Umgebung verstehen, um sie bei der Planung unterstützen zu können.

Wenn Unternehmen beginnen, Private 5G und die dadurch möglichen Anwendungsszenarien zu nutzen und ihre Sicherheits- und Erkennungsfunktionen entsprechend anpassen, muss auch die Notfallplanung aktualisiert und getestet werden, um sicherzugehen, dass sie weiterhin robust und zuverlässig ist.

Ebenso wichtig ist es, im Fall eines Angriffs zusätzliche Ressourcen als Backup zur Verfügung zu haben. Die meisten Unternehmen können es sich nicht leisten, Mitarbeiter zu beschäftigen, die nur auf einen Angriff warten, um diesen abzuwehren. Angriffe sind zwar wahrscheinlich, aber diese Mitarbeiter würden trotzdem oft untätig herumsitzen. Industrieunternehmen sollten daher Mitarbeiter in anderen Rollen auf die Angriffsabwehr vorbereiten oder einen externen Partner ins Boot holen, der auf Abruf bereitsteht. Auch eine Kombination aus beiden ist denkbar.

Wiederherstellen

Bei der Planung der Wiederherstellung müssen die Verantwortlichen in Unternehmen noch einmal zu den Antworten auf die oben gestellten Fragen zu den spezifischen Anforderungen und den betroffenen Endpunkten ihres Unternehmens zurückkehren, um die Auswirkungen auf ihr Unternehmen zu minimieren.

Beim Einrichten eines privaten 5G Netzwerks arbeiten sie höchstwahrscheinlich mit einem für sie neuen Technologieanbieter zusammen. Sie müssen sich also ein Verständnis dafür verschaffen, welche Art von Unterstützung sie bei der Wiederherstellung von diesem Anbieter benötigen und dies in den Wiederherstellungsplan einarbeiten.

Fazit

Mit 5G hält die Zukunft in Unternehmen Einzug – und Private 5G bietet eine zukunftsorientierte Basis für die Neuausrichtung von Industriebetrieben. Die Manager in den Geschäftsbereichen und den IT- und Sicherheitsteams müssen enger zusammenarbeiten als je zuvor, um von den Vorteilen der vierten industriellen Revolution zu profitieren – und die damit einhergehenden Risiken unter Kontrolle zu behalten.

Den Unternehmen, die die in 5G integrierten Sicherheitsvorkehrungen und das NIST CSF richtig nutzen, eröffnet sich ein sicherer Weg zu unendlich vielen Innovationschancen.

Schauen Sie unter verizon.com/business/de-de/solutions/5g/ vorbei, um herauszufinden, wie Private 5G von Verizon die Welt verändert.

verizon