Sicherheitsarchitektur für ein neues digitales Zeitalter

Erleben,
was verbindet.

T SECURITY

Inhaltsverzeichnis

In a nutshell

Erfolgreiche digitale Transformation bedeutet auch eine Transformation der Sicherheitsarchitektur. Das Whitepaper zeigt auf, welche Prinzipien beim Umbau der Sicherheitsinfrastruktur berücksichtigt werden sollten und welche Chancen und Vorteile sich daraus ergeben. Das Schlagwort Zero Trust wird dabei eingeordnet und konkretisiert. Anhand eines Beispiels wird schließlich veranschaulicht, wie ganzheitliche Security in einem modernen, dezentralen Firmennetz aussehen kann.

Warum wir eine neue Sicherheitsarchitektur brauchen

Die digitale Transformation läuft. Sie macht vieles einfacher, effektiver und nachhaltiger. Sie verändert die Art, wie wir arbeiten. Wo wir arbeiten, wird zunehmend unwichtiger. Es strömen nicht mehr alle Mitarbeitenden in die Firmenzentrale. Auch der Kontakt zu Kunden und Partnerunternehmen läuft vermehrt digital und ohne lange Anfahrten ab. Fernwartung wird zur Normalität.

Wichtiger wird hingegen eine stabile und sichere Konnektivität überall dort, wo Datenverkehr stattfindet. Also auch im Homeoffice auf dem platten Land oder dort, wo ein mit dem Internet der Dinge verbundener Container herumgefahren wird.

Die meisten Unternehmen wechseln im Zuge der Cloudifizierung und der Zunahme mobilen Arbeitens von MPLS zu anderen, dezentralen und internetbasierten Netzwerktechnologien wie SD-WAN, die einen direkten Cloud-Zugang für alle Netzwerkenden ermöglichen. Somit wird der Flaschenhals, der durch den zentralen Netzwerkzugang entsteht, vermieden. Zudem sind Internetleitungen kostengünstiger, was sich insbesondere auszahlt, wenn über mehrere Standorte oder geografische Regionen hinweg eine hohe Bandbreite benötigt wird.

Internetbasierte Netzwerktechnologien bieten außerdem eine deutlich höhere Flexibilität: Statt der langen Bereitstellungszeiten von MPLS können Änderungen oder neue Anbindungen schnell und einfach konfiguriert werden.

Die Nutzung von internetbasierten Netzwerktechnologien wie SD-WAN bedeutet jedoch, dass die Sicherheitsarchitektur grundlegend überdacht werden muss. Denn der Datenverkehr bleibt nicht mehr im privaten Netzwerk, sondern geht über öffentliche Internetleitungen. Eine dezentrale Netz-Architektur, die den direkten Zugang zu den Clouds ermöglicht, braucht eine neue Architektur, um Sicherheit an allen Enden zu gewährleisten. Im Folgenden wird es darum gehen, wie eine solche neue Sicherheitsarchitektur aussehen sollte.

Garantierte Netzwerk-Performance?

SD-WAN und andere internetbasierte Technologien sind stark von der Qualität und Zuverlässigkeit der Internetverbindungen abhängig. Wenn Internetleitungen ausfallen oder unzureichend sind, kann die Leistung und Verfügbarkeit stark beeinträchtigt werden. SLAs auf Netzwerk-Performance wie bei MPLS gibt es hier normalerweise nicht. Neue Maßstäbe setzt diesbezüglich das Premium Internet Underlay (PIU), das im Kapitel „Orchestrierte Sicherheit in der Praxis“ noch genauer vorgestellt wird.

Neue Angriffswaffen: KI

Angriffs-Software kann mit Hilfe von Künstlicher Intelligenz schneller und zielgenauer entwickelt und skaliert werden.

Neue Angriffsflächen

Homeoffice

Digitale Produktion

Hyper-Automatisierung

Edge Computing

Mobile Datennutzung

Internet der Dinge (IoT)

Anwendungen in der Cloud

Mitarbeitergeräte (BYOD)

Mentalitätswandel in der Sicherheitsarchitektur: Von der Festung zu Zero Trust

Wie sieht eine zeitgemäße Sicherheitsarchitektur aus? Zero Trust ist in aller Munde, wenn es um aktuelle IT-Sicherheit geht. Was steckt hinter der Null-Vertrauen-Philosophie und wovon hebt sie sich ab?

Die Festung

Um den Mentalitätswandel zu erklären, für den das Schlagwort Zero Trust steht, wird gern die Analogie zu einer mittelalterlichen Festungsanlage herangezogen. Der klassische, perimeterbasierte Security-Ansatz, so das Bild, funktioniert wie eine Festung. Die Sicherheitsarchitektur mit Burggraben, dicken Mauern und Zugbrücke zielt darauf ab, einen Ort, die Burg, zu schützen und einen Angriff von außen abzuwehren. Analog versucht klassische IT-Security, das Unternehmensnetzwerk gegen Angriffe und unerlaubte Zugriffe von außen zu schützen. Hierbei kommen Maßnahmen wie Netzwerksegmentierung, Angriffserkennungssysteme und Zugangsbeschränkungen des Netzwerkzugriffs via Firewalls zum Einsatz.

IT-Sicherheit als Festung: Ein Ort wird gegen Angriffe von außen geschützt

Angriffe von innen

Doch reicht das aus? Seit Erfindung des trojanischen Pferdes wissen wir, dass Angriffe auch innerhalb der Burg- oder Stadtmauern erfolgen können. Und sie nehmen zu: Seit der vermehrten Remote-Arbeit im Jahr 2020 ist die Zahl der Angriffe von innen stark gestiegen. Eine globale Studie mit dem Fokus auf Angriffe von innen berichtet von einer Zunahme um 44% für den Zeitraum von 2020 bis 2022[1]. Verdoppelt haben sich dabei die Fälle von Zugangsdaten-Diebstahl. Die meisten Angriffe werden jedoch nach wie vor durch fahrlässiges Verhalten von Mitarbeitenden oder Auftragnehmern verursacht.

56%
Fahrlässiges Verhalten durch Mitarbeitende oder Auftragnehmer

26%
Kriminelle oder böswillige Insider

18%
Diebstahl von Zugangsdaten

Bedrohungen der IT-Sicherheit von innen[2]

[1+2] 2022 Ponemon Cost of Insider Threats Global Report | Proofpoint US

Sicherheit auch jenseits der Festung

Veraltet ist das Sicherheitsmodell der wehrhaften Festung aber auch, weil sich in Zeiten von Clouds, mobiler Arbeit und software-definierten Netzwerken die zu schützenden Grenzen nicht mehr so klar ziehen lassen. Es reicht nicht mehr aus, nur den einen Ort zu schützen. Genau an diesem Punkt setzt Zero Trust an.

> *Zero Trust setzt den Fokus auf den Schutz von Ressourcen (Assets, Services, Workflows, Netzwerk-Zugängen), statt auf den Schutz von Netzwerksegmenten, da der Standort innerhalb des Netzwerks nicht mehr als wichtigste Komponente für die Sicherheit der Ressource angesehen wird.“*
>
> *– NIST, NIST Special Publication 800-207: Zero Trust Architecture, 2020*

Wurde zuvor das Netzwerk geschützt und alles, was innerhalb des Netzwerkes passierte, als vertrauenswürdig eingestuft, wird bei Zero Trust, wie der plakative Name bereits verrät, nichts und niemandem vertraut. Jeder Datenfluss wird auf Vertrauenswürdigkeit geprüft.

Anwendungsfälle von Zero Trust

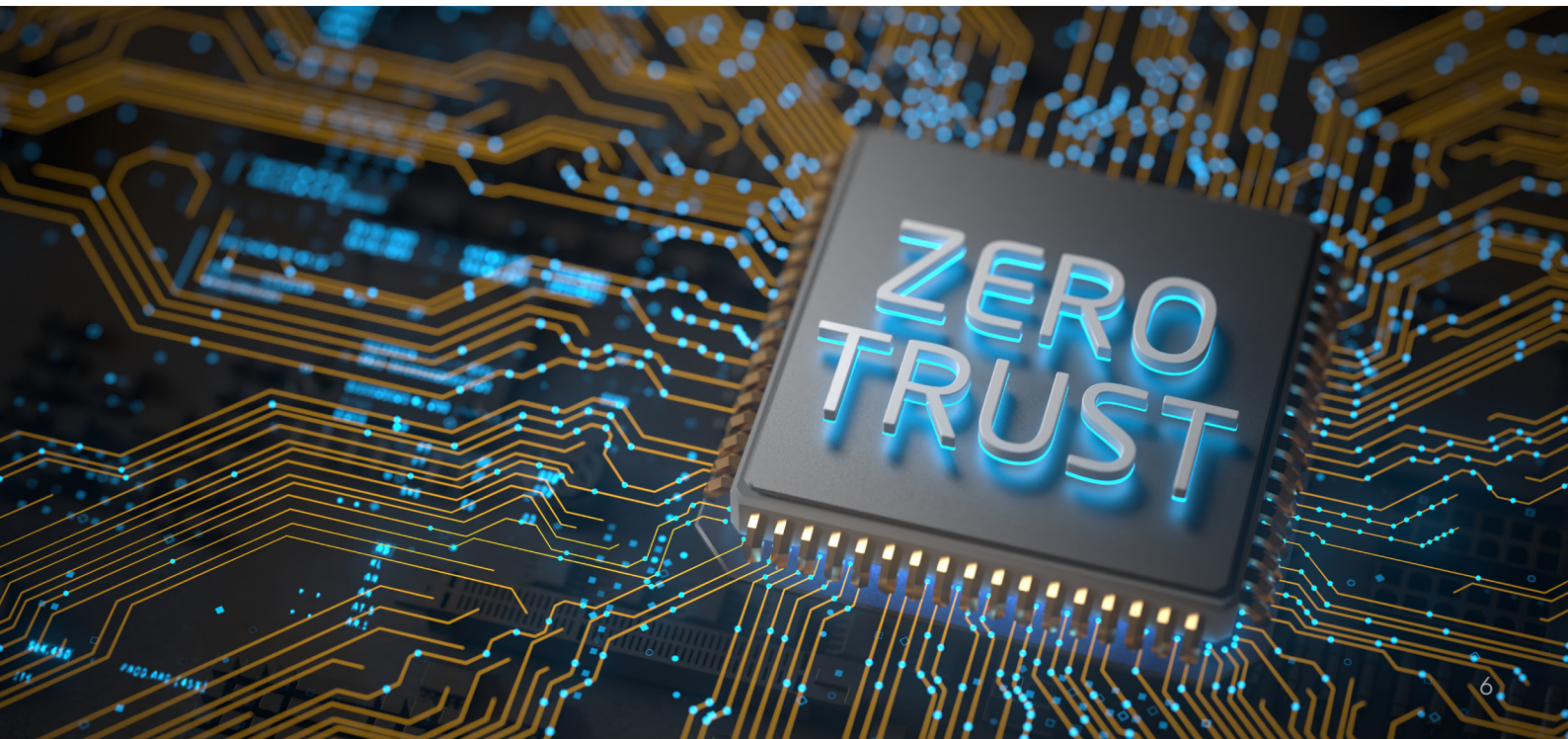
Remote-Arbeit
Sichere Anbindung von Homeoffices und mobiler Arbeit

Cloud-Zugriff
Sichere Nutzung cloudbasierter Dienste

Onboarding Externer
Sicherer Zugriff für Zulieferer, Auftragnehmer und Partner

Onboarding neuer Mitarbeitender
Schnelle und sichere Anbindung neuer Mitarbeitender

OT / IoT
Sichere Anbindung von vernetzten Maschinen und IoT-Sensoren



Die Prinzipien der neuen Sicherheitsarchitektur

Zero Trust ist kein Produkt und keine spezifische Technologie, sondern ein Sicherheitsansatz. Basierend auf den Prinzipien der kontinuierlichen Kontrolle von Zugriffen, der minimalen Rechtevergabe und der automatisierten Durchsetzung definierter Richtlinien bietet Zero Trust ein neues Framework für IT-Sicherheit. Im Folgenden schauen wir uns diese Prinzipien und deren Umsetzung näher an.

Kontinuierlich kontrollieren

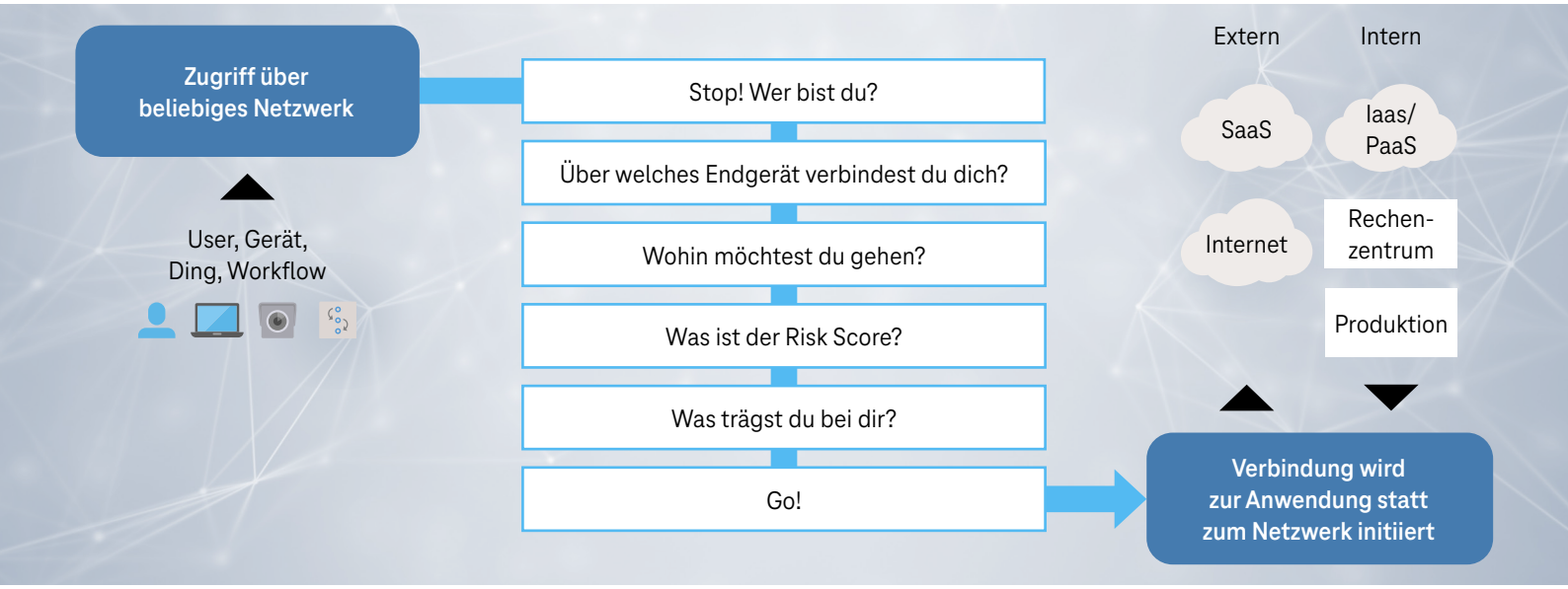
Die Idee, jeden einzelnen Datenzugriff zu kontrollieren, ist nicht ganz neu – in der Wissenschaft wird sie bereits seit ca. 20 Jahren diskutiert. Doch erst heute stehen uns die Technologien und die Rechenleistung zur Verfügung, die eine kontinuierliche Kontrolle sämtlicher Zugriffe auch in der Praxis umsetzbar machen.

Kontextualisieren

Um eine dynamische und granulare Steuerung des Zugriffs auf Ressourcen umzusetzen, spielt die Kontextualisierung eine wichtige Rolle – Zugriffsberechtigungen erfolgen stets nur unter Berücksichtigung verschiedener Kontextinformationen. Damit sind nicht nur Benutzeridentitäten und Netzwerkstandorte gemeint, einbezogen werden etwa auch:

- **Benutzerkontext:** Dies umfasst Informationen wie Benutzeridentität, Rollen, Berechtigungen, Zugriffshistorie, Geräteprofile und Authentifizierungsfaktoren (z. B. Multi-Faktor-Authentifizierung).
- **Gerätekontext:** Hierbei werden Informationen über das Gerät, von dem aus auf das System zugegriffen wird, einbezogen. Dies kann den Gerätetypen, das Betriebssystem, den Patch-Level, die Sicherheitskonfiguration und die Integrität des Geräts umfassen.
- **Anwendungskontext:** Hier werden Informationen über die verwendete Anwendung und ihre Sicherheitsmerkmale berücksichtigt. Das sind zum Beispiel die Art der Anwendung, ihre Sensitivität, die Versionsnummer, bekannte Schwachstellen oder der aktuelle Zustand der Anwendung.
- **Standortkontext:** Hierbei wird der physische Standort des Users oder des Geräts einbezogen. Dies kann verwendet werden, um den Zugriff von bestimmten geografischen Standorten zu erlauben oder zu beschränken.

In der **Policy Engine** werden die Kontextdaten verarbeitet und im Falle einer positiven Bewertung ein sitzungsbasierter Datenzugriff erlaubt. Die Kontextualisierung bei Zero Trust ermöglicht somit eine **dynamische und granulare Zugriffskontrolle,** die auf aktuellen Bedingungen und Risiken basiert. Sie trägt dazu bei, das Sicherheitsniveau zu erhöhen und unbefugten Zugriff zu verhindern, selbst wenn ein Benutzer bereits im Netzwerk ist oder eine Identitätsauthentifizierung erfolgreich abgeschlossen hat. Ein Beispiel für eine solche Zugriffskontrolle ist der Zero Trust Network Access (ZTNA).



Zugriffskontrolle im Zero Trust Modell

Zero Trust Network Access (ZTNA)

Zero Trust Network Access (ZTNA) ist, anders als bisherige Sicherheitskonzepte mit VPN, ein rollenbasiertes Konzept. Zero-Trust-Zugriff auf das Netzwerk bedeutet, dass der Zugriff präzise regulierbar ist und anwendungsbezogen vergeben wird. ZTNA-Lösungen beziehen Nutzeridentität, Standort, Endgerät, Tageszeit und die jeweilige Vertraulichkeitsstufe in Echtzeit ein, um eine Risikoberechnung anhand definierbarer Parameter durchzuführen und den Zugriff dementsprechend zu regeln.

Angriffsflächen verringern

Ein weiterer wichtiger Grundmechanismus von Zero Trust ist es, Angriffe möglichst schon im Vorfeld zu verhindern, indem die Angriffsflächen möglichst klein gehalten werden. Denn je weniger Möglichkeiten zum Angriff sich bieten, desto besser.

Berechtigungen einschränken
Das Least Privilege Prinzip (Prinzip der geringstmöglichen Berechtigung) bedeutet, dass einem User oder einer Entität nur die Zugriffsrechte und -berechtigungen gewährt werden sollten, die für die Ausführung seiner Aufgaben oder den Zugriff auf bestimmte Ressourcen unbedingt erforderlich sind. Diese Berechtigungen sollen zudem auf "Need-to-know"- oder "Need-to-access"-Basis gewährt werden.
Durch die Anwendung des Least-Privilege-Prinzips können potenzielle Angriffsvektoren reduziert werden. Wenn User nur die Berechtigungen und Zugriffsrechte haben, die für ihre unmittelbaren Aufgaben benötigt werden, wird das Risiko von Missbrauch oder versehentlichem Zugriff auf sensible Ressourcen minimiert. Selbst wenn Hacker Zugriff auf ein Benutzerkonto erhalten, wird ihre Fähigkeit, Schaden anzurichten, auf diese Weise stark eingeschränkt sein, da sie nur begrenzte Rechte haben.

Netzwerke segmentieren
Mikrosegmentierung ist ein Konzept, das darauf abzielt, Netzwerke in kleine, isolierte Segmente oder Zonen aufzuteilen und den Datenverkehr zwischen ihnen stark einzuschränken. Jedes Segment enthält eine begrenzte Anzahl von Ressourcen und hat klare Regeln für den Zugriff und die Kommunikation. Durch die Anwendung der Mikrosegmentierung wird der Zugriff auf Ressourcen auf Basis von definierbaren Parametern wie Benutzeridentität, Geräteintegrität oder Anwendungsanforderungen gesteuert.

Die Vorteile der Mikrosegmentierung:

- **Begrenzung der Angriffsfläche:** Durch die Aufteilung des Netzwerks in kleine Segmente wird die Angriffsfläche reduziert. Selbst wenn ein Angreifer Zugriff auf einen Teil des Netzwerks oder eine Ressource erhält, hat er nur begrenzten Zugriff auf andere Segmente. Dies verringert das Risiko einer lateralen Bewegung (Ost-West-Bewegung) und einer weiteren Ausbreitung von Angriffen.
- **Isolation von Ressourcen:** Jedes Segment enthält nur die Ressourcen, die für eine spezifische Aufgabe oder einen bestimmten Zweck benötigt werden. Dadurch können Berechtigungen und Zugriffsregeln genau definiert werden. Bei Kompromittierung eines Segments wird der Zugriff auf andere Segmente eingeschränkt.
- **Feinabstimmung der Zugriffssteuerung:** Mit der Mikrosegmentierung können granulare Zugriffsregeln auf Ebene der einzelnen Segmente definiert werden. Jedes Segment kann spezifische Zugriffsrichtlinien basierend auf dem Kontext (z. B. Benutzeridentität, Gerätetyp, Standort) haben. Dies ermöglicht eine präzise Steuerung des Datenverkehrs und minimiert das Risiko von unautorisiertem Zugriff.
- **Erhöhung der Sichtbarkeit und Kontrolle:** Durch die Segmentierung des Netzwerks wird die Sichtbarkeit und Kontrolle über den Datenverkehr verbessert. Es wird einfacher, verdächtige Aktivitäten zu erkennen und zu überwachen, da der Datenverkehr innerhalb der Segmente beschränkt ist und ungewöhnliche Verbindungen oder Kommunikationsmuster leichter erkannt werden können.

Die Mikrosegmentierung wird häufig durch Virtualisierungstechnologien, Netzwerk-Firewalls und Sicherheitsrichtlinien implementiert.

Automatisiert reagieren

Da die Geschwindigkeit von Bedrohungen und Angriffen zunimmt, ist die Automatisierung und Orchestrierung von Sicherheitsmaßnahmen im Security Monitoring von entscheidender Bedeutung. Denn so wird eine schnelle Reaktion auf Vorfälle und eine effektive Durchsetzung von Sicherheitsrichtlinien möglich.

Protokollieren und analysieren
Grundlage der automatisierten Reaktion ist die Transparenz über den Datenverkehr. Anomalien können so besser erkannt werden. Hierfür kommt ein SIEM zum Einsatz.

Security Information and Event Management (SIEM)

Im SIEM werden Log-Daten aus verschiedenen Quellen wie z. B. Protokolldateien von Netzwerkgeräten, Betriebssystemen, Anwendungen, Firewalls, Intrusion-Detection-Systemen (IDS), Intrusion-Prevention-Systemen (IPS) und anderen Sicherheitslösungen gesammelt und gespeichert.
Die gesammelten Ereignisdaten werden korreliert, um Zusammenhänge und Muster zu erkennen. So können Sicherheitsereignisse, potenzielle Bedrohungen oder verdächtige Aktivitäten in Echtzeit identifiziert werden. Auch die Einhaltung von Compliance-Anforderungen wird durch das SIEM überwacht und dokumentiert.

Überwachen und reagieren
Ein SOAR-System (Security Orchestration, Automation and Response) integriert Sicherheitstools, -technologien und -prozesse, um den gesamten Lebenszyklus eines Sicherheitsvorfalls zu unterstützen, von der Erkennung über die Untersuchung bis hin zur Reaktion und Wiederherstellung. Die entsprechenden Technologien, die dies ermöglichen, werden unter dem Akronym SOAR (Security Orchestration, Automation and Response) zusammengefasst.

SOAR orchestriert die Zusammenarbeit und Koordination verschiedener Sicherheitstools und -technologien. Es ermöglicht die nahtlose Integration von Sicherheitslösungen wie SIEM, IDS/IPS, EDR (Endpoint Detection and Response), Firewalls, Antivirus-Programmen und anderen Sicherheitsprodukten. Durch die Orchestrierung wird der Informationsaustausch und die Zusammenarbeit zwischen diesen Tools verbessert, was zu einer effizienteren Reaktion auf Sicherheitsvorfälle führt.

Vor allem aber automatisiert SOAR Sicherheitsaufgaben und -prozesse, um menschliche Eingriffe zu reduzieren und die Reaktionszeit zu verkürzen. Beispiele für automatisierte Aufgaben sind die Verarbeitung von Ereignisdaten, die Durchführung von Überprüfungen, die Quarantäne von infizierten Systemen und die Benachrichtigung von Stakeholdern.

SOAR unterstützt zudem den gesamten Incident Response-Prozess, von der Erkennung eines Sicherheitsvorfalls bis zur Wiederherstellung der betroffenen Systeme. Es ermöglicht die automatische Erfassung, Priorisierung und Eskalation von Sicherheitsvorfällen. SOAR kann auch vorgefertigte Incident Response-Playbooks oder -Workflows verwenden, um vordefinierte Maßnahmen und Handlungsanweisungen für bestimmte Vorfallstypen durchzuführen.

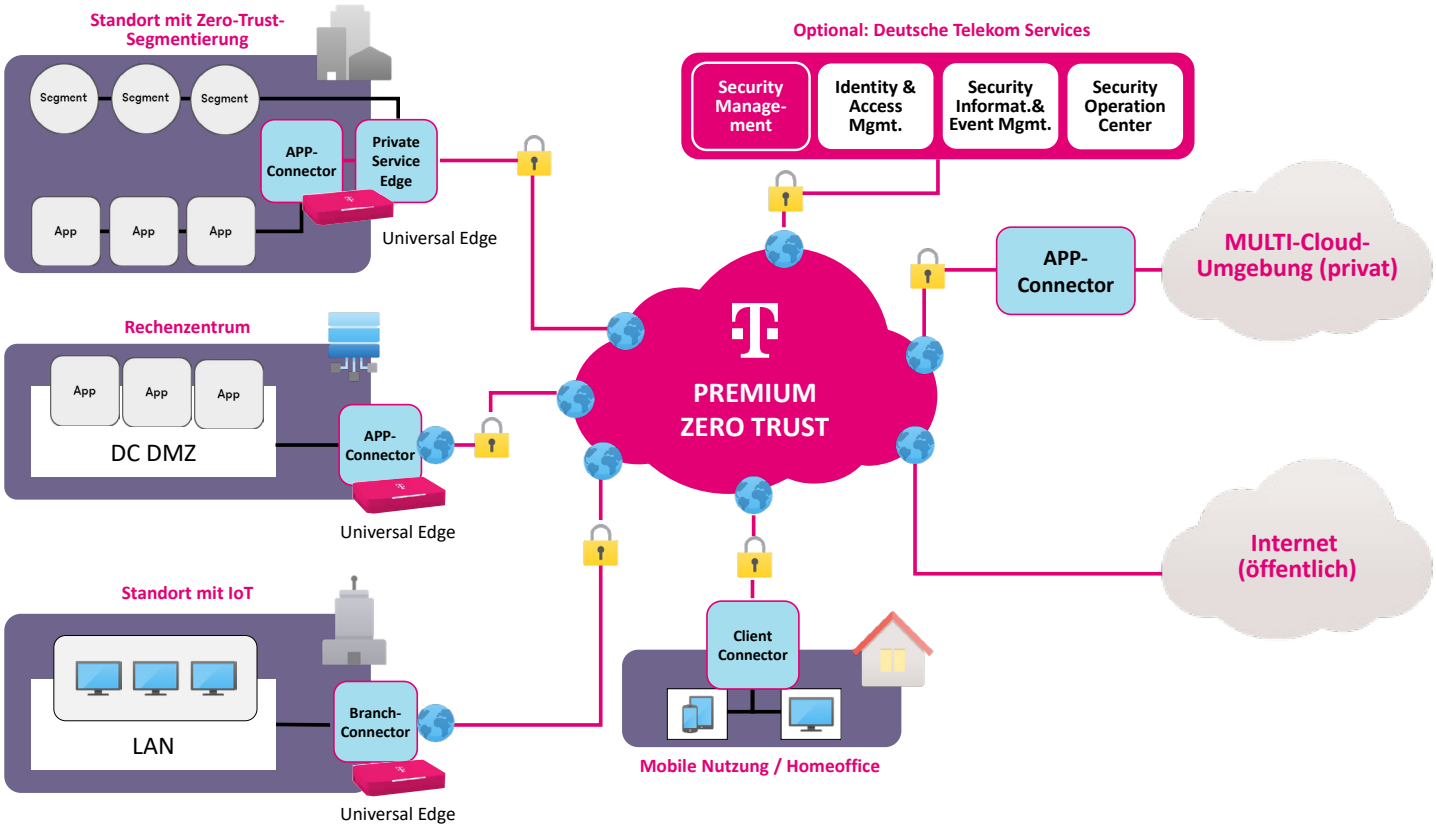
Für die Analyse von Sicherheitsdaten und zur Erstellung von Berichten über Sicherheitsvorfälle und deren Auswirkungen bietet SOAR verschiedene Funktionen. Es ermöglicht die Erstellung von Dashboards, Berichten und Metriken, um Einblicke in die Effektivität der Sicherheitsmaßnahmen und -prozesse zu erhalten. Ausserdem ermöglicht SOAR die Erfassung von Fallnotizen, Kommunikationsverläufen und Dokumentationen während der Untersuchung und Behandlung von Sicherheitsvorfällen. Diese Informationen sind wichtig für die Nachverfolgung und Dokumentation von Ereignissen, die Einhaltung von Compliance-Anforderungen und die Verbesserung der Incident Response-Verfahren.

Das Security Operations Center (SOC)

Im SOC (Security Operations Center) laufen die Fäden zusammen. Auch wenn hier natürlich viele Tools und Technologien zum Einsatz kommen, sind die Sicherheits-Schaltzentralen nicht komplett automatisiert. Hier arbeiten Spezialist*innen – und zwar rund um die Uhr. In großen SOC wird die IT-Sicherheit vieler Unternehmen überwacht. Der Vorteil: Je mehr Prozesse überwacht werden, umso schneller können Anomalien erkannt werden. Telekom Security betreibt einige der größten integrierten SOC weltweit.

Orchestrierte Sicherheit in der Praxis

Wie lassen sich die Prinzipien des Zero Trust Modells in eine moderne Sicherheitsarchitektur überführen? Das soll am Beispiel der Premium Zero Trust Architektur veranschaulicht werden. Innovativ und einzigartig an der im folgenden vorgestellten Lösung ist, dass ein Premium Internet Underlay eingesetzt wird, das Service Level Agreements zur Netz-Performance gewährleistet. Denn ein stabiles Netz ist die Grundlage sicherer Digitalisierung.



Premium Zero Trust Architektur

Sämtliche Netzwerkenden dieser Architektur – Standorte, IoT-Geräte, Mobile Nutzer und Mitarbeitende im Homeoffice – haben einen direkten Zugang zum Rechenzentrum, zu den privaten Cloud-Anwendungen und zum Internet.

Damit die verteilte Architektur sicher ist, wird die **Premium Zero Trust Plattform** zwischengeschaltet. Sie liefert eine vollständige Inline-Überprüfung, Zero-Trust-Zugangskontrolle und KI-gestützte Bedrohungsabwehr. Der gesamte Traffic aller User wird mithilfe einheitlicher Schutzmaßnahmen überwacht, kontrolliert und abgesichert. Integriert sind CASB/DLP zum Schutz von Daten in web- und SaaS-basierten bzw. privaten Unternehmensanwendungen sowie die Browser-Isolation zum Schutz von Daten bei der Übertragung auf Mitarbeitergeräte. Mit Endpoint DLP wird die Sicherheit von Daten auf Firmengeräten gewährleistet. Weitere Funktionen der Plattform sind E-Mail DLP für die Absicherung des Mailverkehrs, SSPM zur Behebung riskanter Fehlkonfigurationen sowie Third-Party App Security für die Kontrolle von SaaS-Backdoor-Verbindungen.

Als Router wird die von der Telekom entwickelte **Universal Edge** eingesetzt. Sie vereint und virtualisiert Netzwerk-Dienste in einem Gerät: SD-WAN, Firewall, Routen-Optimierung und weitere Funktionen. Bisher waren dafür jeweils eigene Geräte notwendig, insbesondere, wenn die Dienste von verschiedenen Anbietern kamen. Die Universal Edge bedeutet einen deutlich geringeren logistischen Aufwand, wenn neue Standorte angebunden werden müssen und lässt sich einfacher installieren und betreiben. Alle gebuchten Funktionen stehen sofort bereit und neue Software oder Updates lassen sich aus der Ferne administrieren. Der universelle Router bringt Unternehmen nicht nur ungeahnte Flexibilität und Kombinationsfreiheit, sondern punktet auch mit Nachhaltigkeit: Hardware kann auch beim Wechsel von Technologien weiter genutzt und die Rechenleistung vor Ort viel besser ausgeschöpft werden.

Die physische Netzwerkinfrastruktur bildet das **Premium Internet Underlay (PIU)** der Telekom. Im Gegensatz zum herkömmlichen dedizierten Internetzugang, der keine Performance-Versprechen gewährleistet, bietet Telekom Premium Internet dedizierte Qualitätsparameter in nahezu MPLS-Qualität – und das weltweit. Das heißt, Performance wird in Form von Service Level Agreements vertraglich zugesichert. Möglich wird diese garantierte Netzleistung durch die Kombination des globalen Netzes der Telekom mit dem Backbone der führenden Cloud-Anbieter und dem Service ausgewählter internationaler Internet Access Partner. Nationale und internationale Kunden können so ihre privaten Cloud-Umgebungen von überall über den Telekom Global Hybrid Backbone erreichen und von der hohen Zugriffs- und Performance-Qualität profitieren.

Im Zusammenspiel ergeben diese Bausteine ein Unternehmensnetz, das den Ansprüchen des digitalen Zeitalters gerecht wird. Standorte, Rechenzentrum, Zweigstellen, Homeoffices, OT und IoT werden sicher verbunden und sämtliche Zugriffe kontinuierlich kontrolliert. Die Netzwerkenden sind außerdem hochperformant ans Internet angebunden, so dass die Nutzung von Clouddiensten nicht nur abgesichert ist, sondern auch unterbrechungsfrei funktioniert. Ebenfalls wichtig: das Netz lässt sich problemlos und ohne Abstriche in puncto Sicherheit oder Performanz skalieren. Optional kann die Sicherheit zudem durch die Telekom gemanagt werden, so dass interne Kapazitäten frei werden und das sichere Unternehmensnetz als Serviceleistung bereitsteht.

Wir managen Ihre Security

Die Telekom Security bietet als Managed Security Provider hochwirksame und professionelle Sicherheitsmaßnahmen für den Schutz vor Cyberangriffen. Mit über 25 Jahren Erfahrung ist die eigenständige Gesellschaft unter dem Dach der Deutsche Telekom AG Marktführer in DACH und einer der europäischen Leader in der Cyber Security Branche. Für das breite Portfolio – von Cyber Defense über Cloud Security bis zu OT Security – kooperiert die Telekom Security mit weltweit führenden Unternehmen und bietet so digitale Sicherheit aus einer Hand – von der Beratung über individuelles Design bis zur Implementierung.

Deniz Barbaros
Business Development Manager
bei Deutsche Telekom Security GmbH

Deniz Barbaros beschäftigt sich seit mehr als 19 Jahren intensiv mit den Bereichen Technik, Betrieb und Vertrieb von Cyber Security. Daraus resultiert sein fundiertes Wissen über Netzwerk- und Sicherheitsarchitekturen. Bei der Deutschen Telekom Security GmbH verantwortet er für das Security-Portfolio der Geschäftskundensparte der Deutschen Telekom vertrieblich die Produkte rund um Netzwerksicherheit sowie Partnerschaften mit weltweit führenden Security-Technologieanbietern.

Deniz.Barbaros@telekom.de

Mit Sicherheit zum Erfolg!

Wir kümmern uns um ganzheitliche Netz- und Sicherheitsarchitektur und übernehmen auf Wunsch Management, Betrieb, Integration und kontinuierliche Sicherheitsanalyse Ihres Netzwerks im Telekom Security SOC.

Kontakt
Persönlicher Ansprechpartner
Freecall: 0800 33 04444
E-Mail: security.dialog@telekom.de
Web: security.telekom.de

Herausgeber
Deutsche Telekom Security GmbH
Office Port 1
Friedrich-Ebert-Allee 71–77
53113 Bonn

Erleben,
was verbindet.