Zero Trust Networking in der Industrie

Acht Fragen an Steffen Ullrich, IT-Sicherheitsforscher und Technology Fellow

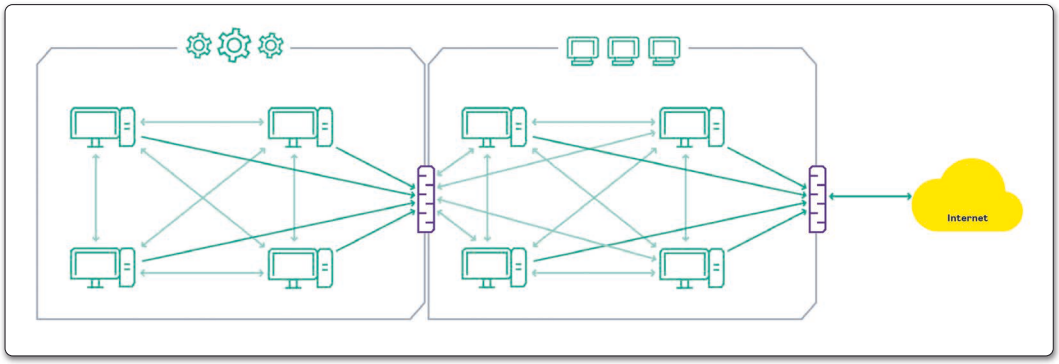

Bild 1: Klassische Koppelung von OT (links) und IT (rechts). Beide Netzwerke werden am Netzwerk-Perimeter bzw. -Übergang von einer Firewall geschützt. Eine Kompromittierung in der IT kann zu einer Kompromittierung des kompletten OT-Netzwerks führen

OT (Operation Technology) und IT wachsen immer mehr zusammen. Das Problem ist: Waren Produktionsnetzwerke früher abgeschottet, wird heute durch die Vernetzung mit der IT der Zugriff von außen erleichtert. Was bedeutet das konkret für die OT-Sicherheit?

Steffen Ullrich: OT-Umgebungen sind betriebskritischer als IT-Umgebungen. Produktionsausfälle oder Fehlfunktionen haben typischerweise drastischere Auswirkungen als in der IT. Entsprechend vorsichtig geht man beim Betrieb vor. Eine Folge davon ist, dass verglichen mit der IT die Änderungsrate in der OT deutlich geringer ist, und somit auch das Alter der eingesetzten Geräte und Software deutlich höher als in der IT. Technologien und Design stammen oft aus einer Zeit, als Cyber-Sicherheit eine geringe Priorität in der Entwicklung hatte. Entsprechend breit ist die Angriffsfläche.

Zusätzlich muss man von einer unzureichenden Sicherheit der IT-Umgebungen ausgehen. Das betrifft nicht nur die Office-IT mit den typischen Angriffsvektoren über Phishing, Malware und Ransomware. Auch Cloud-Dienste oder eine vom Dienstleister betreute Fernwartung führen dazu, dass Betreiber immer weniger Kontrolle über ihre eigenen Netzwerke haben.

Eine direkte Vernetzung von OT und IT exponiert also die breite Angriffsfläche der OT in eine potenziell unsichere IT. Dies führt nicht nur zu einer Gefährdung der zuverlässigen Produktion. In gefährlichen Bereichen wie z. B. dem Chemiesektor kann es auch zu einer Gefährdung der Safety und damit von Menschenleben führen. Bild 1 zeigt eine klassische Koppelung von OT und IT.

Wie können produzierende Unternehmen mit diesen Unsicherheiten umgehen?

Steffen Ullrich: Zum einen ist es wichtig, die potenzielle Angriffsfläche so weit wie möglich zu verkleinern. Ausgehend von einen Minimalitätsprinzip, bei dem nur das wirklich notwendige möglich sein sollte, schränken Zero-Trust-Konzepte wie Mikrosegmentierung oder Software-Defined Perimeter proaktiv die möglichen Kommunikationswege ein und reduzieren damit die Angriffsfläche auf ein Minimum. Dabei ist zunächst konkret festzulegen, welcher Zugriff und welche Kommunikation für wen erlaubt sein soll. Nur diese werden konsequent sowohl auf Applikations- als auch auf Netzebene zugelassen. Zusätzlich gilt es, die Komplexität zu verringern. Je weniger Features eine Software hat und je klarer die Schnittstellen sind, desto verständlicher, leichter und wirksamer ist eine Absicherung.

Dennoch: Keine Sicherheitskomponente ist hundertprozentig zuverlässig. Daher ist es wichtig, mehrschichtige Sicherheitsarchitekturen aufzubauen, bekannt unter dem Begriff Defense in Depth. In der Praxis bedeutet dieses, Zugriffsbeschränkungen auf mehreren

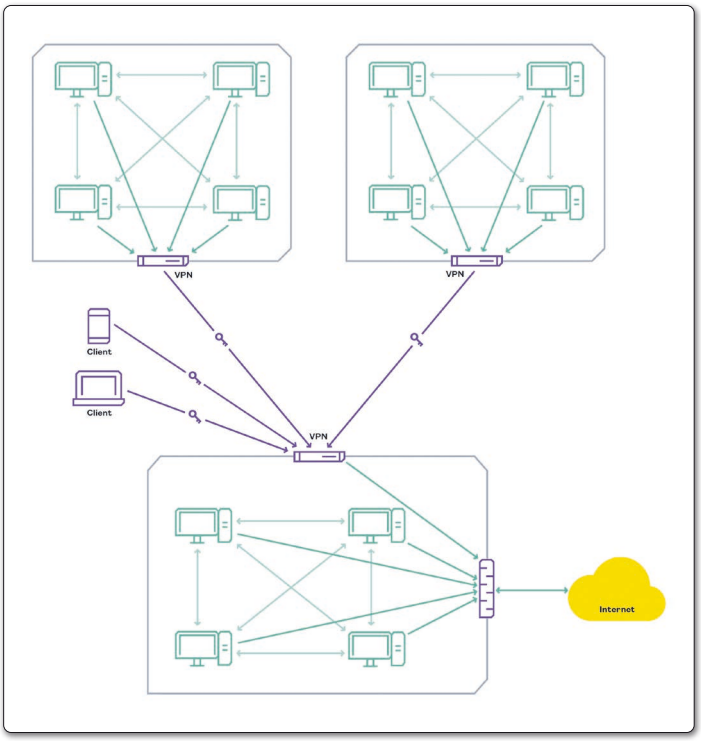

Bild 2: Komplexe Netzwerkinfrastruktur aus Unternehmenszentrale (unten) sowie zwei Unternehmensstandorten und Remote Clients, die über VPN angebunden werden. Der Schwerpunkt der IT-Sicherheit liegt traditionelle auf der Absicherung des Netzperimeters

Steffen Ullrich
IT-Sicherheitsforscher
Genua GmbH
www.genua.de

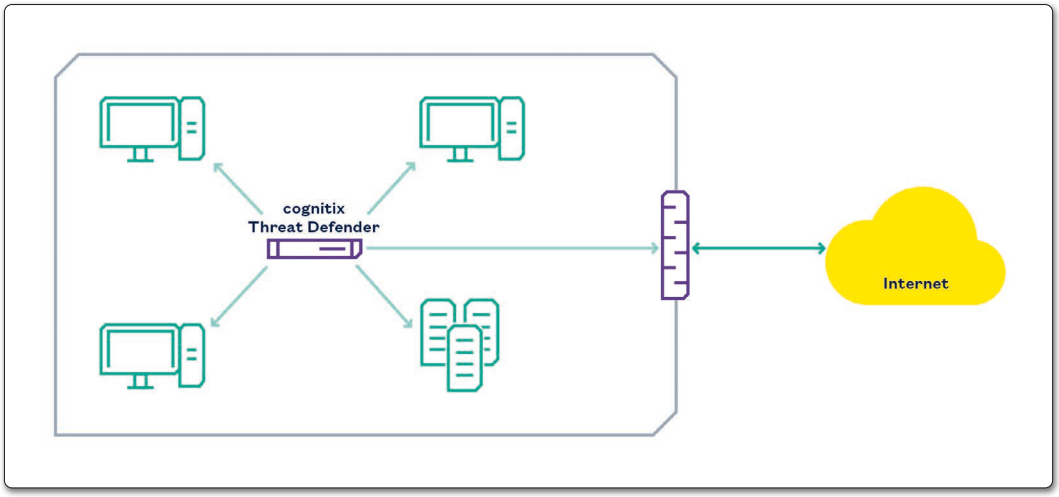

Bild 3: Mikrosegmentierung nach Forrester. Einzelne Dienste oder Geräte werden voneinander abgetrennt und die Kommunikation zwischen ihnen reguliert und überwacht

Ebenen durchzusetzen, zum Beispiel durch die Beschränkung des Zugangs zum Netz, die Beschränkung der Kommunikation im Netz und die Zugriffskontrolle an dem Dienst bzw. Gerät. Versucht ein Angreifer dann, in ein Netzwerk einzudringen, kommt er nicht weit.

Zusätzlich zu den proaktiven Maßnahmen sollten auch reaktive eingesetzt werden. Ausführliches Monitoring ist die Voraussetzung für eine frühzeitige Angriffserkennung sowie für eine zeitnahe Reaktion im Angriffsfall. Wichtig sind auch eine Sensibilisierung von Mitarbeitern und funktionierende Notfallpläne.

Was bedeutet das Zero-Trust-Paradigma?

Steffen Ullrich: Der traditionelle Ansatz zur Absicherung von Geschäfts- und Produktionsprozessen ging davon aus, dass sich alle Geräte, Applikationen sowie die Kommunikation zwischen diesen unter der eigenen Kontrolle befinden. Es wurde sich daher auf die Absicherung des Netzes am Perimeter fokussiert. Innerhalb des Netzes selbst war überwiegend unbeschränkte Kommunikation möglich. Dieser Ansatz passt nicht mehr zur Realität. Heutige Infrastrukturen sind in ihrer Komplexität wesentlich größer und erstrecken sich oft über mehrere Netze (Bild 2). Hinzu kommen immer mehr fremdverwaltete Systeme wie Cloud-Umgebungen oder ferngewartete Maschinen. Gleichzeitig werden immer kritischere Geschäftsprozesse digitalisiert und vernetzt. Dadurch steigen die Anforderungen an die Verfügbarkeit und Zuverlässigkeit sowie den Datenschutz. Der einfache Ansatz der netzfokussierten Sicherheit skaliert in der heutigen Zeit immer schlechter. Das Zero-Trust-Paradigma fokussiert daher auf die Absicherung der einzelnen Prozesse, statt die Absicherung der kompletten Netze.

Mit dem Zero-Trust-Paradigma entfernt man sich von der Idee, dass eine Kontrolle am Netzperimeter ausreichend möglich ist. Statt das komplette Netz zu sichern, fokussiert man sich auf die Absicherung der an einem Geschäfts- oder Produktionsprozess beteiligten Endgeräte, Nutzer und Dienste sowie der Kommunikationspfade zwischen diesen.

Welche Ansätze gibt es in der Produktionswelt, Zero Trust Networking zu implementieren?

Steffen Ullrich: Es gibt drei wesentliche Ansätze, die sich primär darin unterscheiden, an welcher Stelle die Sicherheitsregeln durchgesetzt werden. Zero Trust Networking Access nach Forrester bedeutet eine Mikrosegmentierung (Bild 3). Das heißt, in einem vorhandenen Netz werden an strategisch sinnvollen Stellen Zugriffskontrollen und Analysen implementiert, welche die Kommunikation innerhalb des Netzes beschränken und überwachen. Dies kann man zum Beispiel mittels einer Next Generation Firewall oder unserem cognitix Threat Defender realisieren. Letzterer erlaubt es, das gesamte interne Netz kleinteilig zu segmentieren, einzelne Geräte voneinander abzutrennen und die Kommunikationspfade nach dem Minimalitätsprinzip zu reglementieren und zu überwachen. Machine-Learning-Algorithmen helfen dabei, die Netzwerkkommunikation über einen bestimmten Zeitraum im Betrieb zu analysieren und so die passenden Regeln zu erstellen.

Der zweite ZTNA-Ansatz ist der Software-defined Perimeter. Hier wird nicht ein vorhandenes Netz abgesichert, sondern der externe Zugang zu einzelnen Diensten. Konzeptionell ist das ähnlich zu einem klassischen Virtual Private Network, wobei jedoch bei einem Software-defined Perimeter nur Zugriff auf spezifische Dienste und nicht das komplette Netz erlaubt wird (Bild 4). Dies ist zum Beispiel wichtig bei einer Fernwartung, die nur einen Zugriff auf einzelne Dienste bzw. Systeme ermöglichen sollte, nicht aber einen Zugriff auf das komplette Produktionsnetz.

Das dritte ZTNA-Konzept, das im Industrieumfeld wahrscheinlich weniger relevant ist, ist unter dem Begriff BeyondCorp beziehungsweise BeyondProd bekannt und wurde von Google propagiert (Bild 5). Hier geht es darum, den Zugang zu einem einzelnen Dienst abzusichern. BeyondCorp ist primär für Web-Anwendungen gedacht. Für alles andere eignet es sich weniger. Im Industriekontext ist es zum Beispiel für die Anbindung eines IIoT-Geräts an einen cloudbasierten Dienst nutzbar.

Wie können Mikrosegmente nach Forrester konkret bestimmt werden?

Steffen Ullrich: Dafür gibt es verschiedene Wege, je nachdem, wie viel man investieren möchte und wo die Angriffsflächen und Sicherheitsprobleme liegen. Zum Beispiel könnte man die Clients, IoT Devices und Server voneinander isolieren. In der OT können das fremdgesteuerte Maschinen sein, bei Servern sind es vielleicht kritische Umgebungen. Die Clients sind am wenigsten verwundbar. Wenn man diese Kategorien voneinander trennt, ist bereits einiges erreicht. Man kann aber auch so weit gehen, jedes Gerät von jedem zu trennen. Generell geht es darum, die Angriffsflächen zu verkleinern und die Kommunikation zu kontrollieren. Das heißt, je angreifbarer die Software auf einem Gerät ist und je kritischer die Umgebung, desto enger und granularer sollte

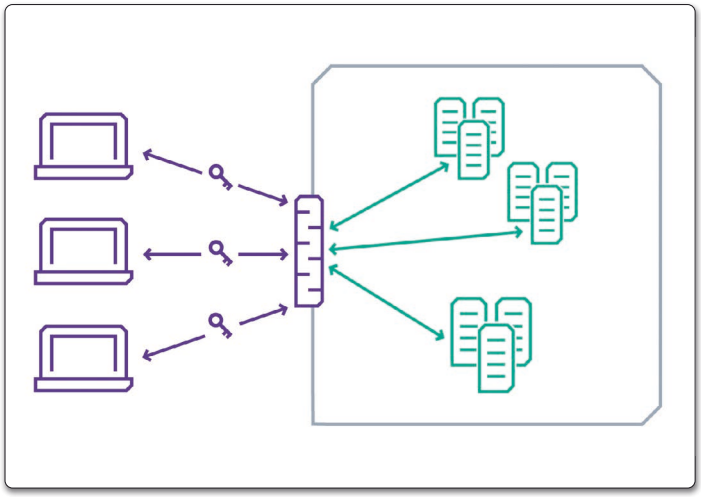

Bild 4: Implementierung eines Software-Defined Perimeter, welcher externen Clients nach einer Authentisierung Zugriff auf bestimmte Dienste in einer internen Infrastruktur erlaubt

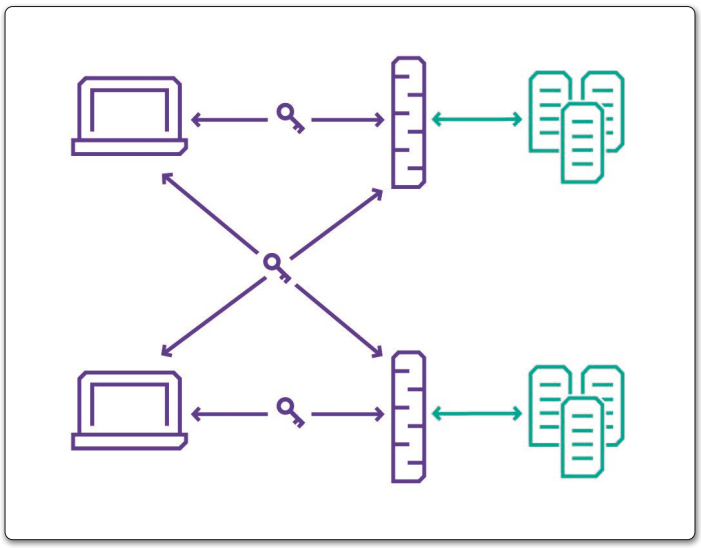

Bild 5: BeyondCorp-Ansatz. Die Authentifizierung und Zugriffskontrolle findet direkt am Dienst über einen vorgeschalteten Identity Aware Proxy (IAP) statt. Die Verbindung zwischen Client und IAP ist per HTTPS verschlüsselt

man den Mikroperimeter um diese Geräte und die Dienste ziehen.

Wie finden Anwender den für sie richtigen Zero-Trust-Ansatz?

Steffen Ullrich: Dieser ist abhängig vom konkreten Use Case. Möchte man potenziell verwundbare Geräte in einem existierenden Netz besser schützen, so ist die Mikrosegmentierung das Mittel der Wahl. Möchte man zum Beispiel einzelne Dienste im lokalen Netzwerk oder in der Cloud von außen erreichbar machen, wie zum Beispiel bei der Fernwartung, dann eignet sich der Software-defined Perimeter. Geht es aber darum, die Anbindung an einzelne Web-basierte Anwendungen skalierbar zu schützen, z. B. im Industrial IoT-Bereich, dann sind Konzepte wie BeyondCorp gut geeignet.

Allen ZTNA-Ansätzen ist gemein, dass sie Sicherheits-Policies auf der Basis von Identitäten benutzen. Das betrifft Identitäten von Geräten, Nutzern und Diensten. Die Leistungsfähigkeit einer ZTNA-Lösung ist stark davon abhängig, wie flexibel das sogenannte Identity Access Management ist.

Es lassen sich auch mehrere Ansätze parallel betreiben; zum Beispiel, um einen Dienst im internen Netz mittels Mikrosegmentierung abzusichern und zusätzlich über einen Software-defined Perimeter von außen für die Fernwartung erreichbar zu machen. Und man kann auch mehrere dieser Konzepte ineinander schachteln, um eine Defense-in-Depth-Strategie zu fahren.

Eine typische IT-OT-Anwendung ist die Fernwartung. Wie wird hier das Zero-Trust-Verfahren implementiert?

Steffen Ullrich: Exemplarisch lässt sich das an unserer Fernwartungslösung genubox zeigen, die ein Software-defined Perimeter implementiert. Das heißt, ein oder mehrere interne Dienste sollen von außen nur nach entsprechend starker Authentifizierung erreichbar sein. Bei der genubox Fernwartung haben wir das so umgesetzt, dass zunächst eine hochsichere Verschlüsselung und Authentifizierung mittels eines SSH-Tunnels stattfindet. Dieser Ansatz ermöglicht nur einen dedizierten Zugang zu explizit definierten Services (Bild 6). Das heißt, im Gegensatz zu häufig eingesetzten VPN-Lösung findet hier keine Netzkopplung statt. Zusätzlich zur Zugangskontrolle werden die Aktivitäten auf dem Remote Desktop sowie die Terminal Session (SSH-Verbindung) per Video aufgezeichnet und die übertragenen Dateien auf Viren überprüft. Und der Mitarbeiter in der Produktionsanlage hat die Möglichkeit, die entsprechende Session jederzeit physisch zu erlauben beziehungsweise zu unterbrechen, indem er den entsprechenden Schlüsselschalter umdreht. Er behält also zu jeder Zeit die Kontrolle über seine Anlage.

Wie zukunftsfähig sind Zero-Trust-Konzepte mit Blick auf die sich ständig weiterentwickelnde Gefahrenlage in der Cyber Security?

Steffen Ullrich: Die selektive Begrenzung von Geschäfts- und Produktionsprozessen mittels Zero-Trust erlaubt eine deutlich höhere Granularität und Spezifität der Absicherung, als wenn man das ganze Netz im Stück sichert. Die Nutzung von organisatorischen Identitäten als Basis von Sicherheitsregeln anstatt von IP-Adressen und Ports führt zu einem besseren Einklang von sicherheitstechnischen und betrieblichen Anforderungen, das heißt, Regeln sind präziser und bieten so einen höheren Schutz.

Eine proaktive granulare Beschränkung der Kommunikation erhöht auch das Verständnis über den zu erwartenden Datenverkehr und erleichtert so die Anomalie- und Angriffserkennung. Das Accounting der Zugriffe innerhalb von Zero Trust ermöglicht auch eine frühzeitige Detektion kompromittierter Zugänge und erlaubt eine zügige Schadenseingrenzung.

ZTNA bietet also zum einen eine höhere proaktive Sicherheit, weil nur bestimmte Verbindungen erlaubt sind, und zum anderen eine deutlich bessere reaktive Sicherheit, weil sich der Schaden wesentlich einfacher und schneller beurteilen und eingrenzen lässt. Und ergibt sich eine neue Bedrohungslage oder Sicherheitslücke in einem Gerät, kann die Angriffsfläche durch einen engen Mikroperimeter zeitnah verkleinert werden, selbst wenn noch kein Patch existiert. Man kann zum Beispiel dafür sorgen, dass zeitweise nur noch bestimmte Clients auf dieses Gerät zugreifen dürfen oder nur unter bestimmten Bedingungen oder bestimmten Tageszeiten. Zero Trust bietet hier eine hohe Flexibilität. ◄

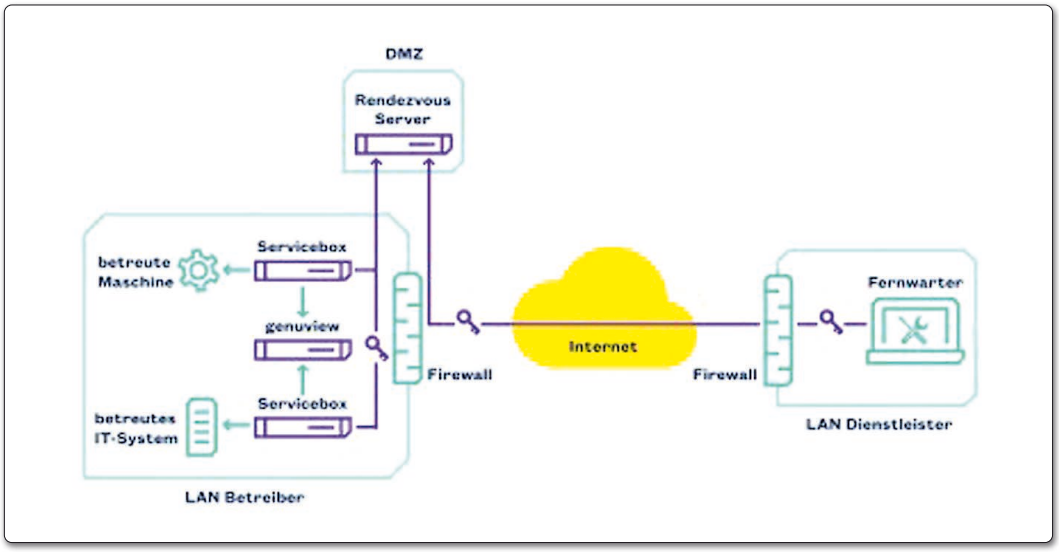

Bild 6: Exemplarische Implementierung eines Software-Defined Perimeter für sichere Fernwartung, umgesetzt mit der Fernwartungslösung von genua. Der Fernwarter authentifiziert sich über einen Rendezvous-Server und kann dann nach Freigabe nur auf den benötigten Dienst im Betreibernetzwerk zugreifen. Im Gegensatz zu VPN-basierten Ansätzen findet hierbei keine Netzkoppelung statt