Industrielle Netzwerke vor modernen Bedrohungen schützen

Zero Networks sieht Trend zu OT-Segmentierung

© AdobeStock/ Pungu x

Autor:
Kay Ernst
Zero Networks
www.zeronetworks.com

OT-Netzwerke wurden nicht für die Herausforderung durch moderne Cyberbedrohungen entwickelt. Eine typische OT-Umgebung umfasst Hunderte von nicht verwalteten Geräten von Anbietern, die teilweise schon Jahrzehnte alt sind. OT-Netzwerke sind daher schwer zu überwachen, schwer zu kontrollieren und es ist unglaublich kostspielig, wenn sie gestört werden. Diese Netzwerke ordnungsgemäß zu sichern, ist äußerst schwierig, obwohl genau das immer dringlicher wird.

Kay Ernst, Experte für automatisierte Mikrosegmentierung, erklärt wie selbst in die Jahre gekommene OT-Netzwerke durch Segmentierung widerstandsfähiger gegen Attacken werden können.

Fakten

Die Zahl der Ransomware-Gruppen, die es auf OT abgesehen haben, stieg im letzten Jahr um 60 Prozent, aber nur 19 Prozent der Unternehmen fühlten sich im gleichen Zeitraum vollständig auf OT-Sicherheitsprobleme vorbereitet. Um den zunehmenden OT-Sicherheitsbedrohungen entgegenzuwirken und die allgemeine Sicherheitslage zu verbessern, benötigen Unternehmen eine robuste OT-Netzwerksegmentierung, die keine neue Komplexität mit sich bringt.

Was ist OT-Netzwerksegmentierung?

Die Segmentierung von OT-Netzwerken ist der Prozess der Isolierung von industriellen Steuerungssystemen (ICS), Sensoren, speicherprogrammierbaren Steuerungen (SPS) und anderer OT-Infrastruktur von umfassenderen IT-Netzwerken und voneinander. Segmentierte Zonen werden anhand von Faktoren wie Funktion, Asset-Typ, Kritikalität oder Risikostufe definiert und durch Zugriffskontrollrichtlinien geschützt, die festlegen, welcher Datenverkehr zwischen ihnen stattfinden darf.

Die OT-Segmentierung reduziert die Angriffsfläche und begrenzt die laterale Bewegung zwischen Systemen, wodurch industrielle Unternehmen vor dem kostspieligen Risiko von Ausfallzeiten geschützt werden. Mit anderen Worten: Bei der OT-Segmentierung geht es um Eindämmung. Wenn ein Bereich kompromittiert wird, trägt die Segmentierung dazu bei, dass sich der Schaden nicht ausbreitet.

OT-Netzwerksegmentierung vs. OT-Mikrosegmentierung

Die OT-Netzwerksegmentierung isoliert das Netzwerk in sichere Zonen. Die OT-Mikrosegmentierung sichert die Infrastruktur zusätzlich, indem sie den Datenverkehr zwischen einzelnen Assets innerhalb dieser Zonen kontrolliert. Während die herkömmliche Netzwerksegmentierung auf Grenzen wie VLANs oder Subnetzen basiert, arbeitet die Mikrosegmentierung auf Asset-Ebene und ermöglicht so eine präzise Datenverkehrskontrolle und reduziert das Risiko lateraler Bewegungen, selbst in flachen oder älteren OT-Umgebungen.

Sicherheit ist wichtig

Warum ist die OT-Netzwerksegmentierung für die Sicherheit wichtig? Ein flaches Netzwerk ist ein Spielplatz für Angreifer. Ohne sinnvolle interne Grenzen können sie, sobald sie einen Endpunkt geknackt haben, sich seitlich bewegen, um die Produktion zu sabotieren, kritische Systeme zu blockieren und Lieferketten zu stören. Der Erstzugriff auf einen fragilen Endpunkt erfolgt durch Phishing, einen Fernzugriffsdienst oder ein anfälliges Legacy-System.

Die Zeiten der „Air Gap"-isolierten Industrienetzwerke sind vorbei. Die Einführung der Cloud, das IoT, Remote-Betrieb und der durch Industrie 4.0 bedingte Druck hinsichtlich Effizienz und Verfügbarkeit führen dazu, dass OT-Systeme zunehmend mit der IT-Infrastruktur von Unternehmen verflochten sind. Es wird prognostiziert, dass im nächsten Jahr 70 Prozent der OT-Systeme mit IT-Netzwerken verbunden sein werden – ein Anstieg von 20 Prozent gegenüber dem Vorjahr. Diese Konvergenz modernisiert zwar die Prozesse und verbessert die Effizienz, vergrößert aber auch die Angriffsfläche und setzt die Betriebstechnologie Risiken aus, für die sie nie konzipiert wurde. Durch Segmen-

tierung können Sicherheitsteams die Kontrolle zurückgewinnen und Grenzen durchsetzen, wo herkömmliche perimeterbasierte Sicherheitsmaßnahmen versagen.

Ransomware-Angriffe auf OT beginnen in der IT

Während Ransomware-Angriffe für fast jedes Unternehmen nach wie vor ein wichtiges Thema im Bereich Cybersicherheit sind, ist keine Branche stärker und konsequenter von Ransomware betroffen als der Industriesektor. Im Jahr 2024 stieg die Zahl der Ransomware-Angriffe in Industrieunternehmen um 87 Prozent gegenüber dem Vorjahr, wodurch diese Branche zum vierten Mal in Folge das Hauptziel von Ransomware war. Insbesondere im Jahr 2024 war ein Anstieg von 60 Prozent bei Ransomware-Gruppen zu verzeichnen, die OT/ICS-Systeme angreifen.

Zunehmende Bedrohung

Angesichts der zunehmenden Ransomware-Bedrohungen und der Konvergenz von OT/IT-Netzwerken können Sicherheitsteams nicht ignorieren, dass 75 Prozent der Angriffe auf OT-Systeme mit einer IT-Sicherheitsverletzung beginnen. Schwachstellen in der Unternehmensumgebung – wie VPNs, Webanwendungen oder kompromittierte Anmeldedaten – bieten Hackern einen ersten Zugang. Von dort aus bewegen sie sich seitlich, oft unentdeckt, bis sie OT-Systeme erreichen. Aus diesem Grund müssen Sicherheitsteams die OT-Segmentierung überdenken, um ihre Sicherheitsstrategien auf eine konvergierte IT/OT-Umgebung auszurichten.

Implementierung einer OT-Netzwerksegmentierung

In Umgebungen, in denen die Verfügbarkeit nicht verhandelbar ist, kann die Segmentierung eine gewaltige Aufgabe sein. Mit dem richtigen Ansatz ist sie jedoch machbar – und muss nicht unbedingt komplex sein. Was man nicht sieht, kann man nicht schützen, und nur wenige Unternehmen verfügen über eine vollständige Bestandsaufnahme ihrer OT-Geräte, geschweige denn über ein Verständnis ihrer Kommunikationswege. Der erste Schritt besteht darin, eine Echtzeit-Inventur der OT-Geräte (und im Idealfall auch der IT-Assets für einen umfassenden Ansatz) zu erstellen, ihr Verhalten zu erfassen und ihre Kommunikationsmuster zu verstehen. Automatisierung kann hier helfen, indem sie Traffic-Baselines lernt, um unbefugte oder riskante Datenflüsse leicht zu identifizieren.

Minimale Berechtigungen erstellen

Sobald die Assets entdeckt wurden, gilt es sie logisch nach Funktion, Standort, Kritikalität oder Kommunikationsanforderungen zu gruppieren. Dies erleichtert die Definition von Segmentierungsrichtlinien, ohne notwendige Arbeitsabläufe zu stören.

Die beobachteten Verhaltensweisen und Gruppierungen dienen dazu, um Zugriffsrichtlinien mit minimalen Berechtigungen zu erstellen. Dies bedeutet, nur explizit erforderlichen Datenverkehr zuzulassen und alles andere standardmäßig abzulehnen. Diese Richtlinien sollten über Firewalls auf Geräteebene, Switches oder Sicherheitsanwendungen durchgesetzt werden, die eine detaillierte Anwendung von Regeln unterstützen.

Moderne OT-Segmentierung

Worauf Unternehmen achten sollten: Nicht alle Segmentierungslösungen sind gleich. In dynamischen Umgebungen sind manuelle Strategien nicht skalierbar – und herkömmliche Tools reichen oft nicht aus. Zu achten ist auf moderne Funktionen wie:

- **Automatisiertes Lernen und Erstellen von Richtlinien:** Manuelle Konfiguration, Tagging, Gruppierung sowie die Erstellung und Verwaltung von Richtlinien sind fehleranfällig und nicht nachhaltig. Eine Lösung, die Verhaltensweisen automatisch lernt und Segmentierungsrichtlinien vorschlägt, beschleunigt die Bereitstellung, optimiert die laufende Verwaltung und verbessert die Genauigkeit.

- **Kontinuierliche Überwachung und Just-in-Time-Zugriffskontrollen:** Bedrohungen entwickeln sich weiter. Netzwerke verändern sich. Eine effektive Segmentierung sollte so dynamisch sein wie die Umgebungen, die sie schützt.

Sinnvoll sind Lösungen, die das Netzwerkverhalten in Echtzeit überwachen und Just-in-Time-MFA für privilegierte Ports und sensible Systeme durchsetzen, sodass Benutzer nur dann auf das zugreifen können, was sie benötigen, und zwar genau dann, wenn sie es benötigen.

- **Agentenlose Architektur:** Anstatt Agenten auf Endpunkten zu installieren, sollten Unternehmen einer Lösung den Vorzug geben, die native Betriebssystemkontrollen wie hostbasierte Firewalls und Zugriffskontrolllisten (ACLs) nutzt, um ältere und anfällige OT-Systeme ohne das Risiko von Unterbrechungen zu schützen.

- **Einheitliche Abdeckung über alle Umgebungen hinweg:** Moderne Sicherheit erfordert eine nahtlose, konsistente Durchsetzung von Richtlinien sowohl für IT- als auch für OT-Ressourcen. Ein Flickenteppich aus Lösungen schafft Lücken, die Hacker auszunutzen wissen. Unternehme sollten nach Plattformen suchen, die die Segmentierung in konvergenten Umgebungen vereinheitlichen.

Einheitliche IT/OT-Segmentierung

So funktioniert die einheitliche IT/OT-Segmentierung: Ein umfassender und einheitlicher Ansatz für die OT-Segmentierung, wie Zero Networks ihn verfolgt, erleichtert die granulare Segmentierung von IT- und OT-Netzwerken und sorgt so für kompromisslose Sicherheit in Zeiten komplexer Cyberbedrohungen. Nachdem alle Netzwerkverbindungen erfasst wurden, erstellt die einheitliche OT/IT-Mikrosegmentierungslösung entsprechende Regeln und hochpräzise Richtlinien mit minimalen Berechtigungen für IT- und OT-Netzwerke, die mithilfe von Automatisierung zentral auf die hostbasierten Firewalls der verwalteten IT-Geräte und auf die ACLs der Switches angewendet werden, die die nicht verwalteten OT-Geräte verbinden.

Administratorprotokolle wie RDP, SSH, RPC, WMI und SMB gehören zu den beliebtesten Angriffsmethoden von Hackern. Um sicherzustellen, dass keine versteckten Schwachstellen für Hacker übrigbleiben, bietet die Just-in-Time-MFA auf Netzwerkebene eine zusätzliche Sicherheitsebene, die nur den notwendigen Datenverkehr zulässt, ohne den normalen Betrieb zu stören. Von Rechenzentren und OT bis hin zu Legacy-Systemen und darüber hinaus sorgt hierbei eine einzige Plattform mit einem einzigen Regelwerk für die Mikrosegmentierung vielfältiger und dynamischer Landschaften.

Wer schreibt:

Zero Networks ist ein Pionier im Bereich der automatisierten Mikrosegmentierung und Netzwerksicherheit. ◄