paloalto NETWORKS

Best Practices für sichere OT-Assets, -Netzwerke und -Remoteprozesse

Zero-Trust-Sicherheit zum Schutz aller OT-Umgebungen

Vielversprechende Fortschritte in OT-Umgebungen dank digitaler Transformation und besserer Konnektivität

Die digitale Transformation verändert industrielle Prozesse grundlegend und eröffnet Organisationen enorme Chancen, ihr Geschäft zu revolutionieren. Die Einführung von OT-Assets, 5G-Technologie und die Migration in die Cloud sind alle Teilbereiche der digitalen Transformation, die viele industrielle Organisationen umsetzen möchten, um die betriebliche Effizienz zu verbessern, Kosten zu senken und die Sicherheit ihrer Mitarbeitenden zu erhöhen.

Diese zunehmende Digitalisierung umfasst Konnektivität von Maschine zu Maschine (M2M), von Maschine zu Mensch und von Maschine zu Endpunkten außerhalb der OT-Netzwerke. So entsteht ein zusammenhängendes Ökosystem aus cyberphysischen Systemen (CPS). Dieser Trend wird durch folgende Faktoren begünstigt:

Intelligente Fertigung

OT-Umgebungen durchlaufen Industrie-4.0-Initiativen, die durch digitale Technologien zur Vernetzung von Mitarbeitenden, Partnerunternehmen, Zulieferunternehmen und Maschinen vorangetrieben werden. Dieses integrierte CPS-Ökosystem verbessert die betriebliche Effizienz, Agilität und Kundenerfahrung.

Alte Systeme mit IT-Anbindung

Viele bestehende OT-Systeme, die ohne Rücksicht auf Sicherheitsaspekte entwickelt wurden, sind jetzt mit dem IT-Netzwerk und dem Internet verbunden, was zu Sicherheitslücken führt. Darüber hinaus haben die zunehmende Komplexität von OT-Systemen und der Flickenteppich an isolierten Sicher-heitstechnologien zu komplizierten, spezialisierten Netzwerkinfrastrukturen geführt, die die Angriffsfläche vergrößern.

Beschleunigte Remoteverbindungen aufgrund der Pandemie

Während der Pandemie wurde der Remotezugriff auf die OT-Infrastruktur über das Internet zu Wartungs- und Betriebszwecken zwingend erforderlich und führte zu einer Beschleunigung der

OT-Sicherheit bietet erhebliche Vorteile

- **Effizienterer Betrieb**
  Weniger Sicherheitsverstöße und automatisierte Prozesse steigern die Verfügbarkeit.
- **Kosteneinsparungen**
  Überwachung und Asset-management per Fernzugriff reduzieren die durch Sicherheits-vorfälle und Wartungsarbeiten verursachten Kosten.
- **Mehr Sicherheit am Arbeitsplatz**
  Das Risiko von Geräteausfällen und Unfällen wird reduziert.

Die Anfälligkeit der OT-Umgebung und die Gefährdung durch Bedrohungen sind so hoch wie nie zuvor und nehmen immer weiter zu. CXOs meistern einen prekären Balanceakt: Sie müssen die Verfügbarkeit und Arbeitsplatzsicherheit aufrechterhalten, während sie gleichzeitig erstklassige Schutzmaßnahmen bereitzustellen und zu verwalten haben.

Trotz der OT-Vorteile birgt die zunehmende Konnektivität aber auch große Risiken für den Betrieb.

Organisationen auf der ganzen Welt stehen vor einer unglaublichen Herausforderung: Sicherheitsvorfälle, die den Betrieb zum Erliegen bringen könnten. Ein Vorfall wirkt sich negativ auf den Umsatz, den Ruf der Marke, die Einhaltung von Lieferketten-SLAs und die Arbeitsplatzsicherheit aus. Vier Trends führen zu einem erhöhten Risiko von Sicherheitsvorfällen.

1. **Größere Angriffsfläche**
   Die Angriffsfläche für Bedrohungen vergrößert sich erheblich, da Initiativen zur digitalen Transformation zu alte und neue OT-Assets anfällig machen. Diese Systeme stellen eine Verbindung mit dem IT-Netzwerk (IT/OT-Konvergenz), 5G, der Cloud und dem Internet her und ermöglichen einen besseren Direktzugriff auf Apps für die Remotewartung von OT-Assets.

2. **Anfällige Ziele für Ransomware und IP-Diebstahl**
   Ransomware und andere Cyberangriffe haben rasant zugenommen, da angreifende Personen anfällige OT-Assets ins Visier nehmen.

3. **Zunehmender Compliancedruck**
   Die Complianceanforderungen der Industrie und Behörden zum Schutz von OT-Umgebungen entwickeln sich ständig weiter, um Bedenken über die möglichen Auswirkungen von Sicherheitsvorfällen auf den Betrieb, die Sicherheit der Mitarbeitenden, den Umsatz und den Markenruf Rechnung zu tragen.

4. **Veraltete und isolierte Sicherheitstechnologien**
   Bei den aktuellen IT- und OT-Sicherheitstechnologien handelt es sich um fragmentierte, unzusammenhängende Technologien, die keinen ausreichenden Schutz bieten und spezielle Schulungen, Fähigkeiten und Wartungsvorgänge erfordern.

Digitalisierung, Bedrohungen, Vorschriften und veraltete Sicherheitsmaßnahmen sorgen für eine brisante Mischung. Leider macht ein Mangel an moderner umfassender Sicherheit für OT-Umgebungen diese sehr anfällig für Cyberangriffe.

CXOs sind sich dessen bewusst und besorgt, tun sich aber schwer, ihre OT-Umgebungen zu schützen.

Da es keine ganzheitliche Lösung zum Schutz von OT-Umgebungen gibt, sind CXOs gezwungen, zwischen drei nicht gerade idealen Optionen zu wählen.

1. **Bewältigen der Herausforderungen mit zu vielen, zu wenigen oder gar keinen Sicherheitslösungen**
   Einige CXOs setzen auf mehrere isolierte Sicherheitsprodukte, um so viele Risiken wie möglich abzudecken, haben daraufhin jedoch mit einer erhöhten betrieblichen Komplexität, möglichen Fehlkonfigurationen und hohen Gesamtbetriebskosten zu kämpfen. Andere CXOs sind besorgt, dass zusätzliche Sicherheitstechnologien in ihrer Umgebung den Betrieb beeinträchtigen könnten, und beschränken daher die Einführung von Sicherheitstechnologien auf ein Minimum. Die dritte Gruppe von CXOs hält an der physischen Trennung zwischen OT und dem Rest der Welt fest und zögert die digitale Transformation so lange wie möglich hinaus.

2. **Tolerieren des vermuteten Sicherheitsrisikos innerhalb des OT-Netzwerks**
   Einige CXOs entscheiden sich dafür, das OT-Netzwerk kaum oder gar nicht zu segmentieren. Dies ermöglicht eine laterale Ausbreitung im Netzwerk, sodass Angreifer sich vollständigen Zugang zur OT-Umgebung verschaffen können, sobald sie eingedrungen sind.

3. **Zulassen des Remotezugriffs ohne konsequente Sicherheitsüberprüfung und -kontrolle**
   Andere CXOs erlauben den Remotezugriff ohne angemessene Sicherheitsrichtlinien, Inspektionen und Kontrollen.

Gartner prognostiziert, dass 30 % aller Organisationen mit kritischer Infrastruktur bis 2025 einer Sicherheitsverletzung zum Opfer fallen werden, die entweder den gesamten Betrieb oder einzelne geschäftskritische cyberphysische Systeme zum Stillstand bringt.

Laut dem FBI Internet Crime Report von 2021 war der US-amerikanische Fertigungssektor seit dem Angriff auf die Colonial Pipeline im Mai 2021 bis Ende desselben Jahres mehr als 60 Cyberattacken ausgesetzt. Das sind etwa zehn erfolgreiche Ransomwareangriffe pro Monat!

Möglichkeiten für Angriffe in OT-Umgebungen

BESTEHENDE UND NEUE OT-ASSETS STELLEN EINE VERBINDUNG MIT DEM IT-NETZWERK UND DER CLOUD HER
Anstieg von 400 % der OT-Assets in der Fertigung erwartet

5G VERBINDET NEUE ARTEN VON ASSETS
15 Milliarden 5G-verbundene Industrieassets bis 2026

REMOTEVERBINDUNGEN SIND AUF DEM VORMARSCH
70 % der ICS/SCADA-Assets weisen externe Verbindungen auf

VIELE OT-ASSETS SIND ANFÄLLIG UND SCHWER ZU PATCHEN
Über 1.000 CVEs in industriellen Steuerungssystemen, über 80 Schwachstellen bei den vier führenden OT-Anbietern

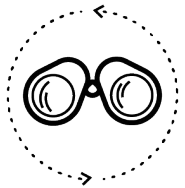
SaaS-APPS BILDEN EINEN WEITEREN ANGRIFFSVEKTOR
33 % der ICS-Angriffe 2021 erfolgten über öffentlich zugängliche Anwendungen

REMOTEVERBINDUNGEN ERÖFFNEN EINEN NEUEN ANGRIFFSVEKTOR
37 % der ICS-Angriffe 2021 erfolgten über externe Remotedienste

Zero-Trust-Sicherheitskonzept zum Schutz von OT-Netzwerken ist unerlässlic

Zero Trust ist eine Cybersicherheitsstrategie, die völlig auf implizites Vertrauen verzichtet und das Sicherheitsniveau kontinuierlich validiert. Diese Strategie lässt sich mit „niemandem vertrauen, alles verifizieren“ zusammenfassen und schützt OT-Umgebungen mit mehreren Maßnahmen. Ein Zero-Trust-Ansatz für die OT-Sicherheit bietet den effektivsten Schutz vor Cyberangriffen auf OT-Assets, -Netzwerke, -Remoteprozesse und 5G-Netzwerke.

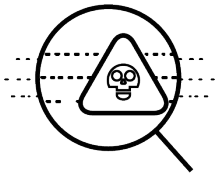
Umfassende Transparenz



Zugriffskontrolle nach dem Least-Privilege-Prinzip

Kontinuierliche Prüfung der Vertrauenswürdigkeit

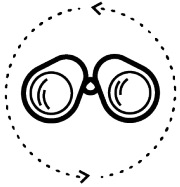
Kontinuierliche Sicherheitsprüfung



* Geschätzte Anzahl der Geräte im Jahr 2030 und Steigerung des Prozentsatzes von 2020 bis 2030

Umfassende Transparenz von OT-Assets, Apps und Benutzern über OT-Assets, -Netzwerke, -Remoteprozesse und 5G-Netzwerke hinweg

Umfassende Transparenz



Zero Trust basiert auf genauen Einblicken in Assets, Apps und Benutzer. Für einen wirksamen Schutz von Netzwerken ist es unerlässlich, alle verbundenen Assets und Geräte zu kennen, einschließlich der genehmigten und nicht genehmigten sowie der neu bereitgestellten. Dazu gehören auch das Netzwerkverhalten, alle Anwendungen und alle Internetverbindungen.

Dank transparenter OT-Assets lässt sich besser nachvollziehen, welche Assets für den Geschäftsbetrieb am kritischsten sind. Außerdem kann durch die Überwachung der internen und externen Kommunikation (z. B. Kommunikation im Remotebetrieb) sowie durch Alarme im Falle von Abweichungen vom normalen Prozessverhalten das Risiko der OT-Assets bestimmt werden. Um Unterbrechungen zu vermeiden, sollten die mit der Assetidentifizierung und der Risikobewertung verbundenen Prozesse passiv ablaufen, ohne Ihren OT-Betrieb zu beeinträchtigen.

Zugriff nach dem Least-Privilege-Prinzip: Sichern Sie den OT-Perimeter und die Assets und setzen Sie Segmentierungsrichtlinien durch

Zugriffskontrolle nach dem Least-Privilege-Prinzip

Der erste Schritt bei der Zero-Trust-Sicherheit ist es meist, den Zugriff nach dem Least-Privilege-Prinzip zu beschränken und die OT-Netzwerkgrenze durch die effektive Abtrennung der OT-Netzwerke von der Unternehmens-IT und dem Internet zu sichern. Dies trägt zum Schutz von lokalen und Remotevorgängen sowie von 5G-Ressourcen bei, indem die Angriffsfläche reduziert und der unbefugte Zugriff sowie eine Ausbreitung von Bedrohungen im Netzwerk verhindert werden.

Im zweiten Schritt werden OT-Assets durch eine weitere Unterteilung in Zonen und Segmente nach asset-, protokoll- oder risikobasierten Kriterien geschützt. Erstellen Sie kontextbezogene und granulare Segmentierungsrichtlinien, um die verschiedenen Teile des Netzwerks wirksam zu trennen und den Zugriff nach dem Least-Privilege-Prinzip durchzusetzen, während Sie gleichzeitig die Best-Practice-Standards für die Segmentierung wahren.

Kontinuierliche Prüfung der Vertrauenswürdigkeit: Bewerten Sie kontinuierlich die Kommunikation und Prozesse von OT-Assets

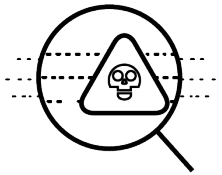
Kontinuierliche Prüfung der Vertrauenswürdigkeit

Die kontinuierliche Prüfung der Vertrauenswürdigkeit identifiziert unerwünschte Kommunikationsvorgänge und Verstöße gegen Segmentierungsrichtlinien in OT-Assets und -Netzwerken. Darüber hinaus bewertet sie auch Änderungen in der Assetsicherheit und im Verhalten von Benutzern und Apps.

Jegliches verdächtige Verhalten sollte sofort erkannt werden, damit der Zugang in Echtzeit gesperrt werden kann. Die kontinuierliche Prüfung der Vertrauenswürdigkeit beschleunigt Incident-Response-Prozesse, indem sie infizierte OT-Assets mit anderen Vorfällen in Bezug setzt, isoliert und vom OT-Netzwerk abtrennt.

Kontinuierliche Sicherheitsprüfung: Vermeiden Sie Bedrohungen für kritische Systeme

Kontinuierliche Sicherheitsprüfung



Die kontinuierliche Sicherheitsprüfung ist der letzte, entscheidende Schritt bei der Einrichtung der Zero-Trust-Sicherheit für mit dem Netzwerk verbundene Assets. Selbst wenn ein Assetprofil erstellt und das Gerät im richtigen Netzwerksegment platziert wurde, kann es durch die Verbindung zum Netzwerk infiziert werden. Eine kontinuierliche Überwachung aller Protokolldateien bis Layer 7 trägt zur Aufrechterhaltung und zum Schutz des Netzwerks bei.

Die umfassende und laufende Prüfung des gesamten Datenverkehrs, auch für zulässige Verbindungen, schützt vor allen Bedrohungen, einschließlich Zero-Day-Bedrohungen. Um Bedrohungen für kritische Systeme und Richtlinien abzuwehren, braucht es Technologien zum Schutz vor bekannten und unbekannten sowie ICS-spezifischen Bedrohungen.

Die umfassendste Zero-Trust-Lösung für OT-Assets, -Netzwerke, -Remoteprozesse und 5G-Netzwerke

Die Vorteile von Digitalisierung und Konnektivität in OT-Umgebungen lassen sich genauso wenig abstreiten wie die damit verbundenen Risiken. Palo Alto Networks bietet die umfassendste Zero-Trust-Lösung mit der größten Abdeckung von Zero-Trust-Prinzipien für OT-Netzwerke, -Remoteprozesse und 5G-Netzwerke.

Reduzieren Sie die betriebliche Komplexität um 95 % und ersetzen Sie acht Punkt-lösungen durch eine einheitliche Sicherheits-plattform. Ziehen Sie den größtmöglichen Nutzen aus allen Assets bei minimalem Cyberrisiko. Machen Sie sich fit für 5G, indem Sie die digitale Transformation mit dem guten Gefühl angehen, dass Palo Alto Networks Ihre mit 5G verbundenen Assets und Netzwerke schützt.

Mit der Leistungsfähigkeit der branchenweit ersten KI/ML-gestützten Transparenz-Engine bietet die Zero-Trust-OT-Sicherheitslösung von Palo Alto Networks die umfassendste OT-Transparenz und konsistente Zero-Trust-Sicherheit, die sowohl die Sicherheitsmaßnahmen vor Ort als auch die in der Cloud bereitgestellten Sicherheitsservices nutzt.

Zero-Trust-OT-Sicherheit hat einen Namen: **Palo Alto Networks.**

Palo Alto Networks hat sich das Ziel gesetzt, zum bevorzugten Cybersicherheitspartner für Unternehmen zu werden und gemeinsam mit ihnen unseren digitalen Lebensstil zu schützen. Palo Alto Networks schützt die Clouds, Netzwerke und Mobilgeräte Zehntausender Unternehmen. Dazu gehen wir durch kontinuierliche Innovation die größten Herausforderungen rund um die Cybersicherheit an, mit denen Unternehmen derzeit konfrontiert sind. Dabei kommen die neuesten Forschungsergebnisse aus den Bereichen der künstlichen Intelligenz, Analysen, Automatisierung und Orchestrierung zum Einsatz.

Sie möchten mehr über Zero-Trust-OT-Sicherheit erfahren?

STÖBERN SIE IN UNSEREN RESSOURCEN

Palo Alto Networks wurde 2005 gegründet und hat seinen Hauptsitz im kalifornischen Santa Clara. Zur Betreuung unserer Kunden haben wir zudem Niederlassungen auf der ganzen Welt.

www.paloaltonetworks.de

Oval Tower, De Entrée 99–197
1101 HE Amsterdam, Niederlande

Telefon: +31 20 888 1883
Vertrieb: +800 723 9771
Support: +31 20 808 4600