Enterprise Strategy Group™ by TechTarget

WIRTSCHAFTLICHE VALIDIERUNG

Analyse der wirtschaftlichen Vorteile von Industrial OT Security von Palo Alto Networks

Senkung des Risikos für industrielle OT-Umgebungen und Bereitstellung eines Return on Investment (ROI) von 351 % bei zu 95 % geringerer Komplexität als bei alternativen OT-Sicherheitslösungen

Von Aviv Kaufmann, Principal Economic Validation Analyst und Practice Director
Enterprise Strategy Group

Februar 2023

Inhalt

Einleitung

Diese wirtschaftliche Validierung durch die Enterprise Strategy Group von TechTarget konzentriert sich auf die quantitativen und qualitativen Vorteile, die Unternehmen von der Aktivierung des ML-basierten SaaS-Abonnements von Industrial OT Security für ihre Next-Generation Firewalls (NGFWs) von Palo Alto oder einem anderen Anbieter erwarten können, um die Betriebstechnologie (OT) in industriellen Umgebungen besser zu schützen.

Herausforderungen

In modernen Unternehmen ist die Cybersicherheit für die meisten Funktionen, die traditionell von der IT-Organisation unterstützt werden, mittlerweile einer der Hauptschwerpunkte. Unternehmen haben erheblich in Technologien investiert, die das Unternehmen vor Angreifern schützen, indem sie Endbenutzer-Geräte, Rechenzentren, Edge-Standorte und Cloud-Services sichern. Da inzwischen vernetzte Technologien auch in kritischeren Geschäftsbereichen eingesetzt werden, muss die Sicherheit auch auf Bereiche ausgedehnt werden, die zuvor vom Unternehmensnetzwerk isoliert oder durch ein Air-Gap getrennt waren. Im Zuge der Modernisierung verzeichnen Industrie- und Fertigungsunternehmen ein erhebliches Wachstum bei der Anzahl von OT-Assets, die eine interne und/oder externe Verbindung mit dem Unternehmensnetzwerk und dem Internet erfordern, um kritische Infrastrukturen am Laufen zu halten, die Effizienz zu optimieren und dem Unternehmen Einblicke und Informationen bereitzustellen. Einige Beispiele für OT-Assets sind industrielle Steuerungssysteme (ICS), Fernbedienungsterminals (RTUs), Prozessleitsysteme (PLS) und Geräte für das industrielle Internet der Dinge (IIoT). Diese Systeme wurden häufig nicht für den Fernzugriff entwickelt oder waren nicht für die Einbindung in IT-Netzwerke und -Praktiken vorgesehen.

Beispiele für OT-Assets

- Kritische intelligente Geräte und Maschinenkomponenten wie Sensoren, Ventilatoren, Pumpen, Schalter, Laser, Robotik, Schalldämpfer usw.
- Prozessleitsysteme (PLS)
- Industrielle Steuerungssysteme (ICS)
- Mensch-Maschine-Schnittstellen (HMI)
- Geräte für das Internet der Dinge (IoT) und das industrielle Internet der Dinge (IIoT)
- Speicherprogrammierbare Steuerungen (SPS)
- Fernbedienungsterminals (RTUs)
- Systeme zur Überwachung, Steuerung und Datenerfassung (SCADA)

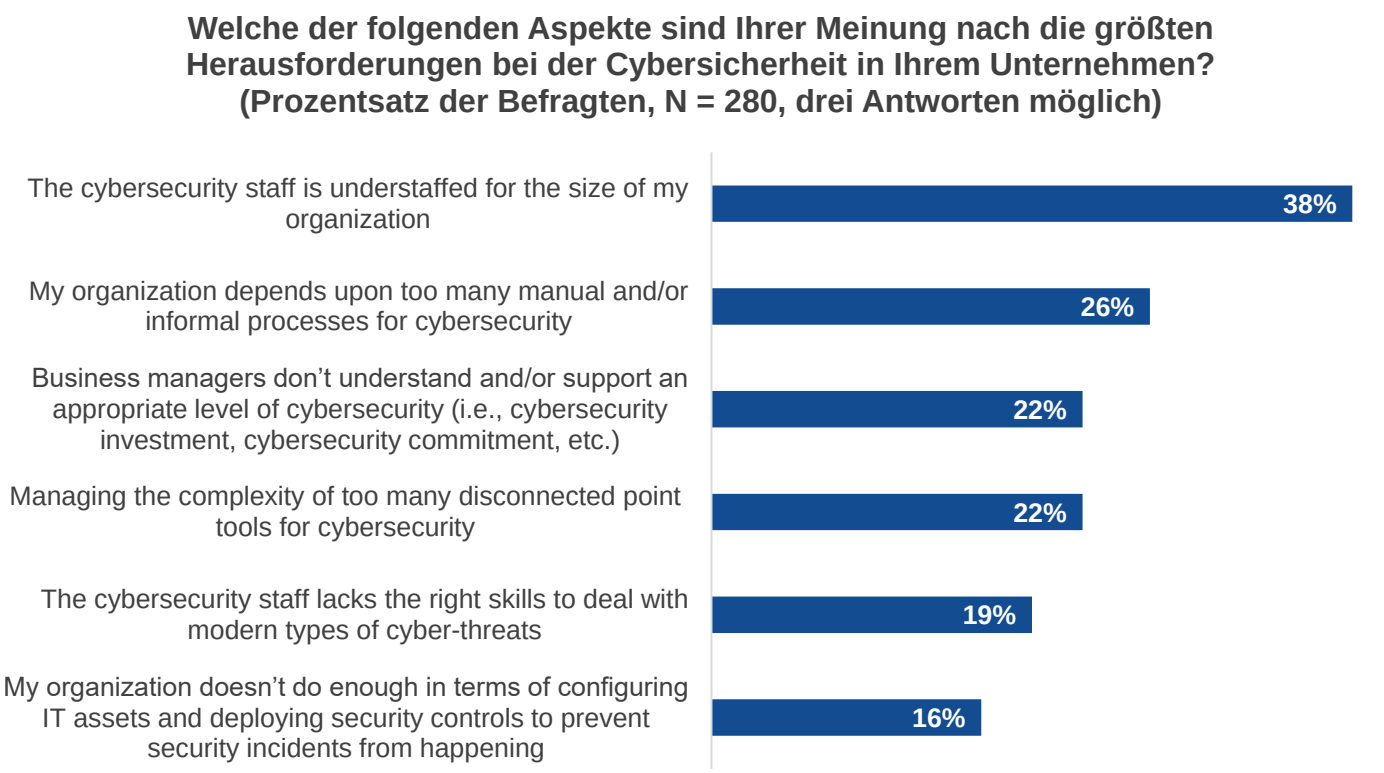
OT-Assets sind in der Regel sehr anfällig für Angriffe, da sie häufig nicht über integrierte Sicherheitsfeatures verfügen, ihre Funktionsweise nicht sichtbar ist und sie mit unverschlüsseltem Datenverkehr arbeiten. Sicherheit ist für die zentrale kritische Infrastruktur, die Fertigungs- und Industrieabläufe unterstützt, von entscheidender Bedeutung. Betroffene Abläufe können eine physische Bedrohung für die Mitarbeitenden darstellen, den Umsatz beeinträchtigen, Produktfehler verursachen oder kritische Services für Kunden beeinträchtigen. Erfolgreiche Angriffe auf Hersteller haben zu extremen finanziellen Schäden für Renault-Nissan (4 Mrd. US-Dollar), Norsk-Hydro (75 Mio. US-Dollar) und FACC AG (61 Mio. US-Dollar) geführt. Angriffe auf Industrieanlagen bei Colonial Pipeline, CPC Corp., Triton, dem ukrainischen Stromnetz und dem MUNI-Stadtbahnsystem in San Francisco verursachten Betriebsausfälle kritischer Anlagen, finanzielle Schäden und Gesundheitsrisiken. So riskant wie die Situation auch ist: Der IoT-Sicherheit wird generell noch zu wenig Priorität beigemessen. Das ist riskant, und Angreifer haben dies erkannt. Laut dem X-Force Threat Intelligence Index 2022 von IBM Security zielte fast jeder vierte Angriff in 2021 auf Fertigungsunternehmen ab, wobei die Ausnutzung von Schwachstellen der größte anfängliche Angriffspunkt im Fertigungsbereich ist.[1]

Angesichts der zunehmenden Vielfalt und Menge von OT- und IIoT-Assets stehen IT-Organisationen und Sicherheitsfunktionen unter Druck, solche kritischen Assets zu lokalisieren, zu identifizieren, zu managen, zu aktualisieren und abzusichern, die aus ihrer Sicht im Netzwerk einfach „auftauchen“, unabhängig davon,

[1] Quelle: IBM Security, *X-Force Threat Intelligence Index 2022*, Februar 2022.

ob ihre Präsenz beabsichtigt ist oder nicht. Warum haben IT-Abteilungen also Schwierigkeiten, OT-Umgebungen zu schützen? Laut einer Studie der Enterprise Strategy Group sind die größten Herausforderungen für Cybersicherheitsteams zu viele manuelle oder informelle Prozesse, die mangelnde Unterstützung durch die Unternehmensleitung, das komplexe Management, fehlende Kompetenzen und die Unfähigkeit, die erforderlichen Schritte zur Vermeidung von Sicherheitsvorfällen zu ergreifen.[2]

Abbildung 1. Die 6 größten Herausforderungen im Bereich Cybersicherheit



Quelle: Enterprise Strategy Group, ein Geschäftsbereich von TechTarget, Inc.

Sicherheitsteams benötigen eine Lösung, die eine effektive Visibilität von OT-Assets bietet. Sie benötigen eine Lösung, mit der sie die Vielzahl der spezifischen Assets in ihren industriellen Netzwerken besser identifizieren und kategorisieren, Bedrohungen und Schwachstellen schnell einschätzen, umfassende Zero-Trust-Richtlinien zum Schutz dieser Assets und des Netzwerks erstellen und automatisieren sowie bekannte und unbekannte Bedrohungen besser abwenden können.

Die Lösung: Industrial OT Security von Palo Alto Networks

Industrial OT Security von Palo Alto Networks bietet umfassende Zero-Trust-Sicherheit für OT-Assets und -Netzwerke und wurde speziell für Industrieunternehmen (Versorgungsunternehmen wie Strom, Öl, Gas usw.) und Fertigungsunternehmen (Automobil, Pharmazie, Lebensmittelverarbeitung usw.) entwickelt. Industrial OT Security bietet:

- **Umfassende Visibilität:** Die auf maschinellem Lernen gestützte, skalierbare Erkennung ermöglicht eine schnelle und genaue Asset-Bestandserfassung und Profilerstellung. Industrial OT Security erkennt und identifiziert alle IT-, IoT- und OT-Assets und -Protokolle. Mit mehr als 50 Attributen für jedes Asset,

[2] Quelle: Vollständige Ergebnisse der Enterprise-Strategy-Group-Umfrage, *ESG/ISSA Cybersecurity Process and Technology Survey*, Juni 2022

einschließlich Anbieter, Modell, Betriebssystem, Firmware, Seriennummer und Prozessbefehle, bietet Industrial OT Security einen umfassenden Asset-Kontext. Die cloudbasierte Management-Plattform bietet eine umfassende Visualisierung von OT-Assets, Risikobewertungen und Kommunikationsmustern in einer intuitiven Ansicht auf Basis des Purdue Model Framework für industrielle Steuerungssysteme und Cybersecurity-Segmentierung.

- **Zero-Trust-Sicherheit**: Die Lösung nutzt ML-basierte Visibilität, Kontextinformationen und Verhaltensprofiling aller IT-, IoT- und OT-Assets, um fein abgestimmte Richtlinienempfehlungen nach dem Prinzip der geringsten Berechtigungen und Segmentierung für OT-Assets nach Profil und kritischen Prozessen bereitzustellen, die in der NGFW mit einem einzigen Klick durchgesetzt werden können. Eine ordnungsgemäße Segmentierung von OT-Assets schützt anfällige OT-Assets und verbundene IT-Systeme vor potenziellen Bedrohungen. Industrial OT Security bewertet kontinuierlich die Identität, das Verhalten und das Risiko von Assets und stellt für jedes OT-Asset eine entsprechende Risikobewertung bereit. Die Risikobewertung berücksichtigt Schwachstellen, Bedrohungen, Anomalien, Veränderungen und Exploits von Assets. Diese kontinuierliche Sicherheitsprüfung trägt dazu bei, Zero-Day-Bedrohungen, unbekannte Bedrohungen und Anomalien im ICS-Prozess zu verhindern, davor zu warnen oder automatische Gegenmaßnahmen zu ergreifen, um die Integrität und Sicherheit zu gewährleisten sowie interne und branchenspezifische Compliance-Anforderungen wie IEC-62443 zu erfüllen.
- **Simplifizierter Betrieb:** Industrial OT Security nutzt die vorhandene Infrastruktur und stellt diese innerhalb weniger Minuten bereit, ohne dass zusätzliche Sensoren, eine Änderung der Infrastruktur oder zusätzliche Kosten erforderlich sind. Geräteinformationen können nativ mit anderen Tools wie Network Access Control (NAC), Security Information and Event Management (SIEM) und IT Service Management (ITSM)-Plattformen ohne intensive API-Integrationen weitergegeben werden.

Abbildung 2. Industrial OT Security von Palo Alto Networks

Quelle: Enterprise Strategy Group, ein Geschäftsbereich von TechTarget, Inc.

Wirtschaftliche Validierung der Enterprise Strategy Group

Enterprise Strategy Group (ESG) hat eine quantitative wirtschaftliche Analyse der Lösung Industrial OT Security von Palo Alto Networks durchgeführt. Der Fokus lag dabei insbesondere auf der Fähigkeit von Unternehmen, den Dienst zur Erkennung, Kategorisierung und zum Schutz von Assets zu nutzen – sowohl in ihren Fertigungs- als auch in ihren industriellen OT-Sicherheitsumgebungen. Der Prozess von ESG zur wirtschaftlichen Validierung ist eine bewährte Methode. Damit lassen sich die wirtschaftlichen Werteversprechen eines Produkts oder einer Lösung verstehen, validieren, quantifizieren und modellieren. Für den Prozess werden die Kernkompetenzen von ESG in den Bereichen Markt- und Branchenanalyse, zukunftsorientierte Forschung sowie technische und wirtschaftliche Validierung genutzt. ESG führte ausführliche Gespräche mit Endbenutzern, um die Herausforderungen und Erfahrungen, die Kunden in Bezug auf die Absicherung von OT-Assets hatten, besser zu verstehen und zu erfahren, auf welche Weise Industrial OT Security von Palo Alto Networks ihren Unternehmen Einsparungen und Vorteile bringt. Die qualitativen und quantitativen Ergebnisse wurden als Grundlage für ein konservatives Wirtschaftsmodell herangezogen, das die möglichen Einsparungen und Vorteile für ein Unternehmen verdeutlicht.

Wirtschaftlicher Überblick über Industrial OT Security von Palo Alto Networks

Unsere wirtschaftliche Analyse ergab, dass Industrial OT Security von Palo Alto Networks den Kunden erhebliche Einsparungen und Vorteile in den folgenden Bereichen bietet:

- **Schnellerer industrieller OT-Schutz**: Unternehmen brauchten weniger Zeit, um die Lösung bereitzustellen, Assets zu erkennen und zu kategorisieren und die Umgebung zu schützen als bei alternativen Lösungen.
- **Geringere betriebliche Komplexität**: Mit Industrial OT Security von Palo Alto Networks benötigten Sicherheitsteams weniger Aufwand für Bereitstellung, Management, Wartung, Schutz und Integration von Informationen als mit anderen Sicherheitslösungen.
- **Weniger Risiken für das Unternehmen**: Durch die schnellere Erkennung und Fehlerbehebung mit Industrial OT Security von Palo Alto Networks konnte das Gesamtrisiko des Unternehmens effektiv gesenkt werden.

Schnellerer industrieller OT-Schutz

Industrial OT Security von Palo Alto Networks ist ein Dienst, der einfach auf vorhandenen Firewalls der nächsten Generation (NGFWs) von Palo Alto Networks aktiviert werden kann. In Kombination mit intelligenten und automatisierten Funktionen und der immer besseren Unterstützung von OT-Umgebungen und -Assets können Unternehmen ihre OT-Umgebungen so schneller vor potenziellen Angriffen schützen. Industrial OT Security ermöglicht einen schnelleren Schutz durch:

- **Schnellere Bereitstellungen**: Kunden konnten die notwendige Zeit für die Planung, Vorbereitung und Installation ihrer OT-Sicherheitslösung im Vergleich zu alternativen Angeboten, die die Bereitstellung von Sensoren und separaten Softwareabonnements erforderten, minimieren. Industrial OT Security lässt sich in weniger als einer Stunde automatisch in der zentralen Panorama-Firewall-Sicherheitskonsole implementieren oder in unter vier Stunden manuell auf NGFWs aktivieren, während alternative Lösungen bis zu 15–20 Stunden für die Planung und Vorbereitung, die Bereitstellung von Sensoren und Software und die Konfiguration der Umgebung benötigen.

> **„Der Erfolg, den wir mit Lösungen von Palo Alto zur Sicherung unserer industriellen Netzwerke hatten, war der Grund, warum wir uns mit Industrial OT Security befassten. Wenn Sie bereits über die Infrastruktur verfügen, ist die Aktivierung der Cloud-Funktion von OT Security einfach.“**

- **Schnellere Erstellung von Richtlinien**: Laut Kunden begann Industrial OT Security sofort nach der Installation damit, den Datenverkehr zu überwachen und Assets passiv zu erkennen. Sobald die Lösung in die Tiefe und Breite der OT-Asset-Daten eingedrungen war, wurden automatisch Kategorien und Zero-Trust-Richtlinienempfehlungen erstellt. Dabei war vonseiten der Kunden wesentlich weniger Aufwand erforderlich als

bei alternativen Lösungen, bei denen die Erstellung von Richtlinien und ACLs (ohne Kenntnis der aus Verhaltensmustern gewonnenen Einblicke) für jede Kategorie und jedes Profil manuell erfolgen muss. Die erstmalige Erstellung von Asset-Profilen ging schnell. Zudem konnten die Kunden im Laufe der Zeit eine kontinuierliche Bewertung und Verbesserung feststellen. Mit der zunehmenden Fähigkeit von Industrial OT Security, mehr Informationen zu sammeln und mehr Datenverkehr zu überwachen, wurden die Geräteprofile und Richtlinienempfehlungen immer genauer. Ein Kunde sagte: „Industrial OT Security weist neu klassifizierte Profile automatisch zu und empfiehlt Richtlinien basierend auf den Daten, die die Lösung im Netzwerk sieht. Je mehr Datenverkehr, desto besser kann das Asset beurteilt werden.“ Richtlinien sind für den Schutz industrieller Umgebungen entscheidend, in denen das Patchen eines Assets zur Behebung einer Schwachstelle nicht möglich ist (weil eine Betriebsunterbrechung erforderlich ist oder kein Patch existiert). Richtlinien sind eine gute Möglichkeit, Gegenmaßnahmen zu implementieren, die das Risiko von Schwachstellen ohne Patchen verringern. Wenn neue Asset-Klassifizierungen freigegeben werden (z. B. ein neues Profil für eine feinere Untersegmentierung eines OT-Asset-Typs), ändert Industrial OT Security automatisch die zugehörigen Richtlinien, ohne dass manuelle Schritte erforderlich sind. So wird sichergestellt, dass die Profile und Richtlinien auf dem neuesten Stand und synchronisiert sind.

- **Schnellere Identifizierung und Behebung von Risiken**: Kunden gaben an, dass sie aufgrund der vollständigen Visibilität der Assets im Netzwerk besser aufgestellt waren, um potenzielle Bedrohungen für ihre OT-Assets zu identifizieren und zu beseitigen. Sie gaben ferner an, dass Industrial OT Security durch die Überwachung des Asset-Verhaltens und die Identifizierung ungewöhnlicher Verhaltensweisen eine kontinuierliche Risikobewertung für ihre OT-Assets bietet. Wenn bekannte Exploits erkannt wurden, konnte Industrial OT Security zusammen mit Threat Prevention durch entsprechende Maßnahmen in der NGFW einen besseren Schutz bereitstellen. Die Kunden wurden über mögliche Maßnahmen informiert, die ergriffen werden sollten. Kunden mit Abonnements für Threat Prevention von Palo Alto Networks konnten die Schritte weiter automatisieren und so die Zeit bis zur Fehlerbehebung verkürzen. Ein Kunde sagte: „In der Vergangenheit sind wir nicht gut damit zurechtgekommen, eine so große Vielfalt und Menge an Assets manuell aktiv zu prüfen, aber Industrial OT Security bietet dafür mit seiner passiven Überwachung ein besseres Tool.“

  „Wir hatten sofort nach der Implementierung von Industrial OT Security einen Überblick über unsere Assets und erhalten Warnmeldungen, wenn sich Muster oder Verhaltensweisen ändern.“

- **Schnellere Umsetzung von Compliance-Initiativen**: Industrial OT Security ermöglicht Kunden die einfache Erfüllung von Compliance-Anforderungen in Industrie und Fertigung, beispielsweise IEC 62443 oder NIST. Palo Alto wird sich auch weiterhin in diesem Bereich engagieren und die Unterstützung solcher Initiativen weiter ausbauen, um zukünftige Kundenanforderungen im Bereich Compliance sicherzustellen.

Geringere betriebliche Komplexität

Der Schutz von OT-Assets ist insbesondere in einer verteilten Umgebung eine komplexe Angelegenheit. Zentrale OT-Sicherheitsteams verfügen nur über eine sehr eingeschränkte Visibilität der Umgebung, und Assets können jederzeit durch lokale IT-Ressourcen, Anlagenmanagerinnen oder -manager oder sogar Anbieter hinzugefügt oder aus dem Netzwerk entfernt werden, wenn dies zulässig ist. Technologie-, Anlagenmanagerinnen und -manager vor Ort sowie Sicherheits- und Netzwerkteams müssen zusammenarbeiten, um Assets zu identifizieren, zu charakterisieren, zu kategorisieren, zu profilieren und zu schützen. In Umgebungen ohne dedizierte OT-Sicherheitslösung sind dafür viele Tools, Tabellen, Diskussionen und manuelle Prozesse erforderlich, die vielleicht nie erledigt werden. Dies führt zur Entstehung einer „Schatten-IT“: Mitarbeitende nehmen die Angelegenheit selbst in die Hand und fügen Geräte hinzu, installieren Software usw. ohne Beteiligung, Kontrolle oder kontinuierliche Überwachung der IT-Abteilung. Industrial OT Security verringert die betriebliche Komplexität bei der Bereitstellung von Sicherheit für OT-Umgebungen durch:

- **Simplifizierte Bereitstellung und Erkennung**: Industrial OT Security verfügt über mehrere Bereitstellungsarchitekturen, mit denen Kunden ihre OT-Umgebungen unabhängig von ihrer vorhandenen Netzwerkarchitektur schützen können. Industrial OT Security kann vorhandene NGFWs als Sensoren und zur Richtliniendurchsetzung nutzen. Palo Alto Networks verfügt außerdem für Industrial OT Security über Bereitstellungsarchitekturen für ältere, teilweise durch ein Air-Gap getrennte Umgebungen, moderne 5G-fähige Umgebungen und Kunden mit Secure Access Service Edge (z. B. Prisma Access). Industrial OT Security verwendet auch eine Kombination aus maschinellem Lernen, AppID-Technologie und nutzergenerierten Telemetriedaten, um automatisch ein Profil für alle Assets und Anwendungen zu erstellen, anstatt eine Klassifizierung durchführen oder Profillogik manuell erstellen zu müssen. Dieser manuelle Prozess kann in größeren Umgebungen Monate dauern und einen professionellen Service erfordern. Aus diesem Grund wird die Arbeit oft nicht vollständig ausgeführt, und die Assets bleiben ungeschützt. Darüber hinaus ändern sich Umgebungen im Laufe der Zeit, und Assets müssen kontinuierlich neu klassifiziert werden, um Änderungen in der Umgebung und Angriffsmethoden besser bewältigen zu können. Dies führt zu noch mehr Nacharbeit, die durch die kontinuierliche Bewertung und Klassifizierung von Industrial OT Security vermieden wird.

  „Die Klassifizierung von OT-Assets ist nicht einfach. Es geht um mehr als nur um die Frage nach der Asset-Kategorie. Es muss auch gefragt werden, was wichtig ist. So kann z. B. ein Temperatursensor, der an einem Ort vielleicht nicht wichtig ist, an einem anderen absolut unternehmenskritisch sein.“

- **Simplifiziertes Management**: Industrial OT Security bietet Kunden eine einzige Konsole und eine einheitliche Plattform zum Schutz aller Assets im Netzwerk (NGFW, Industrial OT Security und andere Dienste zur Sicherheitsprüfung), wodurch das Management und die Überwachung von OT-Assets und -Richtlinien wesentlich einfacher werden. Die cloudbasierte SaaS-Plattform erfordert keine Wartung und eine sehr geringe Einschulung. Kunden können die Verteilung herkömmlicher IT-, Netzwerk-, Betriebs- und industrieller OT-Assets leicht erkennen und die Details der einzelnen Assets einsehen, um mehr über Asset-Profile, verwendete Anwendungen (wobei Anwendung hier dem Netzwerkprotokoll entspricht, z. B. HTTP, BACnet usw.), Netzwerksegmentierung und Risikobewertung zu erfahren, um die Umgebung einfacher managen und Assets absichern zu können.

  „Wir profitieren vielseitig, weil Palo Alto Networks weiterhin neue Funktionalitäten für die Systeme hinzufügt, um unsere Arbeit zu erleichtern. Wenn es Lücken oder Bereiche gibt, die verbessert werden müssen, arbeiten sie sehr gut mit der Community zusammen, um diese zu identifizieren.“

- **Wert der Automatisierung**: Industrial OT Security ermöglicht eine Automatisierung und ein Erlangen von Erkenntnissen und hilft so, die Zeit zu verringern, die Teams normalerweise für die Durchführung der manuellen Aufgaben benötigen, die bei alternativen Lösungen erforderlich sind. Ganz gleich, ob es sich um die Erstellung von Richtlinien, die Generierung von Zertifikaten, die Planung oder die Prüfung auf oder Behebung von Schwachstellen handelt: Die Teams berichteten von einer erheblichen Zeiteinsparung aufgrund des hohen Automatisierungsgrads. Die automatisierte Zero-Trust-Sicherheit von Palo Alto Networks berücksichtigt Benutzende, Assets und den Kontext von Anfragen anhand einer intelligenten Risikobewertung, bevor der Zugriff anhand automatisierter Richtlinien zur Durchsetzung der Segmentierung ermöglicht wird, was einen bis zu 20-fachen Arbeitsaufwand einspart.

- **Simplifizierte Integration mit anderen Produkten und Diensten**: Industrial OT Security bietet eine einheitliche Plattform, die einfach in die Firewall und andere IT- und Sicherheitsprodukte integriert werden kann. Kunden konnten Workflows automatisieren und Industrial OT Security in ihre vorhandenen Tools und Prozesse (wie Asset Management, Security Incident and Event Management [SIEM] und Work Order Management) integrieren, um Netzwerkzugriffskontrollen, verbesserte Visibilität, Bedrohungsschutz und sogar Fehlerbehebungen zu gewährleisten (sofern für den Threat-Prevention-Dienst von Palo Alto Networks lizenziert). Die Automatisierung und Orchestrierung durch diese Integrationen spart Unternehmen nicht nur wertvolle Ressourcen, sondern maximiert auch den Wert ihrer Investitionen, optimiert die Abläufe und hilft, das Risiko manueller Fehler zu vermeiden.

„Alleine um die Zertifikate und Profile für unsere 5.000 Assets zu erstellen, hätten wir einen professionellen Service und viele Monate Zeit benötigt, und dann müssten wir das ja auch in Zukunft aufrechterhalten.“

Geringeres Risiko für OT-Umgebungen

Da Industrie- und Fertigungsbetriebe das Ziel von fast einem Viertel aller Cyberangriffe sind und mehr OT-Assets für eine umfassende Funktionalität und Updates einen Netzwerkzugriff benötigen, müssen Unternehmen gewissenhafter denn je handeln, um die Risiken für diese Umgebungen zu senken. Industrial OT Security senkt Risiken durch:

„Ich habe viele Alternativen zu Palo Alto Networks getestet, aber diese Lösungen können mir nur sagen, welche Art von Anlagen ich habe und welche Schwachstellen möglicherweise für diese Anlagenklasse bestehen, und nicht, ob dies tatsächlich ein Problem für mein spezifisches Gerät darstellt oder nicht.“

- **Geringeres Risiko erfolgreicher Sicherheitsverletzungen**: Kunden berichteten, dass Industrial OT Security ihre OT-Assets schneller und besser geschützt und dazu beigetragen hat, das Potenzial für erfolgreiche Sicherheitsverletzungen und Angriffe zu minimieren. Kunden konnten eine größere Vielfalt von OT-Assets automatisch identifizieren und schützen und für diese Assets Zero-Trust-Richtlinien anwenden und durchsetzen. Die Kunden gaben auch an, dass andere OT-Sicherheitsprodukte, die sie in Betracht gezogen hatten, so konzipiert waren, dass sie auf verdächtige Aktivitäten aufmerksam machen, aber keine sofortigen Maßnahmen ergreifen, um die Risiken zu mindern (z. B. die Bedrohungsabwehr oder das Durchsetzen der Netzwerksegmentierung nach der Erkennung wie bei Industrial OT Security). Darüber hinaus verbessert Palo Alto Networks die Effektivität durch die Verwendung nutzergenerierter Bedrohungsinformationen, um das Wissen über Zero-Day-Bedrohungen speziell für industrielle OT-Assets kontinuierlich zu verbessern. Ohne Industrial OT Security blieben viele Assets einfach unentdeckt, ungeprüft und anfällig.
- **Mehr Visibilität und Informationen**: Industrial OT Security bietet eine intuitive Bedienoberfläche mit leistungsstarker Visualisierung, die auf Informationen entsprechend den Attributsebenen des Purdue-Modells basiert, um industrielle Steuerungssysteme von Unternehmensnetzwerken und dem Internet zu segmentieren. Die Benutzenden erhalten einen Asset-Kontext und können das Asset- und Netzwerkverhalten und die Netzwerksegmentierung visualisieren, um sicherzustellen, dass die aktuelle Implementierung den aktuellen Richtlinien, Standards und Best Practices entspricht. Die Oberfläche von Industrial OT Security ermöglicht Visibilität von Netzwerken, Geräten und Anwendungen, bietet Kunden aktuelle und kontinuierliche Risikobewertungen und überwacht den Netzwerkdatenverkehr, um die Empfehlungen und Durchsetzung von KI- und ML-gestützten Richtlinien besser zu unterstützen. Die Kunden waren der Meinung, dass dieser Grad an Visibilität und Informationen mit den Ressourcen, die ihre Teams zur Verfügung hatten, einfach nicht möglich wäre.

„Ohne Industrial OT Security würden wir nicht wissen, ob ein Asset vorhanden ist, richtig konfiguriert wurde oder sich seltsam verhält.“

- **Geringeres Risiko von Konformitätsverstößen**: Industrie- und Fertigungsunternehmen müssen Sicherheitsrichtlinien einhalten und die Anforderungen an die Datenresidenz durchsetzen (z. B. IEC, ISO, NIST und DSGVO). Die Kunden, mit denen wir gesprochen haben, waren nicht nur der Meinung, dass sie mehr Visibilität und Schutz erhielten, sondern fanden Industrial OT Security von Palo Alto Networks auch äußerst hilfreich bei der Sicherstellung der globalen Konformität bei regionalen Unterschieden in Bezug auf Hersteller von OT-Assets, Technologien und Governance-Regeln. Industrial OT Security war auch äußerst wertvoll für die Durchsetzung und den Schutz der Integrität bestehender OT-Prozesse. Industrial OT Security kann verwendet werden, um zu erkennen, wann kritische Assets offline gehen, und um ungewöhnliche Datenverkehrsmuster oder Werte außerhalb des zulässigen Bereichs (z. B. hohe Temperaturwerte) bei Assets zu identifizieren. Mithilfe einer Rule Engine können dann Trigger angepasst und Warnungen und automatisierte Benachrichtigungen generiert oder Informationen an Integrationen von Drittanbietern zur Durchführung automatisierter Maßnahmen übermittelt werden.
- **Geringeres Risiko von Betriebsunterbrechungen und Nichtverfügbarkeiten**: Für Industrie- und Fertigungsbetriebe ist die Verfügbarkeit von Assets für die Umsatzgenerierung und die Bereitstellung kritischer Dienste entscheidend. Durch einen besseren Schutz von OT-Assets und die Reduzierung der Risiken erfolgreicher Angriffe waren durch Industrial OT Security geschützte Unternehmen der Ansicht, dass sie besser aufgestellt sind, um Betriebsunterbrechungen zu vermeiden. Industrial OT Security von Palo Alto Networks kann Risiken erkennen und beseitigen, die sonst vielleicht unentdeckt bleiben und Angriffe oder Ransomware-Attacken nach sich ziehen würden, die den Betrieb zum Stillstand bringen können. Bei manchen Produkten, die nicht speziell für OT entwickelt wurden, kann die aktive Prüfung von OT-Umgebungen zu Problemen bei Assets führen und kritische Geschäftsprozesse stören. Dies kann unbeabsichtigte Betriebsunterbrechung verursachen (ein Risiko, das durch die passive Protokollerfassung von Industrial OT Security anstelle von Prüfungen vermieden wird). Durch das Zulassen sicherer und vertrauenswürdiger Funktionen für OT-Assets im Netzwerk und das Blockieren aller anderen Ressourcen können diese Assets Firmware von einer vertrauenswürdigen Quelle herunterladen und sicher aktualisieren oder Telemetriedaten mit zugelassenen Cloud-Services teilen. Dadurch, dass Assets auf dem neuesten Stand sind und mit wichtigen Diensten verbunden bleiben, können nachgelagerte Sicherheits- und Betriebsprobleme, die zu Betriebsunterbrechungen führen können, besser vermieden werden.
- **Vermeidung der Risikos von Personenschäden und Markenschäden**: Industrielle Betriebsnetzwerke müssen die Risiken berücksichtigen, die sie für die Gesundheit und Sicherheit von Menschen darstellen: Ein böswilliger Zugriff kann zu Fehlfunktionen von Systemen oder Maschinen führen, die Ausrüstung beschädigen oder gefährliche Änderungen am Fertigungsprozess verursachen können, was wiederum zu Problemen mit der Produktqualität führen kann, was für Menschen unter Umständen schädlich ist. Auch wenn es weniger wahrscheinlich ist, kann ein fehlender Schutz sogar zu einer physischen Gefahr für die Mitarbeitenden führen (z. B. wenn eine Maschine während des Betriebs abgeschaltet oder gestoppt wird oder wenn der Betrieb von Steuerungssensoren oder Temperaturregelungen beeinträchtigt ist).

„Lieferanten und Hersteller können Schwachstellen nicht besonders gut erkennen. Stattdessen werden sie von Sicherheitsforscherinnen und -forschern aufgedeckt. Das ist nicht akzeptabel. Ein Ausfall unserer Produktionsanlagen würde Millionen von Dollar an entgangenen Produktionseinnahmen, Reputationsschäden, den möglichen Verlust von geistigem Eigentum sowie Aufräumarbeiten nach sich ziehen.“

Analyse der Enterprise Strategy Group

Zwecks Erstellung eines Fünf-Jahres-Modells für TCO/ROI hat die Enterprise Strategy Group (ESG) die Informationen herangezogen, die aus vom Anbieter bereitgestellten Materialien, öffentlichen und branchenspezifischen Kenntnissen sowie Kundeninterviews erhoben wurden, sowie die Ergebnisse der technischen und wirtschaftlichen Validierung. Mit dem Modell wurden die Kosten und Vorteile des Schutzes von OT-Umgebungen mit Industrial OT Security von Palo Alto Networks anstelle einer alternativen Lösung verglichen, die auf der Bereitstellung von Sensoren in Verbindung mit einem Abonnement einer industriellen OT-Sicherheitslösung basiert. Zur Grundlage unseres modellierten Szenarios beigetragen haben ESG-Befragungen von Kunden, die kürzlich die Technologie implementiert haben, sowie unsere Erfahrung und Expertise in der wirtschaftlichen Modellierung und der technischen Validierung von Palo Alto Networks und alternativen Technologien.

Unser Modell ging davon aus, dass ein mittelständisches Fertigungsunternehmen acht globale Produktionsstandorte mit jeweils verschiedenen Gebäuden und Betriebsanlagen betreibt. Wir gingen von durchschnittlich fünf Firewalls von Palo Alto Networks an jedem verteilten Standort aus, also insgesamt 40 NGFWs, mit anfänglich durchschnittlich 100 Assets pro Firewall, sodass insgesamt 4.000 OT- und IoT-Assets zu managen waren. Wir unterstellen zudem eine Wachstumsrate von 5 %, sodass bis zum Ende des fünften Jahres 862 neue Assets in die Netzwerke aufgenommen wurden und die Asset-Zahl 4.862 betrug. Obwohl die Anzahl in der Praxis variiert, gingen wir von durchschnittlich 50 Assets pro eindeutiger Profilklasse aus, sodass die Assets bei Bereitstellung von Industrial OT Security in 80 Profile kategorisiert wurden. Diese Zahl stieg aufgrund der Bereitstellung und Profilerstellung zusätzlicher Assets bis zum Ende des fünften Jahres auf 97.

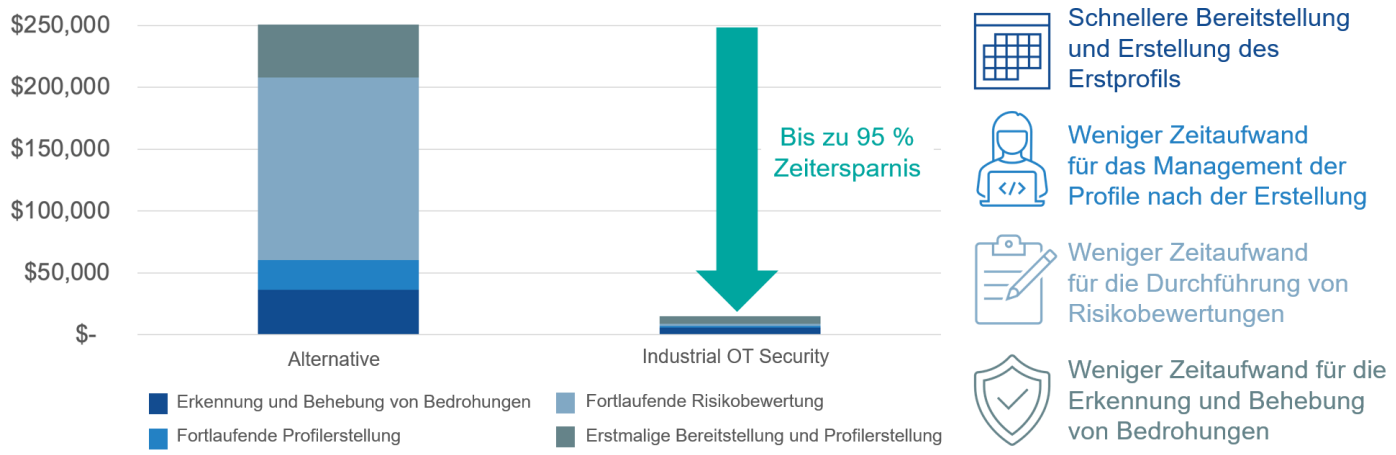
Bedeutung

Wenn Sie OT-Sicherheitslösungen in Betracht ziehen und vergleichen, ist es wichtig, mehr als nur die Kosten für die Lösung zu berücksichtigen.

Unternehmen sollten auch den für die Bereitstellung und den Schutz erforderlichen Zeitaufwand, die durch Automatisierung erzielten Einsparungen bei den Betriebskosten und die durch eine schnellere und effektivere Absicherung und Fehlerbehebung eingesparten Kosten berücksichtigen. Die risikobezogenen Zahlen sind zwar schwer vorherzusagen und zu erfassen, doch ein einziges Ereignis kann dem Unternehmen ein echtes finanzielles Problem bescheren.

Als Nächstes modellierten wir die für die Planung und Bereitstellung der OT-Sicherheitslösungen erforderlichen erwarteten Personenstunden. Wir gingen davon aus, dass Industrial OT Security pro Firewall in etwa 1 Stunde und 15 Minuten aktiviert werden könnte, während die alternative sensorbasierte Lösung durchschnittlich 3,5 Stunden pro Sensor beanspruchen würde (unter der Annahme eines Sensors für jede Firewall). Anschließend modellierten wir die Zeit für die Erstellung der Erstprofile für die Lösung mit 15 Minuten pro Profil für Palo Alto Networks und 5 Stunden manueller Erstellungszeit für die alternative Lösung. Wir verwendeten ähnliche Modelle, um die Zeit für die Durchführung kontinuierlicher Risikobewertungen (automatisiert bei Palo Alto Networks im Vergleich zu 30 Minuten für manuelle Prüfungen pro Asset bei der Alternativlösung), die Zeit für die Bewertung und Behebung von Risiken (15 Minuten pro Profil im Vergleich zu 10 Stunden pro Profil) und die Zeit für die Identifizierung und Behebung von Bedrohungen aufzuzeigen (unter der Annahme, dass 85 % der Bedrohungen mit Palo Alto Networks vermieden werden könnten und die Beseitigung einer Bedrohung durchschnittlich 2 Stunden in Anspruch nimmt). Die in Abbildung 3 dargestellten Ergebnisse prognostizieren die Betriebskosten, die für die Industrial-OT-Sicherheitslösung von Palo Alto Networks um bis zu 95 % niedriger sind, wodurch das modellierte Unternehmen über einen Zeitraum von fünf Jahren 235.000 US-Dollar an Betriebsausgaben einspart.

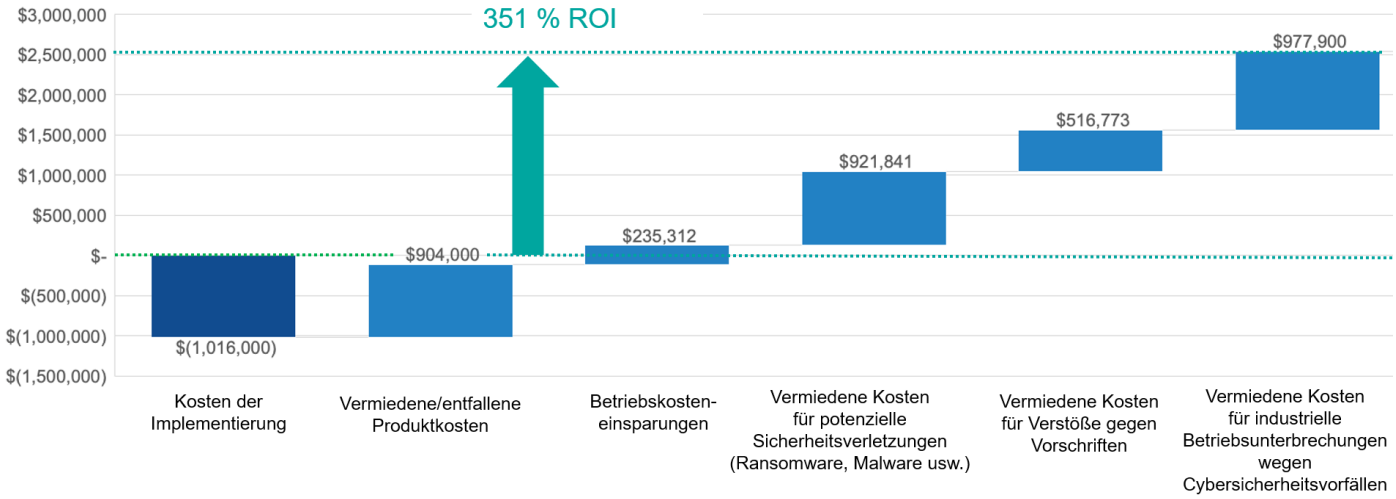
Abbildung 3. Erwartete Personenstunden für die Bereitstellung und den Betrieb von OT-Sicherheitslösungen



Quelle: Enterprise Strategy Group, ein Geschäftsbereich von TechTarget, Inc.

ESG führte anschließend eine einfache Kostenanalyse der Lösungen durch und nutzte unsere proprietären Modelle zusammen mit nach bestem Wissen und Gewissen getroffenen konservativen Annahmen, um die Einsparungen und Vorteile vorherzusagen, die sich aus den vermiedenen Kosten für die Lösung, den Betriebskosten und den vermiedenen Risiken für potenzielle Sicherheitsverletzungen, Compliance-Verstöße und mögliche Betriebsunterbrechungen ergeben können. Ein Vergleich der Ergebnisse mit der Investition in das Abonnement für Industrial OT Security von Palo Alto Networks ergibt sich über fünf Jahre ein erwarteter Return on Investment (ROI) von 351 %. Die Ergebnisse sind in Abbildung 4 dargestellt und werden im folgenden Abschnitt erläutert.

Abbildung 4. Erwartete Einsparungen und Vorteile über fünf Jahre für das modellierte Unternehmen



Quelle: Enterprise Strategy Group, ein Geschäftsbereich von TechTarget, Inc.

Bedeutung der Zahlen:

- **Implementierungskosten:** Enterprise Strategy Group (ESG) modellierte die erwarteten Kosten für die Lösung von Palo Alto Networks (Industrial OT Security-Abonnement) und eine alternative Lösung (Investitionskosten für Hardwaresensoren und Betriebskosten für die Sicherheitslösung). Es wurde versucht, anhand der Anzahl der Firewalls, der max. benötigten Assets und ähnlicher Bandbreitenbegrenzungen zu gewährleisten, dass in größtmöglichem Umfang Gleiches mit Gleichem verglichen wird. Unsere Kostenanalyse enthielt nicht die Kosten für die NGFWs. Wir haben unterstellt, dass diese bereits beim Kunden vorhanden sind und in beiden Fällen verwendet werden. Es ist zu beachten, dass die Preise je nach Firewall-Modell und anderen Anforderungen erheblich variieren können.
- **Vermiedene/entfallene Produktkosten:** Für einen ROI-Vergleich wird die Differenz der erwarteten Kosten für die Lösung über den Gesamtzeitraum von fünf Jahren als vermiedene Kosten dargestellt. Dies sind also die Kosten, die durch die Wahl der kostengünstigeren Lösung anstelle der Alternativlösung vermieden werden konnten. Bei einem TCO-Vergleich würde sich dieser Unterschied einfach als geringere Kosten für die Lösung zeigen. Auch wenn sie nicht in dieser Analyse enthalten sind, sollte beachtet werden, dass die Investitionsausgaben (CapEx) vorab im Jahr 1 anfallen würden, was finanzielle Ressourcen bindet und zu etwas höheren Einsparungen führt, da ein höherer Kapitalwert für die Vorabinvestition berechnet wurde.
- **Betriebskosteneinsparungen:** Dies sind die Einsparungen bei den Betriebskosten oder den erwarteten Personalstunden, die für den Betrieb der beiden im vorherigen Abschnitt beschriebenen und in Abbildung 3 dieses Berichts dargestellten OT-Sicherheitslösungen erforderlich sind. Es ist zu beachten, dass beide Lösungen den Unternehmen Zeit sparen, da sie die Arbeiten nicht mehr manuell durchführen und versuchen müssen, die Lösung mit eigenen Tools oder mit Tools zu entwickeln, die nicht auf OT ausgelegt sind. Dies liegt zwar nicht im Fokus dieses Berichts, würde jedoch deutlich höhere Einsparungen bedeuten.
- **Vermiedene Kosten für mögliche Sicherheitsverletzungen:** Mit den proprietären Modellen von ESG wurden das erwartete vermiedene Risiko und die vermiedenen Kosten einer Sicherheitsverletzung bei einem Industrieunternehmen berechnet. In unseren Modellen wurden die erwarteten Kosten einer erfolgreichen Datenschutzverletzung (basierend auf Daten von IBM und dem Ponemon Institute[3]) für Industrieunternehmen mit ca. 4,47 Mio. US-Dollar angesetzt (Kosten für Benachrichtigung, Reaktion, Erkennung, Eskalation und Auswirkungen auf das Unternehmen). Unter Verwendung eigener individueller Annahmen von ESG zum Risiko einer Datenschutzverletzung in einem bestimmten Jahr für die alternative Lösung und der Reduzierung dieses Risikos durch Palo Alto Networks gingen wir davon aus, dass die alternative Lösung das Risiko um 40 % senken könnte und dass die Lösung von Palo Alto Networks das Risiko um weitere 20 % gegenüber der alternativen Lösung reduziert. Diese Annahme basierte auf der erwarteten Differenz bei der Zeit bis zum Einsetzen des Schutzes. Bei der Alternativlösung blieben die Assets aufgrund der manuellen Profilerstellung, der Zeit und des Aufwands für die Prüfung und der längeren Fehlerbehebungszyklen im Netzwerk gefährdet. Unsere risikogewichtete Analyse ergab, dass die Industrial-OT-Sicherheitslösung von Palo Alto Networks über fünf Jahre im Vergleich zur alternativen Lösung das erwartete Risiko in Höhe von ca. 921.000 US-Dollar und im Vergleich zu einer nicht vorhandenen OT-Sicherheitslösung in Höhe von mehr als 3,9 Mio. US-Dollar vermeiden könnte.
- **Vermiedene Kosten für Compliance-Verstöße:** Um die Einhaltung von Unternehmens-, Branchen- und sogar behördlichen Zielvorgaben und Vorschriften zu gewährleisten, müssen IT-Teams in der Lage sein, OT-Assets genau zu inventarisieren und zu aktualisieren, ihre ordnungsgemäße Funktionalität sicherzustellen und sie anschließend zu schützen. Wenn Unternehmen die Vorschriften nicht einhalten, riskieren sie Kosten für Audits, Bereinigungsarbeiten, Beeinträchtigungen der Produktivität und potenzielle Geldstrafen. Unter Verwendung eines ähnlichen proprietären Modells und ähnlicher Annahmen gingen wir davon aus, dass das Risiko für Verstöße gegen die Vorschriften beseitigt wird, sobald für alle Assets ein Profil erstellt wurde und die Risikobewertungen auf dem neuesten Stand sind. Anhand unserer betrieblichen Berechnungen haben wir eine Reduzierung des Compliance-Risikos von 18 % für Industrial OT Security von Palo Alto Networks gegenüber der alternativen Lösung festgestellt, was im Fünfjahreszeitraum zu Einsparungen bei der Risikovermeidung in Höhe von 516.000 US-Dollar führte.

[3] Quelle: IBM, *Cost of a data breach 2022*.

- **Vermiedene Kosten für industrielle Betriebsunterbrechungen wegen Cybersicherheitsvorfällen:** Unsere Modelle gehen anhand der Informationen aus veröffentlichten Berichten konservativ geschätzt davon aus, dass eine typische Betriebsunterbrechung bei einem Industrie- oder Fertigungsunternehmen 4 Stunden dauern und etwas mehr als 2 Mio. US-Dollar an Geschäftseinbußen, Produktivitätseinbußen und Gefahren von Personenschäden verursachen würde. Aufgrund des Risikos einer Betriebsunterbrechung durch Cyberkriminalität (laut Ponemon Institute 22 % aller Betriebsunterbrechungen) und aufgrund des erwarteten besseren Abschneidens von Industrial OT Security von Palo Alto Networks gegenüber der alternativen Lösung um 20 % prognostizieren unsere Modelle für einen Zeitraum von fünf Jahren Einsparungen in Höhe von 977.000 US-Dollar, da das Risiko potenzieller Auswirkungen auf den Betrieb reduziert wird.

Zu berücksichtigende Probleme

Unsere Modelle gehen nach bestem Wissen und Gewissen von konservativen, glaubwürdigen und validierten Annahmen aus. Kein modelliertes Szenario wird jedoch jemals jede mögliche Situation abbilden können. Industrial OT Security von Palo Alto Networks bietet Unternehmen erhebliche Vorteile und Mehrwert, insbesondere wenn ein Unternehmen bereits Kunde von Palo Alto Networks ist. Enterprise Strategy Group empfiehlt, dass Sie Ihre eigene Analyse der verfügbaren Produkte durchführen und sich mit Ihrer Palo Alto Networks-Vertretung in Verbindung setzen, um die Unterschiede zwischen den Lösungen durch eigene Machbarkeitsstudien zu verstehen und zu erörtern.

Fazit

Industrie- und Fertigungsnetzwerke bilden das Rückgrat für Fertigung, Produktion und wichtige Versorgungsfunktionen. Obwohl sie in der Vergangenheit von Unternehmensnetzwerken und mit dem Internet verbundenen Assets isoliert waren, besteht heutzutage ein immer größerer Druck, diese kritischen Anwendungen, Systeme und Assets mit dem Internet zu verbinden. Dies soll unter anderem die moderne Datenerfassung und -analyse erleichtern, die Aktualisierung und Überwachung wichtiger Komponenten sicherstellen und einen zentralisierten Zugriff ermöglichen. Diese Netzwerke sind jedoch aufgrund der Vielzahl von Assets und Technologien und der allgemein mangelnden Visibilität schwer zu schützen. Cyberkriminelle haben diese Herausforderung erkannt, und in Kombination mit den potenziellen Vorteilen eines erfolgreichen Angriffs (Auswirkungen auf den Umsatz, Schädigung der Marke, großflächige Unterbrechung von Betriebsmitteln) stellt die industrielle OT das perfekte Ziel dar.

„Um unseren derzeitigen Mangel an OT-Sicherheit zu demonstrieren, ging ich mit meinem Laptop in das Gebäude, konnte mich direkt mit einem System verbinden und innerhalb von 10 Minuten zeigen, dass jede beliebige Person unsere Geräte kontrollieren und potenzielle Schäden anrichten könnte. Das war extrem lehrreich und hat allen die Wichtigkeit der Situation vor Augen geführt.“

Enterprise Strategy Group (ESG) hat in einer Reihe von Interviews bestätigt, dass Kunden Industrial OT Security von Palo Alto Networks nutzen konnten, um ihre OT-Assets besser zu verwalten, abzusichern und zu schützen und gleichzeitig einen sicheren Zugang zu Assets und Diensten zu ermöglichen, was für moderne Unternehmen notwendig ist. Dank der integrierten Funktionen für Automatisierung, Orchestrierung und Informationsbeschaffung konnte eine kürzere Time-to-Value erreicht, die Komplexität der betrieblichen Abläufe verringert und das Risiko für das Unternehmen erheblich reduziert werden. Unsere Modelle gehen davon aus, dass Unternehmen durch den Einsatz von Industrial OT Security anstelle einer alternativen Lösung einen konservativen geschätzten ROI von 351 % erzielen und gleichzeitig die Kosten für das Management der Lösung um bis zu 95 % senken können.

„OT-Sicherheit ist komplex. Viele Unternehmen haben gute Strategien in Folien dargestellt, aber wenn man sich tatsächlich vor Ort im Werk umschaut, sind sie noch weit davon entfernt, die Technologie in die Praxis umzusetzen.“

OT-Sicherheit ist sicherlich komplex, und Unternehmen wissen, dass es keine einzige schlüsselfertige Lösung gibt, die sie sofort einsetzen können, um alle ihre Anforderungen für alte, aktuelle und zukünftige Assets zu erfüllen. Dies gilt insbesondere für extrem große und globale Unternehmen, in denen es vielfältige, sehr spezialisierte und regional unterschiedliche OT-Assets geben kann. Die Unternehmen sind sich jedoch einig, dass Industrial OT Security die beste verfügbare Lösung ist, und vertrauen darauf, dass Palo Alto Networks der richtige Partner für die Zukunft ist.

„Ich habe mir vielleicht zehn Anbieter für OT-Sicherheit angesehen, und bisher kann niemand genau die Funktionen bereitstellen, die ich aktuell an allen Standorten benötige. Sie müssen den Partner auswählen, der am besten zu Ihrer Vision passt und bestrebt ist, dorthin zu gelangen.“

„Palo Alto ist wahrscheinlich die beste Firewall der Welt. Mit Industrial OT Security verfügen sie über eine Vision und ein Ziel, die unseren Anforderungen entsprechen. Mitbewerber denken nicht über den Tellerrand hinaus, nutzen keine KI und betrachten noch nicht einmal OT-Organisationen global.“

Wenn Ihr Unternehmen das Risiko für Ihre industrielle OT-Umgebung verringern und gleichzeitig den Betrieb simplifizieren und sichere Zero-Trust-Richtlinien für OT-Assets in einer modernen, vernetzten, aber gefährlichen Welt durchsetzen möchte, empfiehlt Ihnen ESG dringend, Industrial OT Security von Palo Alto Networks in Betracht zu ziehen.

Über die Enterprise Strategy Group
Die Enterprise Strategy Group ist ein integriertes Unternehmen für Technologieanalyse, Forschung und Strategie, das der globalen IT-Community Marktinformationen, umsetzbare Erkenntnisse und marktdienliche Inhaltsservices bietet. © TechTarget 2023.

contact@esg-global.com
www.esg-global.com