Der richtige Zero-Trust-Ansatz für IoT-Geräte

Inhalt

Einleitung

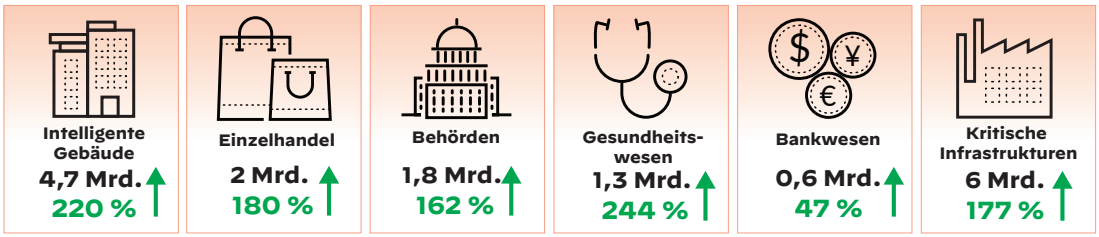
In der Vergangenheit installierten Netzwerk- und Sicherheitsteams Sicherheitsfunktionen am Netzwerkperimeter, um das gesamte Unternehmen zu schützen. Das interne Netzwerk betrachteten sie dabei als vertrauenswürdig und sicher. Alles, was sich außerhalb des Perimeters befand, wurde als potenziell gefährlich und alles im internen Netzwerk als harmlos eingestuft. Daher wurde dort der Anwendungsdatenverkehr auch nicht eingeschränkt. Doch in der letzten Zeit haben viele Unternehmen neue Arbeitsmodelle eingeführt – mit weitreichenden Folgen für die Sicherheit am traditionell verwalteten Netzwerkperimeter.

Die folgenden Trends haben bei Unternehmen zu einem Umdenken in puncto Sicherheit beigetragen:

- **Digitale Transformation:** Es werden immer mehr IoT-Geräte genutzt, um den Mehrwert und die Produktivität zu steigern und die Kosten zu reduzieren.
- **Cloud-Migration:** Immer mehr Geräte, sowohl verwaltete als auch nicht verwaltete, senden Daten in die Cloud oder Multi-Cloud.
- **Hybrides Arbeiten:** Die Beschäftigten können sich nun von beliebigen Orten aus im Unternehmensnetzwerk anmelden und öffnen externen Bedrohungen damit eventuell Tür und Tor.

Der konventionelle Netzwerkperimeter ist nicht mehr die Vertrauensgrenze. Das beweist auch die zunehmende Anzahl an Cyberbedrohungen und Cyberangriffen auf Unternehmen. Auf moderne Unternehmensnetzwerke greifen inzwischen zahlreiche unterschiedliche Geräte zu – von konventioneller IT-Ausrüstung bis zu neuartigen internetfähigen Geräten, die ebenfalls mit dem Netzwerk verbunden sind. Dazu gehören Überwachungskameras, Heizungs- und Klimaanlagen, intelligente Beleuchtung, intelligente Rollladensysteme, Infusionspumpen, Drucker, smarte Kaffeemaschinen, Smart-TV-Geräte, virtuelle Assistenten, Geldautomaten und Kassenterminals. Unter anderem diese Geräte bilden das sogenannte Internet der Dinge (Internet of Things, IoT). Dadurch wächst nicht nur die Angriffsfläche, sondern das Netzwerk wird auch anfälliger für die interne Ausbreitung von Angreifern und Bedrohungen, denn letztendlich ist jede Kette nur so stark wie ihr schwächstes Glied.

Laut dem IoT Threat Report 2020 der Unit 42 von Palo Alto Networks, für den 1,2 Millionen Endpunkte analysiert wurden, machten IoT-Geräte im Jahr 2020 30 % aller Unternehmensgeräte aus. Die Machina-IoT-Datenbank von Gartner prognostiziert zudem, dass die Anzahl der IoT-Geräte von 2020 bis 2030 mit einer durchschnittlichen jährlichen Wachstumsrate (CAGR) von etwa 13 % steigen wird.



10 Mio. neue IoT-Geräte pro Tag im Netzwerk*

Über 30 % der Unternehmensgeräte sind IoT-Geräte.*

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

Abbildung 1: Geschätztes IoT-Wachstum nach Branche (laut der Machina-Datenbank von Gartner)

Die starke Zunahme der IoT-Geräte gibt Grund zur Sorge, denn diese Geräte werden häufig mit Sicherheitslücken ausgeliefert, sind schwer zu patchen und verfügen nicht über adäquate Sicherheitsfunktionen, haben aber dennoch unkontrollierten Zugriff auf das Netzwerk. Nachfolgend finden Sie einige Zahlen zu kürzlich erfolgten Angriffen auf IoT-Geräte in Unternehmen.

In ihrem IoT Threat Report listet Unit 42 von Palo Alto Networks Folgendes auf:

- Zu den größten Bedrohungen für IoT-Geräte gehören:
  - Ausnutzung von Netzwerkscans (14 %)
  - Benutzerverhalten in Bezug auf Passwörter (13 %)
  - Würmer (12 %)
  - Ransomware (8 %)
- 57 % der IoT-Geräte sind anfällig für mittelschwere und schwere Angriffe.
- 83 % der medizinischen Bildgebungsgeräte nutzen nicht unterstützte Betriebssysteme.

Die starke Zunahme der IoT-Geräte und der damit verbundenen Angriffe zwingen Unternehmen, ihre Strategie für das Risikomanagement zu überdenken und zu einem Zero-Trust-Ansatz zum Schutz der IoT-Geräte überzugehen.

Abbildung 2: IoT-Angriffe in verschiedenen Branchen

Was ist Zero-Trust-Sicherheit?

Der konventionelle Netzwerkperimeter wird bald der Vergangenheit angehören. Dafür verantwortlich sind unter anderem die Arbeit im Homeoffice, BYOD-Modelle, die Verlagerung von Unternehmensressourcen in die Cloud und die zunehmende Bedeutung des Internets der Dinge. Berücksichtigt man dann noch die stetig steigende Anzahl von Cyberbedrohungen, wird klar: Ein Zero-Trust-Ansatz als Basis der Unternehmenssicherheit ist ein absolutes Muss. Palo Alto Networks definiert Zero Trust als einen strategischen Cybersicherheitsansatz, der beim Zugriff auf Unternehmensressourcen völlig auf implizites Vertrauen verzichtet und jede Phase digitaler Interaktionen kontinuierlich prüft und verifiziert. Mit diesem zuverlässigen Framework als Fundament können Unternehmen dann ihre Netzwerke modernisieren und neu aufsetzen, die Cloud-Nutzung ausweiten und die Security Operations stärken.

Identifizierung von Assets, kritischen Daten und Transaktionsströmen

Einführung einer Zero-Trust-Architektur und von Zugriffskontrollen nach dem Least-Privilege-Prinzip

Kontinuierliche Überwachung und Überprüfung

Abbildung 3: Allgemeine strategische Ziele der Zero-Trust-Strategie

Palo Alto Networks hat Leitprinzipien für das Zero-Trust-Framework definiert, die die Sicherheit für alle Benutzer, Anwendungen und die Infrastruktur in einem Unternehmen gemäß den vier Grundpfeilern Identität, Gerät/Workload, Zugriff und Transaktion beschreiben (siehe Tabelle 1).

Tabelle 1: Wichtige Zero-Trust-Funktionen und kontinuierliche Validierung

	Identität	Gerät/Workload	Zugriff	Transaktion
Zero Trust für Benutzer	Validiert Benutzer mithilfe einer starken Authentifizierung	Verifiziert die Integrität des Benutzergeräts	Setzt das Least-Privilege-Prinzip beim Benutzerzugriff auf Daten und Anwendungen durch	Prüft sämtliche Inhalte auf schädliche Aktivitäten und Datendiebstahl
Zero Trust für Anwendungen	Validiert Entwickler, DevOps-Mitarbeiter und Administratoren mithilfe einer starken Authentifizierung	Verifiziert die Integrität der Workloads	Setzt das Least-Privilege-Prinzip beim Zugriff von Workloads auf andere Workloads durch	Prüft sämtliche Inhalte auf schädliche Aktivitäten und Datendiebstahl
Zero Trust für die Infrastruktur	Validiert alle Benutzer mit Zugriff auf die Infrastruktur	Identifiziert alle Geräte, einschließlich IoT-Geräten	Segmentierung für Least-Privilege-Zugriffsrechte in nativen und Drittanbieterinfrastrukturen	Prüft sämtliche Inhalte in der Infrastruktur auf schädliche Aktivitäten und Datendiebstahl

Der Schutz nicht verwalteter IoT-Geräte ist eine wichtige Komponente der Zero-Trust-Strategie für die Infrastruktur und diese Prinzipien helfen dabei, praxistaugliche Zero-Trust-Sicherheitsrichtlinien zu definieren.

Der richtige Zero-Trust-Ansatz für IoT-Geräte

Diese Leitprinzipien des Zero-Trust-Frameworks für die Infrastruktur lassen sich in weitere untergeordnete Prinzipien aufgliedern, die speziell für die Zero-Trust-Sicherheit für IoT-Geräte gelten. Im Folgenden wird dieser Ansatz erläutert, den Unternehmen für den Schutz von IoT-Geräten implementieren sollten.

Tabelle 2: Erweiterung von Zero Trust für die Infrastruktur auf IoT-Geräte

Gerät/Workload	Zugriff	Transaktion
Erkennt alle IoT-Geräte	Empfiehlt Zero-Trust-Richtlinien	Überwacht kontinuierlich die IoT-Geräte
Analysiert das IoT-Sicherheitsrisiko	Setzt Zero-Trust-Richtlinien durch	Wehrt bekannte und unbekannte Bedrohungen ab

Viele Anbieter behaupten zwar, dass ihre Lösungen Zero Trust für IoT-Geräte bieten, doch in der Regel erfüllen sie nicht die komplexen Anforderungen der IoT-Sicherheit. Im nächsten Abschnitt haben wir einige der Herausforderungen zusammengestellt, die bei der Implementierung von Zero-Trust-Sicherheit für IoT-Geräte auftreten.

Herausforderungen bei der Implementierung von Zero-Trust-Sicherheit für IoT-Geräte

1. Schwierigkeiten bei der Erkennung und Identifizierung

- Konventionelle agentenbasierte Lösungen für die Endpunktsicherheit sind nicht in der Lage, IoT-Geräte zu erkennen und zu verwalten. Da sie üblicherweise nur über eine geringe CPU-Leistung verfügen, kann darauf kein Endpunktagent installiert werden.
- Die meisten IoT-Technologien erkennen und klassifizieren lediglich Geräte mit bereits bekannten Signaturen. Verfahren, die Fingerabdrücke oder Signaturen von Geräten erfassen, sind in der Regel nicht ausreichend skalierbar, da es zu viele verschiedene IoT-Gerätetypen mit unterschiedlichen Betriebsprotokollen und Standards gibt und ständig neue hinzukommen.
- IoT-Geräte werden in Losfertigung hergestellt und erhalten (im Gegensatz zu IT-Geräten) nur selten eine eindeutige Hardwarekennung. Aus diesem Grund werden die meisten Geräte nicht erkannt oder identifiziert und daher auch nicht im Geräte-Inventar des IT-Teams erfasst. So entstehen Schatten-IoTs.

2. Komplizierte Authentifizierung, Festlegung von Richtlinien und Segmentierung

- Die meisten IoT-Geräte unterstützen die normalerweise in Unternehmen genutzten Prozesse für die Authentifizierung und Autorisierung (wie 802.1X oder Single Sign-On) nicht. Eine MAR-Liste (MAC Authentication Repository) funktioniert aufgrund der unzureichenden Geräteklassifizierung ebenfalls nicht. Da viele IoT-Geräte jedoch geschäftskritisch sind, müssen Netzwerkteams sie manuell integrieren, ohne ihren Risikostatus gründlich prüfen zu können.
- Die manuelle Erstellung von Segmentierungsrichtlinien und -regeln nimmt mehrere Stunden in Anspruch. Zudem erschwert der unzureichende Überblick über nicht verwaltete Geräte die ordnungsgemäße Segmentierung, eine bewährte Methode zur Verhinderung der Ausbreitung von Bedrohungen im Netzwerk.

3. Schwierigkeiten bei der kontinuierlichen Überprüfung

- Da Schwachstellenscanner IoT-Geräte nicht erfassen können, werden sie in der Regel nicht überprüft.
- Viele IoT- und OT-Geräte kommen aber in kritischen Infrastrukturen zum Einsatz und eine aktive Suche oder Überprüfung der Geräte auf Risiken und Sicherheitslücken könnte zu Störungen im Netzwerk führen.

4. Unzureichender Schutz der IoT-Sicherheitslösungen

- Die vorhandenen IoT-Sicherheitslösungen verfügen nicht über die notwendigen Informationen oder Funktionen, um Zero-Trust-Richtlinien zur Risikominimierung zu empfehlen. Daher müssen die Sicherheitsteams die Geräte-Informationen selbst zusammentragen und die Zero-Trust-Richtlinien manuell festlegen – ein langwieriger und fehleranfälliger Prozess.
- Die vorhandenen IoT-Sicherheitslösungen geben lediglich Alarme aus, denn ihnen fehlen integrierte Funktionen für die Bedrohungsabwehr und die Durchsetzung von Sicherheitsrichtlinien.

Zuverlässige Zero-Trust-Sicherheit für IoT-Geräte

IoT Security von Palo Alto Networks integriert IoT-Geräte in das Zero-Trust-Sicherheitsmodell, das auf den drei Grundpfeilern Gerät/Workload, Zugriff und Transaktion basiert und die damit verbundenen Prinzipien umsetzt, um die IoT-Sicherheitsrisiken zu minimieren und die Netzwerke vor Cyberangriffen zu schützen. Dank der Lösung von Palo Alto Networks können Unternehmen den Zero-Trust-Ansatz für IoT-Geräte viel einfacher umsetzen und damit ihr Sicherheitsniveau insgesamt verbessern. Im Folgenden ist der praktische Ansatz beschrieben, wie Unternehmen mit IoT Security von Palo Alto Networks eine Zero-Trust-Strategie implementieren können.

Zero-Trust-Prinzip 1: Gerät/Workload

Identifizierung sämtlicher Geräte, einschließlich der IoT-Geräte

1. Erkennung

Was man nicht sieht, kann man nicht schützen. Wenn Sie die Zero-Trust-Prinzipien ausweiten möchten, müssen Sie nicht nur die Benutzer und typischen IT-Geräte, sondern auch alle nicht verwalteten IoT-Geräte im Netzwerk einbeziehen. IoT Security von Palo Alto Networks ist die einzige agentenlose IoT-Sicherheitslösung, die maschinelles Lernen (ML) und Deep Packet Inspection (DPI) mit Telemetriedaten aus dem Crowdsourcing nutzt, um alle mit dem Netzwerk verbundenen IoT-Geräte zu erfassen und zu klassifizieren – darunter auch Geräte, die der Lösung zum ersten Mal begegnen. ML ist wesentlich effektiver als die konventionellen reaktiven und signaturbasierten Methoden zur Geräteerkennung. Da durch die zunehmende Verbreitung neuer Kommunikationsprotokolle für Drahtlosverbindungen wie 5G und hybrider Arbeitsmodelle zahlreiche neue IoT-Gerätetypen in die Netzwerke integriert werden, sorgt eine ML-gestützte Geräteerkennung dafür, dass diese neuen Geräte schnell und zuverlässig erfasst und in Echtzeit klassifiziert werden.

IoT Security analysiert 200 Parameter, um für die IP-Adressen der einzelnen Geräte den richtigen Typ und Anbieter sowie das korrekte Modell zu ermitteln und mehr als 50 weitere wichtige Geräteattribute zu erfassen. So entsteht ein umfassendes Geräteprofil. Die korrekte und detaillierte Geräteklassifizierung ist unerlässlich, um nicht verwaltete IoT-Geräte von verwalteten IT-Geräten zu unterscheiden. Anschließend können Zero-Trust-Sicherheitsrichtlinien durchgesetzt werden, die nur genehmigten Datenverkehr zur IoT-Umgebung zulassen.

Nachfolgend sehen Sie die wichtigsten Kategorien der Kontextinformationen, die IoT Security bereitstellt:

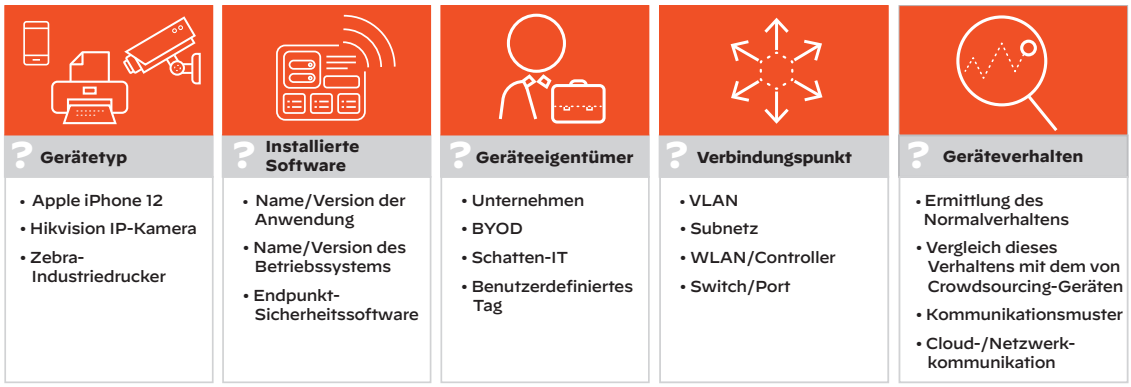


Abbildung 4: IoT Security findet 90 Prozent der Geräte innerhalb von 48 Stunden – und später noch weitere.

2. Risikobewertung

Der nächste Schritt bei der Implementierung eines Zero-Trust-Frameworks ist eine zuverlässige Risikobewertung und die Ermittlung des Risikoniveaus der IoT-Geräte. „Risiko" ist ein etwas schwammiger Begriff und wird inzwischen häufig als Synonym für „Bedrohung" und „Schwachstelle" genutzt. Um Risiken erkennen zu können, müssen wir also zuerst verstehen, was genau damit gemeint ist. Ein Risiko entsteht, wenn eine Bedrohung eine Sicherheitslücke ausnutzt, um Assets zu manipulieren oder zu beschädigen (in diesem Fall IoT-Geräte). Das Risiko für IoT-Geräte hängt daher von drei Vektoren ab: Bedrohungen, Schwachstellen und dem Kontext der Assets. IoT Security von Palo Alto Networks kann Risiken für alle drei Vektoren erkennen und bewerten. Dazu werden per Crowdsourcing erfasste Gerätedaten, ML-gestützte Analysen von Verhaltensanomalien auf Geräten, Threat-Intelligence-Analysen von Unit 42, CVEs, Informationen aus dem Schwachstellenmanagement von Drittanbietern und andere Daten untersucht.

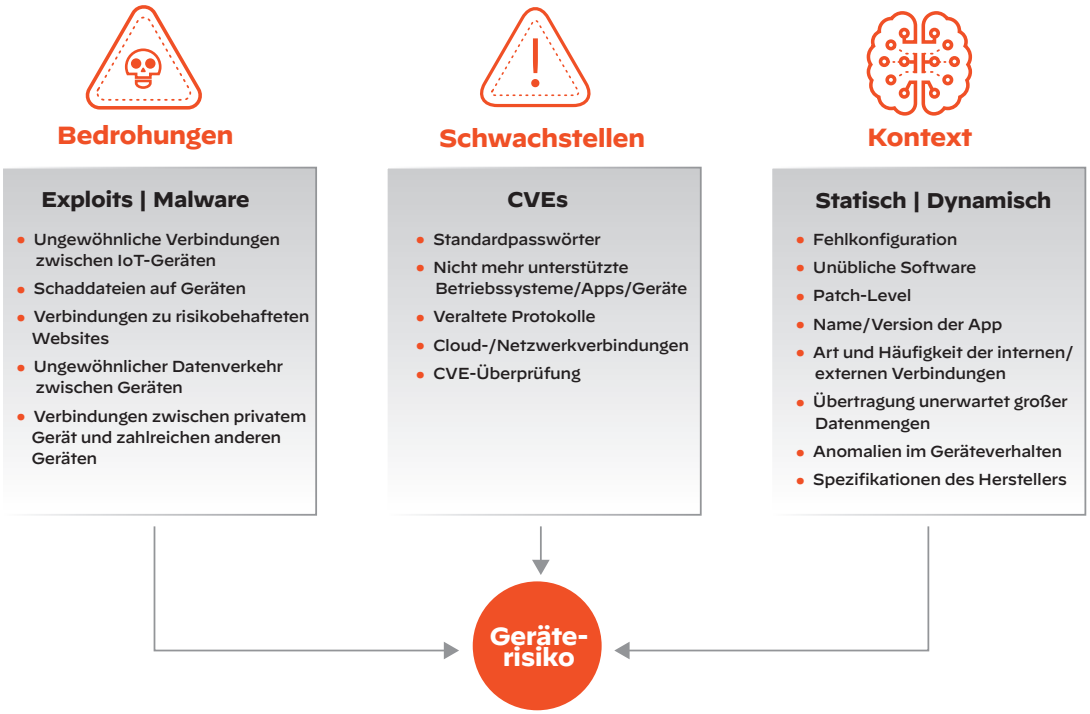


Abbildung 5: Umfassendes Risikoframework und -bewertung

IoT Security analysiert die Risiken und weist sie einer von vier Stufen zu:

1. Einzelne IoT-Geräte
2. Geräteprofil
3. Standort
4. Unternehmen

Bei der Risikobewertung der Geräteprofile, Standorte und Unternehmen berücksichtigt IoT Security nicht nur die Ergebnisse der einzelnen Geräte einer bestimmten Gruppe, sondern auch den Prozentsatz der risikobehafteten Geräte im Verhältnis zur Gesamtanzahl der Geräte dieser Gruppe. Anhand dieser Ergebnisse lassen sich die Risiken an verschiedenen Punkten und in diversen Bereichen des Netzwerks relativ einfach überprüfen.

Erfahren Sie, **wie Sie Schwachstellen der IoT-Geräte in Ihrem Netzwerk innerhalb weniger Stunden statt erst nach mehreren Wochen aufdecken.**

Zero-Trust-Prinzip 2: Zugriff

Segmentierung für Least-Privilege-Zugriffsrechte in nativen und Drittanbieterinfrastrukturen

3. Richtlinie für minimale Zugriffsrechte

Die Durchsetzung minimaler Zugriffsrechte ist ein Grundprinzip von Zero Trust. Auf IoT-Geräte angewendet bedeutet das, dass sie nur den unbedingt notwendigen Zugriff auf das Netzwerk erhalten sollten. Da die meisten IoT-Geräte zweckgebunden sind und ein vorhersehbares Verhalten aufweisen, kann diese Richtlinie in den folgenden Fällen genutzt werden:

- **Virtuelles Patching für geschäftskritische IoT-Geräte:** Mit der Richtlinie für minimale Zugriffsrechte können selbst anfällige Geräte genutzt werden, indem ihnen einfach der Zugriff auf bestimmte Ressourcen verweigert oder nur eingeschränkt gewährt wird. Das ist besonders praktisch, wenn es sich bei den IoT-/OT-Geräten um unverzichtbare Unternehmensgeräte handelt, zum Beispiel kritische IoT-Geräte von Gesundheitsdienstleistern oder in Fertigungsunternehmen. Es sollte jedoch als Übergangsmaßnahme betrachtet werden, die das Risiko der Ausnutzung einer Sicherheitslücke minimiert, während das eigentliche Problem behoben wird.
- **Richtlinie für Netzwerkzugriffskontrollen (NAC):** Mithilfe der Richtlinie für minimale Zugriffsrechte kann auch der Zugriff der IoT-Geräte auf bestimmte Ressourcen beschränkt werden, die sie für ihre Zwecke benötigen. Eine Überwachungskamera muss beispielsweise nur mit dem Videospeicher und der Anbieterwebsite kommunizieren, über die sie Firmware-Updates erhält.

Derzeit erfordert die Festlegung und Entwicklung von Richtlinien zur Risikominimierung anhand individueller Geräteprofile mehrere arbeitsintensive Schritte. Dazu gehören die Erstellung eines Inventars der IoT-Geräte, die Festlegung von Geräteprofilen nach Gerätetyp oder -funktion, die Ermittlung des Normalverhaltens, die Festlegung von Richtlinien, die nicht den Geschäftsbetrieb stören, und die Integration in andere Technologien zur Durchsetzung dieser Richtlinien.

IoT Security von Palo Alto Networks ist derzeit die einzige Lösung auf dem Markt, die einen Schritt weiter geht und nicht nur eine Risikobewertung, sondern zur Risikominimierung automatisch auch Least-Privilege-Zugriffsrichtlinien für das Zero-Trust-Prinzip bietet. IoT Security vergleicht die Metadaten von Millionen IoT-Geräten mit denen in Ihrem Netzwerk und kann dann mithilfe der Geräteprofile das Normalverhalten ermitteln. Die Lösung empfiehlt für jedes IoT-Gerät und jede Gerätekategorie eine Richtlinie, mit der vertrauenswürdiges Verhalten zugelassen oder eingeschränkt wird. So können Zero-Trust-Strategien auch ohne großen manuellen Arbeitsaufwand implementiert werden. Dank dieser Richtlinienempfehlungen lassen sich zahllose Arbeitsstunden einsparen, da das Sicherheitsteam nicht die Anwendungsnutzungs-, Verbindungs- und Port- bzw. Protokolldaten für jedes Gerät zusammentragen und dann manuell Richtlinien festlegen muss. Nach der Überprüfung werden die Richtlinien schnell von der ML-gestützten NGFW importiert und Änderungen automatisch übernommen. Dadurch beschränkt sich der Administrationsaufwand auf ein Minimum.

Erfahren Sie, **wie Sie mit der automatisierten Richtlinienerstellung von IoT Security den Zeitaufwand um den Faktor 20 senken.**

Richtlinie zur Netzwerksegmentierung

Eine Segmentierung der IoT-Geräte zur Einhaltung des Zero-Trust-Prinzips „Niemandem vertrauen, alles verifizieren“ ist ein erster Schritt auf dem Weg zum Zero-Trust-Netzwerk. So wäre es für Gesundheitseinrichtungen beispielsweise nicht verantwortungsvoll, lebenswichtige Geräte zur Herzfrequenzmessung im selben Netzwerk wie Bildgebungssysteme zu betreiben. Eine Segmentierung hingegen, die sich an Geräteprofilen und weiteren Faktoren wie Gerätetyp und -funktion, Bedeutung für den Betrieb und Bedrohungsniveau orientiert, ist eine Isolierungsstrategie, die die möglichen Folgen einer Infektionsausbreitung deutlich begrenzt.

IoT Security auf einer Next-Generation Firewall von Palo Alto Networks sorgt für eine detaillierte Segmentierung basierend auf dem Geräteprofil und ermöglicht daher auch eine entsprechende Isolierung. So kann die Gefahr, dass Infektionen sich zwischen IoT- und IT-Geräten ausbreiten, erheblich reduziert werden. Wenn eine Next-Generation Firewall (NGFW) von Palo Alto Networks als Segmentierungs-Gateway dient, können ihre Netzwerkfunktionen für die nahtlose Bereitstellung in einer vorhandenen Umgebung und die kontrollierte Einführung von Sicherheitsfunktionen für nicht verwaltete IoT-Geräte im Netzwerk genutzt werden.

Falls ein Kunde eine NAC-Lösung für die Segmentierung seines Netzwerks verwenden möchte, bietet IoT Security entsprechende Integrationen für Cisco ISE, Forescout® und Aruba ClearPass®. Da NAC aber nur einen Überblick über Geräte bietet, die authentifiziert werden können, können dabei tote Winkel entstehen, falls IoT-Geräte nicht authentifiziert werden können, da sie keinem Benutzer zugeordnet sind. Deshalb liefert IoT Security der NAC-Lösung alle Daten zu den entdeckten nicht verwalteten Geräten und zusätzliche Kontextinformationen, die eine intelligente Segmentierung ermöglichen. In der nachfolgenden Tabelle sehen Sie das Beispiel eines unserer Kunden, bei dem IoT Security die Ergebnisse der NAC-Lösung ergänzt und dadurch einen besseren Überblick ermöglicht.

Tabelle 3: So leuchtet IoT Security die toten Winkel einer NAC-Lösung aus		
MAC-Adresse	**NAC-Identität**	**IoT Security-Identität**
00:*0:7*:73:37:5*	AmbiCom-Gerät	CareFusion-Infusionspumpe, Basisstation
c8:2*:*4:56:27:06	Apple-Gerät	Medizinische Workstation
08:60:6*:*8:06:83	Asus-Gerät	Medizinische Workstation
00:08:74:*2:50:*5	Dell-Gerät	DICOM-Bildanzeigegerät
00:2*:5*:6*:06:72	HP-Gerät	DICOM-Bildgebungsgerät
00:09:6*:*6:60:7*	IBM-Gerät	Medizinische Workstation
00:*0:*4:2*:*0:94	INSIDE Technology-Gerät	Medizinische Workstation
Geräte insgesamt	**5.958**	**12.012**

Tabelle 4: Von NAC und IoT Security erkannte Geräte	
NAC	**IoT Security**
Erkannte Geräte = 5.698	Erkannte Geräte = 12.012
NAC-Kontext =	IoT Security-Kontext =
AmbiCom-Gerät	AmbiCom CareFusion-Infusionspumpe, Basisstation

Die Partitionierung von IoT-Geräten unter Berücksichtigung des Kontexts ermöglicht die Durchsetzung der Least-Privilege-Zugriffsrechte und die Beschränkung der Verbindungen auf die notwendigen Anwendungen. Außerdem sind sie von Gast- und Unternehmensnetzwerken isoliert und die Ausfallzeiten kritischer IoT-Infrastrukturen werden minimiert, da keine Kompatibilitätsprobleme zwischen den Systemen auftreten.

4. Richtlinienimplementierung

IoT Security kann die empfohlenen Zero-Trust-Sicherheitsrichtlinien nativ in die NGFW oder über Sicherheitspunkte von Drittanbietern implementieren. Im Folgenden sind die beiden Möglichkeiten beschrieben:

- Durchsetzung der empfohlenen Richtlinien mit einem Klick in der NGFW von Palo Alto Networks: Unsere patentierte Device-ID™-Richtlinie verfolgt ein einzelnes Gerät im Netzwerk und stellt detaillierte Informationen als Kontext in der ML-gestützten NGFW für potenzielle Alarme oder Vorfälle bereit – auch bei Änderungen der IP-Adresse oder des Ortes des jeweiligen Geräts. Richtlinienregeln und Layer-7-Kontrollfunktionen werden automatisch aktualisiert, wenn sich Ort und ermittelte Risiken ändern. In der Gegenüberstellung in Tabelle 5 sehen Sie, dass Device-ID besser skalierbar ist und eine schnellere Reaktion auf Bedrohungen sowie deren Behebung ermöglicht.
- Durchsetzung der empfohlenen Richtlinien über NAC-Integrationen für Cisco ISE, Forescout und Aruba ClearPass

Tabelle 5: Schnelle und akkurate Richtlinienimplementierung mit Device-ID	
Ohne Device-ID	**Mit Device-ID**
Da die IP-Adresse als Proxy für die Geräte-Identität genutzt wird, ist keine akkurate Ermittlung der Geräte-Identität möglich.	Die Geräte-Identität ist in der Richtlinie abrufbar.
Da Benutzer, Netzwerk- oder Geräteadministratoren für die korrekte Problembehebung verantwortlich sind, sind die Fehleranfälligkeit und das Risiko des Missbrauchs größer.	Richtlinien werden unabhängig vom Standort und der Konfiguration des Geräts konsistent durchgesetzt.
Die Abhängigkeit von externen Systemen wie NAC oder Ressourcenmanagement erfordert die Entwicklung und Pflege von Integrationen.	Daten aus IoT Security werden direkt an Device-ID übermittelt, sodass keine komplexen Integrationen notwendig sind.

Bei Untersuchungen von Bedrohungen oder Sicherheitsvorfällen muss das SOC-Team mehrere Systeme prüfen, um festzustellen, welches Gerät den Alarm generiert hat.	SIEM-Systeme erhalten Alarme zu Bedrohungen, einschließlich Geräte-Informationen.

Zero-Trust-Prinzip 3: Transaktion

Prüfung sämtlicher Inhalte in der Infrastruktur auf schädliche Aktivitäten und Datendiebstahl

5. Kontinuierliche Überwachung

Die kontinuierliche Überwachung ist der letzte, entscheidende Schritt bei der Einrichtung der Zero-Trust-Sicherheit für IoT-Geräte. Selbst wenn ein Geräteprofil erstellt und das Gerät im richtigen Netzwerksegment platziert wurde, kann es durch die Verbindung zum Netzwerk infiziert werden. Wird eine Sicherheitsverletzung erkannt, muss der Zugriff des Geräts auf die Ressourcen und das Netzwerk sofort gesperrt werden.

Unsere ML-gestützte IoT Security-Lösung ermittelt automatisch die Identität eines Geräts und das „Normalverhalten“ für diesen Gerätetyp. Anhand dieses Normalverhaltens kann die Lösung dann Anomalien ermitteln und potenzielle Abweichungen priorisieren. Die Algorithmen für das maschinelle Lernen ermitteln das Layer-7-Verhalten des IoT-Geräts und liefern zwei Arten von Informationen:

- IoT Security nutzt ML und gleicht die Verhaltensweisen mit den per Crowdsourcing erfassten Daten von ähnlichen Geräten ab, um das erwartete Normalverhalten immer auf dem aktuellen Stand zu halten und Abweichungen zu erkennen. Diese Informationen helfen dabei, die Erstellung von Zero-Trust-Richtlinien zu automatisieren.
- IoT Security überwacht den Datenverkehr und die Kommunikationsmuster auf dem Gerät und gleicht diese Informationen kontinuierlich mit dem VLAN-Design ab, um das passende Design für die Mikrosegmentierung und anschließend die Durchsetzung zu simulieren.

IoT-Geräte generieren einzigartige, identifizierbare Verhaltensmuster im Netzwerk. Mithilfe von ML und KI kann IoT Security diese Muster erkennen und jedes Gerät im Netzwerk identifizieren. So entsteht ein Geräte-Inventar mit Kontextinformationen, das dynamisch angepasst wird und immer auf dem aktuellen Stand ist. Nachdem das Gerät erkannt und sein normales Verhaltensmuster im Netzwerk ermittelt wurde, werden die Netzwerkaktivitäten überwacht, um ungewöhnliches Verhalten zu erkennen, das auf einen Angriff oder eine Sicherheitsverletzung hindeuten könnte. IoT Security informiert die Administratoren über Sicherheitsalarme im Portal und je nach Benachrichtigungseinstellungen auch per E-Mail und SMS über diese Auffälligkeiten. Außerdem verhindert die Lösung, dass Geräte, die gegen die Sicherheits- und Compliancerichtlinien verstoßen, auf das Netzwerk zugreifen.

6. Integrierte Bedrohungsabwehr

IoT Security überwacht alle IoT-Geräte und kann dank der branchenführenden IPS-, Malwareanalyse-, Web- und DNS-Sicherheitstechnologien auch alle Bedrohungen abwehren. Unsere Cloud-Delivered Security Services lassen sich nahtlos in IoT Security integrieren und koordinieren die Threat Intelligence, um alle Angriffe auf IoT-, IoMT-, OT- und IT-Geräte abzuwehren – ganz ohne zusätzlichen Arbeitsaufwand für Ihr Sicherheitsteam. Zur Verkürzung der Reaktionszeiten können IoT-Geräte, auf denen Bedrohungen erfasst wurden, von den ML-gestützten NGFWs dynamisch isoliert werden. So hat das Sicherheitsteam mehr Zeit, einen Plan für die Fehlerbehebung zu erstellen, und von den infizierten Geräten geht keine Gefahr mehr aus.

Infrastrukturweite Umsetzung von Zero Trust

In der Vergangenheit war es üblich, identifizierbare Benutzer, Anwendungen und Geräte innerhalb des Netzwerkperimeters zu schützen. Doch da die Anzahl der nicht verwalteten IoT-Geräte in Unternehmen geradezu explosionsartig angestiegen ist und der Netzwerksicherheitsperimeter sich nicht mehr so einfach bestimmen lässt, ist eine neue Strategie erforderlich. Aus diesem Grund müssen Unternehmen einen neuen, vereinfachten Ansatz bei der IoT-Sicherheit verfolgen, der sich an den Best Practices von Zero Trust orientiert.

Sehen Sie sich die branchenweit umfassendste IoT-Sicherheitslösung in einer kostenlosen Produktdemo an und überzeugen Sie sich selbst davon, dass der IoT Security-Service von Palo Alto Networks die Einführung eines Zero-Trust-Frameworks für nicht verwaltete IoT-Geräte erheblich vereinfacht.

paloalto NETWORKS

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

Telefon: +31 20 888 1883
Vertrieb: +800 7239771
Support: +31 20 808 4600

www.paloaltonetworks.de