EINFACHE ZERO-TRUST-IMPLEMENTIERUNG IN FÜNF SCHRITTEN

Die Entscheidungsträger vieler Unternehmen zögern die Implementierung einer Zero-Trust-Strategie heraus, weil sie Schwierigkeiten, hohe Kosten und Störungen des Geschäftsbetriebs befürchten. Infrastrukturen aus dem 20. Jahrhundert können beim Entwurf eines modernen Zero-Trust-Netzwerks durchaus Probleme verursachen, aber der Aufbau eines Zero-Trust-Netzwerks ist wesentlich einfacher als der Aufbau eines der herkömmlichen, hierarchischen Netzwerke, die im 20. Jahrhundert üblich waren. Die meisten von uns sind an das Netzwerkdesign von außen nach innen gewohnt, das auf der Klassifizierung von Benutzern als „vertrauenswürdig“ und „nicht vertrauenswürdig“ beruht. Und obwohl wir heute wissen, dass dieser Ansatz nicht sicher genug ist, sind viele von uns so in den alten Denkweisen verhaftet, dass es uns schwer fällt, uns an die Zero-Trust-Methodik zu gewöhnen.

Dabei muss gar nicht das gesamte Netzwerk ersetzt werden. Das Zero-Trust-Prinzip verbessert bereits vorhandene Netzwerke, da jedes Zero-Trust-Netzwerk für eine bestimmte Umgebung oder „Schutzfläche“ entworfen wird. Gleichzeitig wird das Zero Trust-Netzwerk mit Ihrem vorhandenen Netzwerk verbunden, um die bereits implementierte Technologie weiterhin zu nutzen. Im Laufe der Zeit verschieben Sie dann einfach schrittweise immer mehr Datensätze, Anwendungen, Ressourcen und Services aus der alten Umgebung in das neue Zero-Trust-Netzwerk. Dadurch wird der Übergang zu einem Zero-Trust-Netzwerk überschaubar, kosteneffektiv und ohne Unterbrechung des Geschäftsbetriebs möglich.

Für die Implementierung sind nur fünf Schritte erforderlich. In diesem Whitepaper beschreiben wir diese Schritte im Detail und erläutern, wie die integrierte Plattform von Palo Alto Networks in jeder Phase den notwendigen Schutz für Ihre kritischen Ressourcen bietet.

Abbildung 1: Implementierung in fünf Schritten

1. Definition der Schutzfläche

Bei dem Fünf-Schritte-Prinzip ging es ursprünglich darum, die sensiblen Daten im Unternehmen zu definieren, um dann die Schutzfläche festzulegen. Die Schutzfläche ist um mehrere Größenordnungen kleiner als die Angriffsfläche und kann in jedem Fall ermittelt und definiert werden. Mit der Zeit wurde allerdings deutlich, dass der Zero-Trust-Schutz nicht auf Daten beschränkt werden, sondern auch andere Netzwerkkomponenten einschließen sollte.

Dazu zählen alle wichtigen Daten, Anwendungen, Ressourcen und Services (kurz: DARS), zum Beispiel:

- **Daten –** Zahlungskartendaten (Payment Card Information, PCI), persönliche Daten im Gesundheitswesen (Personal Healthcare Information, PHI), personenbezogene Daten (Personally Identifiable Information, PII) und geistiges Eigentum (Intellectual Property, IP)
- **Anwendungen –** Standardlösungen und kundenspezifische Software
- **Ressourcen –** SCADA-Systeme, Kassenterminals, medizinische Geräte, Produktionsanlagen und IoT-Geräte (Internet of Things)
- **Services –** DNS, DHCP und Active Directory®

Sowohl die physischen als auch die virtuellen Next-Generation Firewalls von Palo Alto Networks bieten einen umfassenden Überblick über Layer 7 und helfen Ihnen so, wichtige Daten, Anwendungen, Ressourcen und Services zu identifizieren. Palo Alto Networks arbeitet zudem eng mit den Anbietern anderer führender Lösungen für die Erkennung und Katalogisierung von Daten und Ressourcen zusammen. Cortex™ XDR von Palo Alto Networks nutzt Netzwerk-, Cloud- und Endpunkt-Produkte als Sensoren, die Daten an den Cortex™ Data Lake übertragen. Dadurch erhalten Sie einen Überblick über die Aktivitäten der Benutzer, Geräte, Anwendungen und Services sowie mehr Informationen zu den individuellen Schutzflächen in Ihrer Umgebung.

Implementieren Sie eine Next-Generation Firewall in Ihrem Netzwerk, um die Schutzfläche zu definieren

Die Next-Generation Firewalls von Palo Alto Networks können direkt in Ihr Netzwerk integriert werden, ohne dass Sie zuvor Änderungen vornehmen müssen. Dieser Ansatz wird Virtual-Wire-Implementierung genannt. Damit kann die Firewall als „Bump in the Wire" in Ihr vorhandenes Netzwerk integriert werden. Das vereinfacht die Installation und Konfiguration der Firewall, denn Sie müssen ihr weder eine MAC- und IP-Adressen zuweisen noch das Netzwerk überarbeiten oder die anderen Geräte in der unmittelbaren Umgebung neu konfigurieren.

Die Appliance ist für den Datenverkehr und das Netzwerk transparent, kann aktive Bedrohungen aber dennoch ohne Topologieänderungen erkennen und blockieren. Wenn Sie den Datenverkehr über diese Firewall leiten, kann sie Logdateien für die Bedrohungserkennung in der Schutzfläche erstellen, ohne den Netzwerkbetrieb zu stören.

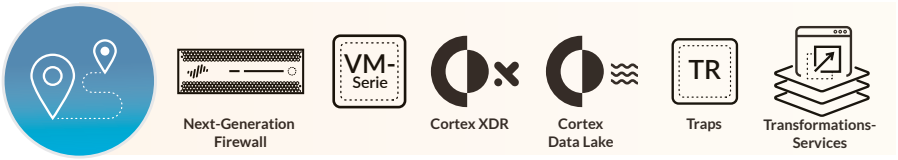
2. Ermittlung der Transaktionsflüsse

Vor dem Entwurf eines Netzwerks müssen Sie die Funktionsweise der Systeme verstehen. Die Details der Datenübertragung im Netzwerk – und speziell von und zur Schutzfläche – haben entscheidenden Einfluss auf die Sicherheitsanforderungen. Sie können sich dieses Verständnis erarbeiten und ermitteln, wie die verschiedenen DARS-Komponenten mit anderen Netzwerkressourcen interagieren, indem Sie die Transaktionen in Ihrem Netzwerk nachverfolgen und zuordnen.

Eine gängige Methode zur Einschätzung der Datenflüsse ist das Dokumentieren aller bekannten Informationen zu den Interaktionen zwischen bestimmten Ressourcen. Auf diese Weise können Sie sich zwar kein umfassendes Bild machen, gewinnen aber dennoch wertvolle Einblicke und müssen Ihre Sicherheitsmaßnahmen nicht völlig blind auswählen.

Zero-Trust-Architekturen basieren auf Datenströmen. Wenn Sie die vom Designer beabsichtigte Funktionsweise Ihres Systems verstehen, können Sie anhand der Flussdiagramme entscheiden, wo Sicherheitsmaßnahmen implementiert werden sollten.

Wie oben erwähnt ist der Aufbau eines Zero-Trust-Netzwerks ein schrittweiser Prozess. Beginnen Sie mit dem, was Sie bereits wissen. Beim Abarbeiten der fünf Schritte werden Sie weitere Informationen finden, die Ihnen dabei helfen, das Netzwerkdesign zu verfeinern. Sie sollten Ihre Zero-Trust-Initiative nicht aufschieben, nur weil Sie noch nicht alle Details kennen.



Die Next-Generation Firewalls von Palo Alto Networks bieten einen umfassenden Überblick über die Anwendungsebene und detaillierte Einblicke in den Datenverkehr. Policy Optimizer ist eine Funktion, die ab Version PAN-OS® 9.0 unserer Next-Generation Firewall verfügbar ist. Dank des umfassenden Überblicks über die Anwendungen können Sie damit die Migration der Regeln priorisieren, Richtlinien identifizieren, die ungenutzte oder zu großzügig skalierte Anwendungen zulassen, und die Durchsetzung der Regeln analysieren.

Cortex Data Lake erfasst zudem Telemetriedaten. Im Netzwerk nutzt die Plattform dazu unsere innovativen Firewall-Appliances, in der Cloud die virtuellen innovativen Firewalls der VM-Serie und auf den Endpunkten Traps™, unseren EDR-Agenten (Endpoint Detection and Response). Diese Daten werden zentral gespeichert und Cortex XDR greift auf Cortex Data Lake zu, um die erfassten Interaktionen zu validieren und zugehörige Details bereitzustellen. Dadurch lassen sich die Kommunikation verbessern und der Datenverkehr genauer nachvollziehen.

3. Entwurf eines Zero-Trust-Netzwerks

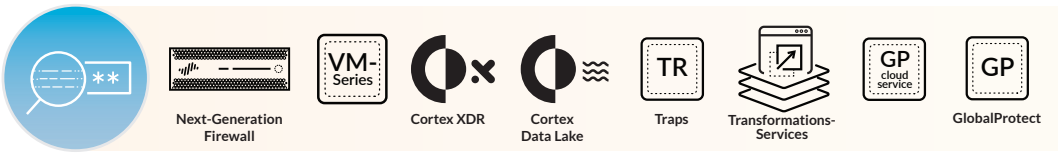
Traditionell begann das Netzwerkdesign mit der Architektur. IT-Teams erhielten eine sogenannte Referenzarchitektur und mussten diese dann an die Anforderungen ihres Unternehmens anpassen. Bei der Zero-Trust-Strategie ist das erst der dritte Schritt, und anstelle von Standardvorlagen werden individuelle Designs konzipiert. Wenn Sie in den ersten beiden Schritten die Schutzfläche definiert und die Transaktionen zugeordnet haben, wird sich Ihre Zero-Trust-Architektur abzeichnen.

Zuerst wird eine innovative Firewall als Segmentierungs-Gateway implementiert, um präzise Layer 7-Zugriffkontrollen als Mikroperimeter um die Schutzfläche einzurichten. In dieser Architektur wird jedes Paket, das an eine Ressource in der Schutzfläche gesendet wird, über eine solche Firewall geleitet, damit die Layer 7-Richtlinie zur Analyse und Überprüfung des Zugriffs angewendet werden kann.

Es gibt ein weit verbreitetes Missverständnis, dass Zero-Trust-Netzwerke nur der Zugriffskontrolle dienen. Die Erteilung minimaler (d. h. nur unbedingt erforderlicher) Zugriffsrechte ist jedoch nur ein Aspekt. Ein weiterer ist die Überprüfung und Protokollierung jedes einzelnen Pakets in der Anwendungsebene, um sicherzustellen, dass die Pakete keine schädlichen Elemente enthalten. Dazu wird der gesamte Netzwerkverkehr mithilfe verschiedener integrierter Sicherheitsfunktionen überprüft, zum Beispiel Intrusion Prevention Systems (IPS), Sandboxen, URL-Filterung, DNS Security-Service und Data Loss Prevention (Schutz vor Datenverlust, DLP).

Ein Maßanzug

Wie entsteht ein Maßanzug? Zuerst nimmt der Schneider Ihre Maße, dann erstellt er ein Schnittmuster und erst zum Schluss beginnt er mit dem Nähen. Bei der Erstellung einer Zero-Trust-Strategie sollten Sie genauso vorgehen. Wenn Sie ein effektives, sicheres Netzwerk aufbauen wollen, müssen Sie zuerst herausfinden, was geschützt werden muss und wie diese Systeme funktionieren.



Die Next-Generation Firewalls von Palo Alto Networks nutzen die leistungsstarken, einzigartigen Technologien App-ID™, User-ID™ und Content-ID™, um offizielle Layer 7-Richtlinien zu erstellen und das Infiltrieren der Schutzfläche zu verhindern. Da die Segmentierungs-Gateways sowohl in physischer als auch in virtueller Form verfügbar sind, kann dieses Architekturmodell für jede Schutzfläche übernommen werden – sowohl in internen und externen physischen Rechenzentren als auch in privaten, öffentlichen und Hybrid-Cloud-Umgebungen.

Traps und andere Sicherheitslösungen für Endpunkte schützen vor bekannten und unbekannten Bedrohungen wie Malware, dateilosen Angriffen und Exploits. Zugriffskontrollen wie der GlobalProtect™ Cloud Service von Palo Alto Networks wenden die Richtlinien jedes Mikroperimeters auf alle Komponenten an, die versuchen, auf die Ressourcen in der Schutzfläche zuzugreifen.

Die Security Operating Platform® überträgt Telemetriedaten von allen Palo Alto Networks Kerntechnologien an Cortex Data Lake, damit die Richtlinien später mit den Cortex XDR-Funktionen für das maschinelle Lernen und die Automatisierung verbessert werden können.

Die Architektur muss nun noch durch wichtige Lösungen anderer Anbieter vervollständigt werden. Die Lösungen von Palo Alto Networks können in diverse Drittanbieterprodukte für die Multi-Faktor-Authentifizierung (MFA) integriert werden. Dadurch wird die Zuverlässigkeit der User-ID gesteigert. Um die Zero-Trust-Architekturen abzurunden und zu vereinfachen, ermöglicht unsere leistungsstarke API eine umfassende Integration in über 250 Lösungen unserer Partner. Dazu gehören Anti-Spam-/Anti-Phishing-Technologien, DLP-Systeme, SD-WAN- (Software-Defined Wide Area Networks) und WLAN-Produkte.

4. Konfiguration der Zero-Trust-Richtlinie

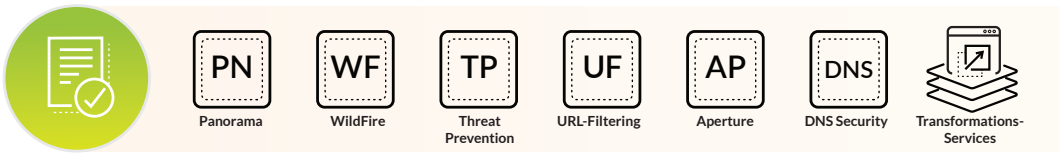
Nachdem Sie Ihr Zero-Trust-Netzwerk konzipiert haben, sollten Sie Ihre Zero-Trust-Richtlinien definieren. Stellen Sie sich dazu die Fragen Wer, Was, Wann, Wo, Warum und Wie? Damit zwei Ressourcen miteinander kommunizieren können, muss der Datenverkehr in einer Whitelisting-Regel zugelassen werden. Mithilfe der Antworten auf diese Fragen können Sie eine Layer 7-Richtlinie erstellen, damit ganz gezielt nur bekannter Datenverkehr und legitime Anwendungskommunikation im Netzwerk zugelassen werden. Dadurch wird zum einen die Angriffsfläche deutlich reduziert, zum anderen aber auch die Anzahl der portbasierten Firewall-Regeln reduziert, die von herkömmlichen Netzwerk-Firewalls durchgesetzt werden müssen. Die Fragen Wer, Was, Wann, Wo, Warum und Wie vereinfachen das Erstellen von Richtlinien:

- **Wer** braucht Zugriff auf diese Ressource? Das ist die „bestätigte Identität".
- **Was** für eine Anwendung nutzt die bestätigte Identität eines Pakets, um auf eine Ressource in der Schutzfläche zuzugreifen?
- **Wann** versucht die bestätigte Identität, auf die Ressource zuzugreifen?
- **Wo** ist die Zieladresse des Pakets? Die Zieladresse wird häufig automatisch aus einem anderen System abgerufen, das an der Ressourcenverwaltung in der Umgebung beteiligt ist, zum Beispiel von einem Server mit Lastausgleich (über eine virtuelle IP-Adresse).
- **Warum** greift das Paket auf diese Ressource in der Schutzfläche zu? Diese Frage bezieht sich auf die Klassifizierung von Daten. Dabei werden Metadaten automatisch von Datenklassifizierungstools eingespeist, um die Richtlinie noch präziser zu definieren.
- **Wie** greift die bestätigte Identität eines Pakets über eine bestimmte Anwendung auf die Schutzfläche zu?

Kein „unbekannter" Datenverkehr:

In einem Zero-Trust-Netzwerk sollte es keinen „unbekannten Datenverkehr" geben. Datenverkehr, der nicht identifiziert werden kann, sollte keinen Zugang zur Schutzfläche erhalten. Unbekannter Datenverkehr bedeutet, dass das Modell versagt hat und korrigiert werden muss. Der unbekannte Datenverkehr muss analysiert werden. Dazu definieren Sie ein Tupel mit den Antworten auf die Fragen oben, um zu entscheiden, ob er zulässig ist oder nicht.

Die Next-Generation Firewalls von Palo Alto Networks blockieren nicht ausdrücklich genehmigten Datenverkehr standardmäßig. Daher benötigen Sie in einer Zero-Trust-Architektur nur wenige Regeln für das Blockieren von Datenverkehr. So können Sie beispielsweise eine Active Directory-Gruppe in eine spezifische User-ID für einen einzelnen Benutzer einbetten, der keinen Zugriff auf die Schutzfläche erhalten soll. Dann können Sie mit den Domain-Anmeldedaten des Benutzers und einer User-ID eine Blockierregel für die Schutzfläche erstellen und müssen keine Änderungen am Active Directory vornehmen.



Wer	Was	Wann	Wo	Warum	Wie	Aktion
User-ID	**App-ID**	**Zeit**	**Systemobjekt**	**Klassifizierung**	**Content-ID**	**–**
Vertrieb	Salesforce	Geschäftszeiten	USA	Schädlich	SFDC_CID	Zulassen
Epic_Users	Epic	Beliebig	Epic_Svr	Schädlich	Epic_CID	Zulassen

Um den Prozess zu vereinfachen, sollten Sie die Richtlinien vorrangig mit dem zentralen Managementtool Ihres Segmentierungs-Gateways erstellen. Mit der Managementlösung Palo Alto Networks Panorama™ können Sie das tun und die oben beschriebene Fragemethode anwenden.

Die leistungsstarken Next-Generation Firewalls von Palo Alto Networks und ihre einzigartigen Funktionen helfen Ihnen, Richtlinien festzulegen, die leicht verständlich und einfach zu pflegen sind, aber dennoch umfassenden Schutz bieten und für die Endbenutzer transparent sind. User-ID hilft bei der Beantwortung der Frage „Wer?", App-ID bei der Frage „Was?" und Content-ID bei der Frage „Wie?". Diese Regeln werden in der gesamten Umgebung konsequent gestellt, zum Beispiel auch von unserem Service WildFire® für den Malware-Schutz sowie den Threat Prevention-, URL-Filterungs- und DNS Security-Services. PAN-OS 9.0 bietet erweiterte Funktionen zur Richtlinienerstellung, vor allem über Policy Optimizer. Damit können Sie kontinuierlich analysieren, wie Sie die Zuverlässigkeit Ihrer Zero-Trust-Richtlinie weiter verbessern können. Zudem können Sie Richtlinien für unseren SaaS-Sicherheitsservice Aperture™ erstellen und dabei berücksichtigen, wie auf die Software-as-a-Service-Anwendungen zugegriffen wird.

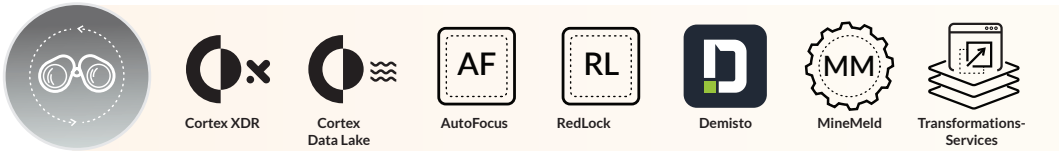
Analyse des richtigen Datenverkehrs

Viele Unternehmen konzentrieren sich auf die falschen Dinge. Sie analysieren beispielsweise den Datenverkehr, der vom System abgelehnt wurde. Das kann gewisse Aufschlüsse geben, aber viel wichtiger ist der zugelassene Datenverkehr, da ein erfolgreicher Datendiebstahl nur in Transaktionen erfolgen kann, die von den geltenden Regeln zugelassen wurden. Die Angreifer suchen nach falsch konfigurierten Technologien und Ressourcen, deren Regeln Lücken haben und schädlichen Datenverkehr passieren lassen.

5. Monitoring und Pflege des Netzwerks

Der letzte Schritt in diesem iterativen Prozess ist das Monitoring und die Pflege des Netzwerks. Dazu müssen kontinuierlich alle internen und externen Logdateien bis Layer 7 analysiert und insbesondere in Bezug auf die Zero-Trust-Prinzipien kontrolliert werden. Die Überwachung und Protokollierung des gesamten Datenverkehrs ist in einem Zero-Trust-Netzwerk unverzichtbar.

Das System benötigt so viele Telemetriedaten über die Umgebung wie möglich. Durch die Analyse dieser Daten ermitteln Sie, wie Sie Ihr Zero-Trust-Netzwerk im Laufe der Zeit verbessern können. Je häufiger Ihr Netzwerk angegriffen wird, desto stärker werden die Abwehrmaßnahmen, da alle neuen Informationen zur Verbesserung der Richtlinien beitragen. Die zusätzlichen Daten geben Ihnen Einblick in die Vorgänge in der Schutzfläche. Sie lernen, welche Komponenten eingebunden werden sollten und welche Abhängigkeiten zwischen den Daten bestehen. Daraus lassen sich dann Maßnahmen zur Verbesserung der Architektur und zur Stärkung der Sicherheitsmaßnahmen ableiten.



Alle von den Palo Alto Networks-Sicherheitstechnologien für Endpunkte, Netzwerke und Clouds erfassten Telemetriedaten werden an Cortex Data Lake gesendet und dort für maschinelles Lernen und Analysen zusammengeführt.

Die Daten aus den Next-Generation Firewalls und der VM-Serie werden in einer zentralen Konsole in Panorama konsolidiert. Dort wird auch eine Warnmeldung ausgegeben, wenn schädlicher oder verdächtiger Datenverkehr überprüft werden sollte. Der Service AutoFocus™ unterstützt diese Überprüfung mit einer Kombination aus Funktionen für maschinelles Lernen in WildFire und dem Know-how des Bedrohungsforschungsteams Unit 42 von Palo Alto Networks. So werden Ihre Richtlinien kontinuierlich verbessert und die Schutzfläche immer präziser definiert. Die MineMeld™-Engine in AutoFocus kann Bedrohungsdaten aus Drittanbieterquellen aggregieren, anwenden und weitergeben. Dadurch erhalten Sie zusätzlichen Kontext zur weiteren Verbesserung Ihrer Zero-Trust-Richtlinie. MineMeld lässt sich nahtlos in die Next-Generation Firewall integrieren, sowohl innerhalb als auch außerhalb Ihrer Palo Alto Networks-Umgebung.

Der Palo Alto Networks Service RedLock® für Sicherheit und Compliance in der öffentlichen Cloud durchsucht alle Audit- und Datenverkehr-Logdateien in Multi-Cloud-Umgebungen nach Aktivitäten von Root-Benutzern und zu laxen Administratoraktivitäten. RedLock bietet einen umfassenden Überblick über Ihre Cloud-Umgebung im Kontext, sodass Anomalien im Verhalten der Benutzer (basierend auf den bisherigen Aktivitäten und ihrem Standort) erkannt werden können. Diese deuten unter Umständen auf gestohlene oder geknackte Anmeldedaten, Brute-Force-Angriffe und andere verdächtige Aktivitäten hin. Außerdem korreliert RedLock die Bedrohungsdaten und kann dadurch einen umfassenden Einblick in verdächtige IP-Adressen und Sicherheitslücken von Hosts bieten. So haben Sie die Möglichkeit, betroffene Ressourcen schnell zu isolieren, um weitere Konsequenzen zu vermeiden, und die entsprechenden Zero-Trust-Berechtigungen besser anzupassen.

Cortex XDR greift auf den Cortex Data Lake zu, um Profile für Benutzer und Geräte zu erstellen, deren Verhalten als normal angesehen wird. Die Engine für die Verhaltensanalyse vergleicht aktuell beobachtete Verhaltensmuster mit diesen Profilen, um Anomalien zu erkennen und Bedrohungen für die Schutzfläche aufzudecken.

Um aktuelle oder neue Richtlinien für die Schutzfläche zu evaluieren, können Sie mit Cortex XDR die Telemetriedaten in Cortex Data Lake nach der Kommunikation und den Interaktionen zwischen Netzwerkkomponenten durchsuchen. Außerdem können Sie die Daten analysieren, um äquivalente Situationen zu finden oder wichtige Einblicke in erforderliche Richtlinienänderungen zu erhalten. In seltenen Fällen werden dadurch sogar bislang unbekannte Angriffsvektoren aufgedeckt, die bei der Definition der Schutzfläche noch nicht berücksichtigt wurden. Anschließend können Sie die neue Bedrohung mit Cortex XDR gründlich untersuchen, um zu rekonstruieren, was geschehen ist und welche Maßnahmen erforderlich sind.

Ihre erste Zero-Trust-Initiative

Zu Beginn Ihrer Zero-Trust-Initiative sollten Sie diese drei Schritte durchführen:

- **Aufbau eines Zero-Trust-Kompetenzzentrums:** Sie sollten unbedingt eine bereichsübergreifende Arbeitsgruppe aus Vertretern aller relevanten Teams zusammenstellen und bereits ab der Planungsphase in die Entwicklung der Zero-Trust-Architektur einbeziehen. Dazu gehören die IT- und Cybersicherheitsteams, die für die Bereitstellung zuständig sein werden, aber auch Führungskräfte, die bei der Definition der kommerziellen Anforderungen helfen können, die eine erfolgreiche, leistungsstarke Architektur erfüllen muss.
- **Durchführen eines Zero-Trust-Workshops:** Um eine gemeinsame Diskussionsbasis zu schaffen, sollte Ihr Zero-Trust-Kompetenzzentrum einen Workshop durchführen, in dem das Grundprinzip der Zero-Trust-Strategie besprochen und die Unternehmensziele sowie die erste Schutzfläche vereinbart werden. Idealerweise sollte bei diesem Workshop auch schon der Prototyp des Zero-Trust-Netzwerks entworfen werden, damit die Architekten und Techniker anschließend mit der offizielleren Entwurfsphase beginnen können.
- **Erste Schutzfläche in einer Umgebung mit geringem Risiko:** Bauen Sie Ihr erstes Zero-Trust-Netzwerk nicht in der für Ihr Unternehmen wichtigsten und wertvollsten Umgebung auf, sondern in einer Umgebung mit geringem Risiko. Dort kann Ihr Implementierungsteam gefahrlos praktische Erfahrungen sammeln.

Bauen Sie ein Zero-Trust-Kompetenzzentrum auf.

Führen Sie einen Zero-Trust-Workshop durch.

Beginnen Sie in einer Umgebung mit geringem Risiko.

Abbildung 2: Ihre erste Zero-Trust-Initiative

Wenn es unternehmensweit umgesetzt wird und Netzwerk, Endpunkte und Cloud umfasst, ist das Zero-Trust-Prinzip eine äußerst effektive Abwehrstrategie. Bei unserer aus fünf Schritten bestehenden Methode wird ein Segmentierungs-Gateway mit einer integrierten Plattform verwendet, um den Schutz Ihrer sensiblen Daten und wichtigsten Ressourcen zu vereinfachen. Wenn Sie alle Funktionen der Security Operating Platform und geeignete Lösungen unserer Technologiepartner nutzen, können Sie einen großen Teil des Zero-Trust-Netzwerks für eine nahtlose Zero-Trust-Umgebung konfigurieren.

Die Professional Services von Palo Alto Networks unterstützen Sie gern bei der Umsetzung der Zero-Trust-Strategie. Unsere erfahrenen Berater arbeiten bei allen fünf Schritten eng mit Ihrem Team zusammen, um Ihre wertvollen Ressourcen effektiv zu schützen. Mit unserem umfassenden Ansatz wird das Zero-Trust-Prinzip ein praxistauglicher, machbarer und effektiver Erfolgsgarant für Ihr Unternehmen.

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

Telefon: +31 20 888 1883

www.paloaltonetworks.de

simplify-zero-trust-implementation-with-a-five-step-methodology-wp-051519-de