TANIUM

WHITEPAPER

Was ist Zero Trust?

Warum die Endpunktsicherheit wesentlich für eine erfolgreiche Zero-Trust-Strategie ist

INHALT

Was ist Zero Trust?

Zero Trust steht für ein einfaches Konzept: Kein Benutzer oder Gerät ist vertrauenswürdig und alle müssen jederzeit überprüft werden. Kurz: Vertrauen Sie nichts und niemandem. Keiner Person. Keinem Endpunkt. Keiner Anwendung. Keinem Netzwerk.

Unternehmen müssen sich darüber klar werden, dass sie in einer grundsätzlich feindseligen Umgebung tätig sind. Ein Zero-Trust-Sicherheitskonzept geht davon aus, dass kein Gerät oder Benutzer ohne Verifizierung vertrauenswürdig ist. Unternehmen dürfen Geräten oder Personen innerhalb oder außerhalb ihrer Perimeter nicht automatisch vertrauen. Schon das Konzept eines Perimeters – ein Analog zu Mauer und Burggraben – hat sein Verfallsdatum als Sicherheitsmodell schon lange überschritten. Der neue Perimeter ist der Endpunkt selbst.

Zero Trust wurde genau für diese neue Realität geschaffen. Der Schlüssel, um Zero-Trust-Sicherheit in großem Maßstab umzusetzen, ist die Endpunkt-Visibilität.

Zero Trust ist eine Lösung, kein Produkt

Die meisten Diskussionen über Zero Trust konzentrieren sich auf die Benutzerauthentifizierung – sicherlich ein wichtiger Teil des Puzzles. Ebenso kritisch ist aber der Endpunkt. Ein Benutzer kann legitim sein, aber gilt das auch für das Gerät, das er verwendet? Wurde es vielleicht ohne sein Wissen kompromittiert? Ein wirksamer Zero-Trust-Ansatz betrachtet nicht nur die Zugangsdaten des Benutzers und die Daten, auf die er zugreifen möchte, sondern auch das Gerät (d. h. den Endpunkt), das die Person verwendet. Immer mehr Menschen arbeiten remote auf privaten Endpunkten. Für Unternehmen ist dies ein Problem, denn sie müssen darauf vertrauen können, dass diese Endpunkte nicht aufgrund schlechter Sicherheitsvorkehrungen infiziert oder übernommen wurden. Damit das gelingt, müssen Unternehmen in Echtzeit genaue Informationen über Endpunkte, Geräte und Benutzerdaten erhalten. Die NIST Special Publication 800-207 unterstreicht die Bedeutung einer kontinuierlichen Überwachung und allgemeinen Cyber-Hygiene für einen erfolgreichen Zero-Trust-Ansatz.

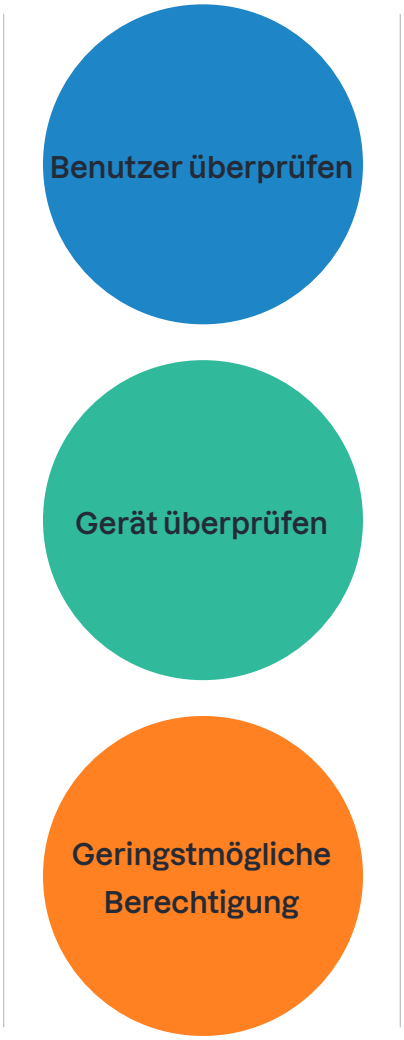
Organisationen müssen in der Lage sein, die folgenden Fragen zu beantworten:

- Wie viele unverwaltete, unterverwaltete und verwaltete Assets haben Sie? Um welche Betriebssysteme handelt es sich?
- Wie viele dieser Systeme sind nicht compliant? Gibt es eine Methode, um diese Systeme schnell wieder in die Compliance zu bringen?
- Wie viele Schwachstellen mit niedrigem, mittleren und hohen Schweregrad gibt es in Ihrer Umgebung? Wie viele dieser Schwachstellen sind ausnutzbar?
- Verfügen Sie über Sicherheitskontrollen, um sich vor diesen ausnutzbaren Schwachstellen zu schützen? Wie sieht es mit allgemeinen Sicherheitskontrollen aus?
- Haben Sie Richtlinien und Verfahren oder Standardarbeitsanweisungen zur Handhabung von Sicherheits- und Betriebsabläufen implementiert?

Der Endpunkt ist der neue Perimeter

Zero-Trust-Sicherheit erfordert, dass Nutzer mittels mehrstufiger Authentifizierung (MFA) nachweisen, wer sie sind. Nachdem sie identifiziert und verifiziert wurden, erhalten Benutzer nur Zugriff auf die spezifischen Ressourcen, die sie benötigen. Ein Zero-Trust-Modell wendet auch Mikrosegmentierung an, um ein Netzwerk in kleinere Sicherheitszonen aufzuteilen und so laterale Bewegungen zu beschränken. Das ist alles großartig, aber ohne Endpunkt-Visibilität können Geräte am Netzwerkrand über ungepatchte Schwachstellen und unsichere Konfigurationseinstellungen weiterhin kritischen Bedrohungen ausgesetzt sein. Neben der Benutzerauthentifizierung müssen Unternehmen die Möglichkeit haben, die „Identität" des Endpunkts zu überprüfen, indem sie den Sicherheitsstatus von Remote-Computern bestätigen. Was passiert, wenn ein Benutzer von einem Heimcomputer, der seit vier Jahren nicht gepatcht wurde, auf das Firmennetzwerk zugreift? Was geschieht, wenn dieser Endpunkt kompromittiert wurde?

Tanium erweitert das Zero-Trust-Modell um die Endpunkt-Perspektive



Mit Tanium Endpoint Identity können Sie Tanium in Identity-and-Access-Management(IAM)-Anbieter integrieren, um festzustellen, ob Geräte, die sich mit Ihren Cloud-Anwendungen und Zero-Trust-Netzwerken verbinden, verwaltet und sicher sind.

Mitarbeiter greifen in der Regel über firmeneigene Computer auf Cloud-Anwendungen zu. Manchmal kann es jedoch vorkommen, dass ein Mitarbeiter einen anderen Computer für die Anmeldung verwenden muss. Ein Beispiel: Ein Angestellter auf Verwandtenbesuch hat seinen vom Unternehmen zur Verfügung gestellten Computer zu Hause gelassen, muss aber jetzt dringend einen Arbeitsauftrag erledigen. Er möchte sich über den unverwalteten Computer seines Verwandten bei der Cloud-Anwendung anmelden. Sobald er die Anmeldung versucht, wird der Endpunkt mit den bekannten verwalteten Endpunkten in Tanium verglichen. Da es sich um einen nicht verwalteten Computer handelt, ist es ihm nicht gestattet, auf Systeme oder Anwendungen mit sensiblen oder geschützten Unternehmensdaten zuzugreifen. Taniums Zero-Trust-Ansatz ist kontextbewusst. Das bedeutet, dass alle Signale kombiniert und mit Echtzeitdaten und Bedrohungsdaten verglichen werden, um einen genauen, umfassenden Überblick und ein Verständnis darüber zu erhalten, was im Netzwerk zu einem bestimmten Zeitpunkt passiert.

Ergänzend zu Endpoint Identity bietet Tanium eine Vielzahl von Funktionen, die bei der Planung und Umsetzung von Zero Trust helfen.

Der Weg zu einer Zero-Trust-Strategie

Angriffe identifizieren und Netzwerk schützen

Kommunikationspfad identifizieren

Zero-Trust-Architektur planen und implementieren

Überwachung und Wartung

Tanium-Lösungen für eine Zero-Trust-Strategie

Tanium Threat Hunting:

- Ermöglicht es Sicherheitsteams, Vorfälle zu erkennen, zu untersuchen und zu beheben
- Stellt sicher, dass Sicherheitsrichtlinien sowohl auf mit Domänen verbundene als auch nicht mit Domänen verbundene Assets angewendet werden. Die größte Stärke von Tanium ist seine Fähigkeit, Visibilität und Kontrolle über verbundene und mobile Assets in der Geschwindigkeit und Größenordnung bereitzustellen, die erforderlich sind, um die für eine effektive Zero-Trust-Architektur erforderlichen Echtzeitbewertungen zu erhalten.
- Stellt Vertrauenstellungen und Berechtigungen, die Benutzern und Assets in einer Active-Directory-Umgebung gewährt werden, visuell dar. Die Kontrolle über diese Beziehungen ist der Schlüssel zur Reduzierung des lateralen Bewegungspotentials. Sie ist auch Ausgangspunkt für die Zero-Trust-Planung, indem Benutzer, Konten und Assets identifiziert werden, die strengere Zugriffsanforderungen erfüllen sollten.

Tanium Asset Discovery & Inventory und Tanium Client Management-Lösungen:

- Bietet Visibilität über verwaltete und nicht verwaltete Assets, die mit dem Unternehmen verbunden sind. Die Visibilität nicht verwalteter Assets ist für viele Unternehmen eine Herausforderung. Oft sind 15–20 % der Assets eines Unternehmens unbekannt, nicht überwacht und nicht verwaltet.
- Führt nicht nur eine Bestandsliste der Online- und Offline-Endpunkte, sondern kann auch verwendet werden, um Daten einer „Schatten-IT“ zuzuordnen. Dabei handelt es sich um zulässige BYOD-Geräte und andere Endpunkte, die sich mit den Unternehmensressourcen verbinden können, aber anders verwaltet werden als dessen Haupt-Assets.
- Bietet eine Anwendungsservicevisualisierung aus mehreren Blickwinkeln, sodass End-to-End-Serviceabhängigkeiten identifiziert und in die Zero-Trust-Planung einbezogen werden können.

Tanium Risk & Compliance Management:

- Führt Schwachstellen- und Compliance-Bewertungen anhand von Betriebssystems-, Anwendungs-, und Sicherheitskonfigurationen und -richtlinien durch. Es liefert die Daten, die für die Schließung der Sicherheitslücken, die Verbesserung der IT-Hygiene und die Vereinfachung der Vorbereitung auf Audits notwendig sind.
- Beugt Sicherheitsvorfällen vor, indem Endpunkte mit Patches auf dem neuesten Stand gehalten werden.

Zero Trust schafft auf Grundlage dieser Eckpfeiler eine robuste Sicherheitsarchitektur, denn ohne die vollständige Kenntnis einer Umgebung lässt sich keine effektive Sicherheitsarchitektur implementieren. Ohne ein wirksames Compliance-Management ist es schwierig zu bestimmen, welche Systeme über bestimmte Ports und Protokolle kommunizieren dürfen. Jede Komponente unterstützt die Funktionen der anderen Komponente und letztendlich eine Zero-Trust-Implementierung.

Fazit

Wir leben in komplizierten Zeiten. Wo es früher ein eindeutiges Netzwerksicherheitsmodell gab – weil klar war, wer auf das Netzwerk zugreift – sind die Dinge heute wesentlich komplexer. Um ihre Sicherheit zu gewährleisten, müssen dezentral organisierte Unternehmen alle Aktivitäten im gesamten Netzwerk für Benutzer und Endpunkte überwachen und steuern. Unternehmen benötigen ein durchgängiges Sicherheitsmodell, das für die neue Realität der Remote-Arbeit, Cloud-Services und mobilen Kommunikation entwickelt wurde. Zero Trust wurde genau für diese neue Realität geschaffen. Der Schlüssel, um Zero-Trust-Sicherheit in großem Maßstab umzusetzen, ist die Endpunkt-Visibilität.

Tanium ist der ideale Partner für Ihre Zero-Trust-Sicherheit. Vorteile von Tanium:

- Echtzeit-Visibilität über alle Ihre Assets, sowohl im als auch außerhalb des Netzwerks.
- Visibilität der Abhängigkeiten zwischen Assets, Anwendungen und Services.
- Visibilität der Vertrauenstellungen und Berechtigungen, die Benutzern und Assets in einer Active-Directory-Umgebung gewährt werden.
- Zuverlässige Anwendung von Sicherheitsrichtlinien auf Endpunkte, unabhängig davon, ob es sich um Domänen- oder Mobilgeräte handelt.
- Verbesserte allgemeine Cyber-Hygiene und Visibilität in mit dem Netzwerk verbundene Geräte.

Vor allem ist Tanium eine flexible Plattform, die mehrere Betriebssysteme (Windows, Linux, Mac und mehr), kundenentwickelte Inhalte und On-Premise-, Cloud- oder As-a-Service-Bereitstellungsmodelle unterstützt.

Erfahren Sie mehr darüber, wie Tanium Ihnen helfen kann, Visibilität, Kontrolle und eine Single Source of Truth über Ihre umfangreichen Asset-Daten zu erhalten, um darauf aufbauend eine Zero-Trust-Strategie in Ihrem Unternehmen einzuführen.

Kontaktieren Sie uns unter **www.tanium.com**.

Tanium ist die Plattform, der Unternehmen vertrauen, wenn sie Visibilität und Kontrolle für alle Endpunkte in lokalen, Cloud- und hybriden Umgebungen erzielen möchten. Unser Ansatz bietet eine Lösung für die wachsenden Herausforderungen der heutigen IT. Durch die Bereitstellung präziser, vollständiger und aktueller Endpunktdaten erhalten Teams für IT-Betrieb, -Sicherheit und -Risiko die Möglichkeit, ihre Netzwerke schnell zu verwalten, zu sichern und zu schützen. Tanium verfolgt die Mission, Organisationen dabei zu helfen, jeden Endpunkt zu erfassen und zu kontrollieren.

Besuchen Sie uns unter www.tanium.com und folgen Sie uns auf LinkedIn und Twitter.