Zero Trust

Über die Grenzen hinaus

Zero Trust

Über die Grenzen hinaus

0.0	WARUM ZERO TRUST?	1
1.0	ZERO TRUST FÜR DIE BELEGSCHAFT	5
2.0	ZERO TRUST FÜR WORKLOADS	7
3.0	ZERO TRUST FÜR DEN ARBEITSPLATZ	10
4.0	ZUSAMMENFASSUNG	13

AUTHORS

J. Wolfgang Goerlich
Wendy Nather
Thu Pham

TRANSLATORS

Simon Alles
Athena Brown

0.0

Warum Zero Trust?

Die unsichtbare Linie, die wir ziehen zwischen was zum Unternehmen gehört und was nicht - Server, Desktops, Netzwerke, Anwendungen und Anmeldungen - hängt traditionell von Firewalls und Endpoint-Resident Sicherheitssoftware ab um diese Grenze zu schützen, aber in den Schlagzeilen finden sich viele Beispiele dafür, dass dies einfach nicht reicht. Die Menschen haben sicherlich den Niedergang des Perimeters seit Jahren gefördert: **das Forum von Jericho** wurde bereits im Jahr 2003 geschaffen, um die "De- Perimeterisierung" anzugehen. Diese Idee nahm zunehmend an Fahrt durch die fortschreitende Akzeptanz der Cloud als gängiger Ort zum Speichern und Verarbeiten von Daten auf. John Kindervag von Forrester Research prägte den Begriff „Zero Trust" um 2009 herum um einen Spezifischen Rahmen vorzuschlagen. Google beschrieb detailliert wie sie das Prinzip intern umsetzten und nannten es “BeyondCorp.” Es ist heute für viele Organisationen durch dieses konkrete Beispiel der Umsetzung praktisch greifbar.

Die Idee sich vom Perimeter zu lösen ist generell zu beängstigend für Unternehmen, speziell wenn diese erst kürzlich eine solche gefestigt haben.

Also versuchen wir nicht über die Beseitigung des Perimeters nachzudenken, stattdessen eher an eine Verstärkung der internen Sicherheit damit das Netzwerkperimeter nicht das einzige ist was Angreifer fern hält.

Der traditionelle Ansatz

Der klassische Ansatz bei der Sicherung von Unternehmensdaten nahm verschiedene Dinge an:

1. Jeder Endpunkt, der für den Zugriff auf Ressourcen verwendet wird, war im Besitz des Unternehmens und wurde von dort ausgestellt und verwaltet.

2. Alle Benutzer, Geräte und Anwendungen befanden sich an festen und vorhersehbaren Standorten, in der Regel in einem Unternehmensnetzwerk hinter einer Firewall.

3. Eine Verifikationsmethode am Ort des Erstzugangs war ausreichend.

4. Vom Unternehmen verwaltete Systeme mit der gleichen Klassifizierung könnten sich alle eigensicher gegenseitig vertrauen.

Im Laufe der Jahre haben wir erkannt, dass diese Annahmen nicht mehr zutreffen. Dies ist der Mobilität, BYOD (bring your own device), der Cloud und der verstärkten Zusammenarbeit zwischen Partnern zu verdanken. Die Konsumisierung der IT hat dieBenutzer dazu veranlasst, eine stärker angepasste Umgebung zu verlangen und darauf zu bestehen, ihre persönlichen Geräte ohne Unternehmensführung zu benutzen. Angreifer, die es über einen Verifizierungspunkt hinaus schaffen (wie eine Firewall oder eine Benutzeranmeldung) kann das inhärente Vertrauen ausnutzen und sich seitlich innerhalb eines Netzwerks, einer Anwendung oder einer Umgebung bewegen, um auf sensible Daten zuzugreifen. Ein Insider, der innerhalb eines vertrauenswürdigen Bereichs beginnt, kann Privilegien eskalieren.
Wir können nicht länger davon ausgehen, dass "interne" Entitäten vertrauenswürdig sind, dass sie direkt verwaltet werden können, um das Sicherheitsrisiko zu verringern, oder dass es ausreicht, sie einmal zu überprüfen.

Auf dem Weg zu Zero Trust

Kindervag definierte das Leitprinzip für „Zero trust" als "niemals vertrauen, immer überprüfen". Anders gesagt, gehen Sie davon aus, dass jeder Teil Ihres Netzwerks potenziell feindlich gesinnt ist, so als wäre er direkt imInternet und behandeln Sie Zugangsanträge entsprechend. Bedrohungen, die es schaffen, die Firewall zu umgehen (z. B. durch kompromittierte Benutzeranmeldeinformationen oder eine anfällige Web-Anwendung), oder die innerhalb des internen "vertrauenswürdigen" Netzwerks beginnen, sollten durch zusätzliche Sicherheitskontrollen gestoppt werden die eine seitliche Bewegung verhindern und dadurch die Auswirkungen eines Verstoßes minimieren.

Anstatt sich den Perimeter als eine Art Zugangskontrolle am "Rand" der Netzwerk vorzustellen, **stellen Sie sich diesen als einen beliebigen Ort vor, an dem Sie eine Zugangskontrollentscheidung treffen.** Das könnte immer noch an der Firewall oder am Switch liegen, aber es könnte auch auf anderen Ebenen liegen: der Unterschied zwischen dem Einloggen in eine SaaS-Anwendung eines Drittanbieters mit einer persönlichen ID und dem Einloggen mit einer persönlichen ID. Die Unternehmens-ID bestimmt, welche Sicherheitsentscheidungen gelten und wer sie trifft. Wo eine Anwendung versucht, auf eine Datenbank zuzugreifen, ist das ein Perimeter. Wenn ein Benutzer die Berechtigung zum Ausführen einer empfindliche Operation erhebt, ist das auch ein Perimeter. Das Zero-Trust-Modell der Sicherheit fordert Sie auf Ihre Vertrauensannahmen jedes Mal zu hinterfragen, wenn es ein Zugriffsereignis gibt.

Der Zero Trust Ansatz

Ein Zero Trust Modell baut auf folgenden Grundlagen auf:

- **Sichtbarkeit informiert die Richtlinien.** Liefern Sie so viele Informationen wie möglich und einen möglichst großen Einblick in die Menschen, die die Technologie verwalten, um eine informierte Richtlinie zu erstellen.
- **Vertrauen ist weder binär noch dauerhaft.** Bewerten Sie kontinuierlich die Aufstellung von Benutzern, Geräten und Anwendungen neu und passen Sie Ihr Vertrauen entsprechend an. Sein Sie bereit auf Ereignisse zu antworten, die das Risikoniveau erhöhen, indem sie neu entdeckte Bedrohungen und Schwachstellen eindämmen.
- **Eigentum ist keine Kontrolle.** Validieren Sie und weiten Sie das Vertrauen aus auf Geräte, Anwendungen und Netzwerke, die Sie nicht besitzen oder verwalten, von BYOD- und IoT-Geräten (Internet der Dinge) bis SaaS und öffentliche Cloud.
- **Der Perimeter ist jeder Ort, an dem Sie eine Zugangsentscheidung treffen.** Wählen Sie die Ebenen und Prozesspunkte die für Ihr Umfeld funktionieren, sei es auf der Netzwerkebene, die Anwendungsebene, am Punkt der Identität-Verifizierung, oder während eines Transaktions-Workflows.
- **Entscheidungen über den Zugang basieren jedes Mal auf der Wiederherstellung von Vertrauen.** Mitgliedschaft in einer Gruppe, ein Anwendungsdienst innerhalb einer Ebene oder ein an ein Netzwerk angeschlossenes Gerät reichen allein nicht aus, um Aktivitäten zu autorisieren.
- **Eindämmung.** Kombinieren Sie aus geringsten Privilegien und Segmentierung mit Reaktionsfähigkeiten zur Überwachung von Bedrohungsaktivitäten und begrenzen Sie seine Verbreitung standardmäßig.

Zusätzlich zur Infragestellung aller Annahmen von Vertrauen sollte Ihre Umsetzung idealerweise diese Merkmale umfassen:

- **Transparenz.** Sicherheit ist für Menschen so unsichtbar wie möglich unter Verwendung der Technologie[1].
- **Zero-Touch für Zero Trust.** Minimierung des administrativen Aufwands durch Rationalisierung, Automatisierung, Orchestrierung und Integration.

GESCHÄFTSERGEBNISSE

Mit dem Zero Trust Modell erhalten Sie eine **bessere Sichtbarkeit** Ihrer Benutzer, Geräte, Container, Netzwerke und Anwendungen, denn Sie verifizieren ihre Sicherheitszustände mit jeder Zugriffsanfrage.

Sie können die Angriffsfläche Ihrer Organisation reduzieren, indem Sie Ressourcen segmentieren und nur diese Berechtigungen und Verkehr erlauben, welche unbedingt erforderlich sind. Und durch den Einsatz von mehr Authentifizierungsfaktoren, das Hinzufügen von Verschlüsselung und der Markierung bekannter und vertrauenswürdiger Geräte, können Sie es **Angreifern erschweren zu sammeln** was sie benötigen (Benutzeranmeldeinformationen, Netzwerkzugang und die Fähigkeit, sich seitlich zu bewegen).

Letztendlich können Ihre Benutzer eine konsistente und produktivere Sicherheitserfahrung haben, unabhängig davon, wo sie sich befinden, welche Endpunkte sie verwenden, oder ob es sich bei ihren Anwendungen um firmeninterne Anwendungen handelt oder in der Cloud.

[1] Einige Experten haben dies auch als "Durchsichtigkeit" beschrieben: es sollte gerade sichtbar genug sein, so dass die Benutzer wenn nötig vergewissern können, dass es da ist.

Einführung in die drei Säulen von Zero Trust

Sicherheit ist keine Einheitslösung, auch nicht innerhalb der gleichen Unternehmensumgebung. Zum Beispiel ist kontinuierliche Authentifizierung eine großartige Idee, bis sie mit den Benutzern in Konflikt gerät die einen reibungsarmen Workflow haben: wenn sie mit mehreren Faktoren zu oft authentifizieren müssen, werden sie es übel nehmen (und versuchen den Kontrollen zu umgehen, die dies erfordern).

Andererseits hat Software selbst nichts gegen häufige Authentifizierung, so dass die Workloads miteinander kommunizieren können und diese Interaktionen unterstützen können. IoT-Geräte, wie z.B. medizinische oder Fertigungsgeräte, können sowohl Auswirkungen auf die Sicherheit als auch auf die Verfügbarkeit haben, die beeinflussen, wie sie an ein Netzwerk angebunden sind. Wir stellen drei Säulen der Zero-Trust-Sicherheit vor, um die Unterschiede zu umreißen

01

Zero Trust für die Belegschaft

Personen wie Mitarbeiter, Auftragnehmer, Partner und Anbieter, die Zugang zur Arbeit haben unter Verwendung ihrer persönlichen oder von Unternehmen verwalteten Geräte. Diese Säule stellt sicher, dass nur die richtigen Benutzer und sichere Geräte auf Anwendungen zugreifen können, unabhängig vom Standort.

02

Zero Trust für Workloads

Anwendungen, die in der Cloud laufen, in Rechenzentren und andere virtualisierten Umgebungen, die miteinander interagieren. Diese Säule konzentriert sich auf sicheren Zugriff wenn eine API, ein Mikrodienst oder ein Container auf eine Datenbank innerhalb einer Anwendung zugreift.

03

Zero Trust für den Arbeitsplatz

Diese Säule konzentriert sich auf den sicheren Zugang für beliebige und alle Geräte (einschließlich IoT) die mit Unternehmensnetzwerken verbunden sind, wie Benutzer-Endpunkte, physische und virtuelle Server, Drucker, Kameras, HVAC-Systeme, Kioske, Infusionspumpen, industrielle Steuerungssysteme und mehr.

In den folgenden Abschnitten untergliedern wir jede Säule nach den angesprochenen Risiken, Optionen für die Umsetzung und vorgeschlagene Reifegrade.

	WER ODER WAS	VERTRAUEN WIRD VERIFIZIERT WENN	VON
BELEGSCHAFT	Personen & ihre Geräte	Zugriff auf Anwendungen	Überall
WORKLOAD	Anwendungen, Dienste, Mikroanwendungen	Mit anderen Systemen kommunizieren	On-Site, Hybrid-Cloud, Öffentliche Cloud
ARBEITSPLATZ	IT Endpunkte & Server, Internet der Dinge (IoT) Geräte, Industrial Control Systems(ICS)	Auf das Netzwerk zugreifen	On-Site, Hybrid-Cloud, Öffentliche Cloud

1.0

Zero Trust für die

Belegschaft

ANGESPROCHENE RISIKEN

Zero Trust für die Belegschaft spricht mehrere wichtige Risiken für das Unternehmen an:

- Primäre Konto-Berechtigungsnachweise (Benutzername und Passwort) werden oft durch Phishing-Angriffe oder kompromittierte Dritte gestohlen, und werden von Angreifern aus abgelegenen Standorten wiederverwendet, einschließlich Botnets. Laut dem ***2019 Verizon Data Breach Investigations Report*** sind nahezu ein Drittel der Datenschutzverletzungen auf kompromittierte Anmeldeinformationen zurückzuführen. Es zeigt sich, dass Passwörter effektiv sind bei dem Umgehen von traditioneller Perimeter-Verteidigung um unerkannt auf Daten zuzugreifen.
- Ein Angriff, der die Firewall umgehen kann oder der auf dem internen Netzwerk startet, kann sich ausbreiten, um kritische Systeme zu kompromittieren und sensible Daten zu stehlen. Und ehrlich gesagt: **ein ausreichend erfolgreicher Außenseiter sieht genauso aus wie ein Insider**. Ein externer Angreifer wird die gleichen Mittel verwenden, um in den Vorgang für den legitimen Benutzer einzudringen, so dass Sie sicherstellen müssen, dass das, was jeder tun kann, begrenzt wird.
- Ein weiteres Risiko besteht darin, dass der Angreifer die Lücken zwischen verschiedenen Richtlinien oder Durchsetzung ausnutzt, welche sich auf dasselbe Objekt beziehen. Wenn die gleichen vertraulichen Daten in zwei verschiedenen Systemen verfügbar sind, die unterschiedliche Arten der Authentifizierung verwenden, wird der Angreifer denjenigen zu verfolgen, der leichter zu erreichen ist - entweder weil er etwas anderem vertraut dass Sie nutzen können, oder weil diese eine Authentifizierungsmethode einen Fehler aufweist. Wenn eine Anwendung oder ein System mit verschiedenen Kontrollen geschützt wird, abhängig davon, ob sich der Benutzer "innerhalb des Perimeters" befindet oder nicht, kann ein Angreifer lockerere Kontrollen kompromittieren.
- Externe Cloud-basierte Anwendungen und mobile Benutzer können Attacken ausgesetzt sein, die sich ausserhalb des Schutzes des Unternehmensperimeters befinden.
- Benutzer können die Organisation durch die Verwendung von unverwalteten und nicht gepatchten Geräten angreifbar machen, die auf kritische Daten und Systeme zugreifen wollen. Diese Schwachstellen können Angriffe durch Ranssomeware und anderer Malware führen, sowie zu unerlaubtem Zugriff.

ÜBERBLICK

Die Umsetzung von Zero Trust für die Belegschaft beruht auf der Kombination von validierten Benutzern mit validiertem Endpunkt-Geräten. Diese Kombination wird weiter verriegelt mit End-to-End-Verschlüsselung zwischen diesen Geräten und den Ressourcen, auf die sie zugreifen.

Schließlich ist den Benutzern nur der bloße Mindestzugang erlaubt Welcher für ihre Rollen benötigt wird (was auch als "geringstes Privileg" bezeichnet wird). Solange der Benutzer mit der richtigen Anzahl an Faktoren authetifiziert wird und er einen Endpunkt nutzt der angemeldet und hinsichtlich Sicherheitsschwachstellen inspiziert wurde, kann er genau auf die Ressourcen zugreifen, die ihnen von einem zentralen Bevollmächtigten zur Verfügung gestellt werden.

BELEGSCHAFTSREIFE MODELL

STUFE 1 BENUTZERVERTRAUEN HERSTELLEN

Stellen Sie sicher, dass Sie über die richtigen Mechanismen und Prozesse verfügen, um sicherzustellen, dass nur autorisierte Benutzer versuchen, auf Ihre Ressourcen zuzugreifen. Dies kann auf verschiedenen Wegen erreicht werden, allerdings ist Multi-Faktor-Authentifizierung (MFA) hier eine weit verbreitete Technologie.

STUFE 2 SICHTBARKEIT VON GERÄTEN UND AKTIVITÄTEN

Welcher Endpunkt oder welches Gerät wird bei jeder Zugriffsanfrage verwendet? Wie ist ihre derzeitige Sicherheitsstatus, und woher kommt der Antrag? Dies ist eine Schlüsselphase zur Erkennung von Kontoübernahmeversuchen und anderen Risiken.

STUFE 3 VERTRAUENSWÜRDIGE GERÄTE

Ob es sich um ein unternehmenseigenes Gerät handelt oder nicht, ob es verwaltet wird oder nicht, das Unternehmen kann verstrauenswürdige, registrierte Geräte markieren um mit diesem bestimmten Benutzer verbunden zu sein.

STUFE 4 ANPASSUNGSFÄHIGE RICHTLINIEN

Führen Sie Anforderungen für den Zugang basierend auf der Sensibilität der Ressourcen und den bekannten Sicherheitszustand ein, um mit den Risiken angemessen umzugehen. Diese Richtlinien reichen von der Zulassung von nur von Unternehmen verwalteten Geräten, bestimmte Versionen von gepatchter Software, bis zu Verschlüsselung oder Step-up-Authentifizierung auf der Grundlage des Benutzerverhaltens.

STUFE 5 ZERO TRUST FOR THE WORKFORCE

At this point, all applications and systems are covered by the previously listed stages; monitoring and response to risk events are going on continuously; and the users get a consistent single sign-on experience.

2.0
Zero Trust für
Workloads

ANGESPROCHENE RISIKEN

Zero Trust für Workloads adressiert verschiedene wichtige Risiken für das Unternehmen:

- Ein Angreifer, der die Schwachstellen einer Anwendung ausnutzt kann sich seitlich verschieben um kritische Systeme zu kompromittieren.
- Ein Angreifer, der an sensible Daten gelangt und der Daten aus dem Netzwerk exfiltriert.
- Uneinheitliche Kontrollen zwischen internen Anwendungen und externen cloudbasierten Anwendungen schaffen Blind Spots für die Abwehr.
- Entwickler machen die Organisation verwundbar durch den Code und Konfiguration von Webanwendungen.
- **Vierundfünfzig Prozent der Schwachstellen bei Web-Anwendungen machen eine öffentliche Ausnutzung möglich,** was bedeutet, dass sie für Fehler offen stehen die durch Angreifer für den Zugriff auf Ihr System ausgenutzt werden können wenn Server und Anwendungen nicht gepatcht sind.

ÜBERBLICK

Unternehmenssysteme neigen dazu, organisch zu sein: sie wachsen in Funktionalität und fügen Verbindungen und Abhängigkeiten hinzu als Antwort auf geschäftliche Bedürfnisse. Um diesen Wachstum zu erleichtern, können Systemdesigner und Entwickler manchmal zu freizügigsten und flexibelsten Sicherheitskonfigurationen neigen. Dies schafft übermäßiges Vertrauen, das Angreifer ausbeuten können und sich seitlich bewegen um auf sensible Ressourcen zuzugreifen.

Die Lehrbuchantwort auf diese Herausforderung lautet Netzwerksegmentierung. Betrachten Sie eine generische dreistufige Webanwendung: Präsentationsschicht, Anwendungsschicht und Datenschicht.

Diese Ebenen können in verschiedene Netzwerke segmentiert werden, mit spezifische Zugriffskontrollen, die die Kommunikation zwischen den Ebenen einschränken. Selbst in diesem einfachen Beispiel wird den Diensten auf der Anwendungsebene vertraut, dass sie mit anderen Diensten auf derselben Ebene kommunizieren, mit wenig Blick auf das Risiko von Seitenbewegungen innerhalb der Ränge. Die Probleme des übermäßigen Vertrauens nehmen mit der Komplexität und der Anzahl der Anträge zu. Darüber hinaus kann eine Organisation mit der Zeit den Überblick verlieren über welche Workloads kritischer Natur sind und welche andere Ressourcen mit ihnen kommunizieren müssen, was eine Sperrung erschwert.

Es gibt zwei philosophische Möglichkeiten, auf die Bedenken einzugehen. Wir können davon ausgehen, dass das Netzwerk nicht vertrauenswürdig ist und die Vertrauensentscheidung bis hinauf in alle Anwendungsebenen verschoben wird. Der Nutzen dieser Philosophie besteht darin, dass wir die Kontrolle in die Anwendung legen. Der Nachteil ist, dass Anwendungen mit diesem Zero-Trust-Ansatz in Kraft entwickelt werden müssen. Entwickler dokumentieren nicht immer wie eine Anwendung im Rahmen des eigenen Workloads kommunizieren soll, umso weniger wie mit externen Ressourcen; dies macht es für die Teams für Netz- und Sicherheitsoperationen schwieriger, wie man die geringsten Privilegien und die Verfügbarkeit von Anwendungen in Einklang bringt.

Alternativ können wir das Vertrauen in das Netzwerk reduzieren, indem wir die Kommunikation auf das zu beschränken, was für die Anwendung notwendig ist. Diese Philosophie funktioniert gut für bestehende Anwendungen, einschließlich Legacy-Anwendungen, und kann ein Weg sein ein bestehendes Ökosystem in das Zero Trust Modell zu integrieren. Der Nachteil dabei ist, dass wir auf das Netzwerk angewiesen sind für die Sicherheit und, sollte diese Sicherheit gefährdet sein, die Anwendungsdienste nichts von der reduzierten Sicherheitsaufstellung wissen.

Diese Philosophien schließen sich nicht gegenseitig aus, und in der Tat können beide nützlich sein, um sich in einer Umgebung auszugleichen wo redundante Kontrollen für eine hohe Sicherheit erforderlich sind.

Zum Bootstrapping bestehender Umgebungen in Zero Trust Modelle müssen unsere Netzwerke das Vertrauen bewerten und Entscheidungen über die Zugangskontrolle zum Zeitpunkt der Netzwerkkommunikation treffen. Dies ist kein einfaches Unterfangen, wenn man unsere Bewerbungsdienste betrachtet, die oft über Cloud-Service-Provider und Rechenzentren und andere heterogene virtualisierte Umgebungen verteilt sind. Wir müssen ein Anwendungsökosystem definieren, das nur die Abhängigkeiten der Anwendung enthält: Dienstleistungen, Prozesse und Netzwerkkommunikation. Wir können dann eine Zugangskontrolle unter Verwendung einer Whitelist oder Standardverweigerung anwenden, so dass nur das, was die Anwendung erfordert erlaubt ist, unabhängig von Netzwerk oder Umgebung. **Wir definieren Vertrauen durch die Einzigartigkeit der Anforderungen der Anwendung, nicht durch den Netzwerkstandort.**

Um diese Mikrosegmentierung zu erreichen, sind drei Technologien erforderlich, die bis vor kurzem außer Reichweite waren.

- **Tiefe und durchdringende Sichtbarkeit der Netzwerkkommunikation.** Verteilte Netzwerksensoren anstelle von traditioneller zentralisierter Überwachung (SPAN/TAP oder NetFlow) haben eine solche Sichtbarkeit in großem Maßstab möglich gemacht.
- **Genaue und Echtzeit-Anwendungsmodellierung.** Große Datenanalyse-Techniken haben den manuellen Aufwand bei der Dokumentation von Anwendungen reduziert, und ermöglichen so ein aktuelles Verständnis der Verkehrsmuster und Abhängigkeiten.
- **Die Fähigkeit, Richtlinien auf mehreren Geräte in mehreren Umgebungen anzuwenden.** Ein Richtlinien-Motor auf hoher Ebene, der die fortschreitende Ausbreitung von Zugangskontrollgeräten in Multi-Cloud-Umgebungen verwaltet, vereinfacht die Schritte, die erforderlich sind, um auf die Sichtbarkeit und Analyse der Anwendung einzuwirken.

Kombiniert verringern Sichtbarkeit, Analysen und Richtlinien das übermäßige Vertrauen in die Anwendungsökosysteme.

Aber was passiert, wenn selbst dieses Vertrauen missbraucht wird? Denken Sie zum Beispiel an das Risiko, dem ein Unternehmen durch die Administratoren und andere privilegierte Benutzer ausgesetzt ist, die in der Regel erhöhten Zugang im Maßstab haben. Jeder Eindringling, der Entwickler- oder Administrator-Zugangsdaten kompromittiert könnte möglicherweise Zugang erhalten, ohne dass die Sicherheitsoperationen es merken. Personelle Sicherheitsoperationen mit Personen zur Überprüfung der einzelnen Workloads und Verbindungen skalieren nicht. Um Zero Trust für Workloads herzustellen wird unverwaltetes maschinelles Lernen sowie Verhaltensanalysen eingesetzt um Anzeichen von böswilliger Aktivität zu überwachen. Wenn es identifiziert wird, kann das Netzwerk durch Quarantäne von Servern und Blockierung der Kommunikation das Vertrauen widerrufen.

Wenn die Beschleunigung des Change die menschliche Kapazität übersteigt ist der Schritt zu automatischen Prozessen unumgänglich. Dies ist der heutige Stand der Segmentierungsbemühungen. Die Annahme eines Zero-Trust-Denkens ermöglicht Systemdesignern und Entwicklern das Problem auf neue Weise anzugehen. Mit besserer Sichtbarkeit, schnellere Analysen und einem tieferen Verständnis der Anwendungskommunikation definiert Zero Trust für Workloads den Umfang um das erwartete Verhalten herum neu. Böswillige Aktivitäten, von anfänglicher Kompromittierung zur lateralen Bewegung bis hin zu Datenexfiltration wird dann offensichtlich und vermeidbar.

REIFEGRADMODELL FÜR WORKLOADS

STUFE 1 VERTRAUEN IN WORKLOADS SCHAFFEN

Entdecken Sie das Ökosystem der Anwendungen und Umgebungen mit missionskritischen Workloads. Diese Stufe legt den Rahmen für die ZeroTrust Initiative fest.

STUFE 2 SICHTBARKEIT DER WORKLOADS

Erhalten Sie Sichtbarkeit in alle Geräte, Prozesse, Pakete, Netzwerk-Flows und Workload-Kommunikationen innerhalb der Umgebung der Anwendung. Diese Bemühungen sind auf das Anwendungsökosystem ausgerichtet, und Sichtbarkeit ist entscheidend, um Einblicke in die Arbeitsbelastung zu gewinnen (wie nicht gepatchte Software und Konfigurationszustände).

STUFE 3 ABHÄNGIGKEITEN VON ZUORDNUNGEN DER ANWENDUNGEN

Analysieren Sie die Netzwerkkommunikation und Datenflüsse, um Anwendungen zu modellieren, kategorisieren Sie die Anwendungsebenen, und identifizieren Sie die Anwendungsabhängigkeiten. Dies wird über einen bestimmten Zeitraum durchgeführt um unregelmäßige Aktivitäten zu erfassen, wie z.B. monatliche Jobs oder ein Buchhaltungsprozess pro Quartal. Je genauer die Zuordnung der Anwendung, desto genauer werden die daraus resultierenden Richtlinien.

STUFE 4 RICHTLINIEN UND MIKROSEGMENTIERUNGEN

Entwickeln Sie Richtlinien um das Vertrauen innerhalb der Ökosystems der Anwendung zu minimieren, simulieren und validieren Sie Richtlinien, und wenden Sie die Richtlinien konsistent in allen Umgebungen an, unter Beachtung der Kontoidentität und der kontextuellen Informationen von den Säulen der Belegschaft und des Arbeitsplatzes wie angemessen. Mikrosegmentierung verfolgt des Ansatz von Traffic Whitelisting, auch bekannt als Default Deny, um zum Verschieben des Zugangs zum Umkreis von genau dem, was für die Workload erforderlich ist.

STUFE 5 ZERO TRUST FÜR WORKLOADS

Entwickelte Zero Trust Organisationen zeigen anhaltende Verbesserung und laufende Überwachung der Umgebungen. Der Change ist die einzige Konstante - bezüglich der Anwendung, der Organisation und den Angriffen – und Zero Trust erfordert eine Weiterentwicklung der Richtlinien im Zuge der Weiterentwicklung des Ökosystems.

3.0
Zero Trust für den

Arbeitsplatz

ANGESPROCHENE RISIKEN

Zero Trust für den Arbeitsplatz spricht mehrere wichtige Risiken für das Unternehmen an:

- Ein Angreifer, der einen Endpunkt, Server oder Schwachstellen in der Anlagenausrüstung ausnutzt, um im Netzwerk Fuß zu fassen und sich seitlich zu bewegen um kritische Systeme zu kompromittieren.
- Ein Angreifer, der durch Angriffe auf vernetzte Geschäftsinfrastruktur den Betrieb stört.
- Schwachstellen im IoT oder Operational Technology (OT).
- Sechzig Prozent aller Unternehmen haben Sicherheitsvorfälle durch Netzwerdrucker, **laut Quocirca**.
- Es gab einen **300%igen Ansteig bei den neuen IoT Malware Varianten von 2017 bis 2018** , laut Kaspersky.

ÜBERBLICK

Der moderne Arbeitsplatz wird durch den Campus, das Rechenzentrum, WAN, dem Zweigstellen- und Cloud-Netzwerk ermöglicht. Vertrauen wird auf jeden Benutzer ausgedehnt, auf Geräte und Anwendung, kabelgebunden oder drahtlos, zur Verbindung mit anderen Benutzern, Geräten, Anwendungen und anderen Teilen des Arbeitsplatzes. Der Arbeitsplatz umfasst Endbenutzergeräte, IT Server und Drucker, industrielle Steuerungssysteme (ICS) und IoT Geräte. Zero Trust für den Arbeitsplatz schafft Vertrauen, wenn alle Arten von Geräten authentifizieren und auf den Unternehmensnetzwerken kommunizieren.

Es gibt jedoch einen sehr realen Unterschied zwischen den Geräten die von der Belegschaft genutzt werden und den Geräten an unseren Arbeitsplätzen. Die Idee der Durchsetzung von Vertrauen in Zugangsentscheidungen für EndBenutzer-Anwendungen gilt nicht für Geräte wie Drucker , Fertigungssteuerungen, HVAC und Ausweisleser. Um alle geschäftsbezogenen Systeme abzudecken, müssen wir uns tiefer im Stapel zum Netzwerk bewegen.

Der stetige Wachstum an Geräten in unseren Netzwerken hat unsere Fähigkeit Geräte zu verwalten, sie zu patchen und gegen Rogue-Geräte zu schützen strapaziert. IoT erhält viel der Aufmerksamkeit dank der Explosion bei netzwerkfähigen Geräten in den letzten Jahren. IoT wird oft auf Plattformen für Verbraucher aufgebaut, es fehlt an Sicherheitskontrollen auf Unternehmensebene und ist möglicherweise nicht patchbar. Das Ergebnis ist, dass wir mehr von diesen Geräten haben, sie haben vergleichsweise mehr Schwachstellen pro Einheit, und das IoT ist vergleichsweise schwieriger zu sichern. Während das IoT im Mittelpunkt steht wir dürfen die traditionelle Geschäftsausstattung nicht übersehen wie Drucker, Videokonferenzen, Sicherheitskameras und VoIP-Telefonie, die nach wie vor ein gangbarer Weg für Kriminelle sind, um Unternehmen zu kompromittieren. Dann müssen wir auch medizinische Ausrüstung und OT zu berücksichtigen. Diese sind oft auf Plattformen die Sicherheitsteams nicht patchen oder sichern können, aufgrund einer Reihe von betrieblichen, funktionellen und technischen Faktoren. Im Großen und Ganzen muss eine Zero-Trust-Strategie die Athentifizierung, Authorisierung, Segmentierung und Verwaltung der gesamten Ausstattung abdecken.

Zero Trust nimmt an, dass das Netzwerk von Natur aus unsicher ist. Wir müssen das Netzwerk vor den Benutzern, Geräten und Anwendungen, die damit verbunden sind, schützen, und umgekehrt. In einem Zero Trust Netzwerk muss jedes ausnutzbare Gerät abgeschirmt werden oder segmentiert werden um die Wahrscheinlichkeit einer strafrechtlichen Feststellung sowie Missbrauch des Geräts zu verringern. Desweiteren müssen in einem Zero Trust Netzwerk die verbleibenden Geräte vor anderen, kompromittierten und missbrauchten Geräten geschützt werden. Diese Schutzmassnahmen gehen Hand in Hand. Beide erfordern ein bekanntes Inventar der Entitäten die das Netzwerk nutzen, und Einblick in die Sicherheitslage von den Geräten.

Die Entscheidung über die Zugangskontrolle findet statt wenn ein Gerät sich versucht mit dem Netzwerk zu verbinden. Traditionell regelten Netzwerktechniker dies mit festgelegten Attributen wie etwa eine Kombination des Netzwerk-Switch-Standorts oder der IP-Adresse. In diesem Modell wird Geräten vertraut ohne das Wissen ob sie gefährdet sind oder missbraucht wurden. Das herkömmliche Vertrauen basiert zudem auf leicht manipulierbaren Attributen. Bei einem Wechseln zu Zero Trust wird die Entscheidung durch eine Vielzahl von Faktoren getroffen, unter ihnen Identität und Verhalten, und muss regelmäßig aufgrund von Geräteverhalten und allen sich ändernden Faktoren verifiziert werden. Insbesondere muss die Organisation in der Lage sein auf neu entdeckte Bedrohungen und Schwachstellen zu reagieren indem sie den Zugang zum Netzwerk beschränkt oder ganz abschneidet.

Network Access Control (NAC) stellt das Fundament einer Zero Trust Umsetzung dar. Die Ausrüstung muss sich im Netzwerk authentifizieren bevor es das Vertrauen zur Verbindung und Kommunikation erhält. Das Ideal ist eine softwaredefinierte Zugriffskontrolle mit 802.1X und zertifikatsbasierter Authentifizierung. Windows-basierte Geräte können die Vorteile von Active Directory- und Windows-Verwaltungsinstrumentation (WMI) um sich gegenüber dem Netzwerk zu authentifizieren. Wenn diese Methoden nicht verfügbar ist, können wir MAC Authentication Bypass (MAB) verwenden. MAB ist manipulierbar; es könnte jedoch die einzige Option sein für ältere Geräte, die neuere Methoden nicht unterstützen, oder Ausstattung die für die Nutzung neuerer Methoden nicht konfiguriert werden kann.

Die nächste Ebene eines Zero Trust Netzwerks ist die gruppenbasierte Segmentierung. Wir authentifizieren Netzwerkverbindungen. Bei der Entscheidung über den Zugang identifiziert das Netzwerk das Gerät als eines von einer oder mehreren Rollen, und als eins von einer oder mehreren Gruppen. Diese Rollen sind unabhängig von der IP-Adressierung oder dem physischer Standort. Tatsächlich umfassen in den meisten komplexen Unternehmen diese Rollen mehrere Subnetze und mehrere Gebäude. Wir definieren dann Segmentierungsrichtlinien auf der Grundlage von welche Gruppen von Entitäten mit welchen Netzwerkressourcen, einschließlich dem Internet, sprechen können. Basierend auf dem Verhalten der Ausrüstung können wir Vertrauen feststellen und beim Anlass zu Sorge den Zugang weiter einschränken. Wir reduzieren weiter das angenommende Vertrauen und stärken die Netzwersicherheit durch andauernde Überwachung der Kommunikation und kontinuirliche Verbesserung der Richtlinien.

Die Vermehrung von arbeitnehmergesteuerten Geräten hat zu einer entsprechenden Zunahme von Geräten innerhalb unseres Unternehmensnetzwerks geführt. Vom IoT zu Druckern, von OT zu medizinischen Geräten - unsere Organisationen verfügen über mehr Ausrüstung als je zuvor. Folglich ist die Angriffsfläche der Ausrüstung größer als je zuvor. Eine Zero-Trust-Strategie für den Arbeitsplatz ermöglicht Sicherheitsoperationen und Netzwerktechnikern einen besseren Einblick in alle Hosts und Kommunikationen. Sie stellt zudem strengere Restriktionen auf Netzwerk kommunikationen und setzt adaptive Richtlinien basierend auf Vertrauen um. Dann können wir das Risiko von schadhaften Aktivitäten, die unsere Geräte ausnutzen, reduzieren und schneller auf verdächtige Vorgänge reagieren.

REIFEGRADMODELL FÜR DEN ARBEITSPLATZ

STUFE 1 VERTRAUEN AM ARBEITSPLATZ SCHAFFEN

Entdecken Sie Arbeitsplatzsysteme, ihre Benutzer und Anwendungen, inklusive IoT und OT, und legen Sie ihre Funktionen innerhalb der Organisation und innerhalb des Betriebs im Netzwerk fest. Definieren Sie den Anwendungsbereich für die Zero Trust Innitiative.

STUFE 2 NETZWERK SICHTBARKEIT

Erhalten Sie Einblick in Benutzer-, Geräte- und Anwendungs kommunikation und Netzwerkflüsse innerhalb ihrer Arbeitsplatzumgebung. Verstehen und Dokumentieren Sie die In-Scope-Netzwerkfähigkeiten und Anforderungen.

STUFE 3 NETZWERKZUGANGSKONTROLLE

Konfigurieren Sie und setzen Sie Netzwerk-Authentifizierung und Authorisierung für die In-Scope-Benutzer (soweit gegeben), Geräte und Anwendungen durch. Verhindern Sie jegliche nicht authentifizierte (und daher nicht vertrauenswürdige). Entitäten vor dem Anschluss an das In-Scope-Netzwerk.

STUFE 4 RICHTLINIEN FÜR DIE SEGMENTIERUNG

Definieren Sie gruppenbasierte Richtlinien die nur solche Netzwerkverbindungen und Kommunikationen zulassen die für den Geschäftsbetrieb erforderlich sind.

STUFE 5 ZERO TRUST FÜR DEN ARBEITSPLATZ

Die letzte Stufe der Zero-Trust-Umwandlung ist die kontinuierliche Verbesserung. Definieren und neu-definieren Sie den Umfang, die Ausrüstung und die Richtlinien, um den Veränderungen bei Geräten, Fähigkeiten und organisatorische Bedürfnisse gerecht zu werden.

4.0

Zusammenfassung

Ein Zero Trust Konzept erfordert keine vollständige Neuerfindung Ihrer Infrastruktur. Die erfolgreichsten Lösungen sollten über einer hybriden Umgebung liegen und diese unterstützen, ohne bestehende Investitionen vollständig zu ersetzen.

Ein gemeinsamer dynamischer Kontext zu Identität, Verwundbarkeit und benutzerbezogener Bedrohung ihrer Geräte und Anwendungen über alle verschiedenen Durchsetzungspunkte ist der beste Weg zur Harmonisierung von Sicherheitsrichtlinien, auch wenn es zwangsläufig notwendig sein wird verschiedene Arten von Richtlinienkonstrukten und Durchsetzungsmethoden die erforderlich sind zu schaffen, um mit verschiedenen Teilen der Umgebung zu arbeiten.

Cisco Zero Trust

Cisco Zero Trust stellt einen umfangreichen Ansatz zur Sicherung jedes Zugriffs auf alle Ihre Anwendungen und Umgebungen bereit, für jeden Benutzer, jedes Gerät und von jedem Standort aus. Es schützt Ihre Belegschaft, Ihre Workloads und Ihren Arbeitsplatz.

- **Duo** schützt die Belegschaft. Mit Duo's Zero Trust Belegschaftssicherheit sichert Cisco, dass nur die richtigen Benutzer and sichere Geräte auf Anwendungen zugreifen können, unabhängig vom Standort.

- **Tetration** schützt Workloads. Mit der Zero Trust Tetrations Workload-Sicherheit von Tetration schützt Cisco alle Verbindungen innerhalb ihrer Anwendungen, über die Multi-Cloud und im Datencenter.
- **Software-Defined Access (SD-Access)** schützt den Arbeitsplatz. Durch die Zero Trust Arbeitsplatzsicherheit von SD-Access werden alle Benutzer und Geräteverbindungen im gesamten Netzwerk geschützt, inklusive IoT.

Dieses gesamte Zero Trust Sicherheitsmodell ermöglicht es Ihnen Risikien in Ihrem gesamten Umfeld abzuschwächen, sie zu erkennen und auf sie zu reagieren.

Erfahren Sie mehr über **Cisco Zero Trust**.