E-Book

Forcepoint | Powered by ConversationalGeek

Schritt für Schritt zu Zero Trust

Praktische Anleitung zur Umsetzung eines lückenlosen Zero-Trust-Modells

Einleitung

Zero Trust ist mehr als nur ein Schlagwort. Es handelt sich um ein neues Paradigma für die Implementierung von Cyber-Sicherheit, das in dem Maße an Dringlichkeit gewinnt, in dem zunehmend dezentral organisierte Unternehmen mit einer wachsenden Anzahl komplexer und raffinierter Bedrohungen konfrontiert sind, die zu Datenschutzverletzungen führen können.

In einer Arbeitswelt ohne feste Grenzen kann es schwierig sein, eine Balance zwischen bequemer Zusammenarbeit und Datensicherheit zu finden. Durch die plötzliche Zunahme mobiler Arbeit wurde die Komplexität um eine zusätzliche Dimension erweitert, da Benutzer und Daten die traditionelle, geschützte IT-Umgebung verlassen, in der implizit den Personen innerhalb des Netzwerks vertraut wurde.

Ein moderner Zero-Trust-Ansatz basiert auf dem Motto „Vertrauen ist gut, Kontrolle ist besser". Statische Alles-oder-Nichts-Annahmen darüber, wer die Benutzer sind und welche Rechte sie haben, werden durch dynamische, explizite Entscheidungen ersetzt, die jedes Mal dann getroffen werden, wenn ein Benutzer versucht, auf eine Ressource zuzugreifen oder Daten zu verwenden. Wie diese Daten übermittelt werden und was die Benutzer damit tun, wird kontinuierlich überwacht, um Auffälligkeiten und riskantes Verhalten schnell zu erkennen, bevor es zu Sicherheitsverletzungen kommt.

Dieser Leitfaden erläutert das Zero-Trust-Paradigma und zeigt Ihnen, worauf Sie bei einer Zero-Trust-Lösung achten müssen. In diesem E-Book erfahren Sie Folgendes:

- → Wie mobile Arbeit die Welt der Cyber-Sicherheit auf den Kopf stellt
- → Warum die Nutzung von VPNs für Remote-Mitarbeiter zahlreiche Probleme verursacht
- → Warum die Kontrolle der Datennutzung genauso wichtig ist wie die Kontrolle des Datenzugriffs
- → Welche Säulen ein modernes Zero-Trust-Modell hat: explizit erteilter Zugriff und laufende Kontrolle der Datennutzung – verbunden mit kontinuierlicher Überwachung, um Vertrauens- und Risikostufen zu überprüfen
- → Warum Zero Trust derzeit so viel Interesse entgegengebracht wird (z. B. von SASE, NIST und anderen)
- → Worauf Sie bei der Implementierung von Zero-Trust-Lösungen achten müssen

„Vertrauen ist gut, Kontrolle ist besser. Immer."

Die Welt – und die Cyber-Sicherheit – steht Kopf

2020 wird als das Jahr in die Geschichte eingehen, in dem eine globale Pandemie die Arbeitsweise der gesamten Wirtschaft grundlegend veränderte.

Zwar ist mobile Arbeit nichts Neues, aber die plötzliche Zunahme der Menschen, die von zu Hause arbeiten, hat Unternehmen weltweit vor große Herausforderungen gestellt. Die Stanford University berichtet, dass sich die USA zu einer „working from home economy" entwickelt haben, da 42 % der amerikanischen Arbeitnehmer während der Pandemie im Home-Office tätig waren und sind.[1]

Um den Mitarbeitern diese dezentrale und flexible Arbeitsweise zu ermöglichen, muss Ihr Unternehmen geschäftskritische Daten auf einfache Weise zugänglich machen, ohne sie der Gefahr von Missbrauch oder Diebstahl auszusetzen. Angesichts der Tatsache, dass immer mehr Benutzer, Anwendungen und Daten außerhalb der Grenzen des traditionellen Unternehmens angesiedelt sind, haben sich die auf internen Netzwerken basierenden Unternehmensgrenzen aufgelöst. Früher konnte man einen durch Firewalls eingezäunten „Garten" errichten, innerhalb dessen alle – hinter diversen netzwerkbasierten Schutzmaßnahmen – arbeiteten, auch wenn sie eine Verbindung von außen herstellten. Heute, wo so viele Mitarbeiter „von außerhalb" arbeiten und zudem Anwendungen und Daten in die Cloud verlagert werden, sind die Prozesse und die Infrastruktur, die für eine Handvoll Remote-Mitarbeiter konzipiert waren, schnell überfordert.

[1] Stanford University

Die Zusammenarbeit wird schwieriger, wenn sich die Mitarbeiter nicht mehr am selben Ort aufhalten. Mitarbeiter benötigen auch weiterhin die Web-Inhalte, SaaS-Cloud-Anwendungen und internen Anwendungen, die sie früher im Büro genutzt haben. Aber wie sie auf diese Ressourcen zugreifen und wie Sie diese schützen, hat sich oftmals dramatisch verändert. Sich darauf zu verlassen, dass Ihre Benutzer die Best Practices zum Schutz der Daten verstehen und befolgen, ist gefährlich, vor allem, wenn es unterschiedliche Kontrollmechanismen innerhalb und außerhalb des Unternehmens gibt. Wie man so schön sagt: „Hoffnung ist keine Strategie."

WFH und BYOD

Die Working From Home (WFH)-Bewegung macht sich die seit langem bestehende Bring Your Own Device (BYOD)-Entwicklung zunutze. Ein Bericht von Syntonic über die Verbreitung von BYOD in Unternehmen ergab, dass 77 % der Unternehmen einen Anstieg der BYOD-Nutzung im Vergleich zum Vorjahr erwarten.[2] Gartner prognostiziert, dass bis 2023 rund 30 % der IT-Unternehmen ihre BYOD-Richtlinien dahingehend erweitern werden, dass auch neue Geräte wie Smartwatches in das Unternehmensnetzwerk eingebunden werden können.[3]

Diese Flexibilität ermöglicht zwar ein produktiveres Arbeiten, erschwert aber die bisherige Sicherheitsstrategie, die davon ausgeht, dass Personen und Geräte innerhalb des Netzwerks bedingungslos vertrauenswürdig und sicher sind.

In einer Umfrage der Enterprise Mobility Exchange (EME) äußerten sich die Befragten besorgt, was folgende Aspekte betrifft:[4]

- → Die Gefahr durch gefälschte WLAN-Netzwerke (28 %)
- → Große Sicherheitsrisiken durch schädliche mobile Anwendungen (25 %)
- → Phishing-Angriffe über mobile Geräte (20 %)

Noch schwieriger wird es, wenn nicht verwaltete Geräte in Heimnetzwerken oder öffentlichen WLAN-Hotspots verwendet werden, wo IT-Sicherheitsteams keinerlei Einblick und Kontrolle haben.

Das Erkennen einer Sicherheitsverletzung über ein mobiles Gerät in einem Netzwerk ist schwierig. Die Wissenschaftler von Thales fanden heraus, dass fast die Hälfte aller Unternehmen eine Sicherheitsverletzung über ein mobiles Gerät im Netzwerk noch immer nicht erkennen kann.

Mehr erfahren

[2] Syntonic
[3] Gartner
[4] Enterprise Mobility Exchange

Das Problem mit VPNs

Virtual Private Networks (VPNs) entstanden ursprünglich, um Remote-Standorte so zu verbinden, dass sie scheinbar Teil desselben (oft internen) Netzwerks sind. Es wurden Softwareversionen entwickelt, um mobile und Remote-Mitarbeiter in das Unternehmensnetzwerk zu integrieren. Dies geschah zu einer Zeit, als nur ein Bruchteil der Belegschaft außerhalb des Unternehmens arbeitete. Im Zuge der Pandemie griffen jedoch viele Unternehmen auf VPNs zurück. Diese boten eine schnelle Lösung, um die vielen neuen Remote-Benutzer auch weiterhin durch die vorhandenen lokalen Abwehrmechanismen zu schützen und ihnen Zugriff auf interne Anwendungen zu ermöglichen. VPNs, die für die Verbindung von Standorten konzipiert und meist für relativ geringe Benutzerzahlen ausgelegt waren, verursachten den Unternehmen leider auch Kopfschmerzen, als sie in bislang unbekanntem Maßstab eingesetzt wurden.

Zum einen verändern VPNs die Art und Weise, wie Menschen arbeiten. Die Benutzer müssen die richtige Software auf ihren Endgeräten haben und wissen, wie und wann sie diese verwenden. VPNs sind bekanntermaßen zu langsam für moderne, interaktive Cloud-Anwendungen wie Microsoft Office 365, weshalb viele Nutzer sie vermeiden, wann immer möglich. Dies zwingt sie jedoch dazu, sich zu merken, welche Anwendungen „intern" sind und nur über das VPN zu erreichen sind und welche nicht. Das Ergebnis? Unzufriedenheit und Produktivitätsverlust.

Zudem treibt die private Nutzung von VPNs die Kosten für Unternehmen in die Höhe. Als die Mitarbeiter aus ihren Büros flüchteten, mussten viele Unternehmen schnell zusätzliche VPN-Hardware kaufen und implementieren, Netzwerkpfade aktualisieren und weitere Helpdesk-Mitarbeiter einstellen, um die steigende Anzahl an Problemen zu bewältigen.

Der langfristig größte Effekt dürften jedoch die erhöhten Risiken sein, die dadurch entstehen, dass interne Netzwerke, Server und Anwendungen den potenziellen Gefahren von Benutzern, Geräten und Remote-Netzwerken ausgesetzt sind. Einige Behörden warnen sogar vor VPNs für mobile Benutzer. Die National Security Agency (NSA) veröffentlichte kürzlich einen Leitfaden zu den Sicherheitsimplikationen von schlecht konfigurierten VPNs und stellte fest: „Die Aufrechterhaltung eines sicheren VPN-Tunnels ist mitunter komplex und erfordert regelmäßige Wartungsmaßnahmen."[5]

Und das ist nur der Anfang des Problems. Die weitaus größere Herausforderung ist oftmals, zu überwachen und zu kontrollieren, was Remote-Mitarbeiter mit den vertraulichen Daten tun, nachdem sie diese erhalten haben.

„Die Aufrechterhaltung eines sicheren VPN-Tunnels ist mitunter komplex und erfordert regelmäßige Wartungsmaßnahmen."

[5] NSA Advisory, Juli 2020

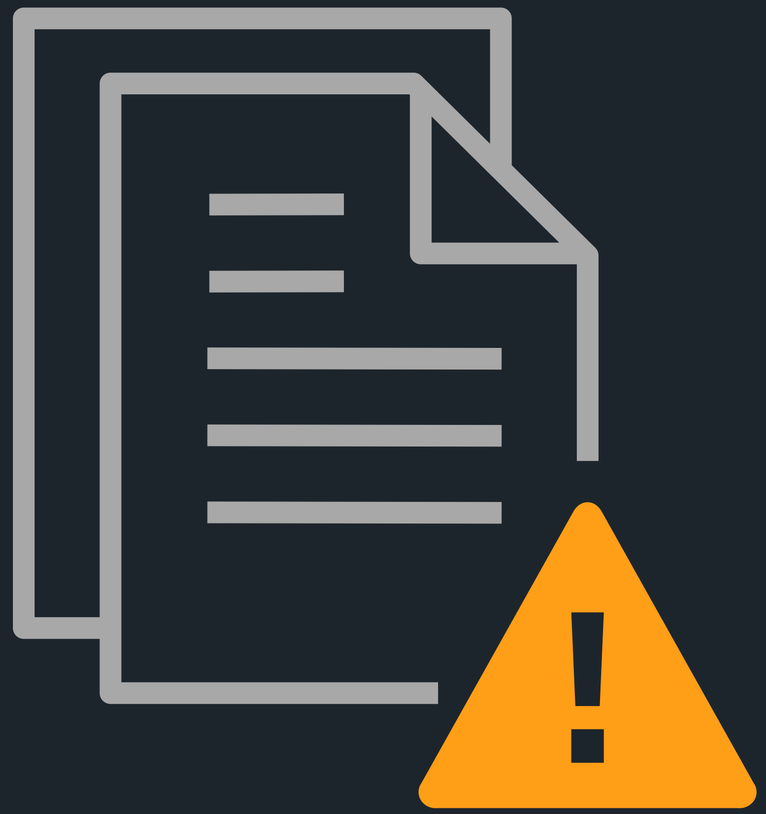
Wo alte Strategien mit „implizitem Vertrauen“ versagen

Veränderung ist die einzige Konstante in der Wirtschaft. Leider können Sicherheitslösungen oft nicht Schritt halten, so dass Daten leicht gestohlen oder versehentlich preisgegeben werden können.

Im Zuge der rasanten Umstellung auf mobile Arbeit machen sich Kriminelle die erweiterte Konnektivität zunutze, um in Unternehmen einzudringen. Dort wird ihnen oft automatisch Vertrauen entgegengebracht und sie haben freie Hand, um sich in verschiedene Anwendungen, Datenbanken und andere Ressourcen einzuschleichen.

Datenverluste

Im Jahr 2019 wurden 15,1 Milliarden Datensätze offengelegt, so viele wie nie zuvor in der Geschichte.[6] Zwischen dem 1. Januar und dem 30. Juni 2020 wurden 27 Milliarden Datensätze exponiert.[7]



[6] Risk Based Security
[7] Risk Based Security: Opt. In

Ein gefährliches Netz

Hacker lieben Internetverbindungen und -kommunikation, da sie ihnen Tür und Tor zum Unternehmensnetzwerk öffnen. Angriffsmethoden wie Phishing, Malvertising (werbebasierte Malware) und infizierte Websites befallen schließlich unzählige Geräte. Schätzungen zufolge ist eine von 100 Online-Anzeigen mit Malware infiziert.[8] Microsoft Office 365 ist die am häufigsten gefälschte Marke für Phishing-Kampagnen, die es auf Anmeldedaten abgesehen haben.[9]

Gut gefüllt ist halb gewonnen

Wurden Anmeldedaten gestohlen, können sie mit einer Methode namens „Credential Stuffing" für den Zugriff auf Unternehmensanwendungen und -portale verwendet werden. Akamai zählte zwischen Juli 2018 und Juni 2020 über 100 Milliarden Credential-Stuffing-Angriffe.[10]

Identitätsverlust

Jede Sicherheitsmaßnahme beginnt mit der Feststellung, wer der Benutzer ist – also seiner Identität. Mithilfe gestohlener Zugangsdaten können sich Kriminelle als Mitarbeiter oder sogar als Führungskräfte ausgeben, um Zugriff auf sensible Informationen zu erhalten.

240.000 USD

Cyber-Kriminelle sind raffiniert und nutzen neue Technologien wie KI: Ein britischer Geschäftsführer wurde um 240.000 US-Dollar betrogen. Der Geschäftsführer wurde vom CEO der Muttergesellschaft gebeten, eine Überweisung zu tätigen. Die Stimme am anderen Ende der Leitung war jedoch nicht die seines Chefs, sondern höchstwahrscheinlich eine Deepfake-Stimme, die speziell für den Betrug erzeugt wurde.

Mehr erfahren

Probleme in den eigenen Reihen

Manchmal geben Angestellte und andere interne Mitarbeiter sensible Informationen preis oder leiten sie an die falsche Stelle weiter. Solche Insider-Risiken können böswillig, versehentlich oder das Ergebnis entwendeter Anmeldedaten sein. Eine Umfrage von Apricorn aus dem Jahr 2020 ergab, dass 57 % der Unternehmen glauben, Remote-Mitarbeiter würden die Gefahr der Datenexposition erhöhen.[11]

(K)Ein Endpunkt in Sicht

Per Definition bedeutet mobile Arbeit, dass die Endgeräte weit von den IT-Systemen und Mitarbeitern entfernt sind, die sonst bei der schnellen Untersuchung und Lösung von Problemen helfen können. Die meisten Unternehmen verwenden eine Reihe von Sicherheitsmaßnahmen, die über eine einfache Virenschutz-Software für Endgeräte hinausgehen, um die Nutzung von Web-Inhalten und Cloud-Anwendungen zu schützen. Wenn diese Sicherheits-Gateways jedoch lokal implementiert werden, sind mobile Benutzer ungeschützt, wenn sie eine direkte Verbindung mit dem Internet herstellen (und nicht das Unternehmens-VPN verwenden).

Auch Experten machen Fehler

Viele der größten Cyber-Angriffe der Welt sind auf falsche Konfigurationen zurückzuführen. Eine schnelle Reaktion auf sich ändernde Umgebungen kann die IT-Teams stark belasten. Sie müssen in Windeseile Sicherheitsprobleme aufspüren und beheben, die entstehen, wenn Mitarbeiter von neuen Standorten aus arbeiten.

[8] MediaPost
[9] VadeSecure
[10] Akamai
[11] Apricorn

Die Zeit vor Zero Trust

Über Zero Trust wird schon seit einigen Jahren gesprochen. Warum kommt das Thema ausgerechnet jetzt in Fahrt? Ein (sehr) kurzer geschichtlicher Abriss darüber, wie wir im Bereich Cyber-Sicherheit dorthin gekommen sind, wo wir heute stehen, trägt zum Verständnis bei.

Der Anfang

Die Computersicherheit nahm ihren Anfang mit einem simplen Kennwort. Das erste Beispiel für die moderne Form eines Computerkennworts wird dem Massachusetts Institute of Technology (MIT) zugeschrieben. Im Jahr 1961 verfügte das MIT über eines der ersten Computersysteme der Welt, das mehrere Terminals unterstützte, die von verschiedenen Personen mit jeweils eigenen Dateien genutzt wurden. Das System verwendete ein Kennwort als Schutz, um den Zugriff auf die jeweiligen Dateien zu steuern.

Kennwörter gibt es nach wie vor, aber sie sind keineswegs perfekt. Angesichts der überbordenden Anzahl von Geräten und Anwendungen, mit denen sich jeder Einzelne beschäftigen muss, wird das Festlegen und Aktualisieren von Kennwörtern immer unübersichtlicher. Obwohl sich Alternativen zu Kennwörtern zunehmend durchsetzen, wird es noch lange dauern, bis Kennwörter der Vergangenheit angehören.

86 %

Das Pew Research Center fand heraus, dass sich 86 % der Benutzer ihre Kennwörter merken. Die Forscher fanden außerdem heraus, dass 49 % ihre Kennwörter auf Papier notieren. Eine Studie von LastPass zeigte, dass sich eine Durchschnittsperson 191 Kennwörter merken muss.

Pew Research

LastPass

Alles – Gutes wie Schlechtes – ist nur einen Klick entfernt

Das Internet hat mehr als jede andere technologische Innovation die Landschaft der Sicherheitsbedrohungen und Gegenmaßnahmen verändert. Mit der zunehmenden Verbreitung des Internets setzten sich neue Kommunikationsformen wie E-Mail schnell in der Gesellschaft durch. Und schon bald darauf wurden E-Mails zum Einfallstor für Viren. Als sich die Internetnutzung ausweitete, wurden Sicherheitsmaßnahmen wie Firewalls und Antiviren-Tools eingeführt, um die Cyber-Bedrohungen zu bewältigen.

Im Web und in der Cloud

Web- und Cloud-basierte Anwendungen waren der nächste große Schritt im Computing, der die Bedrohungslandschaft in Aufruhr versetzte. Cyber-Kriminelle nutzten häufig webbasierte Angriffe, um bösartigen Code in die Browser der Benutzer einzuschleusen, der dann zum Ausgangspunkt für die Verbreitung im gesamten Unternehmen wurde. Social-Engineering-Methoden machten es den Cyber-Kriminellen noch leichter, einzelne Personen ins Visier zu nehmen. So konnten sie unsere menschlichen Instinkte manipulieren und das „Vertrauen" nutzen, das andere ihnen implizit schenkten, um sich Zugang zu kontrollierten Systemen zu verschaffen oder anderweitig darauf zuzugreifen.

99 % aller Cyber-Angriffe benötigen menschlichen Input, um erfolgreich zu sein.

Mehr erfahren

Entwicklung von Zero Trust

Als Darwin vom „Überleben des Stärkeren" sprach, meinte er damit bestimmte Fähigkeiten, z. B. dass ein besserer Geruchssinn einem Lebewesen in einer bestimmten Umgebung einen Vorteil verschafft. Die Geschichte der Cyber-Sicherheitsbedrohungen und Gegenmaßnahmen nimmt einen ähnlichen Verlauf.

Computertechnologien, unsere Arbeitsweise und die Cyber-Sicherheitslandschaft haben sich im Laufe der Zeit gegenseitig beeinflusst und gemeinsam weiterentwickelt. Dies zeigt sich in der Entwicklung von Kennwörtern und Verschlüsselung sowie in der Verlagerung von abgegrenzten Unternehmensnetzwerken in Cloud-Netzwerke. Heute befinden wir uns in einem Labyrinth von unterschiedlichen Remote-Arbeitsmodellen, geräteübergreifender Hyperkonnektivität und raffinierten Cyber-Kriminellen. Daraus resultiert die Notwendigkeit eines flexibleren und vorausschauenderen Umgangs mit Cyber-Angriffen.

Zero Trust hat sich als eine der wichtigsten Methoden herauskristallisiert, diese Bedrohungen zu bekämpfen und sensible Informationen zu schützen.

Die scheinbar über Nacht entstandene Innovation, an der 10 Jahre lang gefeilt wurde, reagiert auf ein Zusammenspiel von Trends, die die Geschäftswelt grundlegend verändern:

- → Schnelle Internetverbindungen sind praktisch überall verfügbar.
- → Der Wechsel zu flexiblen und dezentralen Arbeitsweisen wurde durch die COVID-19-Pandemie beschleunigt.
- → Unternehmen wollen Transparenz und Kontrolle über ihre Daten, egal wo diese sind – vor allem auf Remote-Geräten und in der Cloud.
- → Die Reduzierung der Komplexität durch Automatisierung ist entscheidend für Effizienz und Sicherheit.
- → Der Kampf gegen raffinierte Cyber-Angriffe, die von System zu System überspringen, wird immer härter.

Zero Trust zur lückenlosen Sicherung von Datenzugriff und Datennutzung

Die Idee zu Zero-Trust-Sicherheit wurde erstmalig 2009/2010 von Forrester-Analyst John Kindervag vorgestellt.[12] Anstatt Anwendungen, Datenbanken und andere Ressourcen für jeden im Netzwerk zugänglich zu machen, kombiniert Zero Trust mehrere Grundsätze, um den Schutz der Daten einfacher und berechenbarer zu machen:

- **Zuerst kommen die Daten** – Daten sind das wertvollste Gut eines modernen Unternehmens, und Sicherheitsverletzungen können Ihr gesamtes Unternehmen in Gefahr bringen. Wie die Daten geschützt werden, hängt von den Risiken ab, die bei deren Offenlegung entstehen würden. Um die Sicherheit der Daten zu gewährleisten, brauchen Sie mehr als eine einfache Zugriffskontrolle. Sie müssen steuern können, welche Rechte die Benutzer in Bezug auf die erhaltenen Daten haben.
- **Vertrauen ist gut, Kontrolle ist besser** – Bei Zero Trust geht es darum, statische Alles-oder-Nichts-Annahmen darüber zu beseitigen, was Benutzer allein aufgrund ihres Aufenthaltsortes tun dürfen, und sie durch dynamische Entscheidungen zu ersetzen, die explizit den Zugriff auf und die Nutzung von sensiblen Daten erlauben.
- **Kontinuierliche Überwachung** – Indem Sie die Daten auf ihrem Weg durch das Unternehmen und die Aktionen der Benutzer, die mit ihnen interagieren, nachverfolgen, können Sie überprüfen, ob die Benutzer die sind, die sie vorgeben zu sein, und sicherstellen, dass sie Ihre Ressourcen nicht missbrauchen.

Abkehr von implizitem Vertrauen basierend auf dem Netzwerk oder Standort

Die Special Publication (SP) 800-207[13] des National Institute of Standards and Technology (NIST) definiert Zero Trust wie folgt:

- Zero Trust (ZT) bezeichnet eine Reihe ständig weiterentwickelter Cyber-Sicherheitsparadigmen, bei denen die Abwehrmaßnahmen von den statischen, netzwerkbasierten Grenzen auf die Benutzer, Datenbestände und Ressourcen verlagert werden.
- Zero Trust beruht auf der Annahme, dass Datenbeständen oder Benutzerkonten kein implizites Vertrauen gewährt wird, das ausschließlich auf ihrem Aufenthaltsort oder Netzwerkstandort (d. h. lokale Netzwerke im Vergleich zum Internet) oder auf dem Eigentum der Datenbestände (Unternehmens- oder Privatbesitz) basiert.
- Zero Trust konzentriert sich auf den Schutz von Ressourcen (Datenbeständen, Diensten, Workflows, Netzwerkkonten usw.), nicht auf den Schutz von Netzwerksegmenten.

[12] Forrester – Details zu Zero Trust
[13] NIST SP 800-207

Zero Trust stellt Daten in den Mittelpunkt

Die Implementierung von Zero Trust beginnt mit der Feststellung, welche Daten wichtig sind. Das Motto „Know your data" zieht sich wie ein roter Faden durch die Publikationen von Forrester zum Thema Zero Trust (und alle darauf basierenden Produkte). Dieser datenorientierte Ansatz hat folgende Kernpunkte:

- → Kenntnis des „Was", „Wo" und „Warum" von Daten über den gesamten Datenlebenszyklus
- → Abbildung des Datenflusses im Netzwerk und darüber hinaus

Im Jahr 2018 hat Forrester sein Zero-Trust-Modell aktualisiert. Die neue Version nennt sich „The Zero Trust eXtended Ecosystem (ZTX)".[14] Sie erweitert den Zero-Trust-Ansatz auf Menschen, Geräte und Daten und definiert sie alle von Natur aus als nicht vertrauenswürdig.

Bei Zero Trust muss jeder Benutzer jedes Mal, wenn er eine Ressource anfordert, eindeutig identifiziert werden und eine explizite Berechtigung haben. Daten sind nach wie vor die zentrale Achse, um die sich alle Elemente – Menschen, Geräte, Netzwerke und Workloads – drehen. Dabei werden keine Annahmen aufgrund des Ortes getroffen, von dem aus der Benutzer eine Verbindung herstellt, und die Zugriffs- bzw. Nutzungsberechtigung für eine Ressource kann jederzeit widerrufen werden. Zum Beispiel kann es passieren, dass ein Benutzer eine Datei aus einer Anwendung auf sein Laptop herunterladen kann, ihm dann aber nicht erlaubt wird, sie in eine E-Mail, auf einen USB-Stick oder in ein Cloud-Konto zu kopieren. Um dies dynamisch zu entscheiden, ist eine kontinuierliche Überwachung der Benutzeraktivität erforderlich. Moderne Zero-Trust-Lösungen gehen sogar noch einen Schritt weiter: Sie suchen nach Verhaltensmustern, um permanent zu überprüfen, ob der Benutzer derjenige ist, der er vorgibt zu sein, und ob seine Aktionen ein Risiko darstellen, das eine sofortige Einschränkung der ihm erteilten Berechtigungen erforderlich machen würde.

Forrester betont, dass Unternehmen die Art und Weise ändern müssen, wie sie entscheiden, ob sie Datentransaktionen über ein Netzwerk „vertrauen". Als ersten Schritt empfehlen sie, den gesamten Netzwerkverkehr als „nicht vertrauenswürdig" einzustufen. Die Personen am anderen Ende einer Verbindung müssen beweisen, dass sie diejenigen sind, für die sie sich ausgeben, und sie müssen die explizite Berechtigung haben, die übertragenen Daten zu empfangen und zu nutzen.

[14] The Zero Trust eXtended Ecosystem

Trust-Umgebung zu unterstützen, hat Forrester einen fünfstufigen Prozess[15] entwickelt, bei dem „Kontrollzonen“ (die sie „Mikroperimeter“ nennen) für sensible Daten eingerichtet werden:

Schritt 1: Kategorisieren

Zu wissen, welche Daten kontrolliert werden müssen, ist die Grundlage für jeden Zero-Trust-Ansatz. Das „vereinfachte Datenklassifizierungsmodell“ von Forrester umfasst drei primäre Klassen:

- → Public (Öffentlich)
- → Internal (Intern)
- → Confidential (Vertraulich)

Forrester empfiehlt zu untersuchen, wie und wo Datenpakete, sogenannte „Chunks“, verwendet werden. Diese können dann in Zonen einsortiert und einheitlich kontrolliert werden.

Schritt 2: Abbilden

Wenn Sie wissen, wo sich Ihre sensiblen Daten befinden und wie sie ausgetauscht werden, können Sie potenzielle Risiken und geeignete Sicherheitsmaßnahmen besser abbilden.

Schritt 3: Gestalten

Gestalten Sie Ihre Sicherheitslösung so, dass für jeden Datenfluss die richtigen Kontrollmechanismen – physisch oder virtuell – angewendet werden. Dies macht es einfacher, Ihre Sicherheit zu optimieren, die Auslastung Ihrer Sicherheitsteams zu reduzieren und Sicherheitsverletzungen zu vermeiden.

Schritt 4: Kontinuierlich überwachen

Moderne Zero-Trust-Strategien messen der kontinuierlichen Überwachung aller Aktivitäten, die die Bewegung von Daten im jeweiligen Zero-Trust-Ökosystem beeinflussen, große Bedeutung bei. Technologien zur Verhaltens- und Sicherheitsanalyse ermöglichen es, Auffälligkeiten und potenzielle Risiken frühzeitig zu erkennen, bevor sie zu Sicherheitsverletzungen werden.

Schritt 5: Automatisieren und umsetzen

Automatisierungsrichtlinien und Werkzeuge zur Sicherheits-automatisierung und -orchestrierung (SAO) können dabei helfen, eine Zero-Trust-Infrastruktur aufzubauen und zu betreiben.

[15] Forrester

NIST liefert das Framework für Zero Trust

Neben der Definition von Zero Trust beschreibt die NIST Special Publication 800-207 eine Reihe von Best Practices für die Anwendung von Zero-Trust-Grundsätzen auf Geräte, Personen und Datenbestände. Insbesondere geht es um die Bedeutung einer zuverlässigen Authentifizierung (Feststellung, dass Personen die sind, für die sie sich ausgeben, z. B. durch Anmeldung mit Kennwörtern und mehrstufige Authentifizierungstechnologien) und Autorisierung (Berechtigung, die jedes Mal explizit erteilt wird, wenn eine Aktion durchgeführt werden soll, z. B. der Zugriff auf oder die Bearbeitung einer Ressource).

Die Publikation betont außerdem die Notwendigkeit, fortlaufend nachzuverfolgen, was mit Ressourcen wie Daten und mit den Personen und Programmen, die diese Daten bearbeiten, geschieht. Durch die kontinuierliche Überwachung kann nicht nur kontrolliert werden, ob die Sicherheitsrichtlinien eingehalten werden, auch auffälliges Verhalten kann so schnell erkannt werden. Am Faktor Mensch orientierte Ansätze wie dieser ermöglichen eine sehr viel schnellere Einschätzung des Risikos, das von den Handlungen jedes Einzelnen ausgehen kann. Dadurch können automatisch Abhilfemaßnahmen ergriffen werden, wie z. B. eine bessere Authentifizierung (Aufforderung an Personen, ihre Identität erneut zu bestätigen, ggf. mit anderen Mitteln als den ursprünglich verwendeten) oder die Durchsetzung strengerer Sicherheitsrichtlinien.

„In Verbindung mit bestehenden Cyber-Sicherheitsrichtlinien und -leitfäden, Identitäts- und Zugriffsmanagement, kontinuierlicher Überwachung und Best Practices kann eine ZTA [Zero-Trust-Architektur] vor gängigen Bedrohungen schützen und die Sicherheitslage eines Unternehmens durch einen risikogerechten Ansatz verbessern.“

NIST SPECIAL PUBLICATION 800-207

SASE beinhaltet Zero Trust Network Access (ZTNA)

Zero-Trust-Sicherheit kann auf verschiedene Weise umgesetzt werden. Gartner hat diese explizit in seine SASE-Architektur (Secure Access Service Edge) integriert.

SASE vereint Sicherheit für Internet, Cloud, private Anwendungen, Netzwerk und Daten in einem einheitlichen Servicepaket, das über die Cloud bereitgestellt wird. Zero Trust Network Access (ZTNA) wird explizit als geeignete Methode bezeichnet, mobilen Benutzern einen sicheren Zugriff auf private Anwendungen in internen Rechenzentren oder Private Clouds bereitzustellen. ZTNA – manchmal auch als „Software-defined Perimeter" bezeichnet – versorgt die Mitarbeiter mit den Daten, die sie benötigen, um ihre Arbeit zu erledigen, jedoch ohne die Komplexität, die Engpässe und die Risiken, die der Einsatz von VPNs mit sich bringt.

Mit SASE wird auch der Einsatz von Datenschutztechnologien in den Vordergrund gestellt, die es Unternehmen ermöglichen, nicht nur den Zugriff, sondern auch die Nutzung der Daten zu sichern.

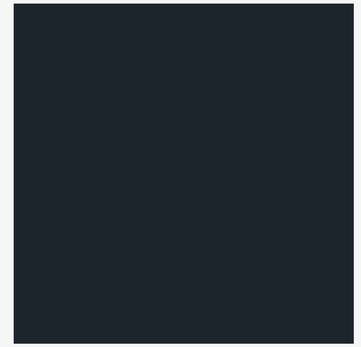
Das „Geheimrezept“ von Zero Trust: Kontinuierliche Überwachung und Kontrolle

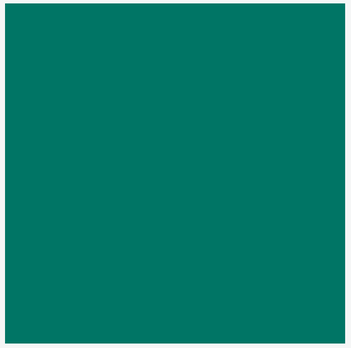
Dreh- und Angelpunkt von Zero Trust ist es, implizite Annahmen über die Vertrauenswürdigkeit durch explizite Entscheidungen zu ersetzen, die jedes Mal getroffen werden, wenn jemand – oder ein Gerät – versucht, auf sensible Ressourcen zuzugreifen oder diese zu nutzen. Zu Beginn konzentrierte man sich dabei auf die Zugriffskontrolle in Netzwerken (ein Prozess, der als Mikrosegmentierung bezeichnet wird) und verlangte von den Benutzern, sich bei jeder Anwendung oder jedem Server anzumelden, um Zugriff darauf zu erhalten. Dieser relativ einfache Ansatz bot eine erste Grundlage für mehr Sicherheit, war aber zu statisch und ließ Benutzern immer noch freie Hand, sobald sie Zugriff auf die jeweilige Ressource hatten.

Moderne Zero-Trust-Systeme hören nicht auf, nachdem der Zugriff gewährt wurde, sondern gehen sehr viel weiter. Um die Sicherheit der Daten zu gewährleisten, muss die Entscheidung darüber, was jemand mit sensiblen Daten tun darf, dynamisch erfolgen, und zwar jedes Mal, wenn eine Aktion durchgeführt wird. Deshalb beinhaltet Zero Trust nun auch das Konzept der kontinuierlichen Überwachung und Kontrolle. Im Grunde genommen erhalten Benutzer, die bestimmte Ressourcen nutzen möchten, eine temporäre Berechtigung, die jederzeit widerrufen werden kann.

Immer mehr Unternehmen setzen Data Loss Prevention-Technologien (DLP) ein, um die Verwendung sensibler Daten zu kontrollieren. Die meisten DLP-Systeme sind in der Lage, Daten sowohl während der Übertragung als auch während der Speicherung in Netzwerken, Cloud-Anwendungen und Endgeräten von Benutzern zu untersuchen. Jeder Versuch, gegen die Datennutzungsrichtlinien des Unternehmens zu verstoßen, kann automatisch blockiert werden, auch für Remote-Mitarbeiter.

Eine neue Generation von Zero-Trust-Lösungen wendet sogar User and Entity Behavioral Analytics-Technologien (UEBA) an, um nach Mustern im Verhalten von Personen zu suchen, die auf potenzielle Risiken für sensible Daten hindeuten. Solche Systeme können die Zusammenhänge zwischen digitalen, physischen und anderen Systemen jenseits der Daten erkennen, um festzustellen, wann die Kontrollen für den Zugriff und die Nutzung von Daten automatisch verschärft werden sollten.





[14] The Zero Trust eXtended Ecosystem

Worauf Sie bei Zero-Trust-Lösungen achten müssen

Worauf sollten Sie in erster Linie achten, wenn Sie sich für eine Zero-Trust-Lösung entscheiden?

Security-as-a-Service-Lösung in der Cloud

Unabhängig davon, ob Sie direkt auf eine SASE-Architektur umsteigen oder schrittweise vorgehen, reduziert die Cloud-basierte Sicherheit den Aufwand für die Absicherung Ihrer Mitarbeiter erheblich, egal wo diese arbeiten.

Kontrolle über Nutzung und Zugriff

Bei allen Zero-Trust-Lösungen geht es um die Sicherung des Zugriffs. Aber das reicht nicht mehr. Auch wenn Sie davon ausgehen, dass Ihre Mitarbeiter immer die sind, die sie vorgeben zu sein, und niemals Betrüger, die ihre Zugangsdaten gestohlen haben, geraten Sie in Gefahr, wenn Sie ihnen freie Hand lassen, Ihre sensiblen Daten nach Belieben zu verwenden.

Kontinuierliche Überwachung von Benutzern und Daten

Moderne Zero-Trust-Lösungen, insbesondere solche, die dem NIST-Modell folgen, untersuchen dynamisch, wie Ihre Benutzer und Daten interagieren. Dies gibt Ihnen laufend Gewissheit, dass die Personen diejenigen sind, für die sie sich ausgeben. So können Sie die Sicherheitsmaßnahmen automatisch an die Aktionen der einzelnen Personen anpassen.

Praxisrelevante und realitätsnahe Lösungen für Zero Trust

Forcepoint hat die Zero-Trust-Grundsätze in alle seine Produktlinien integriert, so dass Sie Ihren Mitarbeitern überall einen sicheren Zugriff auf Web-, Cloud- und private Anwendungen ermöglichen können, während komplexe Bedrohungen draußen und sensible Daten drinnen bleiben. Der einzigartige Ansatz vereint SASE-Kontrolle und -Schutz, modernste Datensicherheit und das branchenweit erste verhaltensbasierte System zur dynamischen Personalisierung der Sicherheitsmaßnahmen in Abhängigkeit von den Aktionen der einzelnen Benutzer.

Forcepoint Private Access (PA)

In der Cloud bereitgestellter Zero Trust Network Access (ZTNA) ermöglicht Remote-Mitarbeitern sicheren Zugriff auf private Anwendungen ohne die Komplexität, Engpässe und Risiken von VPNs.

Forcepoint Cloud Security Gateway (CSG)

In der Cloud bereitgestellte SASE-Sicherheit schützt die Nutzung von Web- und Cloud-Anwendungen, einschließlich echter Data Loss Prevention-Technologie auf Enterprise-Niveau in der Cloud.

Forcepoint Data Loss Prevention (DLP)

Branchenführende Sicherheit für sensible Daten und geistiges Eigentum an allen Orten – in der Cloud, im Netzwerk und auf den Endgeräten der Benutzer.

Forcepoint Dynamic User Protection (DUP)

Die branchenweit erste Lösung zur Überwachung der Anwenderaktivität, die als Cloud-Dienst bereitgestellt wird, bietet Unternehmen Einblicke in riskantes Nutzerverhalten und verhindert Verluste gleich bei der Erkennung der Bedrohung.

Die wichtigste Erkenntnis

Von „Least Privilege“ zu „Zero Trust“: Der Wechsel zu daten- und am Faktor Mensch orientierter Sicherheit

Die zunehmende Bedeutung der datenorientierten Wirtschaft in Verbindung mit einer komplexen Bedrohungslandschaft hat zu einem dringenden Bedarf an besseren Sicherheitsstrategien geführt. Da herkömmliche Tools zur Zugriffskontrolle immer unwirksamer werden, ist Zero Trust nun eine äußerst gefragte Methode, um Unternehmensressourcen besser vor Datenschutzverletzungen zu schützen.

In einer kürzlich von McKinsey durchgeführten Studie über die Auswirkungen von COVID-19 auf Unternehmen und Mitarbeiter gaben 85 % der Befragten Folgendes an:

„Die Implementierung von Technologien, die eine digitale Interaktion und Zusammenarbeit von Mitarbeitern ermöglichen, wie z. B. Videokonferenzen und Filesharing, wurde im Unternehmen beschleunigt oder sogar stark beschleunigt.“

Mehr erfahren

Zero Trust ist mehr als nur eine sicherheitstechnische Modeerscheinung. Es spielt eine Schlüsselrolle, wenn es darum geht, das dezentrale Arbeiten in Unternehmen langfristig zu unterstützen.

Über alle Branchen hinweg gaben 15 % der Führungskräfte an, dass mindestens ein Zehntel der Mitarbeiter auch nach COVID-19 an zwei oder mehr Tagen pro Woche von zu Hause arbeiten wird. In der IT-Branche liegt dieser Wert sogar bei 34 % der Beschäftigten. Vor COVID-19 betrug dieser Wert im Durchschnitt nur 8 %.

Mehr erfahren

Unter dem Motto „Vertrauen ist gut, Kontrolle ist besser. Immer.“ und im Sinne der Mission „Datenschutz“ ersetzt Zero Trust die implizite Annahme, dass Personen „innerhalb“ des Unternehmens sicher sind und zwar durch kontinuierliche, explizite Entscheidungen darüber, wer auf Unternehmensressourcen zugreifen darf und wie diese verwendet werden können. Aus diesem Grund entwickelt sich Zero Trust schnell zu einer der wichtigsten Methoden, mit denen Unternehmen garantieren, dass ihre Daten auch in einer sich schnell verändernden Welt sicher bleiben.

„Vertrauen ist gut, Kontrolle ist besser. Immer.“

[14] The Zero Trust eXtended Ecosystem

Forcepoint

forcepoint.com/contact

Über die Verfasserin

Dr. Christine Izuakor, CISSP, ist die CEO von Cyber Pop-up, einer On-Demand-Plattform für Cyber-Sicherheitsdienste. Sie verfügt über mehr als ein Jahrzehnt Erfahrung in leitenden Cyber-Sicherheitsfunktionen in Fortune-100-Unternehmen. Dabei hat sie zahlreiche Bereiche – von globalen Sicherheitsstrategien und Awareness-Programmen für 90.000 Mitarbeiter an über 300 Standorten bis hin zum Schwachstellenmanagement für Tausende von Unternehmenswerten – betreut.

Christine Izuakor promovierte als jüngste und erste afroamerikanische Frau im Fach Sicherheitstechnik, hat einen Master in Informationssystemsicherheit, schreibt regelmäßig Artikel, hält Vorträge und bietet Beratungen zum Thema Cyber-Sicherheit an.

Über Forcepoint

Forcepoint ist einer der weltweit führenden Anbieter von Cyber-Sicherheit im Bereich Anwender- und Datenschutz und hat es sich zur Aufgabe gemacht, Organisationen zu schützen und gleichzeitig die digitale Transformation und das Wachstum voranzutreiben. Die auf menschlichem Verhalten basierenden Lösungen von Forcepoint passen sich in Echtzeit an das Nutzerverhalten an und ermöglichen Mitarbeitern einen sicheren Datenzugriff bei voller Produktivität. Forcepoint mit Sitz in Austin, Texas, schafft sichere, vertrauenswürdige Umgebungen für Tausende von Kunden weltweit.