Engineer

Zero Trust

ein Modell ohne Vertrauen allein durch den Netzwerkstandort

Was es ist

Zero Trust ist ein Sicherheitsmodell, bei dem nichts allein wegen seines Standorts im Netzwerk als vertrauenswürdig gilt. NIST SP 800-207, die US-Bundesveröffentlichung, die das Modell 2020 darlegte, definiert es als einen auf den Schutz von Ressourcen ausgerichteten Ansatz: Vertrauen wird nie stillschweigend gewährt, sondern muss laufend neu bewertet werden. Eine Anfrage erhält nicht allein deshalb Vertrauen, weil sie aus dem Büronetz, dem VPN oder demselben Rechenzentrum kommt. Über jeden Zugriff auf eine Ressource wird anhand der Umstände entschieden: Wer fragt, von welchem Gerät, wonach und unter welchen Bedingungen? Mit Bindestrichen wird die Bezeichnung einem Substantiv vorangestellt, etwa in „Zero-Trust-Entwurf“. Der Plan, der das Modell in die Praxis überführt, heißt Zero-Trust-Architektur, kurz ZTA.

NIST benennt die Beteiligten genau. Ein Subjekt ist, wer oder was eine Anfrage stellt: ein Benutzer, ein Dienst oder ein Gerät. Eine Ressource ist alles Schützenswerte; die Veröffentlichung zählt neben Daten auch Drucker und Rechenkapazität dazu. Dazwischen stehen drei logische Komponenten. Die Policy-Engine entscheidet über die Freigabe einer Anfrage und protokolliert die Entscheidung. Der Policy-Administrator setzt sie um: Er öffnet oder schließt den Weg zwischen Subjekt und Ressource und stellt die Zugangsdaten oder Tokens für diese eine Sitzung aus. Der Durchsetzungspunkt, der Policy Enforcement Point, liegt auf dem Weg selbst. Er lässt die Sitzung durch, überwacht sie und beendet sie auf Anweisung.

Die Veröffentlichung erklärt den Wechsel am Beispiel eines Flughafens. Passagiere passieren eine Sicherheitskontrolle. Dahinter bewegen sich Reisende, Besatzungen und Flughafenpersonal im Terminal, alle als vertrauenswürdig behandelt. Dieses Terminal nennt NIST eine implizite Vertrauenszone: einen Bereich, in dem allen bis zu dem Niveau vertraut wird, das die zuletzt passierte

Kontrolle verbürgt. Ein flaches Büronetz funktioniert genauso. Zero Trust hält die Zone möglichst klein, indem es die Entscheidung und ihre Durchsetzung näher an die Ressource verlegt.

Das Konzept für eine Entscheidung nutzen

Nutzen Sie „Was ist Zero Trust?“ für eine konkrete Entscheidung. Wir können helfen, das Konzept mit dem System in Verbindung zu bringen, das Sie entwickeln oder einkaufen. Konten, Passwörter und Berechtigungen werden so geordnet, dass alle genau den beruflich erforderlichen Zugriff haben und ihn am Tag ihres Ausscheidens verlieren.

Unsere Leistungen entdecken Kontakt aufnehmen →

Die Annahmen hinter dem Begriff prüfen

Nutzen Sie die Erklärung und die verlinkten Arbeiten, um Fragen für Ihr Projekt zu formulieren. Wir können die Annahmen gemeinsam mit Ihnen prüfen, bevor ein Werkzeug ausgewählt wird. 1.000 RBAC-Regeln für sichere Linux-Server — 1,000 Zugriffsregeln zum Schließen einer Sicherheitslücke

1.000 RBAC-Regeln für sichere Linux-Server Kontakt aufnehmen →

Warum es wichtig ist

Das ältere Modell zieht eine Grenze um die Organisation und vertraut allem darin. NISTs Einwand ist klar: Haben Angreifer die Außengrenze überwunden, können sie sich ungehindert seitlich im Netz bewegen. Solche unbefugten Seitwärtsbewegungen waren eine der größten Herausforderungen für die Behörden, für die die Veröffentlichung verfasst wurde. Die Grenze passt auch nicht mehr zur Arbeit. Mitarbeiter melden sich von zu Hause und aus Hotelnetzen an, private Geräte dürfen auf manche Systeme zugreifen, und vieles läuft in der Cloud eines anderen. Daraus folgen NISTs Annahmen: Das private Netzwerk ist keine implizite Vertrauenszone, ein Angreifer kann bereits darin sein, und extern arbeitende Mitarbeiter sollten das lokale Netz, aus dem sie sich verbinden, als feindlich behandeln.

Das Team gewinnt eine Begrenzung des Schadens. Nach dem dritten von NISTs sieben Grundsätzen wird Zugriff pro Sitzung und mit den geringsten für die Aufgabe nötigen Rechten gewährt. Eine Authentifizierung an einer Ressource gewährt nichts an einer anderen. Mit einem gestohlenen Passwort oder einem kompromittierten Laptop lässt sich dann nur erreichen, was dieses Konto und dieses Gerät in diesem Moment und über einen Durchsetzungspunkt erreichen dürfen, statt das gesamte interne Netz. Die Entscheidungen hinterlassen außerdem eine Spur. Die Policy-Engine protokolliert jede Freigabe und jede Ablehnung. Wer ein System erreichen konnte und warum, lässt sich damit aus Aufzeichnungen statt aus der Erinnerung beantworten.

Wie es in der Praxis aussieht

Nehmen wir ein Einkaufssystem. NIST schlägt eine solche Anwendung für eine erste Migration vor, weil eine klar umrissene Mitarbeitergruppe sie nutzt, anders als E-Mail, von der die ganze Organisation abhängt. Ein Einkäufer öffnet sie auf einem Firmenlaptop. Die Anfrage erreicht den Durchsetzungspunkt vor der Anwendung, der die Policy-Engine befragt. Ihr Vertrauensalgorithmus gewichtet die von NIST genannten Eingaben: die Anfrage selbst, einschließlich Betriebssystemversion und Patchstand des Geräts; die Subjektdatenbank; die Bestandsdatenbank; die Anforderungen der Ressource, die etwa ein Sicherheitsniveau der Authentifizierung nennen oder ausländische Adressen abweisen können; und Informationen über Bedrohungen. Ein beispielhafter Entscheidungsdatensatz mit selbst gewählten Feldnamen, nicht denen eines Produkts, könnte so aussehen:

```
Anfrage      buyer-17 auf laptop-0417 -> Einkaufs-App, lesen und schreiben
Subjekt      Einkaufsteam; mit phishingresistentem Schlüssel angemeldet
Gerät        unternehmensverwaltet, OS-Patches aktuell, Laufwerk verschlüsselt
Ressource    braucht AAL2 oder höher, verwaltetes Gerät, inländische Quell-IP
Bedrohung    Quelladresse fehlt in den geprüften Bedrohungsfeeds
Entscheidung Lesen und Schreiben für diese Sitzung gewähren; genehmigt vermerken
```

Die Freigabe gilt für diese eine Sitzung und diese eine Anwendung. Öffnet derselbe Einkäufer auf demselben Laptop die im Dokumentenspeicher abgelegten Lieferantenverträge, trifft die Engine eine neue Zugriffsentscheidung. Die Authentifizierung an der ersten Ressource gewährt nicht automatisch Zugriff auf die zweite. Auch der Kontext zählt. In einem NIST-Beispiel fordert ein sonst zu Bürozeiten arbeitender Buchhalter mitten in der Nacht von einem der Engine unbekannten Ort Zugriff auf das Finanzsystem an. Ein kontextbezogener Vertrauensalgorithmus kann Alarm auslösen und vom Subjekt zunächst ein höheres Vertrauensniveau verlangen. Ein weiteres Beispiel ist ein Personalmitarbeiter, der an einem gewöhnlichen Tag 20 bis 30 Personalakten liest und plötzlich mehr als 100 anfordert.

Bei Cloud-Diensten können Clients laut NIST direkt zum Dienst gehen, während die Durchsetzungspunkte der Organisation unterwegs die Richtlinien prüfen. Die Clients werden dabei nicht zuerst über ein VPN ins interne Netz geholt. Jede dieser Entscheidungen braucht ein klares Bild davon, wer worauf zugreifen soll. Deshalb verlangt NIST vor jeder Umsetzung eine Bestandsaufnahme der Geräte und sonstigen Ressourcen, Subjekte, Datenflüsse und Arbeitsabläufe. Diese Vorarbeit entspricht der Zusammenführung in unserer Fallstudie zur

Zugriffsverwaltung über M365 und SSO hinweg: Identitäten und Zugriffe wurden über M365, 1Password, Red Hat SSO und OKTA SSO zusammengeführt, das Prinzip der geringsten Rechte durchgesetzt und Ein- sowie Austrittsabläufe vereinheitlicht, damit Zugriffe zeitnah gewährt und entzogen werden.

Wo es schiefgeht

Das Modell wird als Produkt gekauft. Laut NIST ist Zero Trust eine Sammlung von Leitprinzipien, keine einzelne Architektur. Es gibt auch keine einheitliche Zusammenstellung von Werkzeugen oder Diensten für ein Zero-Trust-Unternehmen. Ein neues Fernzugriffs-Gateway mit diesem Etikett ändert wenig, wenn jedes zugelassene Subjekt weiterhin das gesamte Netz dahinter erreicht. Abhilfe: Behandeln Sie die Umstellung in NISTs Worten als „einen Weg statt eines vollständigen Austauschs“, einen Geschäftsprozess nach dem anderen. Prüfen Sie jedes Produkt an den Grundsätzen, die es erfüllen soll, einschließlich der Frage, ob seine Datenformate später einen Wechsel zu einem anderen Anbieter erlauben.

Die Richtlinien werden vor der Bestandsaufnahme geschrieben. Die Policy-Engine kann nur anhand dessen entscheiden, was sie über Subjekte, Ressourcen und Abläufe weiß. Ist dieses Wissen unvollständig, stoppt laut NIST typischerweise ein Geschäftsprozess, weil die Engine Anfragen mangels Informationen ablehnt. Schatten-IT, also außerhalb der Verwaltung der IT-Abteilung eingerichtete Systeme, verschärft das Problem. Abhilfe: Erfassen und katalogisieren Sie zuerst Ressourcen, Subjekte, Datenflüsse und Arbeitsabläufe, einschließlich der Schatten-IT. Schreiben Sie erst danach die Kriterien für einen infrage kommenden Prozess.

Administratoren behalten pauschalen Zugriff. In vielen älteren Entwürfen können Entwickler und Systemadministratoren jede Ressource erreichen. NIST nennt diese Konten ausdrücklich als besonders prüfbedürftig. Erhalten alle anderen ihren Zugriff nur noch nach einer Entscheidung für jede Sitzung, während Administratorkonten ihren dauerhaften Zugriff behalten, bleiben die wertvollsten Zugangsdaten der kürzeste Weg hinein. Abhilfe: Führen Sie privilegierte Konten durch dieselbe Engine und geben Sie ihnen den für die aktuelle Aufgabe nötigen Zugriff. Ermitteln Sie mit Protokollen und Audits die üblichen Muster, damit Abweichungen auffallen.

Die Policy-Engine wird zur neuen Außengrenze. Keine Ressource kommuniziert mit einer anderen, solange Engine und Policy-Administrator es nicht genehmigen. Wer auf die Regeln der Engine zugreifen kann, kann unzulässige Änderungen vornehmen oder schlichte Fehler machen. Ein Angreifer, der die Durchsetzungspunkte oder den Policy-Administrator stört, kann den Betrieb zum Stillstand bringen. Abhilfe: Protokollieren und prüfen Sie jede Konfigurationsänderung. Betreiben Sie die Durchsetzung in einer angemessen abgesicherten Cloud-Umgebung oder replizieren Sie sie an mehreren Standorten. Beschränken Sie den Zugriff auf gespeicherte Verkehrsdaten und Richtlinien am strengsten: ausschließlich auf eigens dafür vorgesehene Administratorkonten.

Am ersten Tag wird alles strikt durchgesetzt. Wenige Richtliniensätze stimmen im ersten Anlauf. NIST erwartet eine Abstimmungsphase, in der Anfragen abgelehnt werden, die erfolgreich sein sollten. Der direkte Wechsel zur strikten Durchsetzung führt bei jeder Lücke in den Richtlinien dazu, dass Mitarbeiter die nötige Arbeit nicht mehr erledigen können. Abhilfe: Betreiben Sie den neuen Ablauf eine Weile im reinen Berichtsmodus. Gewähren Sie die meisten Anfragen, vergleichen Sie die Protokolle mit den beabsichtigten Richtlinien und setzen Sie nur das Nötigste durch, etwa das Abweisen bei fehlgeschlagener MFA oder bei als feindlich bekannten Quelladressen. Verschärfen Sie die Richtlinien, sobald das normale Muster verstanden ist.

Mit MFA gilt die Arbeit als erledigt. MFA verringert das Risiko, das von einem gestohlenen Passwort ausgeht. NIST weist jedoch darauf hin, dass ein Angreifer mit gültigen Zugangsdaten oder ein böswilliger Insider weiterhin alles erreicht, was das Konto erreichen darf. Abhilfe: Halten Sie den Zugriff jedes Kontos eng begrenzt und verwenden Sie einen kontextbezogenen Vertrauensalgorithmus, der Zeit, Ort und Umfang berücksichtigt. So lösen auch ungewöhnlich verwendete gültige Zugangsdaten einen Alarm aus.

Weiterführende Lektüre

- NIST SP 800-207, Zero Trust Architecture — im August 2020 veröffentlicht: Definition, sieben Grundsätze, logische Komponenten, Bedrohungen und ein Fahrplan für die Migration.
- NIST SP 1800-35, Implementing a Zero Trust Architecture — der im Juni 2025 veröffentlichte NIST-Praxisleitfaden mit 19 Beispielimplementierungen, erarbeitet mit 24 Mitwirkenden.

- NIST SP 800-207A — im September 2023 veröffentlicht: Zugriffskontrolle für cloudnative Anwendungen über mehrere Clouds hinweg, auf Basis von API-Gateways, Sidecar-Proxys und Dienstidentitäten statt Netzwerkadressen.
- NIST SP 800-63B-4 — die Sicherheitsniveaus der Authentifizierung, die eine Ressource verlangen kann. Davon erfordert AAL3 Phishingresistenz.

Glossar

Für Ihre tatsächlichen Rahmenbedingungen auswählen

Beschreiben Sie den Bereitstellungsweg, die Betriebsrisiken und die Bereitschaftsverantwortlichen. Wir können eine Änderung mit Prüfungen, einem Wiederherstellungsweg und klaren Zuständigkeiten abgrenzen.

Preise ansehen Kontakt aufnehmen →

Die Begriffe praktisch nutzbar machen

Fragen Sie, wie „Was ist Zero Trust?“ auf Ihre Organisation zutrifft. Ein konkretes Beispiel aus Ihrem bestehenden System reicht aus, um das Gespräch zu beginnen.

Unsere Leistungen entdecken

welcome@engineer.company +45 50 10 61 84 Kopenhagen, Dänemark

Nehmen Sie diese Seite mit

Kontaktkarte

Mit Sorgfalt und Liebe gestaltet von D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Copyright © 2025 – heute · Engineer ApS · Alle Rechte vorbehalten.

Gedruckt von https://engineer.company/de/glossary/zero-trust/