jamf

ZTNA und Trusted Access:

Best Practices für Identitätszugang und Sicherheits-Compliance

Zero Trust hat die Welt der Cybersicherheit im Sturm erobert. Laut dem **Okta-Bericht: The State of Zero Trust Security 2022** stieg der Prozentsatz der Unternehmen, die Zero Trust entwickeln oder in den nächsten 12-18 Monaten implementieren, von 16 % im Jahr 2019 auf 97 % im Jahr 2022. Die Beseitigung der Netzwerkgrenzen, die aus der Zunahme der Fernarbeit durch die Pandemie resultierte, machte die Zero Trust-Architektur zu einer Notwendigkeit und nicht nur zu einem Nice-to-have.

Zero Trust Network Access (ZTNA) ist eine der Säulen einer Zero Trust-Implementierung. Stellen Sie sich die Zero Trust-Architektur als ein Schloss mit mehreren Räumen vor, das Ihr Netzwerk beherbergt - ZTNA ist die Garnison, die die Identität eines jeden Gastes überprüft, das Tor öffnet und ihn zu den Räumen begleitet, auf die er Zugriff hat. Wenn die Absichten des Gastes zu irgendeinem Zeitpunkt verdächtig werden, wird er sofort des Geländes verwiesen und seine Erlaubnis wird widerrufen.

Abgesehen von den mittelalterlichen Analogien ist das Verständnis der ZTNA von entscheidender Bedeutung für die Verbesserung der Cybersicherheit.

In diesem Papier befassen wir uns damit:

- Gewährung des Zugriffs mit den geringsten Rechten
- Überprüfung der Identität mit Multifaktor-Authentifizierung (MFA) und Cloud Identitätsanbietern (IdP)
- Compliance und Sicherheit
- Unterstützung der Endnutzer*innen

Zugang mit geringsten Rechten

Das Prinzip der geringsten Privilegien ist einfach: Benutzer*innen und ihre Geräte haben nur Zugriff auf das, was für ihre Aufgaben erforderlich ist, und nicht mehr. Einerseits ist dies mit einem gewissen buchhalterischen Aufwand verbunden, da Sie den Überblick darüber behalten müssen, wer Zugang zu was benötigt und wer diesen Zugang derzeit hat. Andererseits werden Sie kein Geld für eine übermäßige Anzahl von Lizenzen ausgeben. Die wahre Stärke liegt jedoch in der Verringerung der Angriffsfläche - wenn Sie die Anzahl der Benutzer*innen mit Berechtigungen begrenzen, begrenzen Sie auch die Anzahl der Konten, die Ihr Netzwerk über eine bestimmte Ressource kompromittieren können. Dies verringert auch das Risiko von Seitwärtsbewegungen, wenn ein böser Akteur/eine böse Akteurin in Ihr Netzwerk eindringt, da die Benutzer*innen keinen Zugriff auf Ihr gesamtes Netzwerk haben.

ZTNA wendet das Prinzip der geringsten Privilegien an, indem es einen softwaredefinierten Perimeter (SDP) schafft. Eine SDP trennt die Netzwerkverbindungen nicht durch VLAN oder Netzwerkadressen, sondern gewährt durch Split-Tunneling nur Zugriff auf die Teilmenge der Ressourcen, für die der Benutzer/die Benutzerin eine Zugriffsberechtigung hat, unabhängig davon, wo er sich im Unternehmensnetzwerk befindet. Ressourcen, für die der Benutzer/die Benutzerin keine Zugriffsberechtigung hat, bleiben unsichtbar und für den Benutzer/die Benutzerin unzugänglich.

Identität: Authentifizierung und Autorisierung

Die Grundlage von ZTNA ist die Identität. „Vertraue nie, überprüfe immer”das Mantra von Zero Trust, bedeutet, dass Benutzer*innen und Geräte immer gezwungen werden, ihre Identität nachzuweisen, wenn sie sich bei Ressourcen anmelden, unabhängig von der Häufigkeit oder Wiederholung einer erfolgreichen Anmeldung.

Die Identitätsfeststellung in einer entfernten Umgebung hat ihre Tücken. Unternehmen können sich nicht auf lokale Active Directory (AD)- oder LDAP-Konfigurationen verlassen - insbesondere nicht auf Apple Geräte, für die AD nicht konzipiert wurde. An dieser Stelle kommen Cloud Identitätsanbieter*innen (IdPs) wie Okta, G Suite und Microsoft Entra ID ins Spiel.

Cloud IdPs stellen den Verzeichnisdienst bereit, wo immer sich Ihre Benutzer*innen befinden. Ihr IdP speichert die Informationen eines Benutzers/einer Benutzerin: wer er ist, welche Rolle er hat und auf welche Apps er zugreifen darf. Mit anderen Worten: Es authentifiziert den Benutzer/die Benutzerin und bestimmt seine Berechtigung zum Zugriff auf Unternehmensressourcen.

Appbasiertes Mikrotunneling

Wenn wir über ZTNA sprechen, erwähnen wir oft die Benutzeridentität, aber ein weiterer wichtiger Aspekt ist die Appidentität. Appbasierte Mikrotunneling-Richtlinien arbeiten hinter den Kulissen, um ZTNA Wirklichkeit werden zu lassen. Durch die Zuweisung einer netzwerkunabhängigen Identität für Apps erreichen Sie eine feinere Segmentierung des Netzwerks, während alle Richtlinien unabhängig vom Standort der App auf einem Server vor Ort oder in der Cloud gültig bleiben. Dies erleichtert die Durchsetzung von Sicherheitsrichtlinien in Nord-Süd- und Ost-West-Richtung, da Sie einen klaren Überblick über den Datenverkehr der Apps erhalten.

Die Verwendung von Cloud IdPs mit dieser Art von Mikrotunneling ermöglicht Ihnen die Nutzung einer Cloud basierten Implementierung. Sie müssen die Identität nicht verwalten oder Apps ausschließlich auf Ihren Servern hosten - Ihr ZTNA-Anbieter*in kann den Datenverkehr nach Bedarf umleiten. Auf diese Weise müssen Sie keine Server oder Hardware warten oder überwachen, die Sie nicht benötigen, und gleichzeitig den Benutzer*innen den sicheren und bequemen Zugang ermöglichen, den sie benötigen.

Einheitliche Zugangspolitik

Dies alles gipfelt in einer einheitlichen Zugangsrichtlinie. Diese Richtlinie sollte alle für Ihr Unternehmen relevanten Hosts abdecken, unabhängig davon, ob sie sich vor Ort, in einer privaten oder öffentlichen Cloud, innerhalb einer SaaS-App, auf einem modernen Betriebssystem oder einem anderen Verwaltungsparadigma befinden. Eine wirksame Richtlinie umfasst:

- Verzeichnisdienste und Single Sign-On-Funktionen über einen Cloud IdP
- Multi-Faktor-Authentifizierung
- Rollenbasierte Zugangskontrolle nach den Grundsätzen der geringsten Berechtigung
- SSO-fähiges Repository der zugelassenen Apps
- Ein Kontrollsystem, das den Datenverkehr an die richtigen Stellen im Netz leitet (einschließlich des Datenverkehrs vor Ort, in der Cloud, über SaaS und im nicht-geschäftlichen Web)

Compliance und Sicherheit

Identität ist bei ZTNA die halbe Miete - die andere Hälfte ist die Einhaltung der Compliance. Sie wollen nicht, dass kompromittierte oder gefährdete Geräte Zugriff auf Ihre Unternehmensressourcen haben, selbst wenn Sie andere Sicherheitsvorkehrungen getroffen haben.

Wie können Sie also sicherstellen, dass die Geräte, die eine Verbindung zu Ihren Ressourcen herstellen, den Vorschriften entsprechen? Zero Trust bedeutet, dass Sie sich nicht darauf verlassen können, dass Geräte, Server oder Apps frei von Kompromissen sind. Ihre Zugangsrichtlinien sollten Methoden zur Identifizierung anfälliger und/oder gefährdeter Geräte enthalten.

Ihre Compliance Software kann dies überprüfen:

- Ungepatchte/anfällige Versionen von Betriebssystemen oder Apps
- Software für aktiven Endpoint-Schutz
- Verdächtige Aktivitäten, die für den Nutzer/die Nutzerin untypisch sind
- Bedrohungen auf dem Gerät oder bösartige Websites, auf die der Benutzer/die Benutzerin zugreift

Wenn die Konformität eines Geräts infrage gestellt wird, können Sie ihm den Zugang zu den Unternehmensressourcen verwehren. Die Umsetzung dieser Compliance-Prüfungen sieht je nach Gerätetyp und je nachdem, ob es sich um ein unternehmenseigenes oder ein privates Gerät handelt, unterschiedlich aus. In jedem Fall sollte das Gerät über eine Art Verwaltungssoftware verfügen, wenn es sich mit Unternehmensapps verbindet - wobei die Privatsphäre der Nutzer*innen dennoch gewahrt bleiben sollte. Mitgebrachte Geräte (BYO) sollten den persönlichen Datenverkehr direkt und nicht über die Überwachungssoftware des Unternehmens leiten, und persönliche und geschäftliche Daten sollten aus Gründen der Sicherheit und des Datenschutzes vollständig getrennt werden.

Kontinuierliche Überprüfung

Die Überprüfung der Compliance eines Geräts erfolgt nicht nur bei der Anmeldung. Das ist Teil des Paradigmas „Niemals vertrauen, immer nachprüfen" - das Gerät könnte jederzeit kompromittiert werden. Eine kontinuierliche Überprüfung des Gerätestatus ist von größter Bedeutung, denn selbst der gutwilligste Benutzer/die gutwilligste Benutzerin kann Opfer eines Phishing-Versuchs oder einer Malware-Infiltration werden.

Die Benutzererfahrung der Endnutzer*innen

Ein klobiger, schwer zu bedienender und unzuverlässiger ZTNA-Dienst verheißt nichts Gutes für seinen Erfolg. Wenn der Dienst die Benutzer*innen behindert, ist es wahrscheinlicher, dass sie versuchen werden, die Maßnahmen zu umgehen, die Sie zur Sicherung Ihrer Ressourcen getroffen haben.

Wie auch immer Sie ZTNA implementieren, es sollte für die Benutzer*innen kaum spürbar sein und gleichzeitig einen nahtlosen und jederzeit verfügbaren Zugang zu den Geschäftsapps bieten. Die lokale App auf dem Gerät, die die Verbindung verwaltet, sollte die Akkulaufzeit nicht beeinträchtigen und bei Bedarf automatisch einen Tunnel zu Geschäftsapp aufbauen und bei einer Unterbrechung die Verbindung wiederherstellen. Dies macht nicht nur das Leben Ihrer Benutzer*innen einfacher (und wahrscheinlich glücklicher), sondern verhindert auch, dass Schatten-IT versteckte Schwachstellen in Ihre Infrastruktur einführt.

Die Verwendung von Single Sign-on (SSO) mit Ihrem Cloud IdP kann den Prozess weiter rationalisieren, indem das Passwort eines Benutzers/einer Benutzerin für jede verfügbare App verwaltet und der Authentifizierungsprozess vereinfacht wird. Schließlich ist es viel einfacher, sich ein einziges Passwort zu merken und dieses mit biometrischen oder anderen MFA-Methoden zu verifizieren, als sich Passwörter für alle Ihre Geschäftsapps zu merken.

ZTNA-Software :

- Nutzt die Leistungsfähigkeit von SSO und Cloud IdPs für eine einfache Authentifizierung
- Funktioniert überall dort, wo sich Ressourcen in internen oder externen Netzwerken befinden
- Schafft sichere Mikrotunnel zu einer App, ohne einen ganzheitlichen Zugang zu Unternehmensnetzwerken zu ermöglichen
- Einfache und schnelle Verfügbarkeit von Apps, wenn der Zustand des Benutzers/der Benutzerin und des Geräts überprüft wurde
- Schützt die Privatsphäre der Nutzer*innen und die Sicherheit der Unternehmensdaten
- Unbemerkt vom Endbenutzer/von der Endbenutzerin zu handeln ist ein Rezept für eine erfolgreiche Implementierung, die Benutzer*innen, IT- und Sicherheitsteams zufriedenstellt und produktiv hält.

Geben Sie den Trusted Access ein.

Auch wenn Sie den Geräten in Ihrem Netzwerk nicht blind vertrauen können, so können Sie doch darauf vertrauen, dass Ihre Zugangskontrollen die Sicherheit Ihrer Benutzer*innen und Ihres Unternehmens gewährleisten. Die ZTNA-Lösung von Jamf ist das, was Ihr Unternehmen braucht, um Trusted Access zu erreichen. Erfahren Sie mehr darüber, wie Trusted Access Geräteverwaltung, Identität und Zugriff sowie Endpoint-Sicherheit miteinander verbindet. Sehen Sie selbst, warum die sichere ZTNA-Lösung von Jamf bei Administrator*innen und Benutzer*innen gleichermaßen beliebt ist, und testen Sie sie kostenlos.

Testversion anfordern

Oder wenden Sie sich an Ihren bevorzugten Reseller, um loszulegen.

jamf

www.jamf.com/de/