Drei Anforderungen an einen Zero-Trust-Netzwerkzugang (ZTA)

Klassische Security-Modelle arbeiten mit einem „Vertrauensvorschuss“: Grundsätzlich gilt alles als vertrauenswürdig, was sich im Unternehmenswerk befindet. Die automatische Ausweitung des Vertrauens auf ein Gerät oder einen Benutzer – ob absichtlich oder versehentlich – gefährdet jedoch das Unternehmen. Security-Verantwortliche entscheiden sich daher zunehmend für einen Zero-Trust-Access (ZTA), um Benutzer und Geräte innerhalb und außerhalb des Netzwerks identifizieren, authentifizieren und überwachen zu können.

Digitale Innovationen steigern die Produktivität, bringen aber auch neue Cyber-Sicherheitsrisiken mit sich: Angreifer, Malware und infizierte Geräte, die Sicherheitsprüfungen am Netzwerk-Rand umgehen, können oft ungehindert auf alles im Netzwerk zugreifen.

Unternehmen können deshalb Benutzern oder Geräten innerhalb und außerhalb des Netzwerks nicht mehr blind vertrauen. Security-Verantwortliche sollten davon ausgehen, dass jedes Gerät im Netzwerk potenziell infiziert ist und dass jeder Benutzer – absichtlich oder versehentlich – kritische Ressourcen gefährden kann. Das Paradigma eines offenen Netzwerks mit pauschalem Vertrauen sollte durch eine Zero-Trust-Strategie ersetzt und mit strengeren Netzwerk-Zugriffskontrollen über ein Zero-Trust-Framework implementiert werden.

Eine ZTA-Strategie konzentriert sich auf die Netzwerk-Konnektivität und erfüllt drei wesentliche Funktionen:

1. WAS: Keine unbekannten Geräte im Netzwerk.

Der Anstieg bei Anwendungen und Geräten erweitert den Netzwerk-Rand und schafft unzählige Randbereiche, die verwaltet und geschützt werden müssen. Überforderte IT-Teams können die Flut von Geräten kaum noch kontrollieren – ganz gleich, ob diese zum Internet der Dinge (IoT), zu BYOD-Initiativen (Bring-Your-Own-Device) oder aus einem anderen Bereich der Unternehmensumgebung stammen.

Der erste Schritt bei der Einführung einer ZTA-Strategie besteht darin, alle Geräte im Netzwerk zu ermitteln und zu identifizieren – z. B. private Smartphones, Laptops, Netzwerk-Server, Drucker, Headless-IoT-Geräte wie HLK-Steuerungen oder Lesegeräte für Sicherheitsausweise. Dank dieser Transparenz kennen Security-Teams dann jeden Gerätetyp, jede Funktion und jeden Zweck innerhalb des Netzwerks und können den Zugriff dieser Geräte korrekt steuern. Ist eine ordnungsgemäße Kontrolle vorhanden,

Die Anzahl der Verbindungen, Geräte und Formen der Zusammenarbeit nimmt ständig zu – und damit auch die Bedrohungslage. Benötigt wird ein umfassender Zero-Trust-Ansatz, der alle Benutzer und Geräte im Netzwerk kennt und kontrollieren kann.

lassen sich mit einem Zero-Trust-Access alle Geräte im Netzwerk und ihre Reaktionen permanent überwachen. So kann das IT-Team problematische Geräte erkennen und isolieren, damit sie keine anderen Geräte oder Systeme im Netzwerk infizieren.

2. WER: Kein Netzwerk-Zugriff für unbekannte Benutzer.

Die Benutzeridentität ist entscheidend für die Entwicklung einer effektiven ZTA-Richtlinie. Unternehmen müssen jeden Benutzer kennen, der auf ihr Netzwerk zugreifen will – seien es Mitarbeiter, Auftragnehmer, Gäste oder Lieferanten. Die Benutzeridentität wird bei der Anmeldung mit einer Multi-Faktor-Authentifizierung überprüft (Passwörter allein sind zu schwach und werden häufig gestohlen). Zum Durchsetzen der Identität empfehlen sich Zertifikate. Diese können auch an eine rollenbasierte Access Control (RBAC) gebunden sein, um einem authentifizierten Benutzer bestimmte Zugriffsrechte und Dienste zuzuweisen.

Sobald die Identität feststeht, erhält der Benutzer die Zugriffsrechte, die für seine Rolle im Unternehmen vorgesehen sind. Grundsätzlich lassen sich für eine Rolle oder eine Aufgabe nur absolut notwendige Ressourcen-Berechtigungen einräumen. Ob auf weitere Ressourcen zugegriffen werden darf, wird dann von Fall zu Fall entschieden.

Nach der Einführung des Zero-Trust-Modells in großen Teilen des Unternehmens können Security-Verantwortliche geeignete Steuerelemente implementieren, damit Benutzer von überall aus den richtigen Zugriff auf das Netzwerk erhalten. Ein rollenbasierter Netzwerk-Zugriff für alle Benutzer stärkt die Netzwerk-Sicherheit enorm. Davon profitieren alle: Business, Mitarbeiter, Partner, Lieferanten, Auftragnehmer und andere Drittanbieter, mit denen das Unternehmen zusammenarbeitet.

3. ON-NET und OFF-NET: Sie müssen wissen, wie Assets inner- und außerhalb des Netzwerks geschützt werden.

Laut einem aktuellen Bericht sind 63 % der Unternehmen nicht in der Lage, Endpunkte außerhalb des Netzwerks zu überwachen – und über die Hälfte kann den Konformitätsstatus von Endgeräten nicht überprüfen.[1] Schuld daran sind steigende Mobilitätsanforderungen, aber auch die Arbeit in Homeoffices.

Mit einer ZTA-Strategie können Unternehmen Endgeräte auch außerhalb des Netzwerks absichern, indem sie die Transparenz über Endpunkte verbessern. Das Scannen auf Sicherheitslücken, robuste Patching-Richtlinien und Web-Filter sind wichtige Elemente einer ZTA-Strategie. Auch kann ein Zero-Trust-Ansatz einen sicheren Remote-Zugriff auf Netzwerk-Ressourcen über VPN-Verbindungen (Virtual Private Network) ermöglichen. So können Security-Teams jede Ressource anzeigen, kontrollieren und schützen – unabhängig davon, ob sie sich im Netzwerk befindet oder nicht.

Überlegungen für die nächste Phase

Ein echtes Zero-Trust-Framework identifiziert, segmentiert und überwacht kontinuierlich alle Geräte. Unternehmen können so sicherstellen, dass interne Ressourcen, Daten, Anwendungen und geistiges Eigentum geschützt bleiben. Ein weiterer Vorteil ist der wesentlich einfachere Netzwerk- und Security-Betrieb.

Mit einer ZTA-Strategie für Geräte können Sie:

- alle Geräte identifizieren, profilieren und auf Schwachstellen überprüfen
- eine kontinuierliche Netzwerk-Kontrolle einrichten und durchsetzen
- automatisch und abgestimmt im gesamten Netzwerk Bedrohungen abwehren

Mit einer ZTA-Strategie für Benutzer können Sie:

- die Identität bei der Anmeldung mit einer Multi-Faktor-Authentifizierung und Zertifikaten absichern
- rollenbasierte Informationen aus der Authentifizierungsquelle für privilegierte Zugriffe bereitstellen
- mit einer einmaligen Anmeldung (SSO) für zusätzliche Sicherheit und mehr Benutzerfreundlichkeit sorgen

[1] „The Cost of Insecure Endpoints“. Ponemon Institute, 2019.

FORTINET

www.fortinet.com/de

7. Dezember 2020, 13:56 Uhr

696154-0-1-DE