CISO-Leitfaden für einen effektiven Zero-Trust-Access (ZTA)

Wie Sie kontinuierliche Transparenz und Kontrolle über alle Geräte und Benutzer erreichen

Inhaltsverzeichnis

Zusammenfassung

Best Practices für den Netzwerk-Zugriff sehen einen grundlegenden Zero-Trust-Access (ZTA) vor – nach dem Motto „Traue nichts und niemandem“. Wollen CISOs einen solchen ZTA-Ansatz implementieren, stehen zahlreiche Technologien zur Auswahl, die die NIST-Anforderungen an Zero Trust-Architekturen erfüllen.[1] Problematisch wird es nur beim Zusammenspiel unterschiedlicher Security-Technologien im Unternehmen, was jedoch zum Verhindern von Sicherheitsvorfällen entscheidend ist.

Fortinet besitzt jahrzehntelange Erfahrung im Bereich Cyber-Security und hat bei der Implementierung neuster Standards in seine Lösungen festgestellt, dass die effektivste ZTA-Strategie ein ganzheitlicher Ansatz ist, der Transparenz und Kontrolle in drei Kernbereichen bietet: „Wer ist im Netzwerk?“ „Was ist im Netzwerk?“ und „Was passiert, wenn verwaltete Geräte das Netzwerk verlassen?“

Einleitung

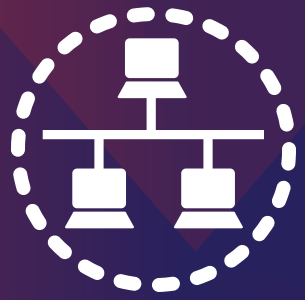
Digitale Innovationen (DI) sind mittlerweile ein „Dauer-Stresstest“ für die Netzwerk-Security. CISOs haben mit immer fragmentierteren Netzwerken und ständig wachsenden Angriffsflächen zu kämpfen. Da heutige Netzwerke unterschiedlichste Randbereiche haben – Stichwort „Edge“ –, lässt sich eine pauschale Verteidigungslinie nur noch schwer realisieren. Perimeterbasierte Zugangskontrollen sind mittlerweile praktisch wirkungslos. Dazu kommt, dass die Unterscheidung zwischen internen vertrauenswürdigen Anwendern und externen, unbekannten oder nicht vertrauenswürdigen Benutzern immer schwieriger wird – zu oft wurden schwerwiegende Sicherheitsverstöße schon durch Mitarbeiter oder Auftragnehmer verursacht. Aber selbst Anwender, die sämtliche Regeln befolgen, können zum Angriffsvektor werden, wenn sie regelmäßig mit privaten Geräten auf das Unternehmensnetzwerk zugreifen.

CISOs müssen deshalb die Vertrauensgrundlage überdenken, wenn Benutzern und Geräten Zugriff auf Netzwerk-Ressourcen eingeräumt werden soll. Auch die Best Practices haben sich weiterentwickelt: Früher galt alles und jeder innerhalb des Netzwerks als grundsätzlich vertrauenswürdig, dann wurde eine einmalige Prüfung der Vertrauenswürdigkeit eingeführt und heute darf nichts und niemandem mehr vertraut werden – Geräte und Benutzer erhalten nur noch absolut notwendige Zugriffsrechte. Das letzte Zugangsmodell wird auch als Zero-Trust-Access (ZTA) bezeichnet.

Die ZTA-Anforderungen wurden nach dem Aufkommen des Begriffs vor über einem Jahrzehnt laufend verfeinert. Dass ein ZTA-Konzept jedoch als Prozess verstanden werden muss, bestätigt auch das aktuellste NIST-Dokument zu Zero-Trust-Architekturen: Statt eine konkrete Architektur zu definieren, handelt es sich beim ZTA eher um Leitprinzipien. Security-Experten wird daher empfohlen, die Umstellung auf einen ZTA-Ansatz als laufende Entwicklung zu betrachten.

Um CISOs bei diesem Prozess zu unterstützen, hat Fortinet einen ganzheitlichen Ansatz für einen effektiven Zero-Trust-Access entwickelt, der auf drei Grundprinzipien beruht:

- ZTA-Lösungen müssen jederzeit Transparenz über die mit dem Netzwerk verbundenen Geräte und Benutzer sowie über die Netzwerk-Ressourcen bieten, auf die zugegriffen werden soll.
- Die Lösungen müssen in der Lage sein, Sicherheitsrichtlinien unabhängig von Gerätetyp, Standort oder Zugriffsmethode durchzusetzen.
- Durchsetzung und Transparenz müssen auch dann gegeben sein, wenn Geräte offline sind – also das Unternehmensnetzwerk verlassen haben.



Netzwerke haben unterschiedlichste Randbereiche, die sich mit einer perimeterbasierten Zugangskontrolle nicht mehr effektiv schützen lassen. Ein Zero-Trust-Access ist das vorherrschende Paradigma für den Netzwerk-Zugriff – und ein ganzheitlicher ZTA-Ansatz ist der Schlüssel zum Erfolg.

Sehen und kontrollieren, wer im Netzwerk ist

Das grenzenlose digitale Unternehmen unterstützt eine wachsende Vielfalt von Benutzern. Zum herkömmlichen Benutzer-Typ „Mitarbeiter“ sind andere Anwenderkategorien wie Auftragnehmer, Partner, Lieferanten und Kunden hinzukommen. Sie alle benötigen Zugriff auf Daten und Anwendungen, die sich On-Premises oder in der Cloud befinden können. Die Zugriffskontrolle auf Netzwerk-Ressourcen umfasst dabei sowohl die Identifizierung des Benutzers, der den Zugriff anfordert, als auch die Überprüfung, ob der Benutzer die Berechtigung zum Zugriff auf die angeforderten Ressourcen besitzt.

Sichere Identifizierung und Authentifizierung

Benutzeridentitäten sind leicht kompromittierbar: Cyber-Kriminelle können Benutzernamen und Passwörter mit Brute-Force-Angriffen – was oft einfach ist, weil viele Passwörter schwach sind – oder durch Social-Engineering-Taktiken wie E-Mail-Phishing stehlen. Unternehmen ergänzen deshalb den Anmeldeprozess um eine Multi-Faktor-Authentifizierung (MFA). Bei der MFA werden zwei Elemente kombiniert: etwas, was nur der Benutzer weiß – z. B. Benutzername und/oder Passwort – und etwas, das der Benutzer besitzt. Letzteres kann z. B. ein Hardware-Token sein, der einen Einmal-Code generiert, oder auch ein Software-Token. Bis 2024 werden voraussichtlich 70 % der Anwendungen eine MFA verwenden.[2] Neue biometrische Lösungen wie Fingerabdrücke, Gesichts- und Iris-Scans dürften ebenfalls das Risiko gestohlener Anmeldedaten minimieren.

Nur absolut notwendige Zugriffsrechte

Die zweite Herausforderung besteht darin zu verhindern, dass authentifizierte Benutzer ihre Zugriffsrechte missbrauchen. CISOs sollten deshalb grundsätzlich nur absolut notwendige Berechtigungen zulassen, die Benutzer und Auftragnehmer für ihre Arbeit unbedingt brauchen. Auch sollten Authentifizierungs- und Autorisierungslösungen in die Netzwerk-Security-Infrastruktur des Unternehmens (und in eine richtlinienbasierte Active-Directory-Datenbank) integriert werden, um die automatisierte Durchsetzung minimaler Zugriffsrechte und ein einfaches Richtlinien-Management zu gewährleisten.

Wichtig ist auch, dass Sicherheitsmaßnahmen weder die Produktivität der Anwender noch die Nutzererfahrung beeinträchtigen. CISOs sollten deshalb eine ZTA-Lösung wählen, die Single-Sign-On-Funktionen (SSO) unterstützt und mit minimaler Latenz arbeitet. Das vereinfacht nicht nur die Einhaltung der Compliance, sondern macht auch Benutzern das Leben leichter.

Zero-Trust-Access-Lösungen müssen Zugriffsrichtlinien strikt durchsetzen und zugleich die Produktivität und Erfahrung autorisierter Benutzer verbessern.

Sehen und kontrollieren, was im Netzwerk ist

Während CISOs zu Recht über das regelwidrige, unvorhersehbare Verhalten von Benutzern besorgt sind, sollten sie Geräten mit Netzwerk-Zugriff nicht weniger Aufmerksamkeit schenken. Dazu gehören Endbenutzergeräte (wie Computer, Laptops, Smartphones, Tablets), vernetzte Bürogeräte, Frontend-Systeme im Einzelhandel (z. B. Kassensysteme, POS), Betriebstechnologien sowie eine Fülle an überall installierten Sensoren und anderer Geräte, die zum Internet der Dinge (IoT) gehören. Ungeachtet schwankender Wachstumsprognosen für installierte IoT-Geräte kann man davon ausgehen, dass in den nächsten Jahren weltweit Milliarden IoT-Geräte eingesetzt werden.

Die Herausforderung beim Management all dieser Geräte liegt in ihrer breiten Verteilung im Netzwerk, der unterschiedlichen Geräteüberwachung und der mangelnden Unterstützung von Standard-Kommunikationsprotokollen in älteren Geräten. CISOs können Security-Administratoren beim Endpunkt-Management unterstützen, indem sie ihnen die richtigen Tools bereitstellen, um alles im Netzwerk effizient zu erkennen, zu kategorisieren und den Zugriff zu kontrollieren.

Die Netzwerk-Zugangskontrolle (NAC) sollte Transparenz in Sekunden liefern

Um zu jedem Zeitpunkt zu wissen, was sich im Netzwerk befindet, benötigen CISOs NAC-Tools (Network Access Control). Mit solchen Tools lässt sich jedes Gerät, das auf das Netzwerk zugreifen will, automatisch identifizieren und auf Schwachstellen überprüfen. Auch kann damit ein Geräte-Profil angelegt werden. Während des Discovery-Prozesses sollte die NAC-Lösung MAB-Angriffsversuche (MAC Authentication Bypass) erkennen und diese Vorfälle protokollieren. Auch sollten die erfassten Informationen in Echtzeit mit anderen Netzwerk-Geräten und Komponenten der Security-Infrastruktur ausgetauscht werden.

NAC-Prozesse dürfen nur Sekunden dauern, um das Risiko von Geräte-Kompromittierungen zu minimieren. Aus diesem Grund ist von Lösungen abzuraten, die zuerst den Datenverkehr scannen. Hierbei können sich Geräte schon während der Identifizierung mit dem Netzwerk verbinden, die bis zu einer halben Stunde dauern kann – mehr als genug Zeit, um Bedrohungen ins Netzwerk einzuschleppen.

Auch Lösungen, die auf dem 802.1X Wi-Fi-Protokoll basieren, sind nicht unproblematisch. Sie mögen zwar gut in WLANs funktionieren, in denen jeder Client einen Supplicant als Teil der Kommunikationssteuerung hat (was die Ausführung von 802.1X vereinfacht). 802.1X-basierte Lösungen lassen sich jedoch nur schwer in Switched-Netzwerken implementieren. Idealerweise sollte eine NAC-Lösung von einem zentralen Standort aus einfach bereitstellbar sein und den LAN- und WLAN-Betrieb einheitlich regeln, um ein schnelles Unternehmenswachstum zu unterstützen. Mit einer solchen zentralen NAC-Lösung entfallen auch zusätzliche Sensoren an jedem Gerätestandort, die sonst schnell zur Kostenfalle bei der Implementierung und Verwaltung werden.

Die Mikro-Segmentierung ermöglicht eine ZTA-Kontrolle

Die Durchsetzung von Zugriffsrichtlinien ist natürlich für alle Geräte notwendig, aber IoT-Geräte sind ein Kapitel für sich: Hierbei handelt es sich meist um kleine Geräte mit geringem Stromverbrauch, die weder eine CPU noch Speicherkapazitäten zur Unterstützung von Security-Prozessen haben. Viele IoT-Geräte arbeiten zudem mit nicht standardisierten Betriebssystemen, die oft inkompatibel zu den eingesetzten Tools für den Endpunkt-Schutz sind. Die Folge ist eine unzuverlässige Gerätesicherheit, die vom Netzwerk kompensiert werden muss.

IoT-Implementierungen sind oft umfassend und stark dezentral. CISOs müssen deshalb bei der Entscheidung für eine ZTA-Lösung die Zugangskontrolle von IoT-Geräten priorisieren. Da die Zugriffssteuerung nicht in den Geräten selbst implementiert werden kann, muss sie im Netzwerk erfolgen. Das lässt sich z. B. mit einer Mikro-Segmentierung über Next Generation Firewalls (NGFWs) erreichen, bei der ähnliche IoT-Geräte gruppiert werden. Dies härtet das Netzwerk gleich zweifach: Erstens wird der laterale Pfad (Ost-West-Datenverkehr) quer durch das Netzwerk unterbrochen, wodurch Hackern, Viren und Malware der Zugriff auf Geräte erschwert wird. Zweitens sinkt das Risiko, dass ein infiziertes Gerät zum Angriffsvektor wird, über den ein Hacker das restliche Netzwerk angreifen kann.

Wie alle anderen Elemente einer ZTA-Lösung sollten auch NGFWs den gesamten Datenverkehr zwischen Netzwerk-Segmenten mit minimaler Latenz verarbeiten können. So wird sichergestellt, dass der ZTA-Kontrollprozess für Geräte nicht die Produktivität im gesamten Unternehmen beeinträchtigt.

CISOs sollten Security-Administratoren die richtigen Tools bereitstellen, um alles im Netzwerk von zentraler Stelle effizient zu erkennen, zu kategorisieren und zu kontrollieren.

Verwaltete Geräte außerhalb des Netzwerks kontrollieren

Ein Merkmal digitaler Unternehmen ist die vorübergehende Natur der Netzwerk-Konnektivität und -Nutzung. Cloud-Dienste haben den allgegenwärtigen Zugriff und das Roaming für Benutzer ermöglicht: Anwender können Geräte an einem Ort vom Netzwerk trennen und an einem anderen wieder mit dem Netzwerk verbinden oder zuerst auf dem einem Gerät arbeiten und die Arbeit später auf einem anderen Gerät fortsetzen. Die Steuerung verwalteter Geräte außerhalb des Netzwerks ist eine echte Herausforderung: Selbst wenn Geräte beim ersten Herstellen einer Verbindung zum Netzwerk sicher sind, können sie in der Zwischenzeit – als sie offline waren – kompromittiert werden und das Netzwerk beim erneuten Zugriff infizieren.

CISOs sollten deshalb den Endpunkt-Schutz als Teil einer ZTA-Lösung betrachten. Eine Security-Lösung für Endgeräte muss auch außerhalb des Netzwerks Sicherheitsvorgaben durchsetzen können, z. B. Richtlinien zum Scannen von Sicherheitslücken oder das Anwenden von Web-Filtern und Patches. Weiter sollte sie sichere, flexible Optionen für die VPN-Konnektivität (Virtual Private Network) bieten. Genau wie Tools für das Identitätsmanagement sollte auch der Endpunkt-Schutz aus Gründen der Benutzerfreundlichkeit eine einmalige Anmeldung (SSO) unterstützen. Und sobald ein Endgerät mit dem Netzwerk verbunden ist, sollte der Endpunkt-Schutz den Gerätestatus zur Risikobewertung und Bestimmung der geeigneten Zugriffsebene an andere Netzwerk- und Security-Komponenten weiterleiten.

Fazit

Der Zero-Trust-Access (ZTA) bei der Zugriffskontrolle ist kein neues Konzept und vermutlich werden CISOs mit Tipps zu ZTA-Technologien und -Lösungen überhäuft. Branchenrichtlinien wie NIST SP 800-207[3] bieten einen praxisnahen Weg für die sukzessive Umstellung auf einen ZTA-Ansatz. Die Zusammenarbeit mit führenden Netzwerk-Security-Anbietern und die Auswahl integrierter, automatisierter Tools können dazu beitragen, die wichtigsten Herausforderungen beim ZTA-Netzwerk-Zugriff zu bewältigen: zu wissen, wer und was sich im Netzwerk befindet, den Ressourcenzugriff zu kontrollieren und die mit diesem Zugriff verbundenen Risiken zu minimieren.

[1] Scott Rose et al.: „Draft (2nd) NIST Special Publication 800-207, Zero Trust Architecture“. NIST, Februar 2020.

[2] Michael Kelley et al.: „Gartner Magic Quadrant for Access Management“. Gartner, 12. August 2019.

[3] Scott Rose et al.: „Draft (2nd) NIST Special Publication 800-207, Zero Trust Architecture“. NIST, Februar 2020.

www.fortinet.com/de

693421-A-0-DE

7. Dezember 2020, 13:53 Uhr