Zero-Trust-Architektur
Was ist das und wie wird es umgesetzt?

Alcatel·Lucent
Enterprise

E-Book
Zero-Trust-Architektur

Inhalt

Zero-Trust-Architektur – was ist das?

Was bedeutet Zero-Trust-Architektur (ZTA)? Bei dieser Strategie müssen jeder Nutzer und jedes Endgerät authentifiziert und autorisiert sein, bevor ein Datenzugriff erlaubt ist. Ganz nach dem Motto „Vertraue niemandem, authentifiziere alles“.

Ziehen wir einen Vergleich:

Wenn wir uns die klassische Sicherheit als Festung vorstellen, die ein Dorf schützt, dann würde die Festungsmauer (die Firewall) um das Dorf (das Unternehmen) herum gebaut. Alles, was außerhalb der Festung liegt, gilt als nicht vertrauenswürdig und wird überprüft. Was sich innerhalb der Festung befindet, genießt vorbehaltloses Vertrauen und gilt als zulässig. Diese Vertrauensgrenze verläuft sowohl physisch als auch implizit, je nachdem, auf welcher Seite der Festungsmauer man sich befindet. Auf der „richtigen“ Seite wird nichts weiter kontrolliert. Übertragen auf ein Unternehmensnetzwerk: Es ist vielleicht eine grundlegende Segmentierung in Form von VLANs, SSIDs, Subnetzen oder Schnittstellen vorhanden, die mit einer Firewall verknüpft sind. Aber diese Segmentierung ist statisch und hat mehr mit der Skalierbarkeit und Verwaltbarkeit des Netzwerks als mit der Sicherheit zu tun.

Heutzutage reicht der Firewall-Ansatz (Festung) allein jedoch nicht mehr aus. Dafür gibt es verschiedene Gründe. Da ist zunächst die Mobilität. Nutzer verbinden sich mit externen Netzwerken und schleppen auf diese Weise Bedrohungen ein. Zweitens gilt, dass Gäste nicht unbedingt vertrauenswürdig sind. Selbst Mitarbeitern (innerhalb der Festung) − so ließe sich argumentieren − sollte nicht blind vertraut werden. Drittens werden dem Firmennetzwerk zunehmend IoT-Geräte hinzugefügt. Das stellt ein höheres Sicherheitsrisiko dar: Die Geräte sind möglicherweise nicht von der IT-Abteilung genehmigt und verwaltet und es fehlen ihnen in der Regel Sicherheitsfunktionen. Beim klassischen Ansatz − „Festung/Dorf“ = „Firewall/Unternehmen“ − lässt sich, wenn ein Nutzer oder ein Endgerät kompromittiert ist, einer Bedrohung wenig bis gar nichts entgegensetzen: Sie kann auf andere Nutzer und Endgeräte übergreifen. Wer drinnen ist, kann sich frei bewegen.

Wenn nichts als die Festungsmauer das Dorf vor Eindringlingen schützt, wird es an dem Tag, an dem sie überwunden wird und das wird sie ,ein Chaos geben.

Es stellt sich die Frage: Was können wir dagegen tun? Setzen wir einmal voraus, dass niemandem vertraut wird.

Zero Trust – kein Vertrauen, weder für Nutzer noch Endgeräte. Ob inner- oder außerhalb des Areals, alles wird zunächst überprüft. Auch internen Nutzern wird nicht automatisch vertraut. Jeder Zugriff wird authentifiziert und autorisiert.

In unserer Analogie: Zusätzlich zu den Festungsmauern, die das Dorf vor Bedrohungen von außen schützen, ist auch jedes Gebäude noch einmal gesichert, um die Gefahr durch Akteure innerhalb der Festung zu bannen. Eine so genannte softwaredefinierte Mikrosegmentierung – im Fall eines Unternehmens – geht noch einen Schritt weiter. Neben der Festung und der Absicherung der Gebäude gibt es persönliche Sicherheitsbeamte, die uns auf Schritt und Tritt folgen. Und überall werden wir nach unserem Ausweis gefragt. Im Unternehmensnetzwerk ist diese Vertrauensgrenze fließend, verteilt und flexibel. Sie ist nicht an einen bestimmten Standort, Switch-Port oder an ein VLAN gebunden. Ausschlaggebend sind vielmehr die Identität, das Endgerät, die Situation, die Tageszeit und mehr. Die Grenze ist softwaredefiniert und wird im laufenden Betrieb angepasst. Das Entscheidende bei diesem Ansatz: Die Komponenten werden verwaltet und es muss möglich sein, im Fall einer Bedrohung oder Änderung im Workflow einzugreifen und sie neu zu konfigurieren.

Makro- und Mikrosegmentierung verstehen

In einer Zero-Trust-Architektur gibt es zwei Arten der Segmentierung – die Makro- und Mikrosegmentierung. In unserer Analogie ist die Festungsmauer die Makrosegmentierung und die persönlichen Sicherheitsbeamte sind die Mikrosegmentierung.

Bei **der Makrosegmentierung** wird das physische Netzwerk in verschiedene logische Segmente unterteilt. Diese Segmente können ein VLAN, eine Kombination aus VLAN und VRF, ein VPN (bei Shortest Path Bridging (SPB)), MPLS oder sogar ein VXLAN oder GRE-Tunnel sein. Der Traffic zwischen Nutzern oder Endgeräten in verschiedenen Segmenten wird durch eine Firewall kontrolliert. Alle Unternehmen arbeiten mit Segmentierung, allerdings nicht immer aus Sicherheitsgründen. Häufig wird für eine bessere Skalierbarkeit aus administrativen oder organisatorischen Gründen segmentiert. Wenn zwei Endgeräte verschiedenen VLANs zugeordnet sind, jedoch ohne Firewall dazwischen kommunizieren können, befinden sie sich im selben Makrosegment. Ein typisches Beispiel für diese Art der Segmentierung ist die IP-Telefonie in separaten, logisch von PCs isolierten VLANs und VRF.

Wie lassen sich Nutzer oder Endgeräte diesen Segmenten zuordnen? Eine statische Zuordnung wäre möglich, z. B. nach Switch-Port oder SSID, aber das ist eine inzwischen veraltete Methode. Sie ist zu starr und nicht im Sinne mobiler Nutzer. Im Idealfall verfügen Sie über ein softwaredefiniertes Authentifizierungssystem, über das ein Nutzer oder Endgerät bei der Verbindung und Authentifizierung ein Profil zugewiesen bekommt. Das Profil stellt den Nutzer oder das Endgerät, unabhängig vom physischen Standort, Switch-Port oder SSID, im richtigen Segment bereit.

Die Makrosegmentierung bietet zwar auch Sicherheitsvorteile, sie erfolgt aber häufig aus organisatorischen oder administrativen Gründen. So fallen beispielsweise Kameras und Türschlösser unter die Kontrolle der Gruppe für Zugangssicherheit, Thermostate hingegen unter die Kontrolle der Gruppe für Gebäude-Instandhaltung.

Die Mikrosegmentierung geht noch einen Schritt weiter. Nicht alle Nutzer sind gleich und nicht alle Nutzer müssen unbedingt auf alle Ressourcen zugreifen können. Ein Profil, das die Nutzer einem Segment zuordnet, enthält auch eine Reihe von Richtlinien, die eine fein abgestufte Kontrolle über die Nutzer-/Endgeräteberechtigungen ermöglichen. Sie sind für verschiedene Rollen wie die Personal- oder Finanzabteilung unterschiedlich. Dies wird als **„rollenbasierter Zugriff“** bezeichnet. Dazu gehört der **„Grundsatz des geringsten Privilegs“**. Obwohl also Kameras und Türschlösser demselben Segment zugeordnet sind, muss ihr Zugriff auf Ressourcen nicht gleich sein. Die Kamera muss mit dem Videorecorder und das Türschloss mit seinem Server kommunizieren. Eine Kamera muss nicht mit einem Türschloss kommunizieren, genauso wenig wie ein Türschloss mit anderen Türschlössern kommunizieren muss. Die fein abgestuften Berechtigungen werden durch in das Profil integrierte Richtlinien umgesetzt, die nach der Authentifizierung dynamisch auf das Endgerät angewendet werden.

Die Mikrosegmentierung muss aus mehreren Gründen softwaredefiniert sein. Weder Nutzer noch IoT-Geräte sind statisch: Sie bewegen, verbinden und trennen sich. Die Richtlinien dürfen daher nicht an einen Standort oder einen Anschluss gebunden sein. Die Konfiguration einer Mikrosegmentierung muss dynamisch sein und auf der Kombination mehrerer Faktoren beruhen, unter anderem auf der Identität des Nutzers oder Endgeräts, der Tageszeit und dem Standort.

Wenn also die Kommunikation zwischen Segmenten durch eine Firewall kontrolliert wird, spricht man von Makrosegmentierung. Wenn die Kommunikation innerhalb ein und desselben Segments durch NAC-Richtlinien (Network Access Control) kontrolliert wird, die mit dem Endgerät oder der Benutzerrolle verknüpft sind, handelt es sich um Mikrosegmentierung.

Warum beides notwendig ist

Was passiert, wenn nur eine Art der Segmentierung verwendet wird?

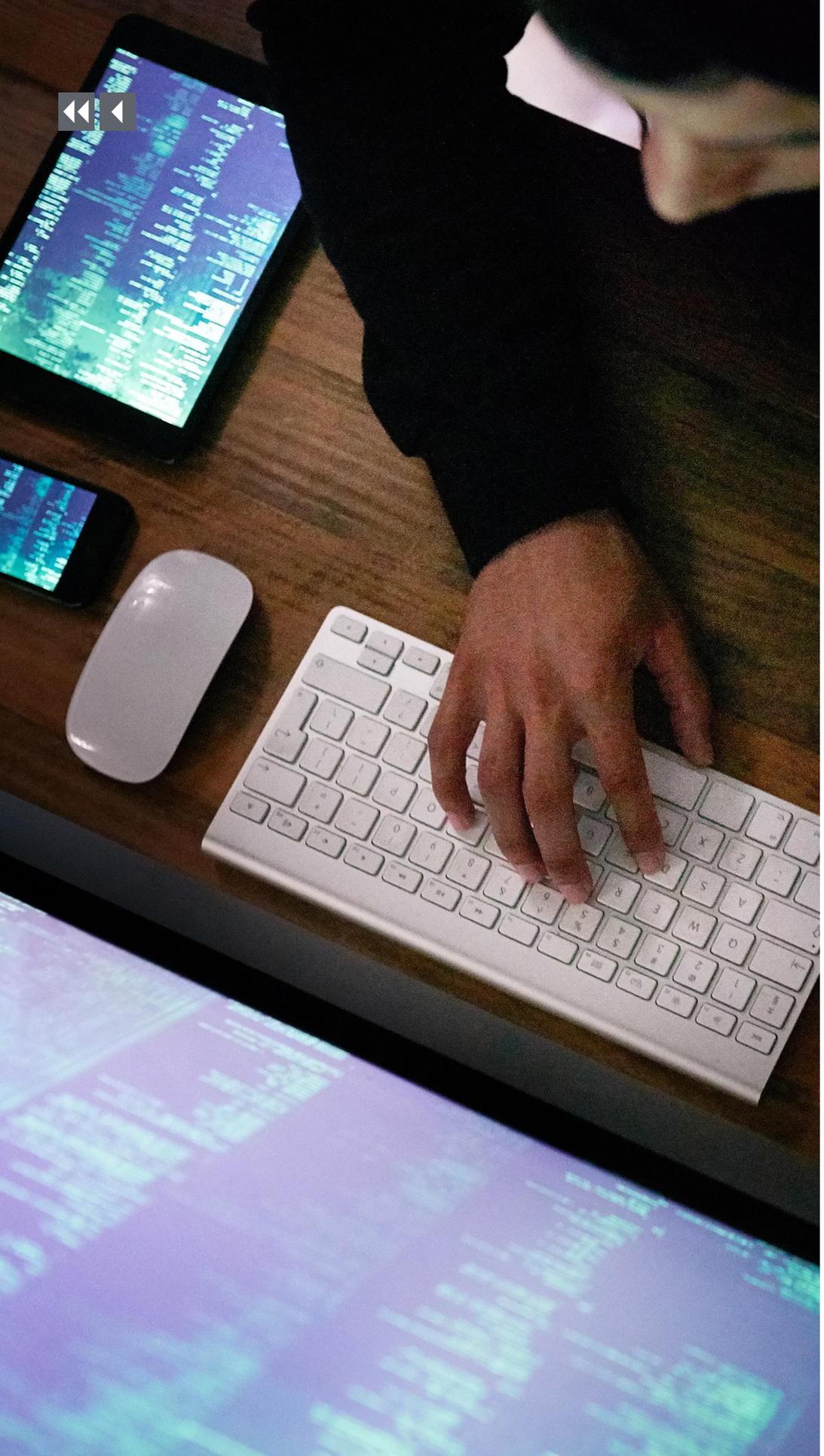
Betrachten wir die Makrosegmentierung. Das Problem: Die Firewall wird zum Engpass, da der gesamte Traffic zu Authentifizierungs- und Autorisierungszwecken dort hindurch muss. Das kann zu Leistungsproblemen führen. Sie können weitere Firewalls auf der Verteilungsschicht einrichten, aber das ist zum einen recht kostspielig und verbessert zudem nicht unbedingt die Leistung, da Firewalls nicht ausreichend durchsatzstark sind. Auch erhöht sich dann die Zahl der Stellen, an denen Richtlinien durchgesetzt und auf dem neuesten Stand gehalten werden müssen. Das erschwert die Verwaltung.

Die andere Option − nur Mikrosegmentierung − ist ebenfalls problematisch. Wenn die Durchsetzung ausschließlich über NAC-Richtlinien erfolgt, werden die Richtlinienlisten sehr lang und komplex und die Endgeräte geraten ggf. an ihre Kapazitätsgrenzen.

Im Endeffekt ist ein ausgewogener Einsatz beider Arten von Segmentierung anzuraten. Die Firewall sollte den Traffic zwischen verschiedenen Segmenten (vertikal) und die NAC-Richtlinien den Traffic innerhalb eines Segments (lateral) kontrollieren.

Durch die Kombination beider kann auf Sicherheitsbedrohungen, die von einem Sicherheitssegment auf ein anderes übergreifen, ebenso reagiert werden wie auf solche, die sich seitlich (lateral) in einem Segment bewegen. Konkret: Durch Mikrosegmentierung ist ein Angreifer, der erfolgreich eine Kamera gekapert hat, nicht mehr in der Lage, diese Lücke zu nutzen, um andere Ressourcen wie z. B. ein Türschloss zu kompromittieren.

Das Ziel besteht darin, jede Verbindung zu authentifizieren und jedem Nutzer oder Endgerät Berechtigungen zuzuweisen. Das heißt, dass die Ausbreitung einer seitlich fortschreitenden Bedrohung mittels Segmentierung verhindert wird, und eine kontinuierliche Überwachung und Quarantäne jedes nicht mehr konformen Nutzers oder Endgeräts stattfindet.



Der Weg dorthin

„Auf der grünen Wiese“ wäre der Aufbau einer Zero-Trust-Architektur mit Mikrosegmentierung von Grund auf relativ einfach. Doch in der Praxis kann es in einem nachgerüsteten Netzwerk passieren, dass Nutzer, Endgeräte und Anwendungen aufgrund fehlgeschlagener Authentifizierung oder unvollständiger Richtlinien aus dem Netzwerk ausgesperrt werden. Es wäre schwierig bzw. unwahrscheinlich, dass ein Unternehmen die Migration in einem Zug − in einem einzigen Aktualisierungszyklus − durchführen könnte.

In einer gewachsenen Umgebung werden Non-Zero-Trust- und Zero-Trust-Architektur eine Zeit lang nebeneinander bestehen müssen, und die Migration wird Schicht für Schicht bzw. standortweise erfolgen. Stellen Sie nur sicher, dass die von Ihnen eingesetzten Infrastrukturelemente, und die Art wie Sie sie nutzen, flexibel und zum Zero-Trust- oder Mikrosegment-Modus in der Lage sind, wenn andere Infrastrukturelemente bereit sind. Die Infrastruktur muss also mit bestehenden und künftigen Komponenten interoperabel sein.

Die Methodik

Es gibt fünf Schritte auf dem Weg zu einer Zero-Trust-Architektur: Überwachen, validieren und bewerten, planen, simulieren und durchsetzen.

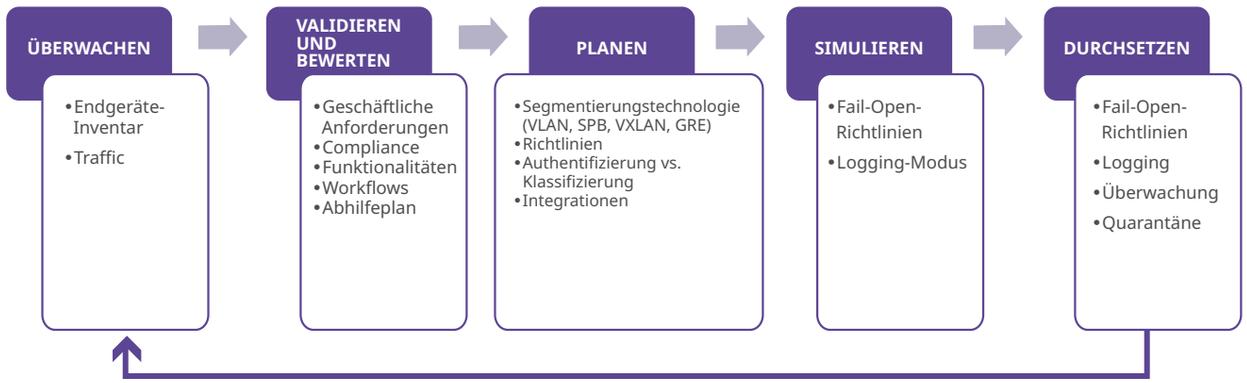


Abbildung 1 − Die Methodik

Schritt 1: Überwachen

Bevor Sie irgendetwas anderes tun, müssen Sie mit der Überwachung beginnen und eine Karte und eine Bestandsaufnahme erstellen, von allem was in Ihrem Netz vorhanden ist.

Die Migration zur ZTA setzt eine detaillierte Kenntnis der (physischen und virtuellen) Assets, der Subjekte (einschließlich der Nutzerrechte) und der Geschäftsprozesse voraus, die mit dem Netzwerk in Berührung kommen oder darauf laufen. Unvollständiges Wissen führt meistens zum Scheitern: Es wird dann der Zugang aufgrund unzureichender Informationen verweigert. Das ist besonders dann ein Problem, wenn es in einer Organisation eine unbekannte „Schatten-IT“ oder „Schatten-IoT“ gibt.

Beginnen Sie damit, Endgeräte und Datenströme zu überwachen. Erstellen Sie eine Inventarübersicht mit allen Endgeräten, die im Netzwerk gesichtet werden − kategorisiert nach Endgerätetyp, Hersteller, Modell, Betriebssystem usw. Der Bericht sollte auch aufzeigen, wo und an welchem Switch-Port oder SSID das Endgerät zuletzt gesehen wurde. Hierüber geben Elemente wie die MAC-Adresse, DHCP-Signatur und der HTTP-Benutzeragent Aufschluss.

Die meisten Tools von Drittanbietern liefern nur die IP-Adresse, nicht aber den Endgerätetyp. Ideal wäre ein Tool zur Erstellung eines IoT/Endgeräte-Inventars, das die schnelle und einfache Erstellung von NAC-Profilen für jeden Endgerätetyp ermöglicht.

Für die Richtlinien wird als Informationsgrundlage ferner der Traffic benötigt. Je nach Ihrer IT-Ausstattung erhalten Sie diese Informationen von Tools zur Überwachung der Datenströme wie sFlow, Netflow oder Deep Packet Inspection (DPI).

Es ist ein iterativer Prozess. Wenn Sie die Überwachung zum ersten Mal durchführen, sind Ihre Berichte vielleicht noch nicht sehr aussagekräftig. Aber mit jedem weiteren Schritt werden sie immer spezifischer und nützlicher. Die Informationen, die Sie hier sammeln, sind für die nächsten Schritte entscheidend.

Schritt 2: Validieren und Bewerten

Im nächsten Schritt werden diese Ergebnisse validiert. Bewerten Sie Ihre geschäftlichen Anforderungen. Schatten-IoT ohne Existenzberechtigung sollte entfernt werden, da es die Angriffsfläche unnötig vergrößert. Für den Rest müssen Sie die Subjekte (Nutzer und Endgeräte), Datenströme und Workflows identifizieren, um diese in Ihren Richtlinien zu berücksichtigen. Zum Beispiel, wer Zugang zu bestimmten Assets erhält und was er damit tun darf. Wenden Sie den Grundsatz des geringsten Privilegs an.

Mikrosegmentierung bedeutet nicht, dass andere Sicherheitsvorkehrungen wie Passwort-Richtlinien oder Firmware-Updates gelockert werden. Jede Funktionalität muss einzeln bewertet werden. Unterstützen diese Endgeräte eine Authentifizierung über Zertifikate? Gibt es ein Tool, mit dem diese Zertifikate ausgestellt und angewendet werden können? Welche Datenströme sind erforderlich? Möglicherweise müssen Sie diese Informationen beim Hersteller erfragen. Sie sollten sie aber auch mit Ihren eigenen Traffic-Analysen abgleichen. Wenn Sie Assets finden, die gegen die Unternehmensrichtlinien verstoßen, benötigen Sie einen Abhilfeplan, um die Compliance wiederherzustellen, oder Sie müssen zusätzliche Kontrollen einrichten.

Schritt 3: Planen

Sie kennen jetzt bereits die Assets, die Subjekte (Nutzer), den Traffic und die Workflows. Nun müssen Sie dieses Wissen in Authentifizierungs- und Sicherheitsrichtlinien umsetzen, um Ihre Mikrosegmentierungsarchitektur zu implementieren. Wie bereits erklärt, bietet sich für optimale Ergebnisse eine Kombination aus Makro- und Mikrosegmentierung an. Denken Sie daran, dass Sie in der Praxis durch die bereits vorhandene Architektur eingeschränkt sind.

Für die Makrosegmentierung gibt es viele Optionen, etwa VLANs, VRFs, SPB VPNs, VXLAN oder GRE-Tunnel und spezielle Funktionen wie Private VLAN. Jede dieser Möglichkeiten hat ihre Vor- und Nachteile und kann sich je nach Situation als nützlich erweisen. Für die Mikrosegmentierung müssen Sie wissen, welche Richtlinien für jeden Nutzer- oder Endgerätetyp in das Profil aufzunehmen sind. Am Ende müssen Sie noch festlegen, wie Sie Nutzer und Endgeräte ihrem Segment und den für sie geltenden Richtlinien zuordnen. Das ist eine Frage von Authentifizierung versus Klassifizierung. Auch ein Fingerabdruck des Endgeräts ist möglich.

Idealerweise sollten Sie in Technologie (softwaredefinierte Segmentierung) investieren, die flexible Authentifizierungsrichtlinien ermöglicht, so dass Sie Ihre Netzwerkprofile leicht aktualisieren können.

Wir empfehlen Ihnen folgende Reihenfolge für Ihren Authentifizierungsablauf:

1. Authentifizierung durch 802.1x-Zertifikate mit dem RADIUS-Server. Die Authentifizierung generiert einen Authentifizierungsdatensatz. Diese Information kann mit einer Firewall geteilt werden.
2. Wenn das Endgerät nicht über 802.1x-Zertifikate authentifizierbar ist, sollten Sie es als Nächstes mit der MAC-Authentifizierung versuchen. Die MAC-Authentifizierung ist nicht annähernd so sicher wie 802.1x, aber besser als nichts, bis Sie bereit sind, auf 802.1x umzusteigen.
3. Wenn kein Profil ausgegeben wird, versuchen Sie, einen Fingerabdruck zu erstellen. Er ist auch für die Zuordnung zu einem Profilsegment und zu Regeln nutzbar. Dabei wird kein Authentifizierungs- oder Buchhaltungsdatensatz generiert, aber er wird in der Datenbank des IoT-Inventars registriert.
4. Schließlich können Sie ein „Catch all“ als Default für den Fall vorsehen, dass keine Profile ausgegeben werden oder alles andere fehlschlägt. In der Anfangsphase müssen Sie das Endgerät noch einem Profil zuordnen, das zu demselben Segment und denselben Regeln führt und das Endgerät in der Inventar-Datenbank erfasst.

Dieser Workflow sollte flexibel gestaltet sein, damit Sie ihn nach und nach anpassen können. Sie könnten zum Beispiel die MAC-Authentifizierung zunächst ausschließen und später hinzufügen, wenn Ihnen die Liste der MAC-Adressen aus der Inventarübersicht vorliegt. Und im Zuge der zunehmenden Prozessverfeinerung können Sie zum Beispiel das Segment und die Regeln, die mit dem Standardprofil verknüpft sind, in sehr restriktive Regeln ändern, die nur Zugriff auf einen Bastion-Host erlauben.

Möglicherweise möchten Sie auch die Endgeräterolle mit der Firewall teilen, damit die Firewall-Regeln auch auf der Endgeräterolle und nicht nur auf der Subnetz/IP-Adresse basieren. Diese Integration hat zweierlei Vorteile. Erstens kann die Firewall feiner abgestimmte Richtlinien auf diese IoT-Geräte anwenden. Zweitens sind die Firewall-Richtlinien dann nutzer- oder rollenbasiert und somit nicht mehr an eine Subnetz- oder IP-Adresse gebunden. Das erleichtert eine zukünftige Neugestaltung und Neusegmentierung des Netzwerks.

Der Prozess ist iterativ: Sie werden ihn optimieren, abstimmen und verfeinern müssen, wenn Sie mit Authentifizierung und Segmentierung mehr Erfahrung gesammelt haben.

Schritt 4: Simulieren

Egal, wie gut Sie planen: Es ist eher unwahrscheinlich, dass Sie auf Anhieb alles richtig machen. Jeder Fehler in der Gestaltung des Authentifizierungsschemas, jede versehentliche Lücke in der „Freigabeliste“ der Sicherheitsrichtlinie führt zu gestörten Geschäftsprozessen. Für Authentifizierungs- und Zugriffsrichtlinien muss daher ein „Fail-Open“-Modus gelten. Das bedeutet, dass Endgeräte und Nutzer, die sich nicht authentifizieren können, weiterhin im Netzwerk zugelassen und auch unerwartete Datenströme weiterhin erlaubt sind. Diese Fälle werden protokolliert, und anhand der Logs können Sie Ihre Authentifizierungs- und Richtlinienpläne verfeinern.

Schritt 5: Durchsetzen

Nach ein wenig Feinabstimmung werden Sie keine Authentifizierungsfehler oder die Verweigerung legitimer Datenströme mehr feststellen. Sie können die Richtlinien dann von „Fail-Open“ auf „Fail-Close“ umstellen: Unbekannte Endgeräte werden blockiert und unerwartete Datenströme nicht durchgeleitet.

Es versteht sich von selbst, dass Sie die Überwachung im Hinblick auf fremde Endgeräte und unerwarteten Traffic fortsetzen und den ganzen Vorgang bei Bedarf wiederholen müssen.

Eine letzte Sache

Für die Zwecke der kontinuierlichen Überwachung, Logging und Quarantäne empfehlen wir Ihnen, in ein externes Intrusion Detection System (IDS) zu investieren. Zwar wird eine Reihe von DDoS-Angriffen (Distributed Denial of Service) direkt vom Switch selbst erkannt, doch erfasst ein externes IDS eine breitere Palette von Angriffen, etwa durch Viren, oder andere Unregelmäßigkeiten. Vielleicht erinnern Sie sich, wie vor einigen Jahren mehrere Videoüberwachungskameras mit der Mirai-Malware infiziert wurden oder wie es zum koordinierten Angriff auf globale DNS-Server kam, was Dienste wie Twitter, Spotify oder Paypal in Mitleidenschaft zog. Diese Angriffe werden von Ihren Switches möglicherweise nicht erkannt, aber ein spezielles IDS wird dies mit Sicherheit tun.

Sobald der Angriff erkannt wird, übermittelt das IDS an Ihr Netzwerkmanagementsystem (NMS) die IP-Adressen der betroffenen Endgeräte. Im Idealfall ist Ihr NMS in der Lage, diese Endgeräte in seiner Datenbank zu finden und deren Profile in eine „Quarantäne-Rolle“ zu versetzen.

Die „Quarantäne-Rolle“ ist sehr restriktiv und erlaubt in der Regel nur die Kommunikation mit einem Bastion-Host, damit das Endgerät z. B. durch Setzen eines starken Passworts oder ein Update der Firmware usw. regularisiert werden kann.

Warum Alcatel-Lucent Enterprise?

Die Digital Age Networking-Lösungen von Alcatel-Lucent Enterprise bieten eine robuste und flexible softwaredefinierte Segmentierung mit dynamischen DPI NAC-Richtlinien, die einen schrittweisen Umstieg auf eine Zero-Trust-Architektur ermöglichen.

Digital Age Networking ist ein Konzept von Alcatel-Lucent Enterprise, das Unternehmen den Weg ins digitale Zeitalter weist und mit dem sie ihr digitales Geschäft ausbauen können. DAN stützt sich auf drei Säulen:

- Ein autonomes Netzwerk, das Menschen, Prozesse, Anwendungen und Objekte einfach, automatisch und sicher miteinander verbindet. Das autonome Netzwerk von ALE basiert auf einem optimierten Portfolio mit konsequent einheitlicher Managementplattform, die gemeinsame Sicherheitsrichtlinien für unser LAN und WLAN bereitstellt. Darüber hinaus bietet es eine flexible Bereitstellung in Gebäuden, im Freien und in industrieller Umgebung. Die Netzwerkverwaltung kann je nach Kundenwunsch vor Ort, in der Cloud oder hybrid erfolgen.
- Sicheres und effizientes Onboarding von IoT-Geräten: Durch Segmentierung bleiben die Endgeräte in ihren spezifischen Segmenten. Das minimiert das Risiko einer Kompromittierung einzelner Endgeräte und des Netzwerks. Durch die IoT-Segmentierung können Unternehmen unkompliziert und automatisch feststellen, ob sich Endgeräte richtig verhalten. Das trägt zur Sicherheit ihres Netzwerks bei.
- Geschäftsinnovation durch Workflow-Automatisierung: Die Integration von Nutzer-, Anwendungs- und IoT-Metriken in Echtzeit und mit Geolokalisierungsdaten in Plattformen für die Zusammenarbeit vereinfacht den Aufbau und die Einführung neuer automatisierter digitaler Geschäftsprozesse und Dienstleistungen. Sicherheits- und Netzwerk-Administratoren werden bei einer Sicherheitsverletzung in Echtzeit benachrichtigt.

Besitzen Sie ein Tool zur Erstellung eines IoT-/Endgeräte-Inventars? Verfügen Sie über ein Tool, mit dem Sie die Datenströme der Anwendungen überwachen können? Sind Ihre aktuellen Switches und Wireless Access Points für die softwaredefinierte Segmentierung bereit? Wenn Sie derzeit nicht über diese Tools verfügen, wenden Sie sich gerne an uns. Wir beraten und unterstützen Sie.

Das wissen wir – mit Sicherheit

Abschließend einige wichtige Erkenntnisse im Überblick:

- Eine wirklich effiziente ZTA setzt sowohl Makro- als auch Mikrosegmentierung voraus.
- Eine ZTA besteht aus fünf Schritten: Überwachen, validieren und bewerten, planen, simulieren und durchsetzen.
- Eine auf Mikrosegmentierung basierende ZTA stützt sich auf drei Säulen: Authentifizierung, mit 802.1x EAP-TLS als Goldstandard; differenzierte, mit der Nutzer- oder Endgeräterolle verbundene Richtlinien nach dem Grundsatz des geringsten Privilegs; und kontinuierliche Überwachung und Quarantäne.
- In hybriden und mobilen Umgebungen muss die Mikrosegmentierung softwaredefiniert, d. h. dynamisch und richtlinienbasiert sein. Sie darf aus praktischen Gründen nicht statisch definiert sein.

Der Umstieg auf eine ZTA durch Mikrosegmentierung ist ein Prozess, den ein Unternehmen egal welcher Größe wahrscheinlich nicht in einem einzigen Aktualisierungszyklus bewältigen kann. Aber mit jeder Aktualisierung, Umgestaltung oder kontinuierlichen Verbesserung kommen Sie diesem Ziel näher, wenn Sie auf die richtige Infrastruktur und das richtige Design setzen.

Alcatel-Lucent Enterprise arbeitet mit Nachdruck an der Entwicklung von Netzwerktechnologien und -lösungen, die Unternehmen den Weg in die digitale Zukunft ebnen.

Alcatel·Lucent
Enterprise