Aufbau eines kosteneffizienten Zero-Trust-Netzwerks

Maximale Netzwerksicherheit, geringstmögliche Kosten

Lösung im Überblick

Alcatel·Lucent Enterprise

Cybersicherheit und Zero Trust

Cybersicherheit wird zu einem immer größeren Thema: Die Technologie entwickelt sich rasant weiter und Cyberbedrohungen nehmen an Zahl und Komplexität ständig weiter zu. Manche Bedrohung wechselt so schnell ihre Gestalt, dass es schwierig ist, sie vorherzusagen und abzuwehren. Cybersicherheit-Profis müssen unentwegt neueste Trends kennen und Schwachstellen beobachten.

Da es viele verschiedene Quellen und Angriffsvektoren gibt – u. a. Phishing-E-Mails, Social Engineering und Software-Schwachstellen –, erfordert die Abwehr je nach Cyberangriff einen eigenen Ansatz.

Alle potenziellen Schwachstellen in einem komplexen System zu erkennen und dieses zu schützen, ist eine Herausforderung. Nur wer versteht, wie verschiedene Systeme und Netzwerke zusammenarbeiten, kann wirksame Sicherheitsmaßnahmen in Stellung bringen.

Menschliches Versagen ist eine häufige Ursache für Cybersicherheitsvorfälle, und bis 2025, so schätzt man, werden mehr als die Hälfte solcher Vorfälle auf Fachkräftemangel oder menschliche Fehler zurückzuführen sein.[1]

Komplexe Vorschriften und Standards im Bereich der Cybersicherheit, etwa die Datenschutz-Grundverordnung (DSGVO) oder der Health Insurance Portability and Accountability Act (HIPAA), sind eine weitere Hürde, die spezielle Kenntnisse und Expertise voraussetzt.

1 Gartner® Predicts 2023: Cybersecurity Industry Focuses on the Human Deal | Bitsight, Januar 2023.

Anatomie von Cybersicherheitsvorfällen

Die Abbildung unten zeigt, wie ein Cyberangriff – das Vordringen in ein Netzwerk und der Diebstahl wertvoller Daten – abläuft. Zunächst wird spioniert (Reconnaissance): Der Angreifer recherchiert Ziele, wählt sie aus und beginnt, nach Sicherheitslücken im Netzwerk zu suchen.

Im nächsten Schritt bringt der Angreifer sein Angriffswerkzeug in Stellung (Weaponisation), visiert sein Ziel an und setzt seine vergiftete Ladung ab.

Danach folgt Exploitation: Der platzierte Schädling wird getriggert, wodurch der Angreifer auf dem Zielsystem Privilegien erhält, die er nutzt, um sich lateral durchs Netzwerk zu bewegen.

Der nächste Schritt ist die Installation: Der Angreifer etabliert einen Remote-Shell-Zugang, installiert Malware und setzt sich damit im System fest.

In der Command-and-Control-Phase baut der Angreifer verschlüsselte Kommunikationskanäle auf, die zu Command-and-Control-Servern zurückführen, um den Angriff aus der Ferne zu steuern.

Die letzte Phase ist die laterale Bewegung und Exfiltration, bei der unter Umständen mehrere Ziele verfolgt werden, etwa Datendiebstahl, Zerstörung oder Veränderung kritischer Systeme und Denial-of-Service.

Ein Angriff lässt sich am wirkungsvollsten dadurch stoppen, dass die verschiedenen Phasen des Angriffs frühzeitig erkannt werden und ihnen ein Riegel vorgeschoben wird.

Dazu sind eine Reihe von Maßnahmen notwendig, z. B. Schwachstellen- und Patch-Management, Malware-Erkennung und -Prävention, Blockierung riskanter Anwendungen und Dienste sowie Protokollierung und Überwachung aller Netzwerk-, Endpunkt- und natürlich Cloud-Aktivitäten.

Netzwerkseitig muss technologisch aufgerüstet werden, sodass eine granulare Kontrolle der Anwendungen möglich und der Traffic zwischen Zonen oder Segmenten mittels Zero-Trust-Modell überwachbar ist. Zero Trust beruht auf dem Prinzip, dass alles standardmäßig als nicht vertrauenswürdig eingestuft wird.

Das Konzept wurde zur Abwehr immer zahlreicherer ausgeklügelter Cyberangriffe auf Computernetzwerke entwickelt. Der klassische Weg hatte darin bestanden, Netzwerke durch Sicherheitslösungen am Netzwerkrand, z. B. Firewalls und Antiviren-Software, zu schützen. Mit zunehmender Raffinesse und Komplexität der Cyberangriffe erwiesen sich diese perimeterbasierten Lösungen jedoch als unzureichend. Es muss stattdessen jede Zugriffsanfrage überprüft und authentifiziert werden, bevor der Zugriff auf Ressourcen gewährt wird.

Source: XDR for Dummies, Palo Alto Networks, Sonderausgabe, 2022

Ihre Zero-Trust-Strategie

Alcatel-Lucent Enterprise ist Partner seiner Kunden in Sachen Sicherheit und unterstützt die Einrichtung einfacher und kosteneffizienter Zero-Trust-Umgebungen. Wir bei ALE wissen, wie wichtig ein Zero-Trust-Modell für die Netzwerk- und Datensicherheit unserer Kunden ist. Wir bieten eine Reihe von Lösungen für die Implementierung eines Zero-Trust-Netzwerks an. So helfen wir Unternehmen, sich den Herausforderungen durch Cyberbedrohungen zu stellen.

Netzwerkhärtung

Wir härten **Ihr Netzwerk – sowohl von innen als auch außen**. Das beginnt mit einer sicheren Infrastruktur. Auch das Gerät selbst darf nicht kompromittiert sein. Unsere Alcatel-Lucent OmniSwitch® Produktfamilie läuft auf dem sicheren Betriebssystem von Alcatel-Lucent (AOS), das Netzwerke über sicheren diversifizierten Code vor potenziellen Schwachstellen und Angriffen schützt. Der Code wird laufend in Bezug auf aktuelle und zukünftige Bedrohungen aktualisiert, wobei zum Schutz vor Pufferüberlauf-Angriffen eine Software-Diversifizierung durch Address Space Layout Randomisation (ASLR) zum Einsatz kommt. Zudem wird mittels unabhängiger Verifizierung und Validierung (IV&V) der AOS-Quellcode auf potenzielle Schwachstellen, Backdoors, Malware und Exploits analysiert und getestet. Diese Tests führen auf Cybersecurity spezialisierte Drittanbieter durch. Als Grundlage dienen allgemein verfügbare Software-Images, damit die Integrität der Software sichergestellt ist.

Über Makro- und Mikrosegmentierung wird ein Netzwerkzugang gewährleistet, der auf Zero Trust basiert. Beides sind entscheidende Elemente einer Zero-Trust-Sicherheitsstrategie. **Makrosegmentierung** bedeutet, dass das Netzwerk in separate Zonen oder Domänen auf Grundlage von Funktionen, Anwendungen oder Benutzergruppen aufgeteilt wird. Das sorgt für ein hohes Maß an Netzwerksegmentierung, so dass kritische Anlagen und Ressourcen vom Rest des Netzwerks isoliert werden können. Bei der **Mikrosegmentierung** hingegen wird das Netzwerk granular segmentiert, bis hin zum einzelnen Benutzer oder Gerät. Dieser Ansatz bietet eine feiner abgestimmte Kontrolle über den Netzwerkzugang. So lassen sich Sicherheitsrichtlinien auf Ebene der Benutzer oder Geräte durchsetzen.

Shortest Path Bridging (SPB) und **Universal Network Profiles** (UNP) sind eine leistungsstarke Lösung für die Makro- und Mikrosegmentierung von Netzwerken, durch die sich Sicherheit und Performance verbessern, da weniger potenzielle Angriffsfläche geboten wird.

SPB ist ein Layer-2-Netzwerkprotokoll, das Multi-Path-Routing in großen Netzwerken ermöglicht und gleichzeitig die Konfiguration und das Management der Netzwerkinfrastruktur vereinfacht. Funktionen wie virtuelle Netzwerksegmentierung bieten zusätzlichen Schutz vor unbefugtem Zugriff und Cyberangriffen. Der Einsatz von SPB in der Netzwerkinfrastruktur verbessert die Netzwerkeffizienz und -sicherheit. Unternehmen können sich auf geschäftliche Ziele konzentrieren, ohne sich um ihre Sicherheit sorgen zu müssen.

ALE UNP ist eine profilbasierte Zugangskontrolle – eine leistungsstarke Funktion der Switches von Alcatel-Lucent Enterprise. Netzwerkadministratoren können damit Benutzerprofile für den Netzwerkzugang auf der Grundlage von Identität, Standort und Gerät erstellen und verwalten. Ein zentrales Management der Netzwerkrichtlinien ist möglich. Das vereinfacht ihre Konfiguration und Durchsetzung. Ist ALE UNP implementiert, lassen sich die Netzwerktransparenz, -sicherheit und -kontrolle verbessern. Gleichzeitig steigt die Netzwerkleistung, Assets sind geschützt und Ausfallzeiten reduzieren sich.

Im Zusammenspiel ermöglichen SPB und UNP eine effiziente Verwaltung und Absicherung der Netzwerkinfrastruktur:

- **Konsistente Anwendung von Richtlinien im gesamten Netzwerk**
- **Segmentierung und Isolierung der IoT-Geräte von anderen Geräten**
- **Minimierung der Angriffsfläche im Netzwerk**

Robuste Authentifizierung

ALE bietet eine zuverlässige Authentifizierung über Unified Policy Authentication Manager (UPAM).

Ein Schlüsselelement der Cybersicherheit ist die Authentifizierung, d. h. die Überprüfung der Identität eines Benutzers, Geräts oder Systems. Es geht um die Bestätigung, dass ein Benutzer oder Gerät tatsächlich ist, wer er/es vorgibt zu sein, in der Regel durch eine Form der Identifizierung, z. B. über Benutzernamen und Passwort.

Die ALE-Lösung unterstützt eine Reihe von Verfahren zur Benutzerauthentifizierung.

- **802.1X**, ein Netzwerk-Authentifizierungsprotokoll, bietet die Möglichkeit, Geräte – gestützt auf Anmeldeinformationen wie Benutzernamen und Passwort – mit einem sicheren Netzwerk zu verbinden. Wenn ein Gerät versucht, mit 802.1X eine Verbindung zu einem Netzwerk herzustellen, wird es zunächst authentifiziert, bevor der Zugriff auf das Netzwerk erlaubt wird. In einer idealen Welt authentifiziert sich das Gerät über 802.1x. Bei der Authentifizierung wird ein Datensatz erzeugt, der an eine Firewall übermittelt werden kann.
- Wenn das Gerät 802.1x nicht unterstützt, ist die Authentifizierung über die **MAC-Adresse** eine Option. Eine MAC-Adresse ist eine Art digitaler Ausweis für jedes Gerät in einem Netzwerk. Sie ist einzigartig, identifiziert jedes Gerät und ermöglicht deren Kommunikation untereinander, ähnlich einem Namensschild für Ihren Computer oder Ihr Telefon.
- ALE unterstützt **Fingerprinting für Geräte und Systeme**. Wird bei der 802.1X- oder MAC-Authentifizierung kein Profil zurückgegeben, wird Fingerprinting versucht. Unter Fingerprinting versteht man im Bereich der Computersicherheit, dass Informationen über ein Gerät oder System gesammelt werden, z. B. Betriebssystem, Software und offene Ports. Anhand dieser wird es identifiziert und kategorisiert und potenzielle Risiken und Schwachstellen werden bewertet. Auch kann darüber ein Profil eines in der IoT-Datenbank registrierten Geräts zugeordnet werden.
- ALE bietet ferner einen „Catch-all-Default“ für den Fall, dass kein Profil zurückgegeben wird. Die „Catch-all-Default“-Regel kann begrenzten Zugriff erlauben oder den Zugriff vollständig verweigern, wenn die primäre Authentifizierung fehlschlägt.

Um diese verschiedenen Arten einer Authentifizierung durchzuführen, benötigen Sie einen Ort, an dem Sie die Anmeldeinformationen von Benutzern und Geräten erstellen und verwalten. Voraussetzung ist UPAM, eine Komponente der Unified-Access-Lösung von ALE. Sie stellt zentralisierte Authentifizierungs-, Autorisierungs- und Abrechnungsdienste (AAA) für das Netzwerk bereit. Das ermöglicht Netzwerkadministratoren die Erstellung und Verwaltung von Benutzerprofilen für den Netzwerkzugriff, u. a. auf der Grundlage von Identität und Standort. UPAM kann über das Alcatel-Lucent OmniVista® Network Management System konfiguriert und verwaltet werden. So lassen sich Netzwerkzugangsrichtlinien festlegen und durchsetzen.

Reaktionsfähigkeit bei Vorfällen

Die schnelle Reaktion auf Netzwerkvorfälle ist ein Schlüsselfaktor, um Schäden an Systemen und Netzwerken auf ein Minimum zu begrenzen und Ausfallzeiten zu reduzieren, die durch Sicherheitsangriffe wie Distributed Denial of Service (DDoS) entstehen.

Minimieren Sie Risiken, maximieren Sie die Quality of Experience (QoE) und erhöhen Sie die Sicherheit – mit dem Alcatel-Lucent OmniVista Network Advisor. **OmniVista Network Advisor** ist ein KI-basiertes, intelligentes und autonomes System, das Netzwerke in Echtzeit überwacht, Warnungen ausgibt, wenn ein Problem auftritt, und Lösungen für verschiedene netzwerk- und sicherheitsrelevante Fragen, u. a. DDoS-Angriffe, vorschlägt. Es führt kontinuierlich Konfigurationsprüfungen und eine Analyse der Netzwerkleistung durch, so dass potenzielle Probleme sofort **erkannt** und **entschärft** werden können und das Netzwerk mit minimalem oder ganz ohne Eingriff der IT **optimierbar** ist.

Partnerschaften und Integration

Ein wichtiger Aspekt der Authentifizierung ist die Integration mit Firewalls. Durch die Integration mit Fortinet können beispielsweise Benutzer oder Geräte, die für das LAN- und/oder WLAN-Netzwerk authentifiziert sind, gleichzeitig und nahtlos auch für die Fortinet-Firewall authentifiziert werden.

Mittels Integration mit der Next Generation Firewall von Palo Alto Networks (PAN) können Benutzer oder Geräte, die im LAN- und/oder WLAN-Netzwerk authentifiziert sind, gleichzeitig und nahtlos auch für die PAN-Firewall authentifiziert werden.

Unsere Partnerschaft mit Versa Networks ermöglicht einen sicheren Zugriff auf kritische Ressourcen, unabhängig vom Standort der Benutzer, von Daten, Anwendungen oder Geräten. Dies hat besondere Vorteile im Fall regionaler Niederlassungen oder Zweigstellen, die per remote mit der Firmenzentrale oder dem Rechenzentrum verbunden sind. Im Gegensatz zu herkömmlichen Wide Area Networks (WAN), die mehrere Netzübergänge erfordern und ggf. zusätzliche Kosten verursachen, bieten SASE und SD-WAN eine kostengünstige und sichere Lösung für das Client-to-Cloud-Zeitalter. Diese beiden Lösungen zu kombinieren, vereinfacht die IT-Infrastruktur im Unternehmen und schafft, für ortsunabhängiges Arbeiten, einen sicheren Zugang zum Internet und zu Geschäftsanwendungen, z. B. für regionale Niederlassungen oder Mitarbeiter, die von zu Hause oder unterwegs arbeiten.

Das Angebot ALE-Versa Titan ist eine umfassende Lösung, die Secure Access Service Edge (SASE) mit SD-WAN-Services aus der Cloud kombiniert. Dazu gehören das Versa Titan SD-WAN, das cloudbasiertes SD-WAN für eine schlanke IT bietet, sowie Versa Secure Access (VSA) mit NextGen Firewall-Fähigkeit und Geoblocking sowie Zero Trust Network Access (ZTNA) für Work From Anywhere. Auch ermöglicht das Versa Secure Web Gateway (SWG) sicheres Webbrowsing und den Zugriff auf Anwendungen über das Internet (SaaS) für eine sichere Remote-/Homeoffice-Verbindung. Das Versa Titan-Webportal und die App bieten integrierte Netzwerk- und Sicherheitsdienste auf einer einzigen Plattform, wobei alle SASE-Komponenten vom selben Anbieter bereitgestellt werden. Ein einziges Richtlinien-Repository, das Netzwerk- und Sicherheitsrichtlinien umfasst, vereinfacht das IT-Management und bietet die Möglichkeit eines sicheren Zugriffs auf wichtige Ressourcen.

Zero-Trust-Methode

Für ein Zero-Trust-Modell muss ein Unternehmen zunächst die Probleme in seiner Bestandsinfrastruktur erkennen, z. B. inkonsistente Richtlinien, implizites Vertrauen und anfällige IoT-Geräte. Hierbei helfen rollenbasierte Netzwerkzugangskontrollen, Segmentierung und Überwachung. Durch eine angemessene Segmentierung werden sensible Ressourcen aufgeteilt und der Zugang auf die Personen beschränkt, die ihn benötigen. Über Überwachungs- und Quarantänefunktionen werden potenzielle Bedrohungen identifiziert und isoliert.

Eine einfache, aber wirkungsvolle Methode zum Aufbau eines Zero-Trust-Netzwerks mit ALE-Lösungen umfasst mehrere Stufen.

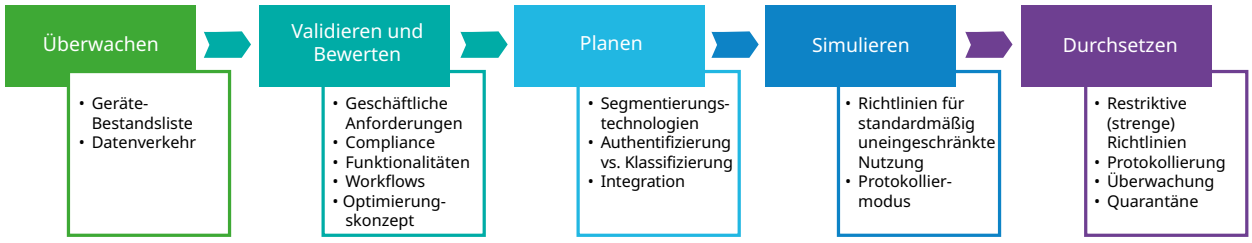
- **Überwachung**: Es sollte eine Überwachung geben, u. a. der Geräte-Bestandsliste und des Datenverkehrs.
- **Validierung und Bewertung**: Zur Validierung und Bewertung gehört die Analyse geschäftlicher Anforderungen, der Compliance-Vorgaben, Funktionalitäten und Workflows.
- **Planung**: Auf Grundlage der Ergebnisse der Bewertung sollte ein Optimierungskonzept erstellt werden. Das Konzept umfasst die Auswahl geeigneter Segmentierungstechnologie und Richtlinien sowie die Frage der Authentifizierung oder Klassifizierung und die Integration.
- **Simulation**: In der Simulationsphase sehen die Richtlinien standardmäßig eine uneingeschränkte Nutzung vor und sind im Protokolliermodus. Dabei werden andere Funktionen getestet.
- **Durchsetzung**: Die Durchsetzungsphase umfasst die Implementierung restriktiver Richtlinien, die Protokollierung, die Überwachung sowie Qzarantänemaßnahmen.

Gesamtbetriebskosten

Die Gesamtbetriebskosten (TCO) umfassen alle Kosten, die mit dem Besitz und Betrieb eines Produkts oder einer Dienstleistung über die gesamte Lebensdauer verbunden sind. Dazu gehören u. a. Kaufpreis, Wartung, Support und Upgrades. Entscheidend ist eine kosteneffiziente Lösung, die langfristigen Wert bietet. Das hält die Kosten im Rahmen und sorgt für eine passgenauere Kapitalrendite (ROI).

Zu unterscheiden ist zwischen der anfänglichen Kapitalinvestition und den laufenden Kosten, die für die Lizenzierung und den Betrieb des Systems anfallen. Einige Komponenten, wie z. B. Firewalls, haben einen rein sicherheitsorientierten Zweck. Aber auch andere Elemente sind für den Aufbau einer umfassenderen Sicherheitsstrategie entscheidend. Dazu gehören das Management der Richtlinien, eine effiziente Technologie der Netzwerkseparierung (erweiterte und automatisierte Makro- und Mikrosegmentierung), die automatische Zuweisung virtueller Netze (VLAN), ein Netzwerkverschlüsselungsprotokoll, die Sichtbarkeit von Anwendungen sowie die unabhängige Validierung und Bestätigung des Betriebssystemcodes.

Die Netzwerk-Cybersicherheitsstrategie von ALE schließt die oben genannten Kernelemente der Netzwerksicherheit kostenlos mit ein. Die Alternativen anderer Anbieter hingegen erfordern spezielle Expertise und zahlreiche teure Komponenten und Lizenzen für Betrieb und Wartung. Der Ansatz von ALE bietet Kunden erhebliche wirtschaftliche Vorteile und gewährleistet gleichzeitig eine starke und effiziente Cybersicherheit des Netzwerks.



Lösung im Überblick
Aufbau eines kosteneffizienten Zero-Trust-Netzwerks

Fazit

Es liegt auf der Hand, dass die Implementierung eines Zero-Trust-Netzwerks für eine hohe Sicherheit seine Herausforderungen hat, wie z. B. die mit der Erstellung und Wartung verbundene Komplexität und die Kosten. ALE bietet hier einen einzigartigen, kosteneffizienten Ansatz. Modernste Makro- und Mikrosegmentierungstechnologien sind, neben den übrigen hier genannten Elementen, ein einfacher und erschwinglicher Weg zur Einrichtung eines Zero-Trust-Netzwerks, das den heutigen Anforderungen im Bereich der Cybersicherheit entspricht. Es ist uns ein Anliegen, unsere Kunden dabei zu unterstützen, ihre Cybersicherheitsrisiken zu beherrschen. Wir sind überzeugt, dass unser Ansatz dazu beitragen kann.

Zu den Lösungen von ALE gehören unser resilientes und sicheres intelligent Fabric (iFab) und UNP sowie das robuste Network Access Control (NAC) mit UPAM, das eine profilbasierte Zugriffskontrolle ermöglicht. Unsere innovative Lösung OmniVista Network Advisor sorgt für einen reibungslosen Betrieb und schnelle Wiederherstellung und verhindert Angriffe. Darüber hinaus arbeiten wir mit SASE-Anbietern wie Versa Networks zusammen und integrieren Firewall-Anbieter wie Palo Alto Networks. So sind wir in der Lage, unseren Kunden umfassende und integrierte Sicherheitslösungen anzubieten.

Alcatel·Lucent Enterprise