Schützen und stärken Sie Ihr Geschäft mit Alcatel-Lucent Enterprise

Bewältigung der zunehmenden Komplexität von Cyberbedrohungen und der sich verändernden rechtlichen Anforderungen

Broschüre

Alcatel·Lucent
Enterprise

Einführung

Während Unternehmen große Veränderungen in ihrem Geschäft durchlaufen, ist die Sicherheit ein Schlüsselbereich, der auf den Kopf gestellt wird. Der Aufstieg der KI-Technologien hat traditionelle Sicherheitsmodelle auf den Kopf gestellt und ein Umdenken langjähriger Praktiken erzwungen.

Als Antwort darauf hat sich unser Team von Cybersecurity-Experten für Netzwerk-, Kommunikations- und Cloud-Lösungen zusammengetan, um wichtige Erkenntnisse über die neuen Risiken zu vermitteln, denen sich Unternehmen gegenübersehen, und darüber, wie sie wichtige Schutzschichten hinzufügen können, um die Nase vorne zu haben.

Die sich verändernde Landschaft der Cybersicherheit

Das Umfeld der Cybersicherheit ist geprägt von einer raschen technologischen Entwicklung, immer raffinierteren Bedrohungen und sich ändernden Vorschriften. Branchenexperten heben drei wichtige Trends hervor, die die Cybersicherheit in Unternehmen derzeit prägen:

1. Die zweischneidige Rolle der künstlichen Intelligenz
2. Der kontinuierliche Anstieg von Ransomware und Angriffen auf die Lieferkette
3. Die Notwendigkeit eines robusten Identitätsmanagements in Zero-Trust-Architekturen

Die zweischneidige Rolle der KI bei der Cybersicherheit

KI als Waffe für Angreifer

Die böswillige Nutzung künstlicher Intelligenz hat sich als eine der größten Bedrohungen für die Unternehmenssicherheit herausgestellt. Cyberkriminelle nutzen KI, um die Aufklärung zu automatisieren, hyperpersonalisierte Phishing-Kampagnen zu erstellen und anpassungsfähige Malware zu entwickeln, die herkömmliche Erkennungssysteme umgehen kann.

KI-gestützte Tools analysieren öffentlich verfügbare Daten, um Profile von Zielpersonen zu erstellen, überzeugende Audio- und Videofälschungen zu erzeugen und Schwachstellen mit chirurgischer Präzision auszunutzen.
Ein bemerkenswertes Beispiel sind KI-generierte Phishing-E-Mails, die einen legitimen Kommunikationsstil imitieren und die Erfolgsquote im Vergleich zu herkömmlichen Methoden um 40 % erhöhen. Diese Angriffe werden durch die Kommerzialisierung von KI-Tools noch verstärkt, die die Einstiegshürde für weniger qualifizierte Angreifer senkt.

Die Deepfake-Technologie stellt eine besonders heimtückische Anwendung von KI dar, die es Bedrohungsakteuren ermöglicht, sich in Echtzeit-Videogesprächen als Führungskräfte oder vertrauenswürdige Kollegen auszugeben, um betrügerische Transaktionen zu autorisieren oder sensible Informationen weiterzugeben. In einem dokumentierten Fall führte ein gefälschtes Video eines Finanzchefs, der eine Überweisung anweist, zu einem Verlust von 25 Millionen Dollar für ein multinationales Unternehmen. Solche Vorfälle unterstreichen den Bedarf an fortschrittlichen Authentifizierungsprotokollen und Mitarbeiterschulungen zur Erkennung synthetischer Medien.

KI als Abwehrmechanismus

Paradoxerweise dient die KI auch als Rückgrat der modernen Cybersicherheitsabwehr. Algorithmen für maschinelles Lernen analysieren riesige Datensätze, um Anomalien zu erkennen, Angriffsvektoren vorherzusagen und die Reaktion auf Vorfälle zu automatisieren. KI-gestützte Sicherheitssysteme können beispielsweise Zero-Day-Schwachstellen durch die Erkennung von subtilen Verhaltensmustern im Netzwerkverkehr identifizieren und so die durchschnittliche Erkennungszeit von Wochen auf Stunden reduzieren. Laut Gartner erleben Unternehmen, die in KI-gesteuerte Bedrohungsintelligenz-Plattformen investieren, 30 Prozent weniger erfolgreiche Angriffe als Unternehmen, die sich auf Altsysteme verlassen[1]. KI-gesteuerte Systeme sind besonders effektiv bei der Identifizierung von Insider-Bedrohungen, indem sie das Benutzerverhalten überwachen und ungewöhnliche Zugriffsmuster aufzeigen, was in den heutigen Remote- und Hybrid-Arbeitsumgebungen immer wichtiger wird.

Regulatorische und ethische Herausforderungen

Der doppelte Verwendungszweck von KI hat zu strengen rechtlichen Maßnahmen geführt. Das im Februar 2025 in Kraft getretene EU-KI-Gesetz verbietet risikoreiche KI-Anwendungen in Bereichen wie der biometrischen Überwachung und schreibt Transparenz bei algorithmischen Entscheidungen vor. Unternehmen müssen nun Audits von KI-Systemen durch Dritte durchführen, die Datenherkunft dokumentieren und eine ethische Nutzung sicherstellen - ein komplexes Unterfangen angesichts der Undurchsichtigkeit vieler maschineller Lernmodelle. Unternehmen richten funktionsübergreifende KI-Ethikausschüsse ein, um sich in diesem Umfeld zurechtzufinden, und arbeiten mit Regulierungsbehörden zusammen, um künftige Rahmenbedingungen zu gestalten.

Eskalation von Ransomware und Angriffen auf die Lieferkette

Kritische Lieferanten ins Visier nehmen

Ransomware-Angriffe haben sich von opportunistischen Kampagnen zu strategischen Operationen entwickelt, die auf wichtige Lieferanten und Dienstleister abzielen. Die Angriffe auf CDK Global und Change Healthcare im Jahr 2024 haben gezeigt, wie die Kompromittierung eines einzelnen Anbieters ganze Branchen lahmlegen kann, was zu Betriebsunterbrechungen und Wiederherstellungsmaßnahmen in Milliardenhöhe führt. Heute konzentrieren sich Angreifer zunehmend auf Software-as-a-Service (SaaS)-Anbieter und Cloud-Infrastrukturfirmen und nutzen deren zentrale Rolle in Unternehmensökosystemen aus. So könnte beispielsweise ein Ransomware-Angriff auf einen großen Cloud-Speicheranbieter Tausende von Unternehmen gleichzeitig von ihren Daten ausschließen, was die Erpressungsmöglichkeiten vergrößert.

Die Ausbreitung vernetzter Systeme und ein unzureichendes Risikomanagement in der Lieferkette erleichtern diese Angriffe. Viele Unternehmen haben keinen Einblick in die Sicherheitsvorkehrungen ihrer Anbieter, wodurch sie anfällig für kaskadenartige Ausfälle sind. Gartner berichtet, dass 60 Prozent der Unternehmen bis 2026 mit einer erheblichen Verletzung der Lieferkette konfrontiert sein werden, die durch Schwachstellen von Drittanbietern in DevOps-Pipelines und IoT-Geräteflotten verursacht wird[1].

Ransomware-as-a-Service (RaaS)-Ökosysteme

Das Aufkommen von Ransomware-as-a-Service-Plattformen hat den Zugang zu fortschrittlichen Angriffswerkzeugen demokratisiert und ermöglicht es auch weniger qualifizierten Kriminellen, ausgefeilte Kampagnen zu starten. RaaS-Betreiber bieten anpassbare Malware, Zahlungsportale und Verhandlungsunterstützung im Austausch für einen Anteil am Lösegeld - typischerweise 20 bis 30 Prozent. Dieses Modell hat zu einem 150-prozentigen Anstieg der Ransomware-Vorfälle seit 2023 geführt, wobei die durchschnittlichen Lösegeldforderungen 5 Millionen Dollar pro Vorfall übersteigen.

Moderne Ransomware nutzt KI-gesteuerte Verschleierungstechniken wie polymorphen Code und zeitverzögerte Verschlüsselung, um der Erkennung zu entgehen. Angreifer exfiltrieren auch Daten, bevor sie die Verschlüsselung einsetzen, und drohen damit, sensible Informationen preiszugeben, wenn sie nicht bezahlt werden - eine Taktik, die als doppelte Erpressung bekannt ist. Unternehmen begegnen diesen Bedrohungen mit Air-Gapped-Backups, dezentralen Speicherlösungen und Blockchain-basierten Integritätsprüfungssystemen.

Unternehmen benötigen durchgängig sichere Technologien, um die Auswirkungen von Ransomware und Angriffen auf die Lieferkette zu verhindern, einzudämmen und zu begrenzen.

1. https://www.gartner.com/en/newsroom/press-releases/2025-03-03-gartner-identifiesthe-top-cybersecurity-trends-for-2025
2. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Identitätsmanagement und das Gebot der Vertrauensfreiheit

Die Krise der Maschinenidentität

Da Unternehmen generative KI, IoT und Cloud-native Architekturen einführen, haben maschinelle Identitäten - Anmeldeinformationen für Geräte, APIs und automatisierte Arbeitslasten - menschliche Identitäten in Bezug auf Umfang und Risiko überholt. Im Jahr 2025 identifizierte Gartner nicht verwaltete Maschinenidentitäten als einen der wichtigsten Angriffsvektoren im Jahr 2025, wobei kompromittierte API-Schlüssel und Dienstkonten 45 Prozent der Cloud-Verletzungen ermöglichen[1]. Um diesem Problem zu begegnen, setzen Unternehmen zunehmend Tools zur Zertifikatsverwaltung ein, die eine häufigere Rotation der Berechtigungsnachweise automatisieren und ihre Least Privilege Policies stärken, um abnormales Maschinenverhalten in Echtzeit zu erkennen.

Zero-Trust-Architekturen in der Praxis

Zero-Trust-Konzepte, die davon ausgehen, dass keine menschliche oder maschinelle Entität von Natur aus vertrauenswürdig ist, haben sich von einem erstrebenswerten Ziel zu einer operativen Notwendigkeit entwickelt. Die Implementierung konzentriert sich auf kontinuierliche Authentifizierung, Mikro-Segmentierung und verschlüsselte Kommunikation. Ein Zero-Trust-Netz könnte beispielsweise eine biometrische Verifizierung für den Zugang zu sensiblen Daten verlangen, Entwicklungsumgebungen von Produktionssystemen isolieren und den gesamten Ost-West-Verkehr innerhalb von Rechenzentren verschlüsseln.

Das U.S. National Institute of Standards and Technology (NIST) in einer Bewertung der Wirksamkeit, dass Unternehmen, die Zero Trust Architektur[2], die Auswirkungen von Sicherheitsverletzungen im Durchschnitt um 70 Prozent reduzieren. Der Erfolg hängt von der Integration der Zero-Trust-Prinzipien in die bestehende Infrastruktur ab - eine Herausforderung für Unternehmen mit Altsystemen. Hybride Ansätze sind auf dem Vormarsch, wie z.B. softwaredefinierte Perimeter für On-Premises-Anlagen und Cloud-native Zero-Trust-Lösungen.

Menschliche Faktoren und Insider-Bedrohungen

Nach Angaben des Weltwirtschaftsforums sind 95 Prozent der Vorfälle im Bereich der Cybersicherheit auf menschliches Versagen zurückzuführen. Phishing-Angriffe, die KI-generierte Inhalte nutzen, umgehen E-Mail-Filter 30 Prozent effektiver als herkömmliche Methoden, während 25 Prozent der Sicherheitsverstöße auf Mitarbeiter zurückzuführen sind, die versehentlich Anmeldedaten in kollaborativen Tools preisgeben. Insider-Bedrohungen werden durch manuelle Fehler bei der Konfiguration des Netzwerkzugangs und durch Remote-Arbeiten verschärft, bei denen persönliche Geräte und ungesicherte Netzwerke Einstiegspunkte für Angreifer darstellen.

Es ist unabdingbar geworden, den Nutzern zu helfen, sich besser zu schützen und gleichzeitig die Belastung durch zunehmend restriktive Sicherheitsrichtlinien zu verringern. Für Netzwerk- und Anwendungsadministratoren müssen die Automatisierung des Betriebs und die aktive Unterstützung durch KI die notwendigen Werkzeuge bereitstellen, um sich vor den Folgen möglicher Fehlkonfigurationen zu schützen.

Der ALE-Ansatz zur Sicherung von Kommunikations- und Netzwerkprodukten

Der Sicherheitsansatz von Alcatel-Lucent Enterprise besteht darin, zu gewährleisten, dass digitale Interaktionen effektiv sind und Branchenstandards und -regeln eingehalten werden. Die digitale Technologie ist weit verbreitet und wird zunehmend von KI und IoT-Geräten genutzt, die Daten sammeln, um Echtzeit-Alarme und Zukunftsplanungen zu unterstützen. Die Sicherung und Stärkung der Netze und der Kommunikation, die die heutigen Unternehmen antreiben, ist von entscheidender Bedeutung für die Vermeidung von Serviceunterbrechungen. ALE-Lösungen für die Unternehmenskommunikation und die Netzwerkinfrastruktur implementieren Cybersicherheit von Anfang bis Ende, denn nur so kann eine umfassende Sicherheit gewährleistet werden. Dieser Ansatz zur Cybersicherheit hilft Unternehmen und öffentlichen Einrichtungen bei:

- der Verhinderung von Cyberangriffen durch die Implementierung von Cybersicherheit in jedem Aspekt der Produktentwicklung, um die Angriffsfläche zu verringern
- dem Schutz vor Cyberangriffen durch Implementierung der neuesten Sicherheitsstandards und bewährten Verfahren in allen Lösungskomponenten zur Erhöhung der Widerstandsfähigkeit
- der Reaktion auf Cyberangriffe durch rasche und angemessene Maßnahmen zur Begrenzung der Auswirkungen und zur Verbesserung der Widerstandsfähigkeit, falls ein Angriff erfolgt

Als Hersteller von hardware- und softwarebasierten Produkten konzentriert sich der Cybersicherheitsansatz von ALE auf die unten beschriebenen Bereiche, um potenzielle Schwachstellen in der Cyber-Bedrohungslandschaft anzugehen.

1. Sicher durch Design

In der Vergangenheit waren die meisten Lösungsdesigns von der Notwendigkeit neuer Funktionen bestimmt, und die Sicherheit war ein wesentlicher, aber zweitrangiger Aspekt. Mit dem Wandel der Landschaft haben sich die traditionellen Prioritäten für die Gestaltung umgekehrt. Die Anforderungen an die Cybersicherheit müssen nun die Lösungskonzepte bestimmen. Bei Hardware- und Softwarelösungen, die sicher konzipiert sind, wird die Sicherheit bei jedem Schritt der Produktdefinition, -entwicklung und -bereitstellung berücksichtigt. Die gesamte Hardware und die Betriebssysteme sind gehärtet, der Schutz vor Denial of Service (DoS) ist integriert, und die Lösungen implementieren die für die Branche wichtigsten Best Practices im Bereich der Cybersicherheit.

2. Zero-Trust-Netzwerkzugriffssicherheit

Sicherheitsstrategien, die Vertrauen auf der Grundlage des Standorts eines Benutzers innerhalb der Unternehmensfirewall, den von ihm eingegebenen Anmeldeinformationen oder der von ihm verwendeten Anwendung oder dem von ihm verwendeten Gerät schaffen, sind selbst bei Kombination mehrerer Sicherheitsmechanismen nicht mehr ausreichend. Heute sollte kein Nutzer, kein Gerät und keine Anwendung automatisch Vertrauen genießen. Das Sicherheitsmodell Zero Trust Network Access (ZTNA) hilft Unternehmen dabei, sich ständig weiterentwickelnden Bedrohungen wirksam entgegenzuwirken. ZTNA vertraut keinem Nutzer, Gerät oder einer Anwendung, unabhängig vom Standort. ALE erzwingt ZTNA durch rollenbasierte Richtliniendurchsetzung, standortbezogene Zugriffskontrolle und dynamische Segmentierung über Benutzer, Geräte und Anwendungen hinweg - unabhängig davon, ob sie verwaltet oder nicht verwaltet werden.

3. Makro- und Mikro-Segmentierung

Makro- und Mikrosegmentierung ermöglichen einen granularen und hochkontrollierten Ansatz zur Cybersicherheit für alle Benutzer, Geräte und Anwendungen, die auf das Netzwerk zugreifen. Die Makrosegmentierung trennt Benutzer, Geräte und Anwendungen entsprechend ihrem Funktionsbereich, so dass sie nicht mit den Elementen in anderen Makrosegmenten kommunizieren können. So können beispielsweise die Unified-Communications- und Collaboration-Anwendungen in einem Makrosegment nicht mit den Sicherheitstechnologien wie Überwachungskameras und Türschließsystemen in einem zweiten Makrosegment oder den Sensoren und Steuerungen für Beleuchtung, Heizung und Klimaanlage in einem dritten Makrosegment kommunizieren.

Die Mikrosegmentierung legt fest, wie die Nutzer, Geräte und Anwendungen innerhalb eines Makrosegments miteinander interagieren können. Sie wird üblicherweise durch sehr spezifische Sicherheitsrichtlinien geregelt. Zum Beispiel sollte eine Überwachungskamera nicht mit einer Türverriegelung interagieren dürfen, obwohl sie sich im selben sicherheitsrelevanten Makrosegment befinden.

4. Ende-zu-Ende-Verschlüsselung

Mitarbeiter, Kunden, Partner und Lieferanten können sich in modernen Organisationen überall befinden. Und die Lösungen, die sie zur Kommunikation und Zusammenarbeit verwenden, können in dem Gebäude installiert sein, in dem sie arbeiten, am anderen Ende der Stadt oder in einem Rechenzentrum am anderen Ende der Welt. In jedem Fall müssen die Menschen in der Lage sein, auf sichere und vertrauliche Weise Informationen per Sprache, Video und Text auszutauschen. Um sicherzustellen, dass nur die Gesprächsteilnehmer auf die ausgetauschten Informationen zugreifen können, muss jedes Gespräch vom Ursprung bis zum Ziel vollständig verschlüsselt sein. Das bedeutet, dass jedes an der Ende-zu-Ende-Kommunikation beteiligte Hardware- und Softwareelement über von Sicherheitsbehörden genehmigte, integrierte Verschlüsselungsmechanismen verfügen muss.

5. Sicherheits- und Datenschutzzertifizierungen und Einhaltung von Vorschriften

Vor einigen Jahren waren die strengsten Sicherheitszertifizierungen und -akkreditierungen nur für Sicherheitsprodukte wie Firewalls oder Branchen wie die Verteidigung erforderlich. Heutzutage müssen sicherheitsspezifische Normen auf alle Technologieprodukte aller Branchen angewendet werden. Die Überprüfung, ob anerkannte Zertifizierungen und Akkreditierungen die Behauptungen zur Cybersicherheit untermauern, ist von entscheidender Bedeutung.

Hier sind einige Beispiele für Vorschriften, auf deren Einhaltung Sie achten sollten:

- Globale Sicherheits- und Datenschutzstandards, wie ISO 27001
- Branchenspezifische Sicherheits- und Datenschutzstandards, wie der Health Insurance Portability and Accountability Act (HIPAA) in den USA und Hébergeurs de Données de Santé (HDS) für das Hosting von Gesundheitsdaten in Frankreich
- Regionale Sicherheits- und Datenschutzbestimmungen, wie die Datenschutz-Grundverordnung (DSGVO) und die NIS-2-Richtlinie in der Europäischen Union

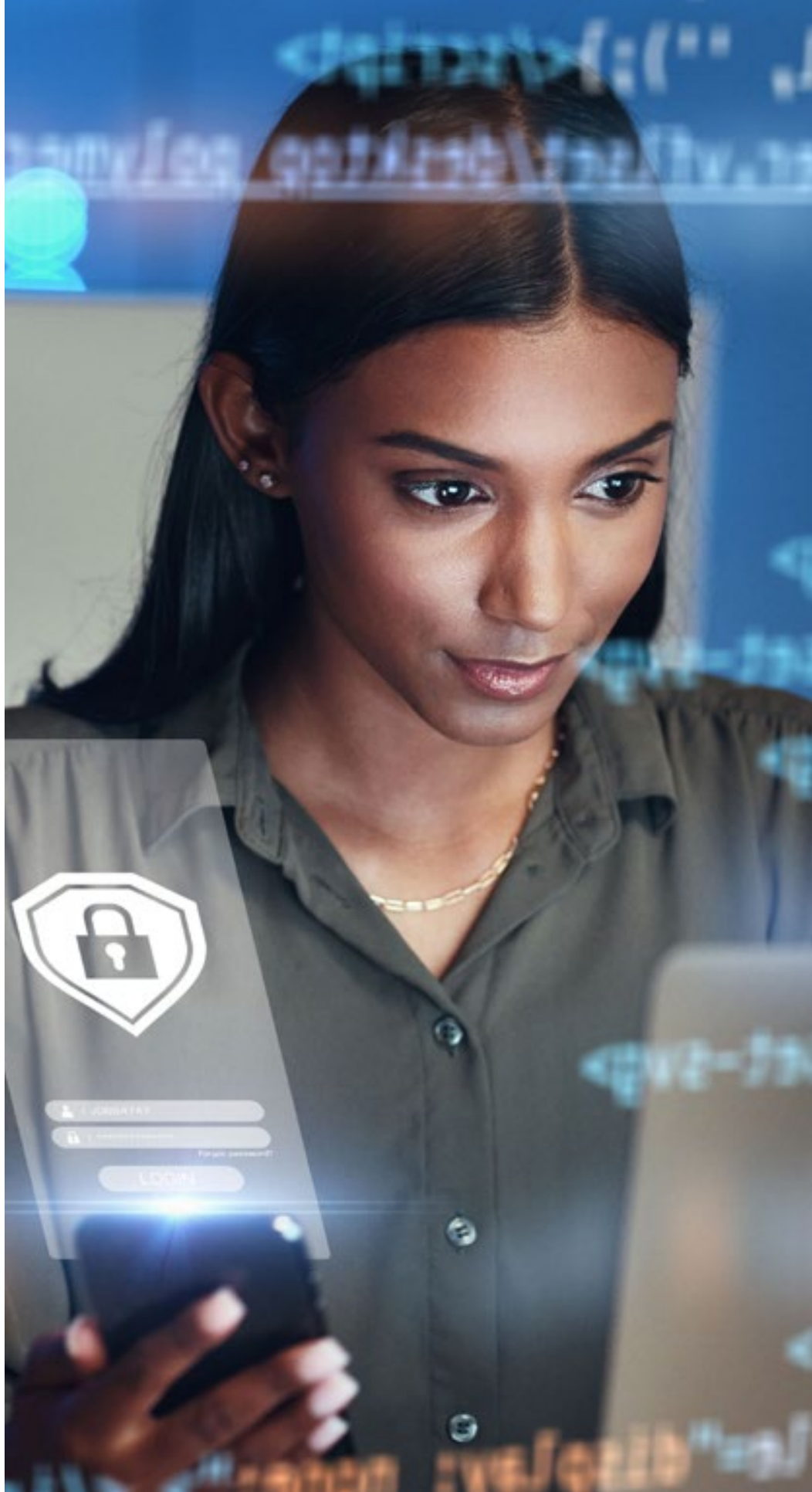
6. Kontinuierliche, spezialisierte Sicherheitstests

Ebenso wie Sicherheitsstandards sind auch spezielle Sicherheitstestprozesse, die früher Sicherheitsprodukten vorbehalten waren, heute für Unified Communications- und Collaboration-Lösungen obligatorisch. Penetrationstests sind ein gutes Beispiel dafür. Bei diesen Tests werden Cyberangriffe simuliert, um Sicherheitsschwachstellen aufzudecken, damit sie proaktiv behoben werden können, bevor Probleme auftreten. Um Cyberbedrohungen in einer sich ständig weiterentwickelnden Landschaft immer einen Schritt voraus zu sein, müssen kontinuierlich Penetrationstests durchgeführt werden, die ausschließlich auf den Anforderungen der Cybersicherheit basieren. Technologieanbieter, die ihre Kunden bei der Aufrechterhaltung eines Höchstmaßes an Cybersicherheit unterstützen wollen, müssen die Ressourcen, Tools und Fachkenntnisse bereitstellen, die für die Durchführung kontinuierlicher Penetrationstests erforderlich sind.

7. Datensouveränität

Die Datensouveränität ist für die meisten Unternehmen, die ihr geistiges Eigentum schützen, das Vertrauen ihrer Kunden erhalten und sich einen Wettbewerbsvorteil sichern müssen, zu einem wichtigen Anliegen geworden. Mit der Einführung neuer Technologien wie der Cloud und in jüngster Zeit auch der künstlichen Intelligenz ist die Offenheit der Kommunikationssysteme von Unternehmen gegenüber der Außenwelt wichtiger denn je, und die Sicherheit des Netzwerkzugangs ist ebenso unerlässlich. Einige Unternehmen entscheiden sich für eine öffentliche Cloud-Lösung, die ihre Anforderungen erfüllt und gleichzeitig die interne Angriffsfläche ihres Informationssystems einschränkt. Andere werden sich für einen traditionelleren Ansatz entscheiden, bei dem Unified Communications-Anwendungen in ihrem privaten Netzwerk gehostet werden, entweder vor Ort oder in einer speziellen privaten Cloud. Unabhängig von der Entscheidung des Kunden kann ALE seine Produkte und Dienstleistungen in allen Einsatzbereichen anbieten, um die Souveränität über kritische Daten zu gewährleisten.

Broschüre
Schützen und stärken Sie Ihr Geschäft mit Alcatel-Lucent Enterprise



8. Intelligente Betriebs- und Sicherheitsautomatisierung

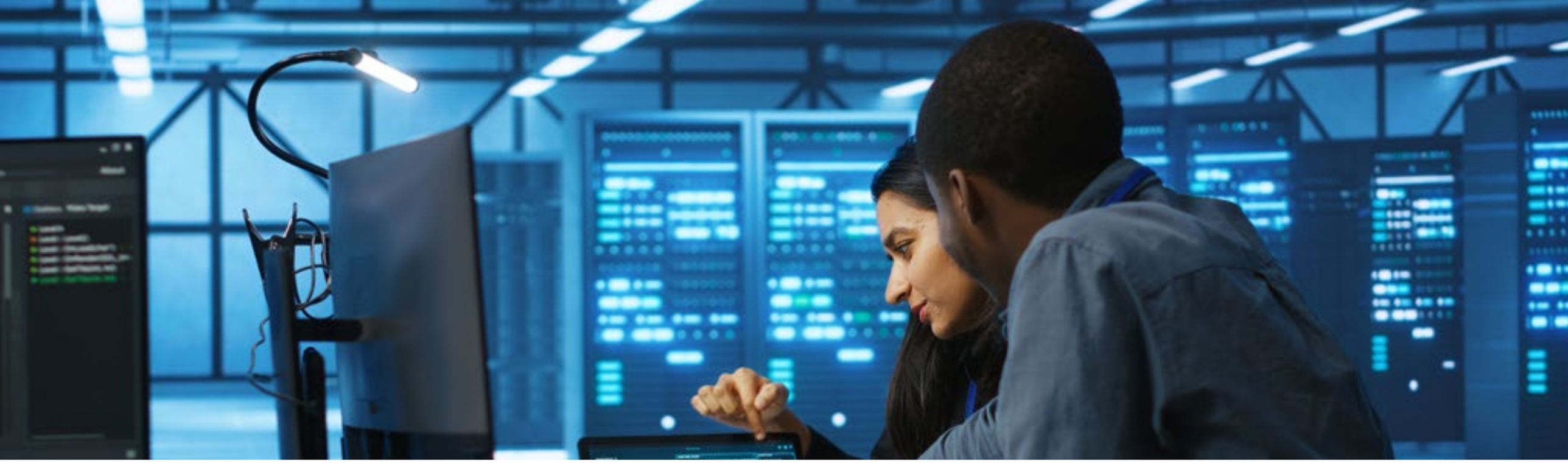
Die OmniVista-Suite und Network Advisor von Alcatel-Lucent Enterprise bieten fortschrittliche betriebliche Sicherheit durch Echtzeitüberwachung, Konfigurationsprüfungen und Automatisierung der Reaktion auf Bedrohungen. Mit eingebettetem AIOps werden Netzwerkanomalien proaktiv erkannt und geführte Abhilfemaßnahmen bereitgestellt, die oft nur einen einzigen Mausklick zur Lösung von QoE- oder Compliance-Problemen erfordern. Dies reduziert menschliche Fehler, beschleunigt die Reaktion auf Vorfälle und gewährleistet die Einhaltung von Richtlinien in komplexen Umgebungen.

9. Sichere Konnektivität überall

ALE unterstützt sicheres SD-WAN für verteilte Unternehmen und Remote-Arbeiten, indem es Netzwerktransparenz, Sicherheit und Leistungsoptimierung kombiniert und sich an moderne Work-from-anywhere-Modelle anpasst. Mit der MACsec-Verschlüsselung werden die Datenintegrität und die Vertraulichkeit in WAN-Umgebungen mit mehreren Standorten gewahrt.

10. Vertrauenswürdige Software-Lieferkette

ALE wendet strenge Maßnahmen zur Sicherung seiner Software-Lieferkette an, darunter signierte Firmware-Images, sichere Boot-Prozesse, gehärtete Betriebssysteme und unabhängige Quellcode-Validierung. Diese Praktiken begrenzen die Anfälligkeit für softwarebasierte Bedrohungen und sorgen für vertrauenswürdige Bereitstellungsumgebungen.



Warum ALE Ihr vertrauenswürdiger Lieferant für die Sicherung Ihrer Netzwerkinfrastruktur und Geschäftskommunikationsplattform ist

Während viele Technologieanbieter Wert auf Cybersicherheit legen, verfügen nicht alle über das umfassende Fachwissen, um Ende-zu-Ende-Sicherheit zu implementieren. Alcatel-Lucent Enterprise geht über andere Anbieter hinaus und implementiert alle erforderlichen Best Practices für eine durchgängige Cybersicherheit.

Wir sind dazu verpflichtet:

- die Best Practices und Empfehlungen des National Institute of Science and Technology (NIST) bei der Durchführung von Risikobewertungen für neue Funktionen und bei der Implementierung von Cybersicherheitsfunktionen, wie z. B. nativer Verschlüsselung, in unsere Lösungen zu befolgen
- ISO 27001-Normen für alle unsere Lösungen anzulegen
- ZTNA, granulare Netzwerksegmentierung und konkrete Sicherheitsrichtlinien zur Verringerung des Risikos nicht autorisierter Aktivitäten zu unterstützen
- für alle unsere Produkte hochspezialisierte, sicherheitsspezifische Tests durchzuführen, wie z. B. Penetrationstests
- sicherzustellen, dass unsere Produkte wichtige Branchenzertifizierungen wie HDS, HIPAA und den Family Educational Rights and Privacy Act (FERPA) und FIPS 140-2 für Regierung und Verteidigung erfüllen
- regionale Zertifizierungen für unsere Produkte zu berücksichtigen, wie CSPN von ANSSI in Frankreich, ENS in Spanien, C5 in Deutschland und ANATEL in Brasilien
- regionale Sicherheits- und Datenschutzvorschriften einzuhalten, wie GDPR, CRA und NIS-2-Richtlinie in der Europäischen Union

Als anerkannte Experten für Cybersicherheit erarbeiten wir Vorschläge für die Cybersicherheitsrichtlinien der Europäische Union. Darüber hinaus nutzen wir unser Fachwissen, um unseren Kunden bei der Auswahl und Implementierung mit den niedrigsten Gesamtbetriebskosten (30–50 % Ersparnis) der richtigen Mischung sicherer Netzwerk- und Kommunikationslösungen für ihre Anforderungen zu helfen und ihre Mitarbeiter in Best Practices zur Cybersicherheit zu schulen. Unser ganzheitlicher Ansatz für eine Zero-Trust-Architektur ermöglicht es unseren Kunden, ihren Versicherern zu zeigen, dass sie einen proaktiven Ansatz verfolgen, und in der Regel von einem Rabatt von bis zu 20–30 % auf ihre Cybersicherheitsversicherung zu profitieren.

Broschüre
Schützen und stärken Sie Ihr Geschäft mit Alcatel-Lucent Enterprise

Fazit

Die Cybersicherheitstrends des Jahres 2026 erfordern einen Paradigmenwechsel in der Unternehmensstrategie. Unternehmen müssen die Doppelrolle von KI als Bedrohung und Verteidiger in Einklang bringen, in widerstandsfähige Lieferketten investieren, um Ransomware-Angriffen zu widerstehen, und Identitätsmanagementsysteme für eine Welt ohne Vertrauen neu gestalten. Die Einhaltung gesetzlicher Vorschriften, die ethische Nutzung von KI und die branchenübergreifende Zusammenarbeit werden bei der Risikominderung von entscheidender Bedeutung sein. Da sich die Angriffsflächen mit der Einführung von Edge Computing und IoT vergrößern, sind Unternehmen, die auf eine adaptive Verteidigung, die Schulung ihrer Mitarbeiter und eine proaktive Bedrohungsjagd setzen, am besten positioniert, um in dieser unbeständigen Umgebung zu bestehen.

Der Weg in die Zukunft erfordert technologische Innovation sowie die Unterstützung und das Fachwissen eines vertrauenswürdigen Bauunternehmens wie ALE.

Weitere Informationen

Um mehr zu erfahren, besuchen Sie bitte ALE Security Solutions. Wenn Sie mit einem unserer Sicherheitsexperten sprechen möchten, kontaktieren Sie uns bitte.

Alcatel·Lucent
Enterprise