Resilienz und Sicherheit als Priorität

Alcatel-Lucent Enterprise Lösungen für den öffentlichen Sektor

Alcatel·Lucent
Enterprise

E-Book

Inhaltsverzeichnis

| Überblick

| Weshalb das Zusammenspiel zwischen IT und OT so wichtig ist

| Resiliente und sichere Netzwerklösungen

| Resiliente und sichere Kommunikationslösungen

| Schutz von Menschen und Ausrüstung

| Datenhoheit und Sicherheit

Überblick

Angesichts der zunehmenden weltweiten Herausforderungen und der vermehrten Cyberrisiken und physischen Risiken müssen die Behörden dem Risikomanagement Priorität einräumen, kritische Infrastrukturen absichern und die Bürger schützen. Laut CloudSek sind die Cyberangriffe auf Regierungsstellen im Jahr 2022 um 95 % gestiegen.[1] Gleichzeitig wird erwartet, dass der Behördenbetrieb in jeder Situation weitergeführt wird und die Bürger in Sicherheit sind. Im gegenwärtigen internationalen Klima ist es wichtiger denn je, die Datensicherheit aufrechtzuerhalten, die Datenhoheit zu schützen und die Verfügbarkeit der Dienste zu gewährleisten.

Der öffentliche Sektor und warum IKT entscheidender denn je ist

In den letzten Jahren wurde die digitale Transformation im öffentlichen Sektor mit Nachdruck vorangetrieben, und immer mehr Bürgerinnen und Bürger nehmen digitale Dienste in Anspruch. Die digitale Transformation hat es den Mitarbeitern der Verwaltung zudem ermöglicht, von überall aus zu arbeiten. Der Druck auf die Behörden, den digitalen Wandel weiter zu beschleunigen, wächst. Einem Artikel von Deloitte zufolge geben siebenundsiebzig Prozent der Regierungsbehörden an, dass die während der Pandemie ergriffenen Initiativen zur digitalen Transformation bereits positive Auswirkungen auf ihre Einrichtung haben.[2]

Alcatel-Lucent Enterprise arbeitet mit Behörden auf der ganzen Welt zusammen und ist sich der Bedeutung des Schutzes von Bürgern, Betriebsstrukturen und Gebäuden vor Cyberrisiken und physischen Risiken bewusst. Bei unseren Lösungen stehen Sicherheit und Datenschutz in jeder Phase des Entwicklungsprozesses im Mittelpunkt. Unsere Lösungen sind mit Resilienzoptionen ausgestattet, die für jede Art von Organisation und Unternehmen geeignet sind. Dieses E-Book vermittelt Ihnen einen besseren Eindruck von der Resilienz und Sicherheit Ihrer Kommunikations-, Cloud- und Netzwerklösungen von ALE.

1 Laut CloudSek haben Cyberangriffe auf Regierungsstellen im zweiten Halbjahr 2022 um 95 Prozent zugenommen. CSO Vereinigte Staaten, Januar 2023.

2 https://www2.deloitte.com/uk/en/insights/industry/public-sector/government-digital-transformation-strategy.html.

Weshalb das Zusammenspiel zwischen IT und OT so wichtig ist

Bevor wir uns damit befassen, wie Sie mit den Lösungen von Alcatel-Lucent Enterprise die Resilienz und Sicherheit verbessern können, ist es wichtig, die sich verändernde Beziehung zwischen Informationstechnologie und Betriebstechnologie zu beleuchten. In der Vergangenheit arbeiteten die IT- und die Betriebsteams nicht eng zusammen, sondern hatten jeweils ihre eigenen Funktionen und Zuständigkeiten. Diese beiden Welten verschmelzen nun zunehmend und müssen als Einheit zusammenarbeiten. IT- und Betriebsteams, die nicht über die Aktivitäten des jeweils anderen Bescheid wissen oder die sich nicht abstimmen und zusammenarbeiten, gefährden die gesamte Organisation.

Nehmen wir zum Beispiel die zahlreichen Geräte aus dem Internet der Dinge (IoT), die in vielen Regierungsbehörden und intelligenten Städten in kürzester Zeit zum Einsatz kommen. Wenn die IT-Abteilung nicht über neue IoT-Geräte informiert ist, die vom Betriebsteam implementiert werden, kann sie nicht sicherstellen, dass die Geräte den Sicherheitsrichtlinien der Behörde entsprechen. IoT-Geräte verfügen über sehr unterschiedliche Cybersicherheitsfunktionen und sind möglicherweise nicht mit den neuesten Schutzmechanismen ausgestattet. Möglicherweise sind auch ihre Funktionen noch nicht vollständig implementiert. Auf diesen unbefugten „Schatten-IT“-Geräten könnte jede beliebige Software ausgeführt werden und sie könnten bereits mit Viren und Malware infiziert sein. Wenn sie nicht kontrolliert werden, droht ganz schnell eine Gefährdung des Netzwerks durch neue Sicherheitsrisiken und Angriffsvektoren. Inzwischen arbeiten die IT- und OT-Abteilungen immer intensiver zusammen. Dies ist absolut unerlässlich, um die Sicherheit und Resilienz des Netzwerks zu gewährleisten.

E-Book
Resilienz und Sicherheit als Priorität

Resiliente und sichere Netzwerklösungen

Die Netzwerkinfrastruktur ist für das Funktionieren staatlicher Organisationen und die Bereitstellung von Diensten für die Bürger von entscheidender Bedeutung. Aufgrund des sensiblen Charakters der in staatlichen Netzwerken enthaltenen Informationen und der wichtigen Dienstleistungen der öffentlichen Verwaltung können Ausfälle oder Unterbrechungen von Netzwerkdiensten schwerwiegende Folgen haben, weshalb Resilienz und Sicherheit an oberster Stelle stehen müssen. Zuverlässige und sichere Netzwerke sind für Behörden unerlässlich, um effektive öffentliche Dienstleistungen zu erbringen, sensible Informationen zu schützen und einen reibungslosen Betrieb zu gewährleisten.

ALE Digital Age Networks sind belastbar und gehen über das hinaus, was viele andere Technologieprovider anbieten. Wir integrieren bereits in der Anfangsphase der Entwicklung von Netzwerken und Lösungen Sicherheitsfunktionen, ohne dass zusätzliche Lizenzkosten anfallen.

Sieben bewährte Verfahren für Ihre Netzwerklösungen

Nachfolgend finden Sie sieben bewährte Verfahren, die dafür sorgen, dass Sie die integrierte Resilienz und Sicherheit Ihrer Netzwerklösung von Alcatel-Lucent Enterprise optimal ausschöpfen können.

1. Überprüfen Sie gemeinsam mit Ihrem Business Partner Ihre Lösung in regelmäßigen Abständen, um sicherzustellen, dass die jeweils neueste Version der Software, Patches und Sicherheitserweiterungen installiert ist. Ein Lifecycle-Management-Tool wie ALE PALM, das Informationen über die Veralterung und Produkteinstellung liefert, ist ebenfalls hilfreich. Die Behörden können dadurch den Austausch von Hardware im Voraus planen und deren Einsatz vorbereiten.
2. ALE Secure Diversified Code wählt die Position der verschiedenen Codesegmente auf Ihren Switches nach dem Zufallsprinzip aus, was die Sicherheit enorm erhöht. Darüber hinaus unterliegt der sichere diversifizierte Code von ALE einer unabhängigen Überprüfung und Validierung (IVV), die von einem externen Cybersicherheitsexperten durchgeführt wird. Dieser analysiert und testet das ALE-Betriebssystem, um potenzielle Sicherheitsrisiken, Hintertüren, Malware oder System-Exploits in allen neuen Releases aufzuspüren und zu beseitigen.
3. Führen Sie eine Zero-Trust-Sicherheitsstrategie ein und implementieren Sie einen Zero-Trust-Netzwerkzugang. Die Makro- und Mikrosegmentierung Ihres Netzwerks ist entscheidend für die Aufrechterhaltung einer resilienten Infrastruktur. Befolgen Sie den schrittweisen Ansatz von ALE für die Mikrosegmentierung, um eine ordnungsgemäße Implementierung zu gewährleisten und störende Folgen zu vermeiden: Überwachen, Validieren, Planen, Simulieren und Durchsetzen.
4. Nutzen Sie Shortest Path Bridging zur Erzielung von Redundanz durch die Fähigkeit, den Datenverkehr bei einem Ausfall eines Pfades dynamisch über mehrere Pfade umzuleiten. Darüber hinaus wird so ein effizientes und automatisches Containernetzwerk geschaffen.
5. Ziehen Sie den Einsatz von Virtual Chassis in Erwägung, um die Zuverlässigkeit in kritischen Bereichen zu erhöhen. Dies ermöglicht Redundanz und Resilienz für Ihr Netzwerk, unterstützt In-Service-Software-Upgrades (ISSU) und ermöglicht dedizierte Mesh- oder Ring-Verbindungen. Das Virtual Chassis ist eine kosteneffiziente Lösung zur Vereinfachung der Netzwerkverwaltung bei gleichzeitiger Gewährleistung einer hohen Verfügbarkeit.
6. Nutzen Sie das Leistungsspektrum von Alcatel-Lucent OmniVista® Network Management System. Mit OmniVista Resource Manager können Sie sicherstellen, dass Sie über alle Sicherungskopien der Konfiguration von Netzwerk-Switches verfügen und in der Lage sind, diese im Ernstfall oder bei Bedarf wiederherzustellen. Dieses leistungsstarke Tool verwaltet den gesamten Lebenszyklus des Sicherungs- und Wiederherstellungsprozesses.
7. Implementieren Sie Virtual Router Redundancy Protocol (VRRP). VRRP verbessert die Ausfallsicherheit des Netzwerks, indem es einen virtuellen Backup-Router bereitstellt, der nahtlos übernehmen kann, wenn der primäre Router ausfällt.

E-Book
Resilienz und Sicherheit als Priorität

Investieren Sie in resiliente und sichere Netzwerklösungen

Investitionen in ein resilientes und sicheres Netzwerk sind immer sinnvoll. Allerdings kann die Entscheidung, wo man am besten investiert, komplex sein und viel Zeit kosten – Planung ist das A und O. Bevor Sie loslegen, sollten Sie einige wichtige Punkte beachten, damit Sie genau die Sicherheit und Resilienz erhalten, die Ihr Unternehmen benötigt:

- Überprüfen und aktualisieren Sie gemeinsam mit Ihrem Business Partner Ihr Netzwerkkonzept, um sicherzustellen, dass das Netzwerk die Anforderungen Ihrer Einrichtung erfüllt, insbesondere in Bezug auf die Ausfallsicherheit sensibler und kritischer Bereiche, die sich auf wichtige Behördendienste auswirken. Für kritische Bereiche sollten Sie, wenn möglich und sinnvoll, Backup-Server und Mehrfachverbindungen einrichten.
- Verbessern Sie die Reaktion auf Vorfälle durch den Einsatz von künstlicher Intelligenz (KI) und maschinellem Lernen (ML) mit dem Alcatel-Lucent OmniVista Network Advisor. Dieses Tool stellt sicher, dass Probleme behoben werden, bevor sie beim Endnutzer spürbar sind. Netzwerk- oder Sicherheitsprobleme werden proaktiv identifiziert und behoben. Es beschleunigt die Fehlerbehebung und verbessert die Netzwerksicherheit durch Konfigurationsprüfungen und die Verwaltung von Warnmeldungen in Echtzeit, falls sich das Netzwerkverhalten plötzlich ändert.
- Erwägen Sie gehärtete Schalter für raue Umgebungen. Die Produktfamilie der robusten Ethernet-Switches von Alcatel-Lucent Enterprise wurde speziell für den Einsatz in schwierigen Umgebungen und bei extremen Temperaturen entwickelt. Diese Switches bestehen aus robusten Komponenten und sind in stabilen Gehäusen untergebracht, um Langlebigkeit und Zuverlässigkeit zu gewährleisten. Sie verfügen über das gleiche Betriebssystem wie die übrigen ALE-Switches. Zur Erhöhung der Sicherheit und zum Schutz sensibler Daten sind einige Switch-Modelle mit Einbruchswarnungen und Alarmrelais ausgestattet, die den Anschluss externer Alarmsysteme ermöglichen. Bestimmte Modelle unterstützen sogar MACsec für eine sichere Datenkommunikation zwischen den beiden Endpunkten. Mit Virtual Chassis-Funktionen in robusten Switches können Sie die Redundanz, Resilienz und Skalierbarkeit verbessern.
- Bieten Sie technische ALE-Schulungen für das Betriebsteam des Netzwerks an, damit es Probleme schnell erkennen und darauf reagieren kann.

Resiliente und sichere Kommunikationslösungen

Im Umgang von Behörden mit Bürgern, Stakeholdern und anderen Regierungsstellen sowie für die Verbreitung wichtiger Informationen ist die Kommunikation von entscheidender Bedeutung. Die Kommunikationssysteme müssen in Krisenzeiten verfügbar sein, wenn die Bürger die Hilfe der Behörden am dringendsten benötigen. Resilienz und Sicherheit unterliegen einem ständigen Wandel. Regelmäßige Überprüfungen tragen dazu bei, dass Ihre Kommunikationslösung von Alcatel-Lucent Enterprise sicher und erreichbar bleibt.

Die Kommunikationslösungen von ALE verfügen über integrierte Sicherheitsfunktionen. Das bedeutet, dass sich das Thema Sicherheit wie ein roter Faden durch alle Phasen der Produktdefinition, -entwicklung und -bereitstellung zieht. Die gesamte Hardware und sämtliche Betriebssysteme sind gehärtet, und ein Schutz gegen Denial of Service (DoS) ist integriert. Wir erfüllen anerkannte Zertifizierungen und Akkreditierungen für globale Sicherheits- und Datenschutzstandards (ISO 27001, ISO 27017 und ISO 27018). Darüber hinaus erfüllen wir branchenspezifische Sicherheits- und Datenschutzstandards wie den Health Insurance Portability and Accountability Act (HIPAA) in den USA und Hébergeurs de Données de Santé (HDS) für das Hosting von Gesundheitsdaten in Frankreich sowie regionale Sicherheits- und Datenschutzstandards wie die Datenschutzgrundverordnung (DSGVO) in der Europäischen Union.

Sieben bewährte Verfahren für Ihre Kommunikationslösungen

Nachfolgend finden Sie sieben bewährte Verfahren, die dafür sorgen, dass Sie die integrierte Resilienz und Sicherheit Ihrer Kommunikationslösungen von ALE optimal ausschöpfen.

1. Überprüfen Sie gemeinsam mit Ihrem Business Partner in regelmäßigen Abständen Ihren Systemstatus, um sicherzustellen, dass die jeweils neueste Version der Software, Patches und Sicherheitserweiterungen installiert und Ihr SPS-Vertrag auf dem neuesten Stand ist.
2. Überprüfen Sie regelmäßig die Komponenten für die Sicherheit und Servicekontinuität in Ihrem Alcatel-Lucent OmniVista 8770 Network Management System. Dort finden Sie wertvolle Informationen und Funktionen zur Resilienz und Sicherheit Ihrer Kommunikationslösung.
    - Erwägen Sie eine automatisierte Remote-System-Sicherung, um den Verlust von Konfigurationsdaten zu vermeiden.
    - Konfigurieren Sie die Alarmüberwachung und sorgen Sie dafür, dass sie regelmäßig mit den richtigen Schwellenwerten aktualisiert wird. Überprüfen Sie außerdem, ob Benachrichtigungen über Ausfälle des Kommunikationssystems oder Qualitätswarnungen an die zuständigen Personen gesendet werden.
3. Überprüfen Sie strenge Kennwortrichtlinien und setzen Sie diese durch, vorzugsweise unter Verwendung einer externen Authentifizierung (RADIUS-Server), und richten Sie Erinnerungsfunktionen für die Nutzer ein, um Gebührenbetrug zu verhindern, der in vielen Ländern immer noch eine Gefahr darstellt.
4. Schulen Sie Ihre Mitarbeiter und sorgen Sie dafür, dass sie über Risiken und Präventionsmaßnahmen informiert sind.
5. Überprüfen Sie geschäftskritische Anwendungsserver auf Zustand, Eignung und Funktionsfähigkeit
6. Erwägen Sie ein spezielles VLAN für Sprachfunktionen. Die Trennung der Sprachübertragung vom übrigen Datenverkehr verringert das Risiko einer Kontaminierung, die den Betrieb und möglicherweise auch die öffentlichen Dienste stören könnte.
7. Vergewissern Sie sich, dass Ihre Session Border Controllers (SBCs) korrekt eingerichtet sind. Die Anforderungen können sich im Laufe der Zeit geändert haben.

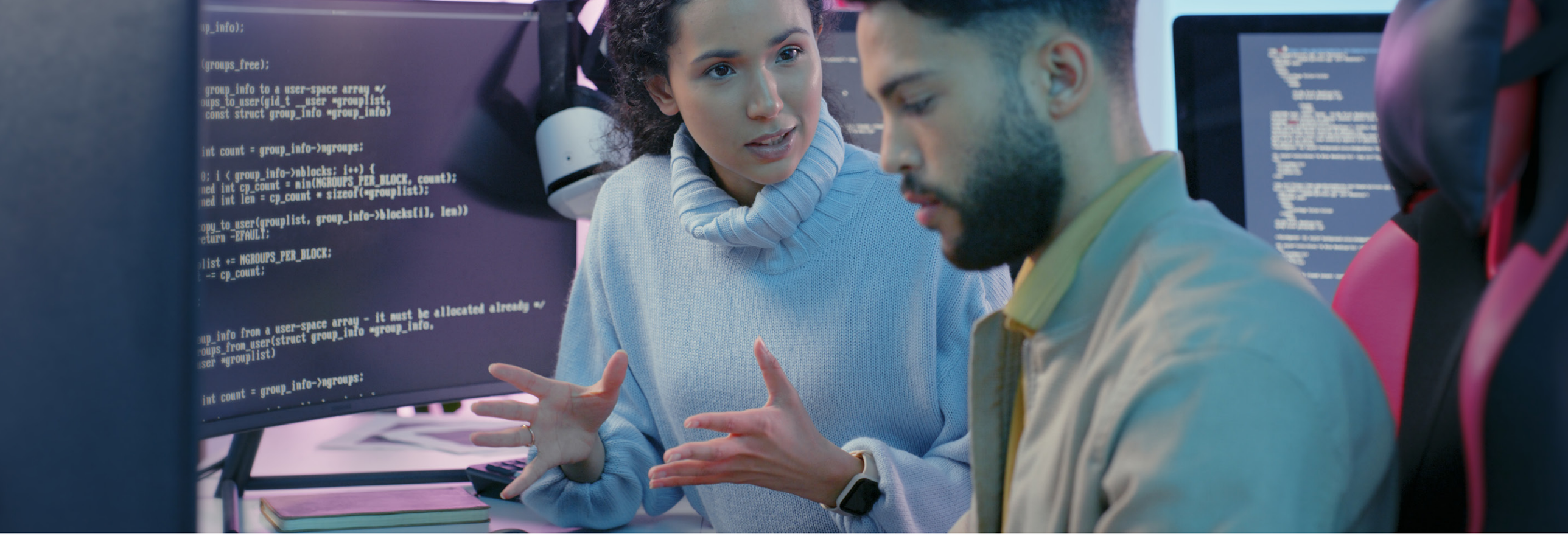
E-Book
Resilienz und Sicherheit als Priorität

Investition in resiliente und sichere Kommunikationslösungen

In den letzten Jahren haben die globalen Rahmenbedingungen die Bedeutung der Kommunikation zwischen Behörden und Bürgern in den Vordergrund gerückt. Nachfolgend sind einige wichtige Bereiche aufgeführt, die Behörden bei der Planung von Investitionen in Kommunikationslösungen zur Verbesserung der Resilienz und Sicherheit berücksichtigen sollten.

- Redundante und widerstandsfähige Architektur. Ihre Architektur sollte vollständig redundant und widerstandsfähig sein. Die Duplizierung von Anrufservern in kritischen Bereichen, die Einrichtung von Redundanzen an entfernten Standorten und die Duplizierung kritischer Anwendungsserver können zusätzlichen Schutz bieten.
- Kunden, die TDM DECT verwenden, sollten eine Ausweitung der Abdeckung auf kritische Bereiche in Erwägung ziehen, um bei einem Ausfall des IP-Systems Resilienz zu gewährleisten.
- Erstellen Sie einen Arbeitsablauf unter Verwendung von Rainbow und/oder Alcatel-Lucent Visual Notification Assistant (VNA) mit automatischen Auslösern (Auslöser kann ein Mensch, das IoT oder ein System sein) zur Benachrichtigung wichtiger Personen über Systemprobleme, damit diese schnell handeln und den Wiederherstellungsprozess beschleunigen können.
- Setzen Sie eine starke Verschlüsselung ein. Die Verschlüsselung basiert auf Branchenstandards, die nativ Bestandteil der Lösung sind – ohne Auswirkungen auf die Sprachqualität und -leistung.

E-Book
Resilienz und Sicherheit als Priorität



- Implementieren Sie Rainbow™ von Alcatel-Lucent Enterprise, Dies ist ein ideales Tool zur Ergänzung von ALE-Kommunikationslösungen, das speziell für die Zusammenarbeit entwickelt wurde. Rainbow bietet ein umfassendes Funktionspaket mit Sprach-, Video- und Instant-Messaging-Funktionen, das eine nahtlose Kommunikation und effiziente Zusammenarbeit ermöglicht. Mit Rainbow können Sie Bilder, Videos und Videoüberwachungsdaten austauschen und so das kontextbezogene Gesamtbild besser darstellen. Dies ermöglicht fundierte Entscheidungen. Rainbow bietet auch hybride Kommunikation mit sicherer Konnektivität zwischen dem Firmengelände und der Cloud. Es sorgt für eine zuverlässige Kommunikation, sodass Sie mit Kollegen und Kunden über Rainbow verbunden bleiben und auch in schwierigen Situationen eine unterbrechungsfreie Verbindung nutzen können. Hybride Kommunikations-lösungen haben zudem den Vorteil, dass der Cloud-Betrieb und der Betrieb vor Ort von verschiedenen Standorten aus erfolgen können. Dies sorgt für ultimative Ausfallsicherheit und die Aufrechterhaltung der Kommunikation.
- Für Behörden mit strengeren Sicherheitsanforderungen bietet Rainbow Edge eine lokale Alternative mit einer Private Cloud-Instanz. Die Instanz kann in jedem beliebigen Rechenzentrum gehostet werden und bietet vollständige Kontrolle über Server, Speicher und Netzwerke, sodass die Behörden die Infrastruktur entsprechend ihren Anforderungen anpassen und konfigurieren können. Personalisierte Sicherheitsrichtlinien können implementiert werden, und Ressourcen können autonom verwaltet werden. Dieses Maß an Kontrolle bietet vollständige Transparenz und Befugnis über die Infrastruktur und ermöglicht es den Behörden, fundierte Entscheidungen zu treffen und die Leistung entsprechend ihrer Ziele zu optimieren.
- Definieren Sie eine sichere Kommunikationsstrategie für die verteilt arbeitende Belegschaft. ALE bietet mehrere Optionen für die Kommunikation und Zusammenarbeit für verteilt arbeitende Mitarbeiter, die von unterwegs aus oder im Homeoffice arbeiten. Dazu zählen beispielsweise folgende Angebote:
  - Rainbow
  - IP Desktop Softphone
  - ALE Softphone
  - Deskphone mit integriertem VPN, das mit integrierter Sicherheit (VPN) in großem Umfang eingesetzt werden kann

Schutz von Menschen und Ausrüstung

ALE bietet flexible, sichere und hochverfügbare Systeme für die Echtzeit-kommunikation und Echtzeitbenachrichtigung. Diese Lösungen können in den Betrieb von Leitstellen für die öffentliche Sicherheit oder für intelligente Städte integriert werden, um die Anrufverteilung und Priorisierung zu optimieren, den Austausch kontextbezogener Informationen mit IoT-Daten zu erleichtern und die Zusammenarbeit zwischen Ersthelfern und verschiedenen Stakeholdern zu verbessern. All dies ermöglicht eine bessere Entscheidungsfindung und Koordination.

Das Zusammenschalten von IoT-Geräten in Gebäuden, an Veranstaltungsorten und in Städten in Kombination mit Analytik und KI verändert die Kommunikationslandschaft grundlegend. Durch die Integration von Sensoren, Videoüberwachung, Rainbow-Workflow und KI ist der Wechsel von einem reaktiven zu einem proaktiven Ansatz möglich, wodurch die Prozesseffizienz verbessert wird. Das spart Zeit und Kosten. Diese Integration ermöglicht ein umfassendes Verständnis des Kontextes, unterstützt die Entscheidungsfindung und verkürzt die Reaktionszeiten im Notfall. Darüber hinaus optimieren Funktionen wie Asset Tracking und die Steuerung von intelligenten Schlössern und Leuchten den Betrieb. Aber damit nicht genug: Die Möglichkeit der Aufzeichnung von Kommunikation und Aktionen vereinfacht die nachträgliche Analyse, verbessert die Sicherheitsprozesse und mindert potenzielle Haftungsrisiken. Um diese Fortschritte zu erreichen, ist eine vernetzte Umgebung mit flächendeckendem Wi-Fi-Zugang und problemlosem IoT-Onboarding entscheidend.

Für zeitkritische, sichere und hochverfügbare Echtzeit-Kommunikationsplattformen ist eine zuverlässige Infrastruktur unerlässlich, um einen reibungslosen Betrieb zu gewährleisten. Ihre technologische Infrastruktur sollte geeignete Software, hochverfügbare Netzwerkprotokolle und die Flexibilität umfassen, robuste Netzwerk-Switches einzubinden, die sich nahtlos in Ihr Ökosystem integrieren und rauen Umgebungsbedingungen standhalten, einschließlich begrenzter Luftzirkulation, Stößen und extremen Temperaturen. Die Entscheidung für robuste Geräte gewährleistet Langlebigkeit an solch schwierigen Standorten, an denen andere Geräte schneller versagen würden.

Im Bereich der physischen Sicherheitssysteme steht viel auf dem Spiel. Jede Minute und jedes einzelne Videobild kann für die Behörden von entscheidender Bedeutung sein, wenn es darum geht, Fehlverhalten zu erkennen, den Ursprung eines Vorfalls zu lokalisieren oder die Ursache einer Katastrophe zu verstehen. Daher ist eine zuverlässige Videoüberwachungsinfrastruktur unerlässlich.
Die Netzwerkinfrastruktur sollte nicht nur eine ausreichende Bandbreite und Power over Ethernet (PoE) für Überwachungskameras bieten, sondern auch nahtlos in die Systeme für die Videoüberwachungsverwaltung integriert werden können. Diese Integration gewährleistet ein effizientes und verlässliches Überwachungsnetzwerk mit reibungslosem Betrieb und einfacher Fehlerbehebung. Das Betriebsteam sollte in der Lage sein, alle Videoprobleme umgehend zu lösen, insbesondere in Umgebungen, in denen jeder Videoausschnitt entscheidend ist. Durch Integrationen der Alcatel-Lucent OmniSwitch®-Lösung, die über Plugins mit den wichtigsten Videoverwaltungssystemen erfolgt, können Sie dieses wichtige Ziel erreichen.

Darüber hinaus gibt es Situationen, in denen die Verfolgung von Ausrüstung (Asset Tracking) oder das Auffinden von Personen oder Geräten innerhalb Ihrer Einrichtung notwendig wird. Eine effektive Asset-Tracking-Lösung muss Personen und Assets problemlos und genau orten können. Ein solches System erhöht auch die Sicherheit, da es die schnelle Entsendung von Hilfe ermöglicht, wenn der Standort von Personen bekannt ist. Mit der Alcatel-Lucent OmniAccess® Asset Tracking-Lösung lassen sich Personal und Ausrüstung schnell auf einer Gebäudekarte lokalisieren und anzeigen. Zudem liefert das Asset Tracking Informationen über Nutzungsmuster. Wenn Sie wissen, ob Assets überlastet oder unausgelastet sind, kann dies sehr aufschlussreich sein.

Datenhoheit und Sicherheit

Alcatel-Lucent Enterprise stellt andere Technologieanbieter bei der Umsetzung der für eine durchgängige Cybersicherheit erforderlichen Best Practices in den Schatten. Wir von ALE:

- befolgen 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
- verfügen über die Common Criteria EAL2+-Zertifizierung
- verwenden ISO 27001-Normen für alle unsere Cloud-basierten Lösungen
- unterstützen ZTNA, granulare Netzwerksegmentierung und hochspezifische Sicherheitsrichtlinien zur Verringerung des Risikos nicht autorisierter Aktivitäten
- führen für unsere Produkte hochspezialisierte, sicherheitsspezifische Tests durch, wie z. B. Penetrationstests
- stellen sicher, dass unsere Produkte wichtige Branchenzertifizierungen wie HDS, HIPAA und den Family Educational Rights and Privacy Act (FERPA) erfüllen

Als anerkannte Experten für Cybersicherheit erarbeiten wir Vorschläge für die Cybersicherheitsrichtlinien der Europäische Union. Darüber hinaus nutzen wir unser Know-how im Bereich Cybersicherheit, um Kunden zu helfen, die richtige Mischung aus sicheren Unified Communications- und Collaboration-Lösungen für ihren Bedarf auszuwählen und zu implementieren und ihre Mitarbeiter in den Best Practices zur Cybersicherheit zu schulen.

© 2024 ALE International, ALE USA Inc. Alle Rechte in allen Ländern vorbehalten. Der Name Alcatel-Lucent und das Logo sind Marken von Nokia, die von ALE unter Lizenz verwendet werden. Unter folgender Adresse finden Sie eine Liste der geschützten Marken von ALE: www.al-enterprise.com/de-de/rechtliches/marken-urheberrecht. DID23070401DE (Mai 2024)

Alcatel·Lucent Enterprise