Sichere Unified Communications- und Collaboration-Lösungen

Das braucht es in der heutigen, sich wandelnden Welt

Whitepaper

Alcatel·Lucent Enterprise

Inhalt

- Stärkerer Fokus auf Cybersicherheit
- Sechs Schlüsselbereiche für umfassende Cybersicherheit
- Geschäftsziele mit weniger Risiken erreichen
- Cybersicherheit im Fokus von Technologieanbietern

Stärkerer Fokus auf die Cybersicherheit

Im Laufe der letzten Jahre hat sich in fast allen Unternehmen und Behörden die Art und Weise geändert, wie Mitarbeiter kommunizieren, zusammenarbeiten und Informationen austauschen. Die rasche Umstellung auf das Arbeiten im Homeoffice war für die Aufrechterhaltung des Geschäftsbetriebs während der Pandemie von entscheidender Bedeutung, hatte jedoch ihren Preis: Die Netzwerkgrenzen reichen nun weit über die traditionellen Bürogrenzen hinaus, was die Angriffsfläche von Unternehmen erheblich vergrößert.

Die Risiken, die mit erweiterten Netzwerkperimetern verbunden sind, werden in absehbarer Zeit nicht verschwinden. Laut Gartner werden bis Ende 2023 weltweit 39 Prozent der Wissensarbeiter in hybriden Remote- und In-Office-Modellen arbeiten. In den USA steigt diese Zahl auf 51 Prozent[1].

Geopolitische Störungen haben die Risiken für die Cybersicherheit weiter erhöht. Die Agentur der Europäischen Union für Cybersicherheit bezeichnete den Einmarsch Russlands in die Ukraine als "Game Changer" für die globale Cyber-Domäne. [2] Nach Angaben des Verbands der ukrainischen IT-Outsourcing-Unternehmen war 2022 jedes fünfte Fortune-500-Unternehmen auf Softwareentwickler aus der Ukraine angewiesen.[3]

Gleichzeitig nehmen die Auswirkungen von Cyberangriffen auf die Gesellschaft zu. Im Jahr 2022 kam es zu schweren Cyberangriffen auf kritische zivile Infrastrukturen, die einen nationalen Notstand in Costa Rica auslösten[4] und zu weiteren Angriffen auf Organisationen im Gesundheitswesen.[5]

Unternehmen können sich Verzögerungen bei der Verbesserung der Cybersicherheit nicht leisten

Die Cyberkriminalität hat die Weltwirtschaft im Jahr 2021 schätzungsweise 5,5 Billionen Euro gekostet, und es wird erwartet, dass der Schaden bis 2025 auf über 10 Billionen Euro ansteigt.[6] Das Problem ist so gravierend, dass die Europäische Union ein Gesetz über die Widerstandsfähigkeit gegenüber Cyberkriminalität (Cyber Resilience Act) erarbeitet und eine erheblich verbesserte Version von zwei Richtlinien über Netz- und Informationssicherheit (NIS) herausgegeben hat, um Verbraucher und Unternehmen zu schützen, die Produkte oder Software mit einer digitalen Komponente kaufen oder verwenden.[7] Die USA setzen auch Maßnahmen zur Stärkung der Cybersicherheit um, darunter die Executive Order 14028, die die Behörden dazu ermutigt, Zero-Trust-Prinzipien für die Cybersicherheit zu übernehmen und die Netzwerkarchitekturen entsprechend anzupassen.[8]

In dem Maße, in dem Unternehmen und Behörden sich um die digitale Transformation und die dauerhafte Unterstützung flexibler Arbeitsmodelle bemühen, haben sie keine andere Wahl, als die Cybersicherheit zu verbessern. Die Lösungen, die ihre Teams für die Kommunikation, die Zusammenarbeit und den Informationsaustausch nutzen, müssen auf allen Ebenen und in allen Funktionsbereichen bewährte Praktiken der Cybersicherheit miteinbeziehen.

1 Gartner prognostiziert, dass 39 % der globalen Wissensarbeiter bis Ende 2023 hybrid arbeiten werden. Gartner, März 2023.
2 Die unbeständige Geopolitik führte 2022 zu neuen Trends in der Cybersicherheits-Bedrohungslandschaft. Agentur der Europäischen Union für Cybersicherheit. November 2022
3 Jedes fünfte Fortune-500-Unternehmen war 2022 bei der Softwareentwicklung auf die Ukraine angewiesen. Ukrainische Hi-Tech-Initiative, Oktober 2022.
4 Die 13 teuersten Cyberangriffe des Jahres 2022: Ein Rückblick. Security Intelligence. Dezember 2022.
5 2022 im Rückblick: Ein ereignisreiches Jahr für die Cybersicherheit. Forbes, Dezember 2022.
6 Neuer Vorschlag der Europäischen Union zur Cybersicherheit zielt auf die Cyberkriminalität ab. Weltwirtschaftsforum, September 2022.
7 EU Cyber Resilience Act. Europäische Kommission, September 2022.
8 Executive Order on Improving the Nation's Cybersecurity. Cybersecurity & Infrastructure Security Agency.

Sechs Schlüsselbereiche für umfassende Cybersicherheit

Unified-Communications- und Collaboration-Lösungen müssen auf eine Ende-zu-Ende-Cybersicherheit achten, denn nur so kann eine umfassende Sicherheit gewährleistet werden. Ein durchgängiger Ansatz für die Cybersicherheit hilft Unternehmen und Behörden 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

Um festzustellen, ob Unified-Communications- und Collaboration-Lösungen Cybersicherheit durchgängig implementieren, sollten Lösungsevaluierungen in den unten beschriebenen Bereichen durchgeführt werden. Durch die Konzentration auf diese Bereiche kann sichergestellt werden, dass die Lösungen umfassend bewertet werden und gleichzeitig auf die wichtigsten Schwachstellen in der gesamten Cyberbedrohungslandschaft abzielen.

1 Integrierte Sicherheit

In der Vergangenheit waren die meisten Lösungsdesigns von der Notwendigkeit neuer Funktionen bestimmt, und die Sicherheit war ein wichtiger, aber zweitrangiger Aspekt. Mit der sich verändernden Landschaft haben sich die traditionellen Design-Prioritäten umgekehrt, und das Lösungsdesign muss sich nun an den Anforderungen der Cybersicherheit orientieren.

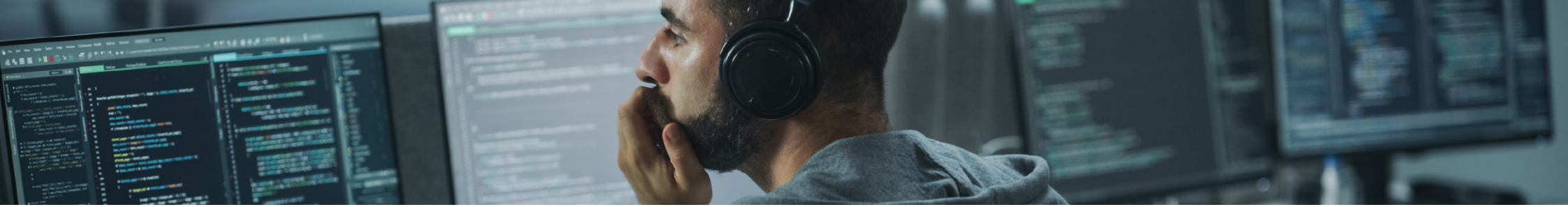
Bei Hardware- und Softwarelösungen, die sicher konzipiert sind, wird die Sicherheit bei jedem Schritt der Produktdefinition, -entwicklung und -bereitstellung berücksichtigt. Die gesamte Hardware und die Betriebssysteme sind gehärtet, der Schutz vor Denial of Service (DoS) ist integriert, und die Lösungen implementieren die für die Branche wichtigsten Best Practices im Bereich der Cybersicherheit.
Eine Unified-Communications- und Collaboration-Lösung für Organisationen der Staatssicherheit erfüllt beispielsweise die sehr hohen Anforderungen dieser Organisationen an Ausfallsicherheit und Vertraulichkeit.

2 Zero Trust Network Access-Sicherheit

Sicherheitsstrategien, die auf dem Standort eines Benutzers innerhalb der Unternehmensfirewall, den eingegebenen Anmeldeinformationen oder der verwendeten Anwendung oder des verwendeten Geräts basieren, sind nicht mehr ausreichend – selbst wenn mehrere Sicherheitsmechanismen kombiniert werden. Heute sollte kein Nutzer, kein Gerät und keine Anwendung automatisch Vertrauen genießen.

Unified-Communications- und Collaboration-Lösungen, die ein ZTNA-Sicherheitsmodell (Zero Trust Network Access) implementieren, helfen Unternehmen, den sich ständig weiterentwickelnden Bedrohungen wirksam zu begegnen. ZTNA bringt keinem Nutzer, keinem Gerät und keiner Anwendung Vertrauen entgegen, egal, wo diese sich befinden: Dabei wird von fünf Annahmen ausgegangen:

- Das Netzwerk ist feindlich
- Externe und interne Bedrohungen lauern überall
- Der Standort und die Identität alleine sind nicht genug, um Vertrauen zu schaffen
- Ausnahmslos alle Geräte, Nutzer und Netzwerkflüsse müssen authentifiziert und autorisiert werden
- Netzwerk- und Sicherheitsrichtlinienmüssen dynamisch sein und so viele Datenquellen wie möglich nutzen



3 Makro- und Mikro-Segmentierung

Makro- und Mikrosegmentierung ermöglichen einen granularen und hochgradig kontrollierten Ansatz zur Cybersicherheit für die verschiedensten 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

In modernen Organisationen können sich Mitarbeiter, Kunden, Partner und Lieferanten überall auf der Welt befinden. Und die Lösungen, die sie zur Kommunikation und Zusammenarbeit nutzen, 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 Hardware- und Softwareelement, das an der Ende-zu-Ende-Kommunikation beteiligt ist, über einen Verschlüsselungsmechanismusverfügen muss, der von den Sicherheitsbehörden genehmigt wurde und von Anfang an eingebaut ist.

5 Zertifizierungen und Akkreditierungen für Sicherheit und Datenschutz

Noch vor wenigen Jahren waren die strengsten Sicherheitszertifizierungen und -akkreditierungen nur für Sicherheitsprodukte wie Firewalls oder in bestimmten Branchen wie der Verteidigung erforderlich. Heutzutage müssen sicherheitsspezifische Normen auf alle Technologieprodukte in allen Branchen angewandt werden.

Es ist äußerst wichtig zu überprüfen, ob die Behauptungen zur Cybersicherheit durch anerkannte Zertifizierungen und Akkreditierungen gestützt werden. Hier sind einige Beispiele für Vorschriften, auf deren Einhaltung Sie achten sollten:

- **Globale Sicherheits- und Datenschutzstandards**, wie ISO 27001 für Informationssicherheit, ISO 27017 für sicherere, cloudbasierte Umgebungen, ISO 27018 für den Schutz personenbezogener Daten in cloudbasierten Umgebungen und Common Criteria Evaluation Assurance Level (EAL) 2 und höher für die Sicherheit von Computersystemen
- **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 Datenschutzstandards**, wie die Datenschutz-Grundverordnung (DSGVO) in der Europäischen Union

6 Kontinuierliche, spezialisierte Sicherheitstests

Ähnlich wie bei den Sicherheitsstandards sind spezialisierte Sicherheitstestverfahren, die früher für Sicherheitsprodukte reserviert 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 den Cyberbedrohungen in einer sich ständig weiterentwickelnden Landschaft einen Schritt voraus zu sein, müssen Penetrationstests, die sich ausschließlich an den Anforderungen der Cybersicherheit orientieren, kontinuierlich durchgeführt werden.

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.

Geschäftsziele mit weniger Risiken erreichen

Einheitliche Kommunikations-und Kollaborationslösungen, die die gesamte Palette der im vorherigen Abschnitt beschriebenen Cybersicherheitsmaßnahmen umsetzen, geben Unternehmen und Behörden die Freiheit und Flexibilität, ihre Aktivitäten voranzutreiben. So lassen sich gleichzeitig Risiken minimieren und die Einhaltung von Vorschriften sicherstellen. Sie können:

- **Mitarbeitern ermöglichen,** sicher und vertraulich über beliebige Medien und Geräte von jedem Ort aus zusammenzuarbeiten und Informationen auszutauschen.
- **das Kundenerlebnis verbessern** durch angereicherte, informative und ansprechende Kommunikation, schnellere Entscheidungsfindung, automatisierte Geschäftsprozesse und die Möglichkeit, Probleme proaktiv zu erkennen, bevor sie sich auf den Kunden auswirken.
- **Operative Exzellenz und Agilität steigern** unter Verwendung einer digitalen Infrastruktur, die dort eingesetzt wird, wo sie für das Unternehmen am sinnvollsten ist: vor Ort oder in einer hybriden, privaten oder öffentlichen Cloud, und das unter Einhaltung strenger Datenschutzrichtlinien und -bestimmungen.

Die nachstehenden Beispiele zeigen nur einige der Möglichkeiten, die sich ergeben und die sich leicht an andere Anforderungen und Branchen anpassen lassen.

Flexible digitale Arbeitsplätze für Mitarbeiter

Mit der richtigen Mischung aus sicheren Kommunikations- und Kollaborationslösungen können Mitarbeiter schneller und flexibler arbeiten, und das unter Einhaltung der branchenspezifischen Vorgaben.

- **Im Gesundheitswesen** kann eine hochgradig mobile Belegschaft unter Einhaltung höchster Datensicherheitsstandards zusammenarbeiten und Informationen austauschen. Mitarbeiter können sich problemlos auf den neuesten Stand bringen und erhalten schnell die benötigte Unterstützung. Medizinisches Personal kann dank sicherer Echtzeitkommunikation die Ergebnisse für Patienten und die Effizienz von Arbeitsabläufen verbessern. Nichtmedizinisches Personal kann Prozesse und Reaktionen auf Wartungsmaßnahmen beschleunigen, die die Sicherheit von Patienten und Personal beeinträchtigen könnten.
- **Im Bildungsbereich** können Lehrkräfte mit einem umfangreicheren und ansprechenderen Remote-Unterricht Lernenden die Teilnahme an mehr Aktivitäten, gemeinsamen Projekten und Interaktionen über das von ihnen bevorzugte Medium ermöglichen. Umfassende Zugriffskontrollen und automatisierte Richtlinien gewährleisten die Datenintegrität, und Analysen priorisieren die wichtigen Kommunikations- und Netzwerkressourcen.
- **In Behörden** können Mitarbeiter in verteilten Teams auf sichere Weise Informationen austauschen. Sie können ihren Bildschirm teilen, den Desktop eines anderen Anwenders fernsteuern und große Dateien austauschen, um die Zusammenarbeit zu verbessern. Und sie können über webbasierte oder mobile Anwendungen per Sprache, Video, Chat oder Instant Messaging sicher mit den Bürgern interagieren.
- **Im Verkehrswesen** ermöglicht der digitale Arbeitsplatz den Angestellten die Nutzung ihrer eigenen Geräte während der Arbeit. Außerdem werden Prozesse effizienter gestaltet und Fahrgastdienstleistungen verbessert, wie zum Beispiel die Möglichkeit, während der Fahrt zu arbeiten. Sichere Kommunikationsprotokolle, gehärtete Installationen und diversifizierter Code schützen die Daten überall im Netz.

Verbinden Sie alles, um das Kundenerlebnis zu verbessern

Durch eine sichere Verbindung von Menschen, Objekten und Anwendungen per Echtzeitkommunikation haben Unternehmen und Behörden viele Möglichkeiten:

- Geräte, Technologien und Daten für Mitarbeiter bereitstellen, um die Kundenunterstützung zu verbessern und gleichzeitig Sicherheitsrisiken durch menschliche Fehler oder mangelndes Bewusstsein zu minimieren
- Integrierte, sichere Endgeräte für die mobile Kommunikation und Zusammenarbeit mit Kunden unter vollem Zugriff auf CRM-Lösungen (Customer Relationship Management) nutzen
- Eine schnell wachsende, vielfältige Palette von Internet-of-Things-Geräten (IoT) optimal schützen, kontrollieren und im Blick behalten
- Kommunikations- und Kollaborationssysteme auf dem neuesten Stand halten, um kein Risiko durch veraltete Anwendungen und Schwachstellen einzugehen
- Wirksame Zugangskontrollen und Ende-zu-Ende-Verschlüsselung auf allen Plattformen implementieren

Ein einheitliches Netzwerkmanagement ermöglicht die ganzheitliche Verwaltung aller Kommunikationsplattformen, Anwendungen und IoT-Geräte. Einheitliches Netzwerkmanagement:

- vereinfacht Verwaltungsaufgaben für kabelgebundene und drahtlose Netzwerke sowie IoT-Geräte, um die Kosten für die Netzwerkverwaltung zu senken, die Netzwerkleistung zu optimieren und die betriebliche Effizienz zu steigern
- beschleunigt die Fehlerbehebung in zunehmend vielfältigen Technologieumgebungen, um das Risiko von Serviceunterbrechungen und Ausfallzeiten zu verringern

Ein branchenübergreifendes, einheitliches Netzwerkmanagement bietet eine ganze Reihe von Vorteilen. Dies zeigt sich an folgenden Beispielen:

Im Gesundheitswesen können IoT-Lösungen den Standort wichtiger Geräte wie Sauerstofftanks, Notfallwagen, Patientenmonitore, Infusionsstangen und Rollstühle verfolgen und so die Sicherheit und Effizienz verbessern. Die Verbindungen von Menschen, Objekten und Anwendungen können auch dazu verwendet werden, Alarme auszulösen, die das medizinische Personal auf Patientenbedürfnisse und Gerätefehlfunktionen aufmerksam machen und jeden in der Einrichtung vor unsicheren Situationen warnen.

Im Bildungswesen gibt es neue Möglichkeiten, intelligente Campus-Geräte und -Anwendungen auf mehreren Sicherheitsebenen zu verbinden, um die Ressourcen der Einrichtung vor unzureichend gesicherten Geräten zu schützen, die auf das Netzwerk zugreifen. Bildungseinrichtungen können auch IoT-Geräte-Fingerabdrücke verwenden, um Geräteeigenschaften wie Typ, Hersteller, Modell und Betriebssystem zu identifizieren und so die Einrichtung eines IoT-Netzwerks und das Onboarding von Geräten zu vereinfachen und zu beschleunigen.

Operative Exzellenz und Agilität steigern

Indem sie Unified Communications- und Collaboration-Lösungen sicher und flexibel vor Ort oder in einer hybriden, privaten oder öffentlichen Cloud implementieren, können Unternehmen und Behörden digitale Technologien so nutzen, wie es ihren Zielen und ihrem Auftrag am besten entspricht. Jedes Unternehmen kann durch den Einsatz von Cloud-Modellen Betriebsabläufe und Agilität verbessern und ein neues Niveau an operativer Exzellenz erreichen und gleichzeitig die branchenspezifischen Anforderungen erfüllen. Hier einige Beispiele:

- **Im Gesundheitswesen** können zur Verbesserung der Patientenversorgung und zur Steigerung der Effizienz digitale Aufzeichnungen verwendet werden mit der Gewissheit, dass die persönlichen Daten in einem sicheren und zertifizierten Datenzentrum in der Cloud gespeichert werden.
- **Im Bildungsbereich** haben Lehrkräfte, Mitarbeiter und Studenten von überall aus sicheren, datenschutzgerechten Zugriff auf Cloud-basierte Anwendungen und Dienste. Für IT-Abteilungen reduziert sich der Zeit- und Kostenaufwand für die Bereitstellung, den Support und die Aktualisierung einer Vielzahl von Anwendungen.
- **In Behörden** wird hochverfügbare, vertrauliche Kommunikation durch integrierte DoS-Mechanismen sowie sicherheitsgehärtete Hardware und Betriebssysteme geschützt.
- **Im Transportwesen**, wo veränderte Kommunikationsmöglichkeiten zu gefährlichen Situationen führen können, sind widerstandsfähige, datensouveräne Lösungen unerlässlich.

Cybersicherheit im Fokus von Technologieanbietern

Zwar legen viele Technologieanbieter großen Wert auf Cybersicherheit, doch nicht alle verfügen über das umfassende Know-how, um eine durchgängige Sicherheit zu implementieren.

Alcatel-Lucent Enterprise bietet mehr als andere Anbieter, indem es alle für eine durchgängige Cybersicherheit erforderlichen Best Practices implementiert. Wir:

- 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 alle 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 unterstützen wir unsere Kunden mit unserem Fachwissen bei der Auswahl und Implementierung der richtigen Mischung aus sicheren Unified Communications- und Collaboration-Lösungen für ihre Bedürfnisse und schulen ihre Mitarbeiter in bewährten Verfahren der Cybersicherheit.

Alcatel-Lucent Enterprise genießt weltweites Vertrauen

Führende Unternehmen aller Branchenvertrauen auf unsere sicheren Kommunikationslösungen für das digitale Zeitalter, um ihre Ziele zu erreichen:

- In der Metropolregion und Stadt Perpignan in Frankreich setzen Behörden einen strategischen Plan für den digitalen Wandel um, der Videokonferenzen und Sprachkommunikation für Mitarbeiter, Unterstützung für IoT-Anwendungen sowie neue Inhalte und Dienste für Einwohner, Touristen und Mitarbeiter der Stadt Perpignan umfasst.
- Die Newman University in den USA, eine katholische Hochschule für freie Künste, stellt ihren Mitarbeitern Mobiltelefonfunktionen zur Verfügung, für die keine direkten Telefonnummern erforderlich sind, und bietet dem IT-Team eine einzige, intuitive, cloudbasierte Plattform zur Verwaltung, Bereitstellung und Überwachung der gesamten Netzwerkinfrastruktur.
- In den Kingsway Hospitals in Indien wurden Echtzeit-Kommunikationsinfrastrukturlösung en implementiert, mit denen klinisches und administratives Personal in Verbindung bleibt, um die Pflege zu optimieren und die Patientenerfahrung zu verbessern.
- J. Malucelli Gruppe in Brasilien, hat ihr Netz mit einer konvergenten Sprach- und Datenlösung modernisiert, die Cloud-Telefonie sowie LAN- und Wi-Fi-Netzwerke mit Cloud-Management umfasst, um die Kommunikationskosten für mehrere Unternehmen der Gruppe zu vereinfachen und zu senken.

Weitere Informationen

Wenn Sie erfahren möchten, wie wir Ihr Unternehmen dabei unterstützen können, die Vorteile sicherer Kommunikationslösungen für das digitale Zeitalter voll auszuschöpfen, besuchen Sie unsere Website oder kontaktieren Sie uns noch heute.

© 2023 ALE International, ALE USA Inc. Alle Rechte in allen Ländern vorbehalten. Der Name Alcatel-Lucent und das Logo sind Marken von Nokia, die unter Lizenz von ALE verwendet werden. Unter folgender Adresse finden Sie eine Liste der geschützten Marken von ALE: www.al-enterprise.com/de-de/rechtliches/marken-urheberrecht. DID23042401DE (Oktober 2023)

Alcatel·Lucent Enterprise