Alcatel-Lucent OmniPCX Enterprise Purple – Native Verschlüsselung

Softwareverschlüsselung der Kommunikation und gehärtete Plattform gegen Cyberangriffe

Die Digitalisierung ist schon seit einiger Zeit im Gange. Heute können Mitarbeiter jederzeit und an jedem Ort in Echtzeit zusammenarbeiten. Aber nicht alle Kommunikationswerkzeuge bieten das richtige Rahmenwerk, das eine **kontinuierliche Verfügbarkeit**, **Sicherheit**, **Vertraulichkeit** und **Compliance** gewährleistet.

Alcatel-Lucent Enterprise hat im Austausch mit Kunden auf der ganzen Welt erfahren, wo die neuen Herausforderungen liegen, und bietet nun digitale **Technologielösungen an, die es ermöglichen, von überall** aus und mit jedem Gerät zu arbeiten.

In diesem Dokument erfahren Sie, wie **ALE Ihre Kommunikation vor Cyberangriffen schützt** mit einer sicheren Kommunikationsplattform, die mit einer hybriden Architektur für die Cloud offen ist, native, erstklassige Verschlüsselungsmechanismen bietet und Ihrem IT-Team volle Kontrolle und die Einhaltung Ihrer Sicherheitsrichtlinien und Best Practices ermöglicht.

Alcatel·Lucent
Enterprise

Cybersicherheit heute

Der Umstieg in digitale Welten hat dazu geführt, dass sich die Phishing- und Ransomware-Angriffe vervielfacht haben. Für die wachsende Zahl remote arbeitender Mitarbeiter und für alle (öffentlichen und privaten) Organisationen ist das ein ernsthaftes Problem. Angesichts dieser zunehmenden Cyberbedrohungen ist der Schutz der Mitarbeiter und Kunden wichtiger denn je.

Die Verlagerung in die Cloud vergrößert die „Angriffsfläche", d. h. Hacker könnten ungesicherte Cloud-basierte Dienste oder Software as a Service (SaaS) ausnutzen. Für die Service Level Agreements (SLAs) von Providern und Anbietern sind strenge Vorgaben des IT-Teams erforderlich.

ALE: konzeptionsintegrierte Sicherheit

Ein umfassender Blick auf die aktuelle Landschaft erlaubt es, Schutzstrategien zu bestimmen, die Unternehmen für ihren EDV-Park benötigen. So bietet ALE Unternehmen Lösungen, die sie benötigen, um regionale oder vertikale Vorschriften und Standards einzuhalten, wie die Datenschutz-Grundverordnung (DSGVO), HDS, HIPAA (für den Gesundheitsmarkt) oder de NIS-2-Richtlinie für die Europäische Union.

ALE bietet auch eine sichere Konnektivität in der Cloud, mit gegenseitiger Authentifizierung und Verschlüsselungselementen, besserer Vertraulichkeit der Kommunikation in Meetings sowie Datenschutz und Kontrolle in der Cloud. Mit einer Ende-zu-Ende-Lösung, die an eine sich dynamisch entwickelnde Sicherheits-umgebung anpassbar ist, können die Teams in jeder neuen Umgebung sicher arbeiten.

Auch der Datenschutz und die Zuverlässigkeit von Cloud-Diensten werden manches Mal infrage gestellt. Die Cloud-Dienste von ALE unterliegen einer strengen Datenschutzpolitik. Datenzentren an verschiedenen Standorten sorgen für eine weltweite Serviceabdeckung. ALE ist in datenschutzgerechten Ländern präsent, etwa Frankreich, Deutschland, USA, Kanada, Singapur und Australien. Es wird vertraglich zugesichert, dass personenbezogene Benutzerdaten nicht für kommerzielle oder Marketingzwecke verwendet werden, und ALE stellt sicher, dass lokale Datenschutzgesetze wie die DSGVO in den europäischen Ländern beachtet werden. ALE-Cloud-Dienste sind außerdem nach ISO 27001 für Informationssicherheitsmanagement und CSPN der französischen Regulierungsbehörde ANSSI zertifiziert.

Die Cloud-Dienste von ALE können die Kommunikationsserver des Kunden nutzen. So können Kunden wichtige Geschäfts-kommunikationssysteme bei sich am Standort belassen und sich mit der Cloud verbinden, um innovative Anwendungen und Dienste für die Zusammenarbeit zu nutzen.

Hybride Architektur für eine vereinheitlichte Kommunikation

Die Plattform für Zusammenarbeit und vereinheitlichte Kommunikation ist ein wichtiges Basisinstrument für das Unternehmen. Dass sich die Investition rentiert, zeigt sich jedoch erst deutlich, wenn alle Gruppen damit arbeiten. Dazu müssen die Beteiligten konsultiert und ihre Bedenken berücksichtigt werden, einschließlich des IT-Teams, das für die Sicherheitsrichtlinien zuständig ist.

Zu oft behindern Sicherheitsmaßnahmen die Nutzung innovativer neuer Dienste. Kollaboratives Arbeiten setzt eine intuitive Benutzererfahrung voraus, damit es gut funktioniert. Auf Admin-Seite ist es wichtig, die Kompatibilität der Plattform mit den Umgebungen zu prüfen, die von der IT-Abteilung genehmigt sind, einschließlich der Frage, ob mobile Apps für Android- und IOS-Smartphones und -Tablets zulässig sind. Darüber hinaus müssen die kollaborative Lösung und der Kommunikationsserver über offene APIs miteinander kommunizieren, um die Verwaltung und Steuerung von Telefondiensten und Echtzeit-Austausch zu erleichtern. Dadurch erhalten IT-Teams mehr Kontrolle im Vorfeld.

Alcatel-Lucent Enterprise **Digital Age Communications** (DAC) bietet zur konkreten Umsetzung der digitalen Transformation ein umfassendes Angebot an standort**- und cloudbasierten Lösungen und Diensten für Kommunikation** und Zusammenarbeit an. Die Kommunikationslösungen von ALE ermöglichen störungsfreie Gespräche an jedem Ort, in jeder Situation und über jedes Gerät.

Wichtigste Features von ALE zum Schutz der Kommunikation:

- **Sichere Konnektivität** zwischen dem lokalen ALE-Kommunikationssystem (IP-PBX und Telefone) und der von ALE betriebenen Cloud-Infrastruktur mit gegenseitiger Authentifizierung, Verschlüsselung und Session Border Controller (SBC) zur Sicherung des öffentlichen Netzwerkzugriffs und von Remote-Mitarbeitern, die mit SIP-Clients und -Geräten ausgestattet sind
- **Nahtlose Verbindung** inner- und außerhalb der Organisation. Die zugrunde liegende Kommunikationsinfrastruktur vernetzt die im Hybridmodell arbeitenden Mitarbeiter mit dem Back-Office und den Mitarbeitern im Kundenkontakt, und zwar unabhängig von deren Endgeräten. Dabei wird eine Vielzahl von Standardtechnologien wie PSTN, TDM, IP, SIP, VoWIFI und DECT genutzt. Darüber hinaus erhält die IT Kennzahlen für die Überwachung der Quality of Service (QoS).
- **Hohe Verfügbarkeit** von 5x9s mit räumlich redundanten Architekturen, vor Ort beim Kunden und in einer privaten Cloud gehostet, 100 % softwarebasiert und vollständig virtuell, mit Schutz vor Denial-of-Service-Angriffen (DoS), integrierte Sicherheit mit gehärteter Hardware und Betriebssystemen.
- **Datenschutz und -sicherheit** mit regelbasierter Zugriffs-kontrolle und Verschlüsselung der gespeicherten Daten. So stellen Sie sicher, dass alle wichtigen Daten, die in der wachsenden Geschäftsumgebung gesammelt werden, durchweg optimal geschützt sind und unter Ihrer Kontrolle stehen.
- **Gut geschützte Kommunikation** durch starke Verschlüsselung auf der Grundlage von Industriestandards, die nativ in die Lösung implementiert ist – ganz ohne Abstriche bei der Sprachqualität und -leistung. Das garantiert die von Kunden und Mitarbeitern erwartete Leistung.

Bei jeder Kommunikation besteht die Gefahr, dass sie abgefangen und abgehört wird über das Unternehmensnetz (LAN oder WLAN) und erst recht über das öffentliche Internet. Gegenmaßnahmen auf Ebene der Netzinfrastruktur verringern dieses Risiko (geswitchte LAN-Umgebung, VLAN-Segmentierung, Verwaltung von ACLs zwischen VLANS, Schutz gegen ARP-Spoofing oder Flooding), aber die einzige Möglichkeit eines vollständigen Schutzes ist die komplette Verschlüsselung des Gesprächs während der Übertragung: Selbst wenn jemand in böswilliger Absicht das Gespräch abfängt, bleibt sein Inhalt geschützt, da es nicht entschlüsselt werden kann.

Alcatel-Lucent OmniPCX® Enterprise Purple (OXE Purple) bietet eine integrierte **native Verschlüsselung**, damit jede Kommunikation über das Netz (privates Netzwerk oder öffentliches Internet) verschlüsselt ist.

Grundsätze der OXE Purple Native Encryption

OXE Purple bietet ein Modell für die Geschäftskommunikation im digitalen Zeitalter. Die Lösung verbindet das gesamte Unternehmen und gibt die **Freiheit**, **Agilität**, Qualität und **Sicherheit**, die für geschäftliches Wachstum benötigt wird.

OXE Purple gibt die:

- **Freiheit**, jederzeit mit Kunden und Kollegen in Kontakt zu treten. Im Büro, in der Werkshalle, unterwegs oder zu Hause. Über ein Smartphone, einen Computer oder ein geeignetes Telefon.
- **Agilität** für automatisierte Geschäftskommunikation mithilfe einer privaten Cloud und zur Integration von Echtzeit-Interaktionen in die Geschäftsprozesse.
- **Sicherheit** für alle Interaktionen inner- und außerhalb des Unternehmens, ob mit Kollegen, Partnern, Kunden oder Mitarbeitern eines Contact Centers. Interaktionen sind telefonisch, über eine App auf dem Computer oder Smartphone, per Videokonferenz und über ein sicheres Messaging-System in der Cloud möglich.

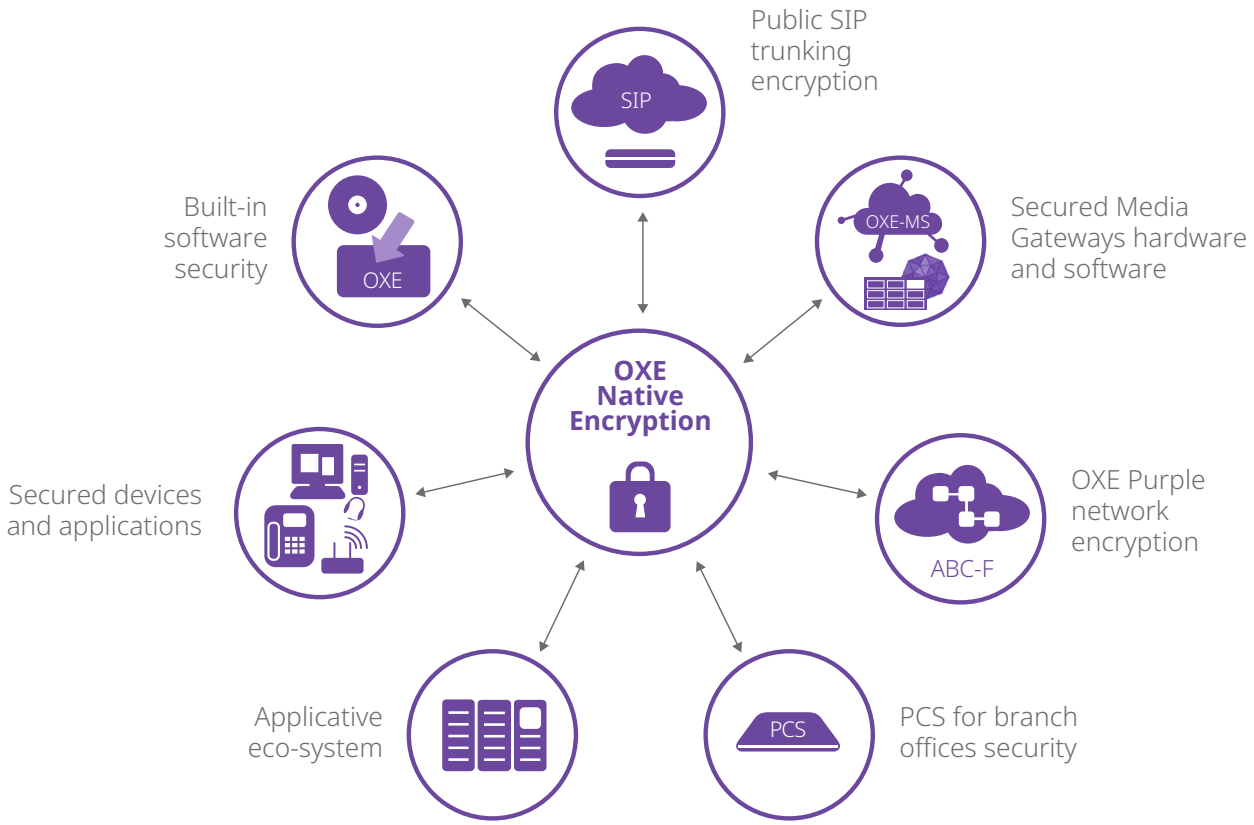
Diese Technologie kann in jeder Umgebung sicher eingesetzt werden: am Standort oder gehostet in einer privaten Cloud. Die Lösung ist **100 % softwarebasiert**, unterstützt **Virtualisierung** und bietet eine **hohe Verfügbarkeit von 5x9s** mit Hot-Redundanz der Kernkomponenten.

Sie bietet Datenschutz und Vertraulichkeit mit modernsten Verschlüsselungsstandards und kompletter Verschlüsselung aller Gespräche in der Übertragung, unabhängig vom Gerät oder der Softwareanwendung. Sie verfügt über eine flexible Architektur, sodass auch sensible Benutzer unter den Mitarbeitern, die IP- oder Nicht-IP-Geräte verwenden, angesprochen werden.

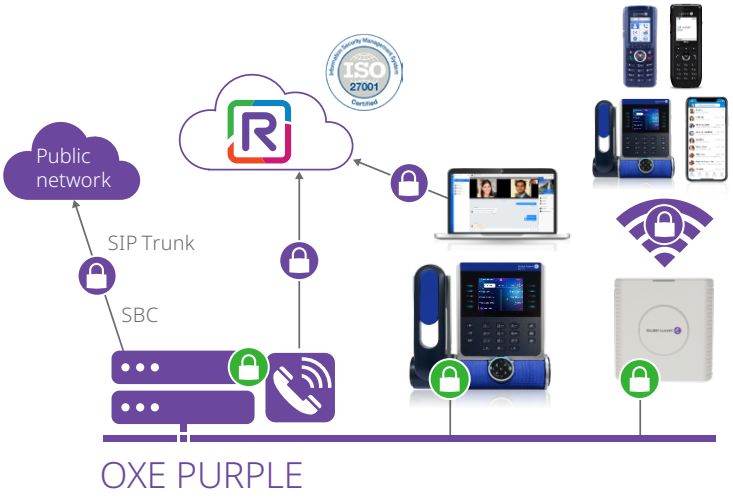
Komponenten der OXE Purple Native Encryption

OXE Purple Native Encryption bietet:

- **Signalflussverschlüsselung** mithilfe der Protokolle Datagram Transport Layer Security (DTLS) oder Transport Layer Security (TLS). Dies gilt für Signalflüsse, die zwischen dem OXE Purple Communication Server und DTLS/TLS-kompatiblen IP-Geräten und Anwendungen ausgetauscht werden.
- **Sprachfluss-Verschlüsselung** mit dem SRTP-Protokoll. Dies betrifft Sprachflüsse, die zwischen DTLS-kompatiblen IP-Geräten und Anwendungen ausgetauscht werden.
- **Gegenseitige Authentifizierung** als Option zwischen Server und Geräten/Clients.
- **Gesicherte IP Media Gateways** (auf Basis reiner Software oder proprietärer Hardware) für verschlüsselte Medienverarbeitung, einschließlich Nicht-IP-Telefone, die mit (digitalen und analogen) Hardware-Karten verbunden sind.
- **Verschlüsselung der Kommunikation** zum öffentlichen Netz über den öffentlichen SIP-Trunk bis zum Border Element des Providers mittels SIP TLS.
- **Verschlüsselung von Gesprächen** mit der Rainbow Client-App (auf Desktop, Web, Android und iOS-Smartphone) über das Rainbow WebRTC Gateway für die interne Kommunikation (zu einem Gerät oder einer anderen Anwendung, die vom OXE Purple Kommunikationsserver verwaltet wird) oder zum öffentlichen Netz.
- **Verschlüsselung der Kommunikation** in einem Netzwerk aus OXE Purple Kommunikationsservern.
- **Unterstützung der Geo-Redundanz** des OXE Purple Kommunikationsservers und des passiven Kommunikationsservers (PCS) für sichere Außenstellen im Survivability-Modus.
- **Eingebettete Zertifizierungsstelle (CA) und Trust Store** für zertifikatsbasierte Authentifizierung mit der Möglichkeit für den Kunden, das Zertifikat für umfassenden Datenschutz mit einer externen Public Key Infrastructure (PKI) anzupassen.



OXE Purple Native Encryption unterstützt die meisten IP-Geräte und Anwendungen, die mit dem Kommunikationsserver verbunden sind (einschließlich Tischtelefone, Softphones und IP-DECT-Basisstationen). Es unterstützt auch die vollständige Verschlüsselung während der Übertragung für Benutzer mit einem Nicht-IP-Gerät (z. B. einem analogen oder digitalen Telefon), das mit einem vom OXE Purple Kommunikationsserver verwalteten Hardware Media Gateway verbunden ist. Darüber hinaus unterstützt das Feature die cloudbasierte kollaborative Anwendung Rainbow™ von Alcatel-Lucent Enterprise.

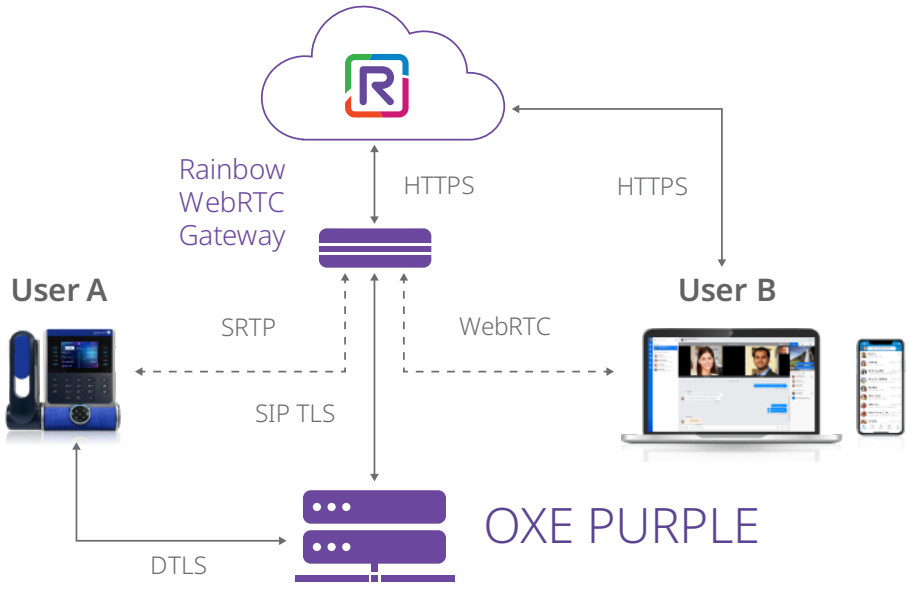


Die Verbindung zwischen dem OXE Purple Kommunikationsserver und den Rainbow Cloud-Diensten wird durch die Softwarekomponente Rainbow WebRTC Gateway sichergestellt.

Das Rainbow WebRTC Gateway generiert ein asymmetrisches Schlüsselpaar und exportiert eine Zertifikatsignierungsanforderung (CSR), die von einer Zertifizierungsstelle (CA) signiert werden muss, bei der es sich um die in den OXE Purple Kommunikationsserver eingebettete Zertifizierungsstelle (CA) oder eine externe Public Key Infrastructure (PKI) handeln kann. Die Identität des Rainbow WebRTC Gateway wird vom OXE Purple Kommunikationsserver während des TLS-Handshake mithilfe der Liste vertrauenswürdiger Zertifikate (CTL) in seinem Trust Store kontrolliert.

Wie in der Abbildung unten gezeigt, werden die Sprachmedien bei der Übertragung zwischen Benutzer A an einem Tischtelefon und Benutzer B, der mit der Rainbow Client-App auf PC/Mac/Web oder Smartphone arbeitet, verschlüsselt. Das Rainbow WebRTC Gateway leitet den SRTP-Datenfluss zwischen Benutzer A und Benutzer B in Echtzeit weiter.

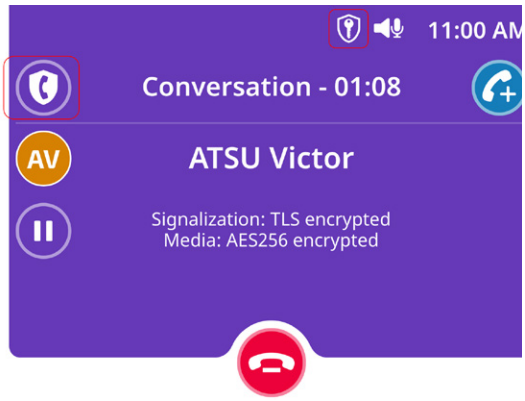
Das Rainbow WebRTC Gateway ist eine vollständig softwarebasierte, virtualisierte Komponente, die für eine bessere Skalierbarkeit Duplizierung und Lastausgleich unterstützt.



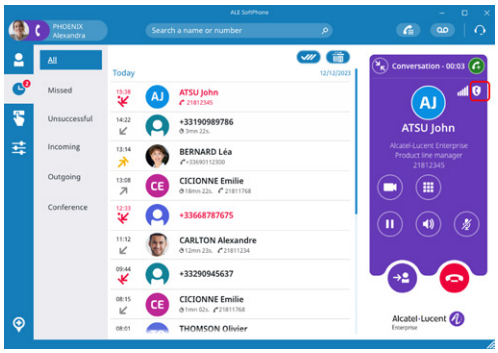
Verschlüsselungssymbol auf ALE-Telefonen und Softphone-Anwendungen

Wenn eine Kommunikation verschlüsselt ist, wird auf dem Telefonbildschirm oder in der Softphone-Anwendung ein Schild- oder Vorhängeschlosssymbol angezeigt. Das erhöht das Vertrauen der Endnutzer in die Vertraulichkeit des Gesprächs.

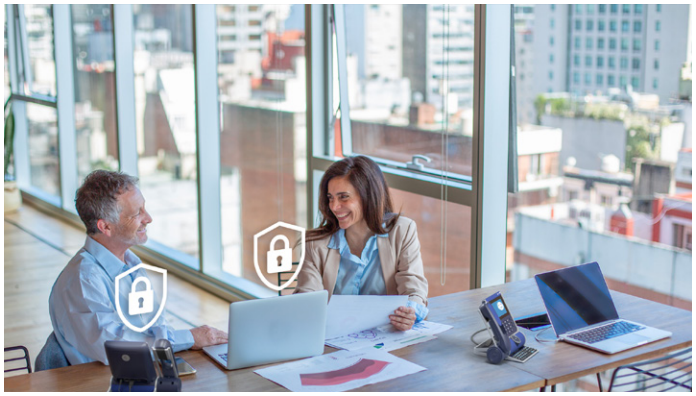
Telefone



Softphones



ALE SoftPhone



Features und Vorteile

Leistungsmerkmale	Vorteile
Client-/Gerätevertraulichkeit (Signalisierungsprotokoll und Datenfluss)	Verhindert Angriffe, Spoofing-Angriffe auf IP-Telefone und Eavesdropping
Gegenseitige Authentifizierung und Integrität der Anrufsteuerungssignalisierung (Gewährleistung, dass Nachrichten nicht geändert wurden) mit der Möglichkeit, Zertifikate zu personalisieren	Schutz der Unternehmenskommunikation vor Denial-of-Service-Angriffen.
Unterstützt DTLS 1.2 und SRTP mit AES 256: • 100 % softwarebasiert • 4096-Bit-SHA2-Zertifikatauthentifizierung • ALE Enterprise und Essential DeskPhones (IP), IP Desktop Softphone, kompatibel mit ALE Premium DeskPhones der S-Serie • GD4-XL / GD4/GD3/INTIP3/OMS und PCS • IP-XBS DECT-Verschlüsselung	Hochmoderne Verschlüsselungsmechanismen für höchsten Schutz und Vertraulichkeit aller Gespräche, unabhängig vom Gerät oder der Software-Anwendung
Unterstützt TLS 1.2 und SRTP mit AES 256: • ALE Enterprise und Essential (ALE-30) DeskPhones im SIP-Modus, ALE-2 und ALE-3, ALE SoftPhone • SIP-Trunks • Rainbow WebRTC Gateway-Verschlüsselung	Schutz von Gesprächen inner- und außerhalb des Unternehmensnetzwerks, einschließlich des öffentlichen Netzwerkzugangs über SIP-Trunks
Verschlüsselungssymbol auf dem Telefon und in der Softphone-Anwendung, um anzuzeigen, dass der Anruf verschlüsselt und sicher ist	Vertrauen der Endnutzer in die Vertraulichkeit des Gesprächs
Verschlüsselung von Anrufen während der Übertragung mit der Rainbow-App über das Rainbow WebRTC Gateway	Garantierte Vertraulichkeit der Gespräche für Mitarbeiter, die die Rainbow Client-App auf PC/Mac, Web, Android-Smartphone und iPhone verwenden
Verschlüsselung der Gesprächsaufzeichnung mit Alcatel-Lucent OmniPCX® RECORD Suite	Garantierte Vertraulichkeit der aufgezeichneten Gespräche
Integrierte softwarebasierte Verschlüsselungsfunktion für die OmniPCX Enterprise Purple-Lösung	Implementierung strenger Sicherheitsprozesse, ohne dass das Kommunikationssystem schwieriger zu verwalten wird
Keine Auswirkungen auf QoS-Einstellungen (Quality of Service) und Netzwerkkonfiguration	Einfache Bereitstellung und Konfiguration, ohne dass Änderungen an der Netzinfrastruktur erforderlich sind
Geografische Redundanz und Unterstützung der Survivability lokaler Zweigstellen	Geschäftskontinuität in jeder Situation ohne herabgesetzte Vertraulichkeit bei Ausfällen des Netzwerks, der Server oder Datenzentren

Empfehlungen und bewährte Verfahren von ALE

Behörden und öffentliche Einrichtungen sind vermehrt das Ziel von Cyberangriffen. Daher muss die sicherste Technik zum Einsatz kommen, die auf dem Markt erhältlich ist. Die integrierten Verwaltungstools müssen Ihnen eine Kontrolle der Sicherheit über alle Komponenten hinweg ermöglichen.

Darüber hinaus ist die Kommunikationslandschaft durch Mobilgeräte im Umbruch. Es steigt der Sicherheitsbedarf, denn Cyberkriminelle machen sich das wachsende Code-Volumen an unterschiedlichen Zugangspunkten zu Nutze. Von der Verschlüsselung auf militärischem Niveau über den Datenschutz bis hin zur sicheren Kommunikation: Alles erfordert eine sichere, hochverfügbare und leistungsstarke Infrastruktur, die sich einfach verwalten lässt.

ALE empfiehlt:

Update und Überwachung Ihres Kommunikationssystems:

- System-Updates sind für die Cybersicherheit hochwichtig. So bleiben Ihre Kommunikationssysteme auf dem neuesten Stand und sind vor Sicherheitsrisiken in der Software geschützt.
- Aktivieren Sie die Überwachung Ihres Kommunikationssystems, um verdächtige Aktivitäten zu verfolgen, indem Sie Nutzungsschwellenwerte und Alarme im Netzwerkmanagementsystem konfigurieren.

Authentifizierung und Verschlüsselung:

- Ermöglichen Sie die gegenseitige Authentifizierung zwischen allen Geräten (Telefonen und Gateways) und dem Kommunikationsserver mit personalisierten Zertifikaten in den sensibelsten Umgebungen
- Die Signalisierung muss verschlüsselt sein, um Protocol-Poisoning- und Man-in-the-Middle-Angriffe zu verhindern.
- IP-Kommunikation muss verschlüsselt werden, um ein Abhören zu vermeiden.

Redundantes Kommunikationssystem inklusive Sicherheitskomponente:

- Risiken können niemals ganz ausgeräumt werden. Wenn ein Gateway oder das Kommunikationssystem ausfällt, kann ein Back-up-System nahtlos übernehmen, sofern eine räumliche Redundanz vorhanden ist.
- Fügen Sie die notwendigen Komponenten zum Schutz Ihres Kommunikationssystems hinzu, wie z. B. einen Session Border Controller (SBC) oder einen Reverse-Proxy (RP). Über Benachrichtigungsserver werden die notwendigen Personen alarmiert.

Information und Schulung:

- Benutzer und Administratoren schulen; wenden Sie Best Practices in Ihren Teams an, einschließlich Erinnerungen für die Aktualisierung von Passwörtern, schulen Sie Benutzer im Kampf gegen Cyberkriminalität und wie Sie einen verschlüsselten Anruf am Schild- oder Vorhängeschlosssymbol auf dem Telefon erkennen

Weitere Informationen finden Sie in unseren zusätzlichen Ressourcen:

Broschüre OmniPCX Enterprise Purple

Datenblatt OmniPCX Enterprise Purple

Absicherung von Unified Communications- und Collaboration-Lösungen

Alcatel·Lucent Enterprise