Schützen Sie Ihr Unternehmen auch im Homeoffice

Sebastien Roche ist Chief Information Security Officer bei Alcatel-Lucent Enterprise.
Er beschreibt, mit welchem Konzept ALE für geschäftliche Kontinuität und Sicherheit sorgt.

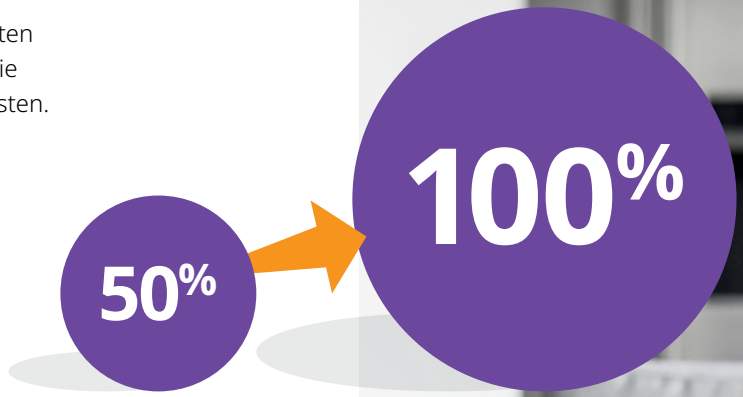
Broschüre

Alcatel·Lucent
Enterprise

Telearbeit: der Berufsalltag im Homeoffice

Seit 2020 sind Unternehmen, die zuvor kein Homeoffice angeboten hatten, gezwungen, sich organisatorisch neu aufzustellen, um die Kontinuität und Sicherheit ihres Geschäftsbetriebs zu gewährleisten.

Bereits vor über 15 Jahren bot Alcatel-Lucent Enterprise seinen Mitarbeitern an, von zu Hause aus zu arbeiten. Über 50 % der Mitarbeiter in den 50 Büros weltweit nahmen das Angebot an. Da schon über die Hälfte der ALE-Belegschaft von zu Hause aus arbeitete, hatten wir bereits das notwendige Netzwerk und die erforderliche IT-Architektur dafür. Die eigentliche Herausforderung bestand darin, den Anteil der Mitarbeiter im Homeoffice von 50 auf 100 % zu katapultieren.



Einsatzbereit

Seit fast 10 Jahren bereits durchläuft ALE eine umfassende IT-Transformation. Es wurde eine Netzwerkarchitektur für eine sichere Cloud eingeführt, um Gefahren proaktiv abzublocken, potenzielle Angriffe zu identifizieren und den Mitarbeitern einen sicheren Zugang zu bieten.

Zur Transformation gehörte:

- Sicherheit in der Cloud mit virtuellen Access Points
- Nachverfolgung in Echtzeit
- Erkennen ungewöhnlicher Verhaltensmuster, um Gefahren besser aufspüren zu können

Broschüre
Schützen Sie Ihr Unternehmen auch im Homeoffice

Broschüre
Schützen Sie Ihr Unternehmen auch im Homeoffice

Agil auf Krisen reagieren – dank guter Vorbereitung

Als die Krise zuschlug, wurde Freitagnachmittag entschieden, direkt am Montag mit der Telearbeit anzufangen. Die Mitarbeiter wurden gebeten, ihre Laptops und Monitore mit nach Hause zu nehmen. Am Montagmorgen lief alles ohne Unterbrechung weiter – mit dem Unterschied, dass unsere Leute im Homeoffice saßen. Das zuvor umgestaltete Netzwerk sorgte für eine sichere Verbindung – unabhängig vom Standort der einzelnen Mitarbeiter.

Der Zugang als Herausforderung

Die Nutzerprofile stellten eine große Herausforderung für unseren Homeoffice-Plan dar. Insbesondere die Forschungs- und Entwicklungsteams und der technische Support benötigen Zugang zu bestimmten Servern und Entwicklungsplattformen, was mit unserer Remote-Zugriffslösung nicht möglich war.

Als wir damit anfingen, den Zugang aller Mitarbeiter auf Telearbeit umzustellen, passten wir auch unsere Infrastruktur an. Das sollte unsere Bandbreite vergrößern und den erhöhten Bedarf an Remote-Verbindungen im Homeoffice abdecken.

Schlüsselfaktor Sicherheit

Die Sicherheit und der Schutz der Unternehmensdaten haben in unsicheren Zeiten absolute Priorität. Das ist ein Knackpunkt für viele Organisationen, die sensible Daten verarbeiten – vom öffentlichen Dienst über Ministerien bis hin zur Stadt- und Gemeindeverwaltung.

Zunächst einmal installierten wir bei Alcatel-Lucent Enterprise eine verteilte und gesicherte Infrastruktur – noch bevor wir uns überhaupt mit den Thema Telearbeit auseinandersetzten. Außerdem richteten wir eine vollständig Cloud-basierte private Verbindungslösung ein, um allen Mitarbeitern einen sicheren Fernzugriff auf das Netzwerk zu ermöglichen. Einige der Teams hatten einen speziellen Bedarf. Für sie behielten wir die alte VPN-Lösung bei – beispielsweise, um ihnen den Betrieb eines IP-Telefons im Homeoffice zu ermöglichen. Außerdem stellten wir unseren Mitarbeitern professionelle PCs zur Verfügung, die sie mit automatischen Software-Downloads und -Updates versorgen.

Nie wieder Sicherheitslücken

Wie nicht anders zu erwarten, stieg durch die verstärkte Telearbeit auch die Zahl der Anrufe und E-Mails: Die User meldeten verdächtige E-Mails und wollten ihre Passwörter aktualisieren. Auch Phishing-Versuche und gezielte Angriffe auf anfällige Software-Komponenten nahmen zu.

Zwar ist Alcatel-Lucent Enterprise dank Proxies vor größeren Sicherheitsproblemen geschützt. Trotzdem kommt es jeden Tag zu neuen Verstößen gegen die Cybersicherheit – sei es durch E-Mails, Downloads oder nicht aktualisierte Software/OS-Versionen.

Im Gespräch bleiben

Bei ALE stehen wir in ständiger virtueller Verbindung mit den ALE-Teams.
Wir kommunizieren regelmäßig miteinander, tauschen Tipps und bewährte Vorgehensweisen aus und sorgen dafür, dass unser Team zur Unterstützung aller Mitarbeiter zur Verfügung steht.

ALE-Checkliste für sichere Telearbeit:

- Erlauben oder unterstützen Sie nicht die Verwendung persönlicher Geräte (PCs) für den Datenaustausch und die Kommunikation im beruflichen Umfeld.
- Geben Sie Ihren Mitarbeitern im Homeoffice einen privaten und sicheren Zugang.
- Automatisieren Sie die Software-Upgrades im gesamten Unternehmensnetzwerk.
- Achten Sie auf verdächtige E-Mails.
- Verwenden Sie zertifizierte Software. Nutzen Sie Audits und Zertifikate, um Software zur authentifizieren.
- Vereinfachen Sie Ihre Entscheidungsprozesse. Im Notfall muss ein CISO oder CIO schnelle Entscheidungen treffen, um Probleme zu beheben, damit alle Dienste verlässlich weiterlaufen.

Sechs Empfehlungen von ALE für sichere Konnektivität im Remote-Betrieb

1. Automatisch an Passwortänderungen erinnern

Helfen Sie Ihren Mitarbeitern, ihre Firmenpasswörter zu ändern, bevor sie ablaufen. Vor Ablauf der Gültigkeit erhalten die Mitarbeiter noch am selben Tag eine E-Mail mit einer Bitte, das Passwort zu ändern. Die E-Mail enthält auch die notwendigen Anweisungen.

2. Datensicherung in der Cloud aktivieren

Ermöglichen und unterstützen Sie eine regelmäßige Datensicherung, um bei Problemen mit dem Laptop einem Datenverlust vorzubeugen. Geben Sie Speicherplatz zur Datensicherung frei und bieten Sie Unterstützung durch ein IT-Servicedesk oder einen IT-Spezialisten aus der Distanz an.

3. Auf bewährte Verfahren zum Schutz der Geräte hinweisen

Achten Sie darauf, dass Ihr Laptop immer top in Schuss ist:

- Schalten Sie den Laptop am Ende des Tages aus. Verwenden Sie nicht den Standby-Modus oder den Sperrbildschirm.
- Halten Sie Ihren Laptop fern von Wärmequellen wie Sonnenlicht oder Heizgeräten.
- Vermeiden Sie es, am Laptop zu essen oder zu trinken.
- Halten Sie die Kabel von Kindern und Haustieren fern.

4. Den Fokus auf die Sicherheit richten

Klären Sie Ihre Teams über Risiken und bewährte Sicherheitsverfahren auf:

- Bitten Sie Ihre Mitarbeiter darum, Links in E-Mails nicht unbedacht anzuklicken – selbst, wenn es so aussieht, als stamme die Nachricht von einer vertrauenswürdigen Person.
- Bieten Sie für Zweifelsfälle eine Betreuung durch den IT-Service an.
- Stellen Sie Melde-Tools für verdächtige E-Mails bereit.
- Nutzen Sie die Gamification, um das Sicherheitsbewusstsein zu steigern. Alcatel-Lucent Enterprise spornt über entsprechende Tools seine Mitarbeiter dazu an, verdächtige E-Mails zu erkennen und zu melden.

5. Kommunizieren

Die Arbeit in Isolation macht Ihre Mitarbeiter anfälliger für Cyber-Angriffe. Finden Sie Wege, um die Verbindung zu Ihren Teams aufrechtzuhalten:

- Planen Sie regelmäßige Aktualisierungen, virtuelle Treffen und Events. Richten Sie Plattformen zur Zusammenarbeit ein oder halten Sie Happy Hours ab.
- Ermutigen Sie die Mitarbeiter dazu, sich regelmäßig mit ihren Teams zu treffen.
- Verschicken Sie regelmäßig E-Mails, in denen Sie Ihre Mitarbeiter wissen lassen, dass ihnen das IT-Team gern weiterhilft. Rufen Sie den Leuten darin auch immer wieder bewährte Vorgehensweisen ins Gedächtnis, die der Sicherheit zuträglich sind.

6. Gesunden Arbeitsrhythmus fördern

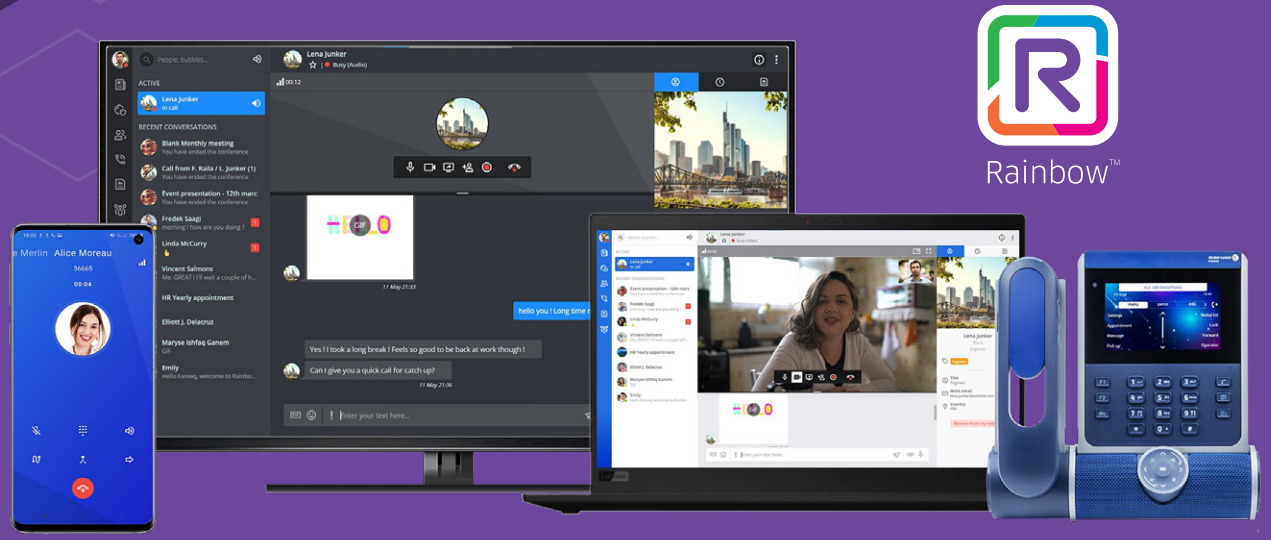
Das Risiko bei der Telearbeit ist, dass Ihre Leute 12 Stunden am Stück online sind oder ein Meeting nach dem anderen abhalten. Ermutigen Sie Ihre Kollegen dazu, sich Auszeiten zu nehmen und das System herunterzufahren, um Zeit mit der Familie oder im Freien zu verbringen.

Broschüre
Schützen Sie Ihr Unternehmen auch im Homeoffice

Rainbow™ by Alcatel-Lucent Enterprise für vernetzte Zusammenarbeit

Rainbow ist eine Cloud-Plattform zur Zusammenarbeit mit Chat-, Video- und Sprachanruf-Funktionen. Das System unterstützt den gemeinsamen Zugriff auf Bildschirme und Dokumente. Es bietet den ALE-Mitarbeitern alle Dienste, die sie fürs vernetzte Teamwork brauchen. Die Plattform wird intensiv für die Zusammenarbeit mit Kollegen, Kunden und Geschäftspartnern genutzt und ist für externe Anrufe mit der Telefonanlage verbunden.

Darüber hinaus vertrauen auch unsere Partner und Kunden auf Rainbow als Teamwork-Plattform ihrer Wahl. Rainbow berücksichtigt die Sicherheitsanforderungen des öffentlichen Dienstes, des Verteidigungssektors, des Gesundheitswesens und anderer spezifischer Sektoren. Die Plattform erfüllt strenge Sicherheitsstandards, darunter die DSGVO und die HDS-Vorgaben. Rainbow ist nach ISO 27001 und CSPN von ANSSI zertifiziert.



Rainbow™

Broschüre
Schützen Sie Ihr Unternehmen auch im Homeoffice

Arbeiten aus der Distanz – vollständig sicher

Unternehmen geben mehr Mitarbeitern die Möglichkeit, aus der Distanz zu arbeiten. Gleichzeitig bestätigen Analysten das erhöhte Risiko von Cyberangriffen.

Bei ALE nutzen wir für die Kommunikation und Kooperation die Anwendungen und Dienste, die wir auch für unsere Kunden bereitstellen. Bei diesen Lösungen ist die Cybersicherheit von Anfang an mitgedacht, unabhängig von den Einsatzbedingungen – im Büro, per Remote-Zugriff oder unterwegs. Die beste Garantie, die wir unseren Kunden geben können: Diese Lösungen sind nicht nur von internationalen Sicherheitsbehörden zertifiziert und entsprechen den geltenden Vorschriften, sondern wir setzen sie auch tagtäglich mit vollem Vertrauen für Tausende von ALE-Mitarbeitern auf der ganzen Welt ein.

Auf unserer Website erhalten Sie weitere Informationen.

© 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. DID20060201DE (Oktober 2024)

Alcatel·Lucent
Enterprise