Kriterien und Lösungen für den digitalen Arbeitsplatz im öffentlichen Sektor

Alcatel·Lucent
Enterprise

E-Book

Inhaltsverzeichnis

Übersicht

In sämtlichen öffentlichen Einrichtungen arbeiten Beschäftigte, die wichtige Verwaltungsaufgaben erledigen, auf die wir alle angewiesen sind. Ihre Rolle darf nicht unterschätzt werden. Sie haben oft direkte Auswirkungen auf das Leben vieler Tausend Menschen.

Die Digitalisierung ist schon seit einiger Zeit im Gange. Der öffentliche Dienst steht bereits seit längerem unter dem Druck, seine Leistungen verbessern und die Kosten senken zu müssen. Die Pandemie hat diesen Trend noch beschleunigt. Allerdings war vor zwei Jahren nicht abzusehen, dass ein so hoher Prozentsatz der Beschäftigten im öffentlichen Dienst in das Homeoffice wechseln würde und dass sich eine verteilt arbeitende Belegschaft herausbilden würde.

Die Herausforderungen der Arbeitnehmer, die eine digitalere Welt erwarten, und die komplexen Anforderungen an die Unterstützung einer verteilt arbeitenden Belegschaft haben dazu geführt, dass die öffentlichen Einrichtungen von temporären Lösungen zu dauerhafteren Lösungen übergehen müssen, um die neue hybride Belegschaft zu unterstützen.

Deloitte[1] erläutert in einer hervorragenden Grafik, wie der digitale Arbeitsplatz aufgebaut ist und welche Vorteile er bietet.

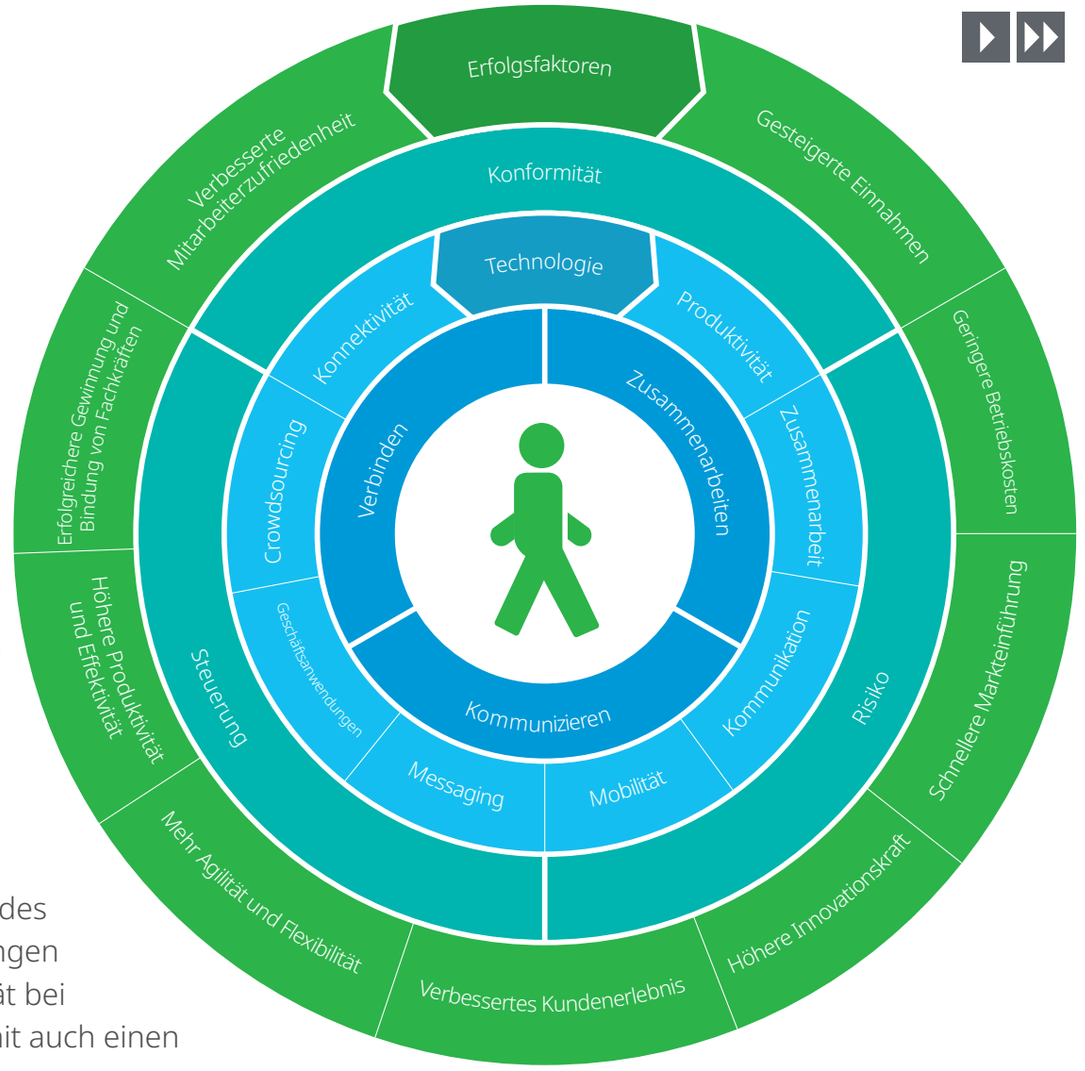
Die Technologie bietet Tools zur Verbesserung der Kommunikation und Zusammenarbeit, und zwar unabhängig von Standort und Gerät. Allerdings kann es sich als schwierig erweisen, die richtige Technologie für das gewünschte Ergebnis zu finden.

Alcatel-Lucent Enterprise hat mit Kunden auf der ganzen Welt zusammengearbeitet, um deren neue Herausforderungen zu verstehen und digitale Technologielösungen anzubieten, die es den Mitarbeitern ermöglichen, von überall aus und mit jedem Gerät zu arbeiten. Der digitale Arbeitsplatz hat für die Beschäftigten des öffentlichen Sektors Effizienzsteigerungen gebracht, die eine höhere Produktivität bei weniger Reisen ermöglichen und damit auch einen Gewinn für die Umwelt bedeuten.

Dieses E-Book befasst sich mit drei Schlüsselelementen des digitalen Arbeitsplatzes im öffentlichen Sektor:

- Kommunikation und Zusammenarbeit
- Konnektivität
- Sicherheit

Außerdem werden wir uns mit ALE-Lösungen befassen, die öffentlichen Einrichtungen dabei helfen können, den Umstieg auf den digitalen Arbeitsplatz mit Flexibilität, Agilität und Sicherheit zu meistern.



1 - https://www2.deloitte.com/content/dam/Deloitte/be/Documents/technology/The_digital_workplace_Deloitte.pdf

Wichtige Kriterien für den digitalen Arbeitsplatz im öffentlichen Sektor

Kommunikation und Zusammenarbeit

Heutzutage pendeln die Mitarbeiter zwischen ihrem Arbeitsplatz zu Hause, in Außenstellen und im Büro. Das Büro ist nicht mehr zwangsläufig der Ort, an dem das Alltagsgeschäft erledigt wird. Vielmehr wird es eher für Gruppenbesprechungen, Schulungen und persönliche Termine mit Bürgern genutzt. Die Mitarbeiter müssen nicht mehr an einem einzigen bestimmten Ort arbeiten und sich dort mit ihren Teams austauschen. Dies hat sich grundlegend auf das Arbeitsumfeld ausgewirkt, sodass Kommunikation und Zusammenarbeit wichtiger sind als je zuvor.

Kommunikation ist eine entscheidende Komponente für einen gelungenen digitalen Arbeitsplatz. Es gilt, die Mitarbeiter involviert, produktiv und motiviert zu halten. Die Mitarbeiter benötigen Kommunikationstools, die ihr Alltagsgeschäft unterstützen und ihnen die Kommunikation und Zusammenarbeit mit Kollegen, Teams und Bürgern ermöglichen, unabhängig vom Standort des Arbeitsplatzes und vom verwendeten Gerät.

Für eine wirklich vernetzte Kommunikation empfehlen wir:

- Erweiterte Kommunikationsfunktionen für Mitarbeiter, einschließlich hochwertiger Sprachfunktionen, Gruppenchats, Sprachnachrichten und der Möglichkeit, auf jedem Gerät von einem Telefonat zu einem Video zu wechseln
- Funktionen für die Zusammenarbeit wie das Teilen von Bildschirmen, die Fernsteuerung des Desktops und die gemeinsame Nutzung großer Dateien
- Sichere Kommunikation und Zusammenarbeit mit externen Ansprechpartnern
- Störungsfreie Gespräche in der gesamten Organisation mit sofortiger Verbindung und einem einheitlichen Adressverzeichnis
- Einen Sendekanal für Neuigkeiten, der alle Beteiligten über die neuesten Mitteilungen oder Vorschriften auf dem Laufenden hält
- Intuitive Kommunikation und Zusammenarbeit

Um sicherzustellen, dass die Mitarbeiter alles haben, was sie brauchen, empfehlen wir:

- Eine Bewertung von Benutzerprofilen und Kommunikationsanforderungen, basierend auf den Aufgaben der Mitarbeiter, ihrer Mobilität und der Notwendigkeit, auf Geschäftsanwendungen zuzugreifen
- Optimierte Endgeräte für die Beschäftigten vor Ort, die einen schnellen Zugriff auf Informationen und Kommunikation von unterwegs aus ermöglichen

- Sicherstellung, dass die Mitarbeiter des Bürgeramts optimierten Zugriff auf das Anruf- und Interaktionsmanagement haben, integriert in CRM- oder Geschäftsanwendungen
- Zusammenarbeit mit Back-Office-Mitarbeitern, um den Bürgerservice und die Lösungsquote bei Erstanfragen zu verbessern
- Bewertung regionaler/landesspezifischer, rechtlicher Anforderungen zur Wahrung des Datenschutzes

Um eine besonders effiziente Arbeit im Homeoffice zu gewährleisten, empfehlen wir:

- Funktionen für Gruppenchats sowie Audio- und Videokonferenzen mit Bildschirmfreigabe zur Zusammenarbeit auf jedem Endgerät
- Störungsfreie Gespräche mit einer zentralen Basisinfrastruktur, die alle Profile miteinander vernetzt
- Eine DeskPhone-Option für Mitarbeiter, die mehr als eine Stunde am Telefon verbringen und wichtige Anrufe bearbeiten, beispielsweise Beschäftigte im Bürgeramt, Gesundheitswesen und in Einsatzzentralen für Notfälle
- Kommunikation innerhalb der bevorzugten Geschäftsanwendung, um die Benutzerakzeptanz zu fördern und den Arbeitsplatz möglichst ordentlich zu halten
- Sicherer Fernzugriff zum Schutz sensibler Daten

E-Book
Kriterien und Lösungen für den digitalen Arbeitsplatz im öffentlichen Sektor

Konnektivität

Der digitale Arbeitsplatz ist auf hochwertige, belastbare und sichere Verbindungen angewiesen. In dem Maße, in dem sich neue Arbeitsmodelle durchsetzen und der digitale Arbeitsplatz Gestalt annimmt, muss die digitale Infrastruktur vorhanden sein, um die Mitarbeiter miteinander zu vernetzen. Unabhängig vom Standort müssen einige wichtige Punkte berücksichtigt werden.

- Die Sicherheit muss oberste Priorität haben. Erforderlich ist eine Netzwerklösung mit mehreren Sicherheitsebenen innerhalb des Netzwerks. Ein Zero-Trust-Framework geht davon aus, dass alle Endgeräte und Nutzer ein Sicherheitsrisiko darstellen. Die Netzwerkzugangskontrolle muss aktiviert sein.
- Der sichere Zugriff auf Anwendungen an jedem Ort macht benutzerbasierte Zugangsverbindungen erforderlich. Benutzerbasierte Profile bieten sichere und flexible Konnektivität ohne Serviceverlust, unabhängig vom Standort.
- Remote-Mitarbeiter mit hohen Anforderungen an Sicherheit und Datenschutz müssen in der Lage sein, sich von zu Hause oder von Zweigstellen aus mit dem Unternehmensnetzwerk zu verbinden. Dadurch wird sichergestellt, dass die Unternehmensrichtlinien und die Sicherheit eingehalten werden und das IT-Team die Kontrolle behält.
- Beschäftigte nutzen inzwischen Laptops für Echtzeitanwendungen (Sprache, Video) im Büro und zu Hause. Für viele öffentliche Einrichtungen ist dies eine große Umstellung. Das drahtlose Netzwerk muss in der Lage sein, eine größere Anzahl von Echtzeitanwendungen in einem größeren Gebiet zu unterstützen. Dies sollte bei der Planung des Netzwerks berücksichtigt werden.
- Die Ausfallsicherheit des drahtlosen Netzwerks ist auf der Prioritätenliste nach oben gerückt, da sich immer mehr Arbeitnehmer drahtlos verbinden. Ein verteiltes, drahtloses Netzwerk mit intelligenten Access Points bedeutet, dass es keinen einzelnen Ausfallpunkt gibt und dass im Falle eines Ausfalls eines Access Points andere Access Points im Netzwerk den Dienst übernehmen. Ein verteiltes, drahtloses, intelligentes Netzwerk macht zudem eine Duplizierung des Netzwerks überflüssig. Dies spart sowohl Zeit als auch Geld.
- Das gestiegene Tempo der digitalen Transformation erzeugt Druck auf das IT-Team, das bereits mit den alltäglichen Aufgaben beschäftigt ist. Daher sollte geprüft werden, welche Effizienzgewinne erzielt werden können. Die Verringerung der Anzahl von Verwaltungsschnittstellen und Betriebssystemen im Netzwerk senkt den Arbeitsaufwand und die Einarbeitungszeit. Darüber hinaus wird eine Automatisierung die Zeit für die Bereitstellung und das betriebliche Netzwerkmanagement reduzieren.
- Ein hochwertiger Zugang ist unerlässlich. Der digitale Arbeitsplatz schafft Effizienz und ermöglicht eine höhere Produktivität. Wenn jedoch die Konnektivität nicht ausreicht, geht die gestiegene Produktivität verloren.

Sicherheit

Kommunikationssicherheit

Behörden und öffentliche Einrichtungen sind ein wichtiges Ziel von Cyberangriffen. Daher muss die sicherste Technik zum Einsatz kommen, die auf dem Markt erhältlich ist. Die integrierten Verwaltungstools müssen Ihnen Sicherheitskontrollen über alle Komponenten hinweg ermöglichen.

Darüber hinaus verwandeln Mobilgeräte derzeit das Gesicht der Kommunikationstechnik. Dadurch steigt der Sicherheitsbedarf. Cyberkriminelle machen sich nämlich das steigende Code-Volumen an unterschiedlichen Zugangspunkten zu Nutze. Von der Verschlüsselung über den Datenschutz bis hin zur sicheren Kommunikation: Alles muss die Anforderungen moderner Sicherheitssysteme erfüllen. Dies erfordert eine sichere, stets verfügbare und leistungsstarke Infrastruktur, die sich einfach verwalten lässt.

Unsere Empfehlungen:

Aktualisieren und überwachen Sie Ihr Kommunikationssystem:

- Systemaktualisierungen sind für die Cybersicherheit von entscheidender Bedeutung. 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 (Telefone und Gateways) und dem Kommunikationssystem.
- 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.

Machen Sie Ihre Systeme überflüssig und fügen Sie eine Sicherheitskomponente hinzu:

- Risiken können niemals ganz ausgeräumt werden. Doch wenn ein Gateway oder das Hauptkommunikationssystem 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 oder einen Reverse-Proxy, während Benachrichtigungsserver verwendet werden, um die notwendigen Personen zu alarmieren.

Information und Schulung:

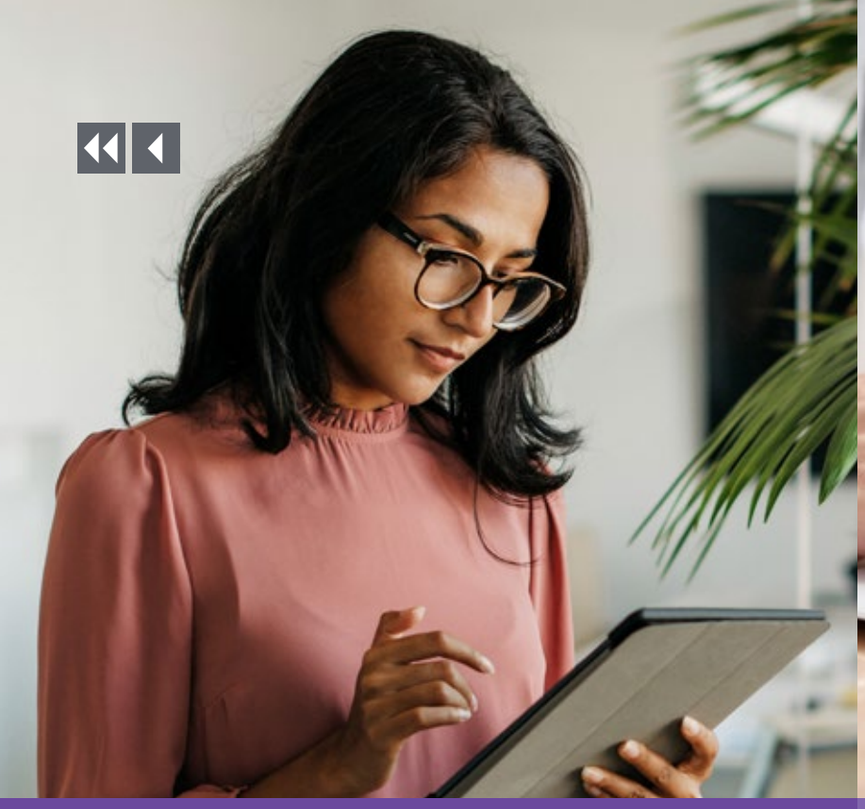
- Informieren Sie Benutzer und Administratoren; wenden Sie in Ihren Teams Best Practics an, z. B. Erinnerungen an die Aktualisierung von Kennwörtern, schulen Sie die Benutzer im Kampf gegen Cyberkriminalität und erklären Sie ihnen, wie sie einen verschlüsselten Anruf an dem Vorhängeschloss-Symbol auf dem Telefon erkennen können.

Netzwerksicherheit

Das Thema Cybersicherheit hat in Behörden bereits seit Langem höchste Priorität. Durch die digitale Transformation ändern sich jedoch auch die Anforderungen an die Cybersicherheit. Die Transformation schreitet immer schneller voran. Die alten Methoden der Netzwerksicherheit von gestern sind heute praktisch schon wieder veraltet. Als grundlegender Bestandteil der Netzwerkarchitektur muss die Sicherheit von Anfang an integriert und universell auf alle Netzwerkzugänge – kabelgebunden und drahtlos – ausgedehnt werden. Im Folgenden finden Sie einige Bereiche, die Sie bei der Absicherung Ihres Netzwerks auf allen Ebenen berücksichtigen sollten.

- **Benutzerebene:** Sorgen Sie dafür, dass Benutzer immer mit den richtigen Zugriffsrechten authentifiziert und autorisiert werden (mithilfe von Richtlinien und Profilen).
- **Geräteebene:** Vergewissern Sie sich, dass Endgeräte authentifiziert werden und den festgelegten IT-Sicherheitsregeln entsprechen. Dies kann mit Agenten erreicht werden, die auf den Endgeräte installiert werden und einen schnellen Sicherheitsscan durchführen, bevor die Endgeräte mit dem Netzwerk verbunden werden. Der Scan kann beispielsweise sicherstellen, dass die Endgeräte, die dem Netzwerk angegliedert werden, über eine aktuelle Antiviren-Software und die neueste Version des Betriebssystems verfügen.
- **Anwendungsebene:** Legen Sie Regeln für bestimmte Anwendungen fest (z. B. Blockierung, Begrenzung der Bandbreite oder Festlegung, wer sie nutzen darf).
- **Intelligente Analytik:** Die Analysefunktionen in Switches und Access Points helfen dabei, Transparenz und detaillierte Informationen über das Netzwerk, die Nutzer, die Endgeräte und die im Netzwerk genutzten Anwendungen zu liefern. Sie können auch Deep-Packet-Inspection-Funktionen bereitstellen, die die Art der Daten und Anwendungen erkennen, die sich durch das Netzwerk bewegen, und es ermöglichen, ungewöhnliche Netzwerkverkehrsmuster sowie unbefugte Aktivitäten und ein Eindringen in das Netzwerk zu erkennen.
- **Verfahren zur Netzwerksegmentierung**: Die Platzierung von IoT-Geräten in sicheren virtuellen Containern ermöglicht es mehreren Geräten und Netzwerken, dieselbe physische Infrastruktur zu nutzen, während sie vom Rest des Netzwerks isoliert bleiben. Tritt eine Sicherheitsverletzung in einem Teil des virtuellen Netzwerks auf, hat sie keine Auswirkungen auf andere Bereiche des Netzwerks oder Anwendungen.

Diese Sicherheitsverfahren helfen beim Aufbau eines Zero-Trust-Frameworks, der nächsten Stufe der Netzwerkarchitektur. Diese beruht auf dem Grundgedanken „Vertraue nie – überprüfe immer“. Daher müssen alle Benutzer authentifiziert, autorisiert und kontinuierlich überprüft werden, bevor sie Zugriff auf Anwendungen und Daten erhalten.



Digitaler Arbeitsplatz

Flexible Cloud-Modelle

Zusammenführen, was zusammengehört

ALE-Lösungen für den digitalen Arbeitsplatz im öffentlichen Sektor

Kommunikation und Zusammenarbeit

Alcatel-Lucent Enterprise Digital Age Communications (DAC) bietet ein umfassendes Angebot an lokalen und Cloud-basierten Lösungen und Diensten für Kommunikation und Zusammenarbeit, die der digitalen Transformation Rechnung tragen. Der digitale Arbeitsplatz entwickelt sich zu einer standortübergreifenden Arbeitsumgebung, in der Remote-Arbeit zur Normalität geworden ist. Dies macht die Echtzeitkommunikation zu einem unerlässlichen Bindeglied zwischen Kollegen, Bürgern und Partnern. Die Kommunikationslösungen von Alcatel-Lucent Enterprise ermöglichen störungsfreie Gespräche an jedem Ort, in jeder Situation und von jedem Gerät aus.

Wichtige Kommunikationsmerkmale von ALE:

- **Nahtlose Verbindung** innerhalb und außerhalb der Organisation. Die zugrunde liegende Kommunikationsinfrastruktur vernetzt die im Hybridmodell arbeitenden Beschäftigten mit Back-Office- und Front-Line-Mitarbeitern, und zwar völlig unabhängig von deren Endgeräten. Dabei wird eine Vielzahl von Standardtechnologien wie PSTN, TDM, IP, SIP, VoWIFI und DECT genutzt. Darüber hinaus stellt sie der IT Messdaten für die Überwachung der Quality of Service (QoS) zur Verfügung.
- Die **Telefonweiterleitung** über das Geschäftstelefon und das Softphone eignet sich perfekt für die hybride Arbeitswelt. So gehen auch ohne Rufumleitung keine Anrufe verloren, unabhängig davon, ob die Mitarbeiter zu Hause oder im Büro arbeiten.

- ALE DeskPhones zeichnen sich durch **3D-Symphonic HD-Qualität**, Mobilgeräte und Smartphone-Apps für mobile Front-Line-Mitarbeiter aus, einschließlich Benachrichtigungen und Alarme während des Roamings vor Ort.
- **Einfacher Zugriff** auf Kundenansagen sowie Agentenfunktionen wie Anrufgruppen und Warteschlangen ermöglichen es den Kundendienstmitarbeitern, alle Kundenanrufe entgegenzunehmen.
- Die **Notruf-Krisenkonferenz** ermöglicht es, vordefinierte Ansprechpartner automatisch per Knopfdruck in eine Konferenz für das Katastrophen- oder Krisenmanagement einzubinden.
- Die **Ende-zu-Ende-Verschlüsselung** bietet die erforderliche Sicherheit und den notwendigen Datenschutz in öffentlichen Einrichtungen.
- Die Kommunikation und Zusammenarbeit sind bei einem digitalen Arbeitsplatz ganz einfach: **Ein Mausklick genügt**, um einen Ansprechpartner anzurufen oder eine Konferenz zu starten. Zudem stehen moderne Funktionen wie Gruppenchat, Bildschirm- und Dateifreigabe, Audio- und Videokonferenzen zur Verfügung – alles in einer einzigen App, die als Web-Client angeboten wird. Es ist keine Installation erforderlich. Die Apps sind auch für Android- und IoS-Geräte sowie für PCs verfügbar. Kunden mit ALE-Lösungen können vorhandene Mobilteile mit WebRTC-Technologie verwenden.
- Dank der Konnektoren für Microsoft® Teams und Google können Mitarbeiter von ihrem digitalen Arbeitsplatz aus **problemlos** mit der gesamten Organisation bzw. dem gesamten Unternehmen kommunizieren. Die Konnektoren für SaaS CRM und ITSM ermöglichen den Mitarbeitern die Kommunikation und Zusammenarbeit über ihre Geschäftsanwendungen.

E-Book
Kriterien und Lösungen für den digitalen Arbeitsplatz im öffentlichen Sektor

Konnektivität

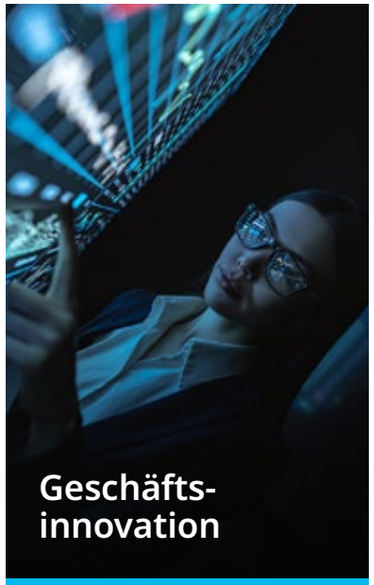
Das Digital Age Networking von Alcatel-Lucent Enterprise bietet mit seinem autonomen Netzwerk ein resilientes, nahtlos vernetztes Erlebnis mit dem Alcatel-Lucent OmniSwitch® (LAN) und dem Alcatel-Lucent OmniAccess® Stellar (WLAN), kombiniert mit ultraschneller Konvergenz, sicherer Netzwerkzugriffskontrolle und gesicherter Quality of Service (QoS). Das Enterprise-WLAN der neuen Generation mit integrierter WLAN-Kontrolle in den Access Points macht physische Controller an zentraler Stelle überflüssig. ALE-Lösungen können sowohl vor Ort als auch über die Cloud verwaltet werden.

Wichtige Konnektivitätsmerkmale von ALE:

- **Ein einziges Network Management System (NMS)** bietet eine zusätzliche Integrationsebene zwischen kabelgebundenen und drahtlosen Netzwerken und reduziert den Arbeitsaufwand des IT-Managers, da er sich nicht mit zwei Managementsystemen und deren zwei unterschiedlichen Gruppen von Richtlinien und Konfigurationsregeln auseinandersetzen muss. Das Network Management System Alcatel-Lucent OmniVista® zeichnet sich durch ein einheitliches Management sowie netzwerkübergreifende Transparenz aus. Diese kann sich positiv auf die Effektivität und die Agilität der IT auswirken.
- **Die automatisierte Bereitstellung** einer sicheren Netzwerkinfrastruktur vereinfacht das Hinzufügen, Verschieben und Ändern von Daten und reduziert gleichzeitig den Zeitaufwand für die Wartung und den Betrieb des Netzwerks. Dadurch wird nicht nur die betriebliche Effizienz gesteigert, sondern gleichzeitig werden auch Kosten und Risiken gesenkt.
- **Shortest Path Bridging (SPB)** wurde entwickelt, um die Einrichtung und den Betrieb eines weniger komplexen Netzwerks zu unterstützen und die Netzwerktypologie zwischen den Knoten dynamisch aufzubauen und aufrechtzuerhalten. Für die SPB-Arbeitslast werden alle verfügbaren physischen Verbindungen geteilt und genutzt, wodurch mehr Bandbreite verfügbar wird.
- **Beschäftigte im hybriden Arbeitsmodell (Option 1). Der sichere Fernzugriff** wird mit dem Remote Access Point (RAP) ermöglicht. Das Unternehmensnetzwerk kann problemlos über den Hauptstandort hinaus erweitert werden, sodass Mitarbeiter an entfernten Standorten so verbunden sind, als befänden sie sich im LAN des Unternehmens. Je nach Modell kann der RAP auch kabelgebundene Konnektivität für IP-Telefone oder andere IoT-Geräte bieten. Der Zugang wird durch zentralisierte und einheitliche Sicherheitsrichtlinien für kabelgebundene und drahtlose Netzwerke unterstützt, die ein einfaches Management sowie eine äußerst zuverlässige und einheitliche Sicherheit gewährleisten.
- **Beschäftigte im hybriden Arbeitsmodell (Option 2) SD-WAN und SASE**. Der Secure Access Service Edge (SASE) stellt eine sichere Verbindung zwischen Remote-Standorten, Zweigstellen und externen Mitarbeitern her. Die SASE-Lösung für Remote-Mitarbeiter besteht aus einer Software auf dem Laptop des Nutzers, die sicheren Zugang zu Anwendungen im Rechenzentrum des Unternehmens, in privaten Rechenzentren, im Internet oder in Public Clouds bietet, mit zentralem Management und ohne erforderliche zusätzliche Hardware am Standort des Arbeitnehmers. SASE bietet fortschrittliche Sicherheit mit Next-Generation Firewall (NGFW), einschließlich URL-Filterung und Application Firewall. Die Sicherheit wird darüber hinaus durch Unified Threat Management (UTM) unterstützt, was auch Next Generation Intrusion Prevention System (NGIPS), Antivirus- und Anti-Malware-Funktionen umfasst.

Geschäftskritische Netzwerkoperationen automatisieren und Nutzererlebnis verbessern

Digitalisierung durch sichere IoT-Einbindung und -Verwaltung ausbauen



Transformation mit automatisierten Workflows beschleunigen

Sicherheit

Kommunikationssicherheit

Es spielt keine Rolle, ob Sie für eine kleine kommunale oder große Regierungsbehörde eines Landes zuständig sind – Ihr Kommunikationsnetzwerk ist stets dem Risiko ausgesetzt, von Hackern angegriffen zu werden.

Die wichtigsten Sicherheitsmerkmale von ALE:

- **Sichere Konnektivität** zwischen dem Kommunikationssystem vor Ort (PBX und Telefone) und der Cloud-Infrastruktur, die vollständig von Alcatel-Lucent Enterprise entwickelt und betrieben wird, mit gegenseitiger Authentifizierung, Verschlüsselung und Security Border Elements (SBC).
- **Hochverfügbarkeit** mit räumlich redundanten Architekturen – vor Ort und in Private oder Public Clouds –, Schutz vor Denial-of-Service-Angriffen (DoS), integrierte Sicherheit mit gehärteter Hardware und Betriebssystemen.
- **Gut geschützte Kommunikation** durch starke Verschlüsselung auf der Grundlage von Industriestandards, die nativ in die Lösung implementiert ist – ganz ohne Beeinträchtigung der Sprachqualität und -leistung. Auf diese Weise wird die von Kunden und Mitarbeitern erwartete Leistung sichergestellt.
- **Datenschutz und -sicherheit** mit regelbasierter Zugriffskontrolle 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.
- **Einhaltung von Vorschriften und Standards**. Dazu zählen unter anderem die Datenschutz-Grundverordnung (DSGVO), ISO27001, Common Criteria EAL2+ oder HDS („Hébergeur Données Santé“, dies ist eine Zertifizierung der ALE-Cloud-Dienste für die Einhaltung des Patientenschutzes in Frankreich).
- **Sicherheit als Prozess** mit dem Product Security Incident Response Team (PSIRT) für aktives Management von Sicherheitsrisiken sowie mit regelmäßig aktualisierter Software und einer Richtlinienplattform.

ANSSI (CSPN)

ENS (Esquema Nacional de Seguridad)

Diese Zertifizierung wurde vom spanischen nationalen Sicherheitssystem eingeführt, um über ein System zu verfügen, das den angemessenen Schutz von Informationssystemen vor externen Bedrohungen und Zwischenfällen gewährleistet.

ISO27001 - 017/018

Die Agentur für ein digitales Italien ist der Präsidentschaft des Ministerrats unterstellt. Sie regelt die Verwendung und Speicherung wichtiger Daten sowie den Zugang zu diesen Daten und gewährleistet so die Sicherheit.

LAUFENDE ZERTIFIZIERUNGEN

BSI-Zertifizierung

Bundesamt für Sicherheit in der Informationstechnik.
Äquivalent zum CSPN der ANSSI (Q3 2021)

E-Book
Kriterien und Lösungen für den digitalen Arbeitsplatz im öffentlichen Sektor

Netzwerksicherheit

Immer mehr vernetzte Geräte, räumliche Entgrenzung, Veränderungen, die sich immer schneller vollziehen: Im Zuge der digitalen Transformation haben sich die Anforderungen an die Cybersicherheit grundlegend gewandelt. Digital Age Networking von Alcatel-Lucent Enterprise sorgt für die Sicherheit von IT-Ressourcen und Daten im heutigen Zeitalter der digitalen Transformation. Mit dieser Lösung können Sie den Benutzerzugriff gezielt verwalten und Sicherheitsrisiken eindämmen, die durch IoT-, Mobil- und Netzwerkgeräte entstehen. So können Sie verhindern, dass die unvermeidliche Sicherheitsverletzung zu einem Angriffspunkt wird, und ein vertrauenswürdiges Unternehmensökosystem bereitstellen.

Folgende Konzepte sorgen für integrierte Sicherheit in ALE-Lösungen:

- **Secure Diversified Code**, der die Sicherheit und Zuverlässigkeit auf der Ebene der Netzwerkgeräte mittels Verifizierung und Validierung durch unabhängige Dritte fördert:
  - Quellcode-Analyse, White-Box- und Black-Box-Tests durch ein auf Cybersicherheit spezialisiertes Unternehmen, um u. a. folgende Sicherheitsrisiken aus dem Weg zu räumen:
    - ¬ Bedrohungen durch die Hintertür
    - ¬ Eingebettete Malware
    - ¬ Ausnutzbare Sicherheitsrisiken
    - ¬ Offenlegung von urheberrechtlichen und/oder geheimen Informationen
- **Software-Diversifizierung:** Die ALE-Software implementiert Address Space Layout Randomisation (ASLR). Jeder Switch-Boot generiert dynamisch ein einzigartiges Speicherlayout, um die Ausnutzung von Software zu erschweren oder zu verhindern.
- **Zero-Trust-Sicherheit (Mikro- und Makro-Segmentierung):** Das Zero-Trust-Framework geht davon aus, dass das System von Hackern bedroht wird. Das Unternehmen wird nicht mehr als implizite Vertrauenszone betrachtet. Dieses Konzept umfasst Maßnahmen wie die Authentifizierung aller Verbindungen. Kein Asset und kein Nutzer ist automatisch vertrauenswürdig.
- **Standardmäßige Sicherheit:** Der Fernzugriff auf den OmniSwitch muss eigens aktiviert werden, anders als bei den meisten anderen Switches, bei denen jeglicher Zugriff auf die Switches/Router standardmäßig aktiviert ist und es den Administratoren überlassen bleibt, herauszufinden, wie sie das Gerät schützen können.
- **Integrierter Denial of Service (DoS)-Schutz:** Schutz des Betriebssystems und der Management-module vor einer Vielzahl von DDOS-Angriffen, die in der Regel dazu verwendet werden, die CPU zu 100 % auszulasten.
- **Keine Softwarepakete**, die gekauft und aktualisiert werden müssen: Alle Funktionen und Leistungs-merkmale, sogar der ALE Secure Code, sind im Preis des Switches enthalten – es müssen keine Module hinzugefügt oder Upgrades erworben werden. Die gesamte Software ist im Lieferumfang enthalten.
- **Automatisiertes und sicheres IoT-Onboarding:** Durch Endgeräte-Fingerprinting, -Klassifizierung und -Containerisierung.

EU-DSGVO

US-Bundesbehörde

US Joint Interoperability

US MIL-STD

US Trade Agreements Act (TAA)

E-Book
Kriterien und Lösungen für den digitalen Arbeitsplatz im öffentlichen Sektor

Weitere Informationen

Erfahren Sie mehr über Alcatel-Lucent Enterprise Lösungen für den öffentlichen Sektor für den digitalen Arbeitsplatz oder kontaktieren Sie uns, um Ihre Anforderungen zu besprechen.

www.al-enterprise.com/de-de/industries/government

Alcatel·Lucent Enterprise