Sichere Collaboration-Lösung für den Öffentlichen Sektor

Controlware Workshop: Der sichere Pfad zu einer souveränen Zero-Trust-Architektur

Situation
Steigender Bedarf an skalierbaren Lösungen

Heute nehmen innovative Themen, wie Videokonferenzen, mobiles Arbeiten und hybride Arbeitsplätze, immer mehr an Bedeutung zu – auch bei Kunden im Öffentlichen Sektor. Die COVID-19-Pandemie hat den Kommunikationsmarkt in kürzester Zeit enorm auf den Kopf gestellt und Unternehmen mussten ad-hoc ihren Geschäftsbetrieb irgendwie – zumindest virtuell – am Laufen halten. Collaboration-Lösungen aus der Public Cloud waren hier durch ihre Skalierbarkeit in der Lage, den immensen Bedarf zunächst kurzfristig zu decken. Jedoch unterschieden diese sich nicht nur in ihrer Funktionsbandbreite und Leistungsfähigkeit, sondern auch in ihren Sicherheitsansätzen und -mechanismen.

Herausforderung
Rechtskonforme Nutzung & digitale Souveränität

In Europa und speziell in Deutschland steht vor allem die Einhaltung der Datenschutz-Grundverordnung (DSGVO) im Mittelpunkt. In dieser Verordnung wird seit 2016 EU-weit einheitlich geregelt, wie private Unternehmen sowie öffentliche Stellen mit personenbezogenen Daten umgehen müssen, denn Datenschutz ist ein Grundrecht.

Weiterhin gewinnen auch Aspekte durch die aktuellen geopolitischen Spannungen an Relevanz: Datenschutz, Sicherheit und digitale Souveränität stehen vor allem bei Kunden im Öffentlichen Sektor auf der Agenda. Beispielsweise prüfen Bund, Länder und Kommunen bereits, inwiefern sich eine stärkere Unabhängigkeit von global agierenden Software- und Diensteanbietern mit dem Aufbau dedizierter Infrastrukturen erreichen lässt. Hier gibt es zahlreiche Lösungsansätze, etwa durch Open-Source-Konferenzlösungen. Die Nutzung ermöglicht es, durch den Einsatz unabhängiger und öffentlich zugänglicher Entwicklungsressourcen, eigene Lösungsplattformen autark von globalen Einflüssen anderer Staaten und Unternehmen zu entwickeln und an geeigneter Stelle einzusetzen

Die Kehrseite der Autarkie liegt aber auf der Hand: Hoher Ressourcen-Aufwand führt zu hohen Kosten, Verlust von Wettbewerbsvorteilen durch langsames Innovationstempo und zu fehlenden Skalierungseffekten.

Das bestätigt auch der Bitkom e. V., Branchenverband der deutschen Informations- und Telekommunikationsbranche, in seiner Stellungnahme zur digitalen Souveränität. Gleichzeitig kann man den Empfehlungen von Bitkom auch entnehmen:

> **„Digitale Souveränität braucht ein praktikables Gleichgewicht, das unsere politische und wirtschaftliche Handlungs- und Leistungsfähigkeit in einer globalisierten, digitalisierten Wirtschaft erhält und ausbaut."**

Dementsprechend können Dienste aus anderen, eher unkritischen Bereichen, für die es nur eine geringere Handlungskompetenz braucht, durch weniger souveräne Dienste erbracht werden. Eine vollständige Autarkie digitaler Technologien ist in der Breite sogar wegen der oben genannten Nachteile nicht erwünscht.

Unser Lösungsansatz
Hybrid = Digital souverän + Cloudvorteil

Controlware unterstützt die Kunden beim Spagat zwischen digitaler Souveränität und dem Weg zu skalierbaren, jedoch hochsicheren Collaboration-Diensten aus der Cloud, On-Premises sowie hybrid. Ohne Frage gibt es nicht den einen Lösungsweg, der allen Anforderungen genügt, daher konzipieren wir für jeden einzelnen Kunden maßgeschneiderte Lösungen. Dabei setzen wir auf das Portfolio von Cisco Systems, einem weltweit agierenden US-Technologieanbieter für Netzwerk-, Collaboration-, Security- und Computing-Lösungen.

Cisco gehört zu den Marktführern im Bereich Collaboration und bietet ein komplettes Collaboration-Portfolio aus einer Hand. Neben der führenden Cloud-Collaboration-Lösung Webex hat Cisco mit dem Unified Communications Manager zudem eine marktführende On-Prem-Kommunikationslösung entwickelt.

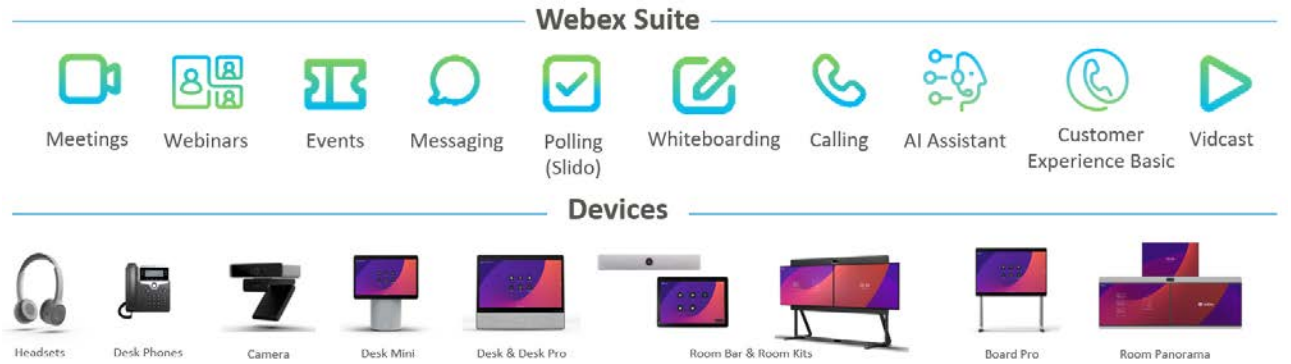

Abbildung: Mehr als nur eine Meeting-Lösung: Mit der Webex Suite bietet Cisco ein abgestimmtes Portfolio aus Soft- und Hardware an

Auch wenn Webex historisch häufig nur als zuverlässige und hochskalierbare Videokonferenzlösung bekannt ist, ist der Funktionsumfang hier mittlerweile deutlich gewachsen: Sicheres Team Messaging, Cloud Calling und Communications Platform-as-a-Service (CPaaS) ergänzen die innovativen Meeting- und Webinar-Funktionen. Ein komplettes Hardware-Angebot aus Telefonen, Microsoft Teams-zertifizierten Videokonferenzsystemen, Headsets, Desktop-Kameras und die dazugehörigen Services runden die One-Stop-Shop-Lösung ab.

Zudem lassen sich alle Komponenten zu einem einheitlichen Hybridsystem zusammenfassen, um eine auf den Kunden abgestimmte Gesamtlösung zu konzipieren. Das zentrale Management erlaubt die Zusammenführung und Administration der Dienste, Nutzer, Geräte und vor allem der sicherheitsrelevanten Funktionen. Und hier sind wir nun beim Kern der Frage angelangt: Wie sicher kann eine Collaboration-Lösung überhaupt sein? Genau diese Frage bewegt nicht nur unsere Kunden aus dem Öffentlichen Sektor, sondern jedes Unternehmen, das sich mit der Verlagerung von Collaboration-Workloads in die Cloud beschäftigt.

Im Folgenden klammern wir die On-Prem-Lösungen aus. Diese sind bereits von Hause aus datensouverän, da die Daten in der Regel in kundeneigenen Rechenzentren oder in gesicherten Private Clouds liegen und der Daten(ab)fluss selbst kontrolliert werden kann. Hier unterstützen wir Sie jedoch gerne auch bei der Auswahl der optimalen Lösung sowie Inbetriebnahme und Betrieb.

Kundenutzen
Technische Absicherung & Vertrauensvorsprung

Als Gold-Partner von Cisco vertrauen wir auf einen US-Amerikanischen Anbieter hybrider Collaboration-Lösungen. Dies erscheint wahrscheinlich durch das Schrems-II-Urteil aus 2020 zunächst paradox. Cisco hat jedoch seine Lösungen weit über die Anforderungen der DSGVO hinaus auf die europäischen Bedürfnisse abgesichert. Im Klartext heißt das:

Webex sorgt durch innovative Sicherheitsmaßnahmen dafür, dass Cloud-Services sogar für Behördenkunden rechtssicher nutzbar sind.

Webex bietet vollständige Datenresidenz in der EU

Seit Juli 2022 werden alle nutzergenerierten Inhalte von europäischen Kunden in Rechenzentren in der EU (DE & NL) gespeichert. Webex ist damit der erste große Collaboration-Anbieter, der Statistiken, Identitäten, Inhalte und sämtliche Abrechnungsdaten ausschließlich in der EU speichert. Die lokale Datenresidenz ist zwar keine Voraussetzung der DSGVO, gibt jedoch gerade Kunden der Öffentlichen Hand deutlich mehr Vertrauensspielraum.

Lokale Schlüsselverwaltung für E2E-Encryption

Mit den Services „Hybrid Data Security“ (HDS) und „Bring Your Own Key“ (BYOK) stellt Webex zwei interessante und nahezu unerlässliche Optionen zur Schlüsselverwaltung von in der Webex Cloud gespeicherten Inhalten zur Verfügung. Damit kann die Schlüsselverwaltung für Nachrichten, geteilte Dateien und Meeting-Aufzeichnungen mittels HDS in das kundeneigene Rechenzentrum verlagert oder sogar ein kundeneigener Schlüssel (BYOK) in der Cloud hinterlegt werden. Kunden behalten die volle Kontrolle über ihre gespeicherten Daten – und nicht einmal Cisco oder die einschlägigen Sicherheitsbehörden können darauf zugreifen.

Sichere Meetings mit Zero Trust Security

Vertrauen ist gut, Zero Trust ist besser. Mit drei technischen Ansätzen unterstützt Webex diesen Paradigmenwechsel, um Meetings für Kunden noch sicherer zu gestalten:

- Die Einführung von in der Branche anerkannten Standard-Protokollen, wie MLS, ACME und SFrame, erlaubt es IT-Experten, die Qualität der Ende-zu-Ende-(E2E)-Verschlüsselung von über Webex geführten Meetings zu bestätigen. Mit MLS bietet Webex derzeit das absolut höchste verfügbare Sicherheitsniveau, das die Ansätze anderer Anbieter in diesem Bereich übertrifft.

- Die aktuellen Webex-Videokonferenzsysteme unterstützen ebenfalls den Zero Trust-Ansatz und können E2E-verschlüsselten Webex-Meetings beitreten und so eine durchgängig verschlüsselte Kommunikation für alle Teilnehmer gewährleisten.
- Mit der durch das MLS-Protokoll unterstützten Zertifikats-basierten Authentifizierung ist sichergestellt, dass nur die gewünschten Teilnehmer an einem Zero Trust Meeting teilnehmen. Das „Hereinschleichen" unter einer falschen Identität ist somit ausgeschlossen.

Vertrauensvorsprung durch Testierung dritter sowie volle Transparenz

- Trotz der US-Amerikanischen Herkunft verfolgt Cisco den Ansatz der vollständigen Transparenz und lässt die durchgängige Sicherheit von Webex nicht nur von Dritten, sondern auch von behördlichen Stellen testieren – und untermauert somit in Europa das von Kunden seit langem entgegengebrachte Vertrauen.
- Cisco Webex hat das Testat nach dem BSI-Anforderungskatalog Cloud Computing Compliance Controls Catalogue, kurz **BSI C5**, erhalten.

  Der Kriterienkatalog des BSI legt fest, welche Mindestanforderungen Cloud-Dienste zur Gewährleistung einer hohen Sicherheit nicht unterschreiten sollten. Wichtig hierbei ist, dass tatsächlich die gesamte Webex-Lösung betrachtet wurde und nicht wie am Markt vorzufinden, lediglich der dahinterliegende Cloud Service oder nur eine bestimmt Client-Version. Dies erhöht die Sicherheit für alle Kundengruppen, insbesondere Behörden, Finanzdienstleister und Betreiber kritischer Infrastrukturen.
- Weiterhin wurde Webex als erster Videokonferenzdienst nach dem EU Cloud Code of Conduct (EU Cloud CoC) zertifiziert. Der EU Cloud Code of Conduct konkretisiert die rechtlichen Anforderungen von Artikel 28 der Datenschutz-Grundverordnung für den Einsatz von Cloud-Produkten. Der Europäische Datenschutzausschuss (European Data Protection Board, EDPB), dem alle Datenschutzbehörden der EU-Mitgliedstaaten angehören, hat den EU Cloud Code of Conduct geprüft und als anerkannte Verhaltensregel nach der Datenschutzgrundverordnung genehmigt. Die unabhängige Kontrollinstanz SCOPE Europe hat bestätigt, dass Webex alle Anforderungen des **EU Cloud Code of Conduct Level 3** erfüllt.
- Mindestens das gleiche Vertrauen spricht auch das kürzlich an Webex vergebene **Swiss Digital Trust Label** (DTL) aus. Diese Akkreditierung gibt Nutzern digitaler Dienste in der Schweiz durch den strengen Zertifizierungsprozess die Sicherheit, dass ein Anbieter mit der Sicherheit und dem Schutz persönlicher Daten transparent umgeht und den gesetzlichen Normen entspricht.
- Zu guter Letzt legen Transparenz und offene Kommunikation einen weiteren Grundstein in Bezug auf das Vertrauen zu einem Cloud-Lösungsanbieter, denn jeder Nutzer hat das Recht zu erfahren, in welchem Umfang und zu welchem Zweck seine personenbezogenen Daten verarbeitet werden. Deshalb spielt Cisco als Vorreiter in der Branche mit offenen Karten und stellt sogenannte Data Privacy Sheets und Data Maps im Sinne des Datenschutzes sowie Transparenzberichte öffentlich zur Verfügung. Transparenzberichte geben anonymisiert Auskunft darüber, in welchem Maße (inter)nationale Regierungsstellen mit Anfragen nach Kundendaten an Cisco herantreten und wie diese beantwortet werden. Im Falle eines behördlichen Datenzugriffsersuchens verpflichtet sich Cisco vertraglich, Daten nicht automatisch auszuhändigen, sondern zunächst den betreffenden Kunden zu informieren und ihm die Möglichkeit zu geben, der Weitergabe selbst entgegenzutreten. Anfragen werden in jedem Fall sorgfältig nach rechtlichen Grundsätzen überprüft und gegebenenfalls auch abgelehnt. **Webex kann daher von Kunden weltweit in Übereinstimmung mit der DSGVO und weiteren Datenschutzgesetzen eingesetzt werden.**

Warum Controlware?
Ihr Collaboration & Security Spezialist!

Die Collaboration-Experten von Controlware unterstützen Unternehmen und Kunden aus dem Öffentlichen Sektor bei der Planung und Realisierung hybrider Lösungen mit Fokus auf Sicherheit, Datenschutz und Transparenz. Darüber hinaus beraten wir unsere Kunden auch bei der Umgestaltung hybrider Arbeitsplatzmodelle, um eine effiziente und sichere Kommunikation zu gewährleisten. Selbstverständlich umfasst unser Lösungsportfolio auch Videokonferenzraumsysteme, die es erlauben, sich an allen am Markt existierenden Meetinglösungen einzuwählen oder sich sogar nativ an Microsoft Teams zu registrieren.
Die Controlware GmbH ist einer der führenden unabhängigen IT-Dienstleistern und Managed Service Provider. Das 1980 gegründete Unternehmen entwickelt, implementiert und betreibt anspruchsvolle IT-Lösungen für die Cloud-, Data Center-, Enterprise- und Campus-Umgebungen seiner Kunden mit nachgewiesener Servicequalität mit dem ISO27001-zertifiziertem Customer Service Center.

Zentrale

Controlware GmbH
Waldstraße 92
63128 Dietzenbach
Tel. +49 6074 858-00
Fax +49 6074 858-108
info@controlware.de
www.controlware.de
blog.controlware.de
Besuchen Sie uns auf: