1-2 | 2021 Jahrgang 162 | ISSN 2366-9594 | B 5398

Vulkan Verlag
www.gwf-gas.de

gwf Gas + Energie

© Teamwire

Datenschutzkonforme und sichere **Team-Kommunikation**

Ob für stationäre oder mobile Mitarbeiter: Die interne Kommunikation muss reibungslos erfolgen, um Themen flexibel und ortsunabhängig besprechen und auch die Zusammenarbeit effektiver gestalten zu können. Für eine ganzheitliche Team-Kommunikation braucht es geeignete und vor allem DSGVO-konforme Lösungen, wie etwa eine Business Messaging App.

COVID-19 und die darum ergriffenen Schutzmaßnahmen haben die Nachfrage nach digitalen Lösungen, wie etwa Webmeeting-Anwendungen, Kollaborationstools und Echtzeit-Messengern, rasant in die Höhe schießen lassen. Um dezentrales Arbeiten umsetzbar zu machen, war schnelles Handeln gefragt. Unternehmen, die überwiegend Non-Desk-Worker wie Produktionsmitarbeiter, Logistikkräfte, Pflege- oder Krankenhauspersonal beschäftigen, stehen nicht erst seit der Corona-Pandemie vor der Herausforderung, eine produktive und sichere Team-Kommunikation zu ermöglichen. Oft greifen sie auf Consumer Apps zurück – allen voran WhatsApp –, um sich intern abzustimmen. Stellt das Unternehmen geschäftliche Devices, können IT-Administratoren die Nutzung unterbinden. Aber gerade bei Firmen, die auf ein BYOD-Konzept (Bring your own Device) setzen, entsteht dadurch eine gefährliche Schatten-IT. Denn: Eine Consumer App ist nicht für einen sicheren und compliancegerechten Informationsaustausch im Business-Bereich geeignet – insbesondere nicht bei Unternehmen mit kritischer Infrastruktur, Behörden mit vertraulichen Informationen oder Organisationen mit schützenswerten personenbezogenen Daten. Auch ist eine solche App nicht auf eine professionelle IT-Steuerung ausgerichtet. Aber auch bei Business-Tools sind Datenschutz und -sicherheit nicht immer zu hundert Prozent gewährleistet. Doch das sollte in der digitalen internen Kommunikation kein Nice-to-have, sondern eine unverzichtbare Standard-Anforderung sein.

Die Gretchenfrage: Wie hast du's mit dem Datenschutz?

Erst unlängst ist eine hitzige Debatte um namhafte Videokonferenz-Lösungen sowie Consumer Apps und deren Einsatz im Business-Bereich entfacht: Vertreter mehrerer Aufsichtsbehörden, darunter Ulrich Kelber, der Bundesbeauftragte für Datenschutz, und Maja Smoltczyk, die Berliner Landesdatenschutzbeauftragte, haben Empfehlungen und Warnungen herausgegeben, was die Nutzung dieser Dienste betrifft. Hinzu kommt, dass der Europäische Gerichtshof, kurz EuGH, das Privacy Shield für ungültig erklärt hat. Dieses transatlantische Abkommen erlaubte US-Unternehmen, Daten von EU-Nutzern zur Verarbeitung und Speicherung in die USA zu übermitteln. Grund für die Entscheidung des EuGH war, dass US-Behörden auf personenbezogene Daten innerhalb von US-Firmen ungehindert zugreifen konnten. Demnach waren auch personenbezogene Daten von EU-Bürgern nicht gemäß DSGVO geschützt.

Sicheres und einfaches Messaging nicht gegeben

Neben zentralen Fragen nach Datenschutz und -sicherheit, die insbesondere bei Lösungen von US-Anbietern oftmals offenbleiben, sind Kollaborationstools, wie beispielsweise Microsoft Teams und Slack, nicht primär auf das Echtzeit-Messaging zwischen mobilen Mitarbeitern einerseits und stationären Kollegen andererseits ausgelegt. Die Anwendungen bringen zahlreiche Features und Funktionen mit, die für

neue flexible Arbeitsmodelle relevant sein können. Für mobile Mitarbeiter eignen sich solche Lösungen nur bedingt, da die vielen Anwendungsmöglichkeiten für ihre Arbeit nicht brauchbar sind. Vielmehr benötigen sie eine business-taugliche WhatsApp-Alternative mit Funktionen, die ihre Anwendungsszenarien weitgehend abdecken und kommerziellen Messaging Apps hinsichtlich Benutzerfreundlichkeit in nichts nachstehen. Das erhöht zum einen die Akzeptanz für die Nutzung solcher Tools und steigert zum anderen die Produktivität.

Kurze Chat-Nachrichten anstatt langwieriger E-Mail-Kommunikation

Schon allein die Tatsache, dass mobile Mitarbeiter für die Team-Kommunikation WhatsApp wählen, anstatt ihre Kollegen anzurufen oder eine E-Mail über ihr Smartphone zu schreiben, verdeutlicht den unaufhaltbaren Wandel in der Team-Kommunikation: Die private Gewohnheit, über Messenger Apps zu kommunizieren, hält Einzug in den beruflichen Alltag. Anders als bei E-Mails, gehen Nachrichten in einer Business Messaging App nicht in einem überfüllten Postfach unter, und die Antwortzeit ist wesentlich kürzer. Um Situationen und Entscheidungen besser beurteilen zu können, muss es möglich sein, digitale Inhalte, etwa Fotos, Videos und PDFs, zu teilen. Gleiches gilt für interne Umfragen, die man direkt im Chat erstellen kann. Zudem sind Alarmierungs-Funktionen sehr hilfreich, um im Falle eines kritischen Ereignisses, etwa einer Kundeneskalation, eines Serverausfalls oder Feueralarms, ausgewählte Teams, Abteilungen oder die gesamte Organisation zu informieren.

Business Messaging App: Das technische A und O

Nicht nur die funktionalen Möglichkeiten sind entscheidend. Die interne Kommunikation darf IT-Administratoren kein Dorn im Auge sein. Vielmehr sollten sie schnell und einfach in der Lage sein, ihren Kollegen eine praktikable und unternehmensweit nutzbare Lösung zur Verfügung zu stellen. Zugunsten einer professionellen und vor allem DSGVO-konformen Team-Kommunikation sind eine Reihe technischer Aspekte zu beachten:

Kompromissloser Datenschutz

Um die Daten, die in einer Business Messaging App entstehen, zu schützen, muss Datensouveränität und -sparsamkeit gegeben sein. Wenn die Daten in einem IS027001-zertifizierten Rechenzentrum mit Standort in Deutschland oder On-Premise, also vor Ort in den eigenen Räumlichkeiten, gespeichert werden, ist man hier auf einem guten Weg. Wichtig ist zudem, dass vollständig verschlüsselt wird und so wenig wie möglich Meta-Daten, wie etwa Standort, Datum und Uhrzeit, erfasst werden. Daneben muss die Business Messaging App auch das „Privacy by Design"-Konzept der DSGVO erfüllen.

Applikationsbereitstellung mittels Container

Nur wenn sich eine Business Messaging Anwendung als sichere Container-App betreiben lässt, ist dafür gesorgt, dass alle Daten auf dem Endgerät geschützt sind und die volle Datenkontrolle beim Unternehmen liegt. Der Container steuert den erlaubten Datenzugriff durch Nutzer und den möglichen Datenaustausch mit anderen Applikationen. Zugleich gewährleistet er, dass auf dem Endgerät gespeicherte Daten per Routine automatisiert reduziert und bei Bedarf aus der Ferne komplett gelöscht werden können.

Vollumfängliche Verwaltung per Dashboard

Mittels eines professionellen Administratorenportals behält die IT jederzeit die Hoheit über die Software. Es ist essenziell, um die Benutzerverwaltung und die Rechteverteilung zu steuern. Über ein Dashboard lassen sich beispielweise Kommunikationsrichtlinien festlegen sowie Nachrichten und Daten revisionssicher archivieren. Um Benutzer oder auch Gruppen direkt aus bestehenden Verzeichnissen, wie etwa dem Active Directory, bequem zu importieren und laufend zu synchronisieren, sollte sich die Lösung bedarfsgerecht integrieren lassen. Auch sollte das Dashboard ermöglichen, Multi-Mandanten zu verwalten und mehrere Domains zu nutzen.

Vollständige Integration in das IT-Ökosystem

Idealerweise verfügt eine Business Messaging App über eine offene API-Schnittstelle, welche die Anbindung von Drittsystemen, etwa CRM und ERP, erlaubt. Eine derartige Integration hilft, nicht nur den Informationsaustausch – durch automatisierte Prozesse und beschleunigte Workflows – zu verbessern, sondern steigert auch die Produktivität erheblich. Über eine zusätzliche WhatsApp Business API können die Mitarbeiter mit Kunden, Partnern und Dienstleistern kommunizieren – das unterstützt insbesondere im Kundenservice.

Direkte Anbindung an das UEM-System bzw. die MDM-Umgebung

Dadurch ist es möglich, die App auf den Geräten der Mitarbeiter automatisch auszurollen und eine nutzerfreundliche Registrierung zu unterstützen. UEM bzw. MDM stellt sicher, dass nur autorisierte Endgeräte auf Ressourcen hinter der Firewall des Unternehmens zugreifen dürfen und Daten bei einem Geräteverlust nicht in unbefugte Hände gelangen.

Den kommunikativen Brückenschlag wagen

Eine ganzheitliche interne Kommunikation im Sinne eines mobilen Büros ist bereits heute mit einer Business Messaging App möglich. Damit die Mitarbeiter eine solche Lösung akzeptieren und in vollem Umfang in der Team-Kommunikation nutzen, müssen IT-Administratoren neben den technischen Anforderungen auch die Mitarbeiter-Bedürfnisse im Blick haben. So gelingt nicht nur der kommunikative Brückenschlag zwischen den Mitarbeitern, sondern auch mit der IT-Abteilung.

Autor:
Tobias Stepan
Gründer und Geschäftsführer von
Teamwire GmbH
www.teamwire.eu