



SICHERHEIT. DAS FACHMAGAZIN.

SICHERHEIT AUF DEN PUNKT GEBRACHT.

SICHERHEITSVORKEHRUNGEN

**Verhalten bei einem
Terroranschlag**

Seite 4

NOTFALL- UND KRISENMANAGEMENT

**Auswahl und Ausstattung
eines Krisenstabsraums**

Seite 9

NOTFALL- UND KRISENMANAGEMENT

**Pandemie:
Betrieblicher Neustart
nach dem „Shutdown“**

Seite 12

SICHERHEITSTECHNIK

**Bodycams:
gesetzeskonformer
Einsatz in Deutschland**

Seite 15

IT-SICHERHEIT

**So wird „Schatten-IT“ in
der Team-Kommunikation
vermieden**

Seite 22

TERRORISMUS



KOMPETENZPARTNER



SO VERMEIDEN UNTERNEHMEN EINE „SCHATTEN-IT“ IN DER TEAM-KOMMUNIKATION

Ob für stationäre oder mobile Mitarbeiter: Die interne Kommunikation muss reibungslos erfolgen, um Themen nicht nur schnell, flexibel und ortsunabhängig besprechen, sondern auch die Zusammenarbeit effektiver gestalten zu können. Für eine ganzheitliche Team-Kommunikation braucht es geeignete und vor allem DSGVO-konforme Lösungen, um der Schatten-IT durch private Smartphones und unautorisierte Apps vorzubeugen.

Die Nachfrage nach digitalen Lösungen wie etwa Webmeeting-Anwendungen, Kollaborationstools und Echtzeit-Messengern steigt in den letzten Jahren rasant. Unternehmen, die überwiegend „Non-Desk-Worker“ wie Produktionsmitarbeiter, Logistikkkräfte, Pflege- oder Krankenhauspersonal beschäftigen, stehen vor der Herausforderung, eine produktive und sichere Team-Kommunikation zu ermöglichen. Oft wird auf unsichere und nicht compliancegerechte Consumer-Apps zurückgegriffen – allen voran WhatsApp –, um sich intern abzustimmen. Bei vielen Unternehmen entsteht dadurch eine Schatten-IT.

„DIE FIRMENBEZOGENE NUTZUNG VON MESSAGING-APPS – INSBESONDERE AUF PRIVATEN GERÄTEN – IST NICHT FÜR EINEN DATENSCHUTZKONFORMEN INFORMATIONSAUSTAUSCH IM BUSINESS-BEREICH GEEIGNET.“

SICHERES, EINFACHES UND DATENSCHUTZKONFORMES MESSAGING NICHT GEBEN

Neben zentralen Fragen nach Datenschutz und Datensicherheit, die insbesondere bei Lösungen von US-Anbietern meist offenbleiben, sind Kollaborationstools, wie beispielsweise Microsoft Teams oder Slack, nicht primär auf das Echtzeit-Messaging zwischen mobilen Mitarbeitern einerseits und stationären Kollegen andererseits ausgelegt. Es wird vielmehr eine business-taugliche WhatsApp-Alternative mit zusätzlichen Funktionen benötigt.

KURZE CHAT-NACHRICHTEN ANSTATT LANGWIERIGER E-MAIL-KOMMUNIKATION

Allein die Tatsache, dass mobile Mitarbeiter für ihre Team-Kommunikation WhatsApp wählen, anstatt Kollegen anzurufen



Bildquelle: Teamwire GmbH

Erst unlängst ist eine hitzige Debatte um namhafte Videokonferenz-Lösungen sowie Consumer-Apps und deren Einsatz im Business-Bereich entfacht: Vertreter mehrerer Aufsichtsbehörden haben Empfehlungen und Warnungen in Bezug auf den Datenschutz herausgegeben, was die Nutzung derartiger Dienste betrifft.

oder eine E-Mail zu schreiben, verdeutlicht den unaufhaltbaren Wandel in der Team-Kommunikation. Anders als bei E-Mails gehen Nachrichten in einer Business-Messaging-App nicht in einem überfüllten Postfach unter und die Antwortzeit ist wesentlich kürzer.

Eine ganzheitliche und vollintegrierte interne Kommunikation ist bereits heute mit einer Business-Messaging-App möglich. Damit Mitarbeiter eine solche Lösung akzeptieren und in vollem Umfang in der Team-Kommunikation nutzen, müssen IT-Administratoren neben den technischen Anforderungen auch die Mitarbeiterbedürfnisse im Blick haben, um die Kommunikation effektiver zu gestalten. Zugleich unterstützt eine solche Lösung IT-Administratoren dabei, Sicherheitslücken zu schließen und die Kontrolle über „die bisherige Schatten-IT“ zurückzuerlangen.

„DERARTIGE ANWENDUNGEN MÜSSEN REGELMÄSSIGEN AUDITS INKLUSIVE PENETRATIONSTESTS UND SCHWACHSTELLEN-ANALYSEN UNTERZOGEN WERDEN, UM CYBER-ANGRIFFEN KEINE CHANCE ZU BIETEN.“

„DIE PRIVATE GEWOHNHEIT, ÜBER MESSENGER-DIENSTE ZU KOMMUNIZIEREN, HÄLT EINZUG IN DEN BERUFLICHEN ALLTAG.“

Dieser Artikel ist mit freundlicher Unterstützung von Tobias Stepan entstanden. Er ist Gründer und Geschäftsführer der Teamwire GmbH, die sich auf sicheres und souveränes Instant-Messaging spezialisiert hat.



WIE KANN DIE KOMMUNIKATION ZWISCHEN STATIONÄREN UND MOBILEN MITARBEITERN SICHER GESTALTET WERDEN UND WAS IST BEI DER AUSWAHL ENTSPRECHENDER TOOLS ZU BEACHTEN?

1. TIPP: PROBLEMBEWUSSTSEIN SCHAFFEN

Dass Mitarbeiter nicht autorisierte Anwendungen auf mobilen Endgeräten für die interne Kommunikation sorglos einsetzen, beruht oftmals darauf, dass die damit einhergehenden Gefahren nicht bekannt sind. Daher sollten IT-Administratoren ein Bewusstsein schaffen, welche Probleme die Nutzung solcher Anwendungen in Bezug auf Datenschutz und Datensicherheit mit sich bringt.

2. TIPP: DIE MITARBEITERBEDÜRFNISSE IM BLICK HABEN

IT-Administratoren sollten genau prüfen, welche Anwendungen die Mitarbeiter für ihre wechselseitige Kommunikation nutzen und in welchen Fällen auf Instant-Messaging zurückgegriffen wird. Das gibt wertvolle Einblicke, auf welche Funktionalitäten (Standortübermittlung, Alarmierung, Anbindung an Drittsysteme) die Anwender besonderen Wert legen und wie eine passende Kommunikationslösung aussehen sollte.

3. TIPP: SCHNELLER ROLL-OUT UND VOLLAUTOMATISCHE EINRICHTUNG

IT-Administratoren sollten in der Lage sein, eine praktikable und unternehmensweit nutzbare Lösung zur Verfügung zu stellen. I. d. R. gibt es bereits ein UEM-System beziehungsweise eine MDM-Umgebung, welche die zentrale Verwaltung von mobilen Geräten sicherstellt. Zugleich ermöglichen zahlreiche administrative Einstellungen, die App organisationsweit vorzukonfigurieren und umfassend abzusichern.

4. TIPP: KOMPROMISSLOSER DATENSCHUTZ

Um die Daten (unabhängig der Strategie der IT-Infrastruktur – Cloud, Private Cloud oder On-Premise), die in einer Business-Messaging-App entstehen, zu schützen, muss Datensouveränität und Datensparsamkeit gegeben sein. Wenn Daten in einem Rechenzentrum mit Standort in Deutschland oder in den eigenen Räumlichkeiten gehostet werden, ist dies ein guter Weg, um den strengen Vorschriften der DSGVO und des Bundesdatenschutzgesetzes zu genügen. Wichtig ist zudem, dass eine vollständige Datenverschlüsselung (moderner Standard) stattfindet, so wenig wie möglich Meta-Daten erfasst werden und keine versteckten Analysen von Meta-Daten, Nutzern und der Kommunikation im Hintergrund erfolgen. Daneben muss eine Business-Messaging-App auch das „Privacy by Design“-Konzept der DSGVO erfüllen. Auf personenbezogene Daten sollte nur dann zugegriffen werden, wenn es aus Bereitstellungs-, Sicherheits- oder Administrationsgründen absolut notwendig ist.



BUSINESS-MESSAGING-APP: DAS TECHNISCHE „A“ UND „O“

Nicht nur die funktionalen Möglichkeiten sind entscheidend für einen compliance- und datenschutzgerechten Umgang mit solchen Messenger-Diensten. Zugunsten einer professionellen und vor allem DSGVO-konformen Team-Kommunikation sind eine Reihe technischer Aspekte zu beachten:

5. TIPP: EINE VOLLSTÄNDIGE INTEGRATION IN DIE IT-LANDSCHAFT ANSTREBEN

Ziel sollte sein, die unterschiedlichen Kommunikations- und Informationssysteme intelligent miteinander zu verknüpfen. Um einen ganzheitlichen Datenaustausch zu unterstützen, sollte eine Kommunikationslösung eine offene API bereitstellen, über die sich Drittsysteme, etwa CRM- und ERP-Systeme, einfach anbinden lassen. Nutzer können somit orts- und zeitunabhängig auf alle relevanten Daten zugreifen. Idealerweise gibt es eine WhatsApp-Business-API, welche die Messenger miteinander verknüpft und damit ebenso die externe Kommunikation beispielsweise im Kundenservice optimiert.

6. TIPP: „SCHATTEN-IT“ VERBANNEN UND „IT-HOHEIT“ ZURÜCKGEWINNEN

Über ein professionelles Administratorenportal behalten IT-Administratoren jederzeit die Hoheit über die Software und folglich auch die Datenflüsse. Dies ist essenziell, um die Benutzerverwaltung und eine Rechteverteilung zu steuern. Über das Portal lassen sich außerdem Kommunikations-, Datenschutz- und Sicherheitsrichtlinien festlegen und neben Nachrichten auch Daten revisionssicher archivieren. In diesem Zusammenhang sollte es möglich sein, Benutzer oder Gruppen direkt aus bestehenden Verzeichnissen, wie etwa dem Active Directory, bequem zu importieren und die entsprechenden Daten laufend zu synchronisieren. Auch Aspekte wie die Mandantenfähigkeit und die Nutzung mehrerer Domains sollten Beachtung bei der Systemauswahl finden.