Zu 100% auf der sicheren Seite

Die notwendigen Sicherheitseinstellungen bei einem Messenger für Organisationen

VERSION 1.0

Inhaltsverzeichnis

Vorwort

Kaum ein Wirtschaftszweig oder ein Sektor des öffentlichen Lebens, der in der Vergangenheit nicht Opfer kritischer Umstände geworden wäre: Umweltereignisse wie Brände oder Fluten, plötzliche Lockdowns, akuter Ressourcenmangel oder gezielte Hackerangriffe – immer wieder stoßen Organisationen, ob Unternehmen, Verbände, Ministerien, Behörden oder öffentliche Einrichtungen, unerwartet an die Grenzen des Lösbaren. Unverzichtbarer Anker, um selbst in ungewissen Zeiten zu bestehen: eine zuverlässige Kommunikation.

Hier spielen vor allem sekundäre Kommunikationskanäle wie Instant Messaging-Lösungen eine wichtige Rolle. Losgelöst von allen übrigen Infrastrukturen ermöglichen sie selbst im Not- und Krisenfall eine reibungslose Kommunikation über verschiedene Standorte, Abteilungen und Teams hinweg. Selbst mobil Arbeitende lassen sich im Handumdrehen erreichen und über die aktuelle Lage in Kenntnis setzen. Aber auch bei der Einführung und Nutzung eines solchen kommunikativen „Sicherheitsnetzes“ sind einige wesentliche Aspekte zu berücksichtigen, denn nicht jedes Messaging-Tool eignet sich für den geschäftlichen Einsatz. Schlimmstenfalls holen sich Organisationen nur noch mehr Probleme ins Haus.

Damit Ihnen das nicht passiert und Sie dennoch von den Vorteilen des Business Messaging profitieren können, erfahren Sie in diesem Whitepaper,

- welche Sicherheits-Themen Sie auf dem Schirm haben müssen
- wie diese sich technologisch umsetzen lassen
- welche Funktionalitäten ein Messenger dabei mitbringen muss
- welche rechtlichen Anforderungen an eine solche Lösung gestellt werden und
- wie Sie Ihre internen Kritiker von einem sicheren Messenger überzeugen

Alle Organisationsebenen, für die das Thema Sicherheit relevant ist – von der Geschäftsführung über die IT-Leitung bis hin zu den Datenschutzbeauftragten – erhalten Antworten auf die für Sie drängenden Fragen. Übersichtlich aufbereitet, steht Ihnen hier alles Wissenswerte rund um die sichere Messaging-Kommunikation zur Verfügung. Wir wünschen Ihnen eine aufschlussreiche Lektüre!

Tobias Stepan
Geschäftsführer Teamwire GmbH

100%

Betriebssicherheit und Handlungsfähigkeit

Sicherheitsanforderungen, die den Betrieb des Messengers gewährleisten

Nicht nur in Krisen- und Ausnahmesituationen sollte die Kommunikation zu einhundert Prozent sichergestellt sein – auch im Alltag sollten Organisationen den reibungslosen Austausch zwischen ihren Mitgliedern oder Mitarbeitenden stets gewährleisten. Denn nur wenn Informationsflüsse ununterbrochen stattfinden können, bleiben Organisationen handlungsfähig, egal, was geschieht. [1]

Für eine Kommunikationslösung wie den Messenger muss daher die Verfügbarkeit und Ausfallsicherheit garantiert sein. Außerdem heißt es, den Betrieb und die gesamte Infrastruktur so zu gestalten, dass die Kommunikation zu jeder Zeit sicher und entsprechend allen Vorgaben möglich ist. Beispielsweise gilt es in Notsituationen, gezielte Informationsflüsse nur für Krisenstabsmitglieder oder Führungskräfte einzurichten. Darüber hinaus muss aus technischer Sicht eine solide Basis geschaffen sein. Diese umfasst die folgenden Aspekte:

- **Hohe Verfügbarkeit und Ausfallsicherheit**
  Eine Hochverfügbarkeit lässt sich vor allem durch redundante Server-Architekturen erreichen. Dazu sollte die Kommunikationslösung auf mehreren Servern betrieben und idealerweise an verschiedenen Standorten gespiegelt werden. Das heißt, es werden drei oder mehr Server eingesetzt, obwohl einer für den Betrieb ausreichen würde. So bleibt selbst bei Ausfall eines Servers die Betriebssicherheit unangetastet.

Was heißt Betriebssicherheit? [1]

Unter Betriebssicherheit versteht man den störungsfreien und anwendungssicheren Betrieb einer Anlage, eines Systems oder einer Infrastruktur. Für Software-Anwendungen und Kommunikationslösungen bedeutet dies konkret, dass deren Einsatzbereitschaft und Verfügbarkeit zu jeder Zeit garantiert sein muss.

100%

Betriebssicherheit und Handlungsfähigkeit

Sicherheitsanforderungen, die den Betrieb des Messengers gewährleisten

Leistungsfähigkeit und Verlässlichkeit

Mithilfe redundanter Cluster-Setups oder Server lässt sich die Verlässlichkeit und Leistungsfähigkeit der Kommunikationslösung jederzeit gewährleisten, und das für Organisationen jeder Größe. Sollte es beispielsweise durch sehr hohe Nutzung Lastspitzen geben, wird die Last automatisch auf die Server verteilt. Die Zustellung von Nachrichten, Inhalten und Statusmeldungen bleibt schnell und ist konstant gesichert.

Skalierbarkeit

Ein Business Messenger sollte skalierbar sein und bei kleinen Organisationen ebenso zuverlässig funktionieren wie bei großen Konzernen. Dazu muss sich die Rechenleistung nach Bedarf anpassen lassen, sodass für alle Nutzer*innen der Organisation die zuverlässige Kommunikation sichergestellt ist. Mit einer skalierbaren Server-Architektur lässt sich das in einer Public oder Private Cloud sowie On-Premises einfach und flexibel umsetzen.

Ein Business Messenger sollte skalierbar sein und bei kleinen Organisationen ebenso zuverlässig funktionieren wie bei großen Konzernen.

Geringe Infrastrukturanforderungen

Auch wenn die Server eines Business Messengers hochverfügbar und skalierbar sein müssen, ist es trotzdem erforderlich, dass sie ressourceneffizient arbeiten und die Infrastruktur wenig belasten. Insofern sollte die Kommunikationslösung möglichst geringe Anforderungen an die Infrastruktur stellen und wenig Hardware benötigen.

Multi-Mandanten- und Multi-Domain-Fähigkeit

Unternehmen mit unterschiedlichen Geschäftsbereichen und Organisationen benötigen eine Softwarelösung, die multi-mandantenfähig ist und es ermöglicht, diese einzelnen Mandanten individuell zu verwalten. Unternehmen, die verschiedene E-Mail-Domains verwenden, sollten auf eine Kommunikationslösung setzen, die multi-domainfähig ist und automatisch Benutzerverzeichnisse für diese Domänen erstellt.

100%

Betriebssicherheit und Handlungsfähigkeit

Sicherheitsanforderungen, die den Betrieb des Messengers gewährleisten

Vollautomatisierter und sicherer Roll-out

Schnell betriebsfähig zu sein, bedeutet auch, dass der Einrichtungs- und Registrierungsprozess der Anwendung auf den Endgeräten automatisch und ohne notwendiges Eingreifen der Nutzer*innen möglich ist. Das garantiert unternehmensweite Sicherheitseinstellung und beschleunigt den Roll-out.

Zentrale Administration von Nutzer*innen

Um die Benutzerverwaltung möglichst umfassend zu zentralisieren und zu automatisieren, sollte man darauf achten, dass die Softwarelösung den Import oder idealerweise eine Synchronisation eines Lightweight Directory Access Protocoll (LDAP) beziehungsweise Active Directory (AD) ermöglicht. Eine solche Funktion stellt ein einheitliches Unternehmensverzeichnis sicher und ermöglicht es Nutzer*innen bei Bedarf einfach für alle Anwendungen zu sperren. Nebenbei sparen solche Funktionen den Administratoren viel Zeit.

100%

Betriebssicherheit und Handlungsfähigkeit

Sicherheitsanforderungen, die den Betrieb des Messengers gewährleisten

- **Nutzungs-Statistiken**
  Für Organisationen kann es auch wichtig sein, den Einsatz einer Kommunikationslösung beobachten zu können und das Nutzungsverhalten zu verstehen. So lassen sich Lastspitzen bei der Nutzung besser nachvollziehen und auch antizipieren. Hierzu sollte die Software Nutzungsstatistiken ausgeben.

Um jetzt und in Zukunft handlungsfähig zu bleiben, bedarf es nicht nur einer betriebssicheren und zuverlässigen Kommunikationslösung. Vielmehr muss diese der Organisation auch die größtmögliche Kontrolle und Datenhoheit gewährleisten – und das beginnt meist schon beim Hosting. Daher kommen in der Regel US-Anbieter nicht infrage. Warum dies so ist und, worauf Organisation in Sachen Datensouveränität achten müssen, erfahren Sie im nächsten Kapitel.

Der Organisation auch die größtmögliche Kontrolle und Datenhoheit gewährleisten – und das beginnt meist schon beim Hosting. Daher kommen in der Regel US-Anbieter nicht infrage.

100%
Datensouveränität

Sicherheitsanforderung, mit denen die Hoheit bei der Organisation liegt

Anknüpfend an die Betriebs- und Zukunftssicherheit von Systemen innerhalb von Organisationen, geht es im Bereich der Kommunikation, Kollaboration und des Informationsaustauschs auch gezielt um den Umgang mit Daten. Hierbei ist die Transparenz und Kontrolle seitens der Organisation als ein besonders hohes Gut zu betrachten: Es geht um deren Datensouveränität. [2]

Im Bereich der Software- und Anbieterwahl gilt es also zu prüfen, welche Einfluss-, Zugriff- und Kontrollmöglichkeiten die Organisation beziehungsweise ihre IT-Abteilung auf die Daten bei der Nutzung des Business Messengers hat. Das betrifft dann sowohl die technische Basis wie das Hosting als auch die Features und vor allem Konfigurationsmöglichkeiten. [3]

Freie Hosting-Wahl

Die Software und deren Hosting sollte zur IT-Strategie der Organisation passen und demnach den Betrieb der Lösung in einer sicheren Public Cloud, Private Cloud oder On-Premises auf firmeneigenen Servern gestatten. Dies sollte zudem keine Einschränkungen auf den Funktionsumfang haben.

Regeln für Datenspeicherungsfristen

Es sollte möglich sein, die Fristen für die Datenspeicherung vom IT-Administrator für alle Endgeräte und Server zu

Was ist Datensouveränität eigentlich? [2] ↓

Datensouveränität beschreibt die größtmögliche Hoheit und Kontrolle über (eigene) Daten. Eine Organisation soll mit den eigenen Daten von Mitgliedern (z. B. Mitarbeitenden) und von externen Personen (z. B. Bewerbern, Kunden oder Partnern) sowie mit eigenen Wirtschafts-, Forschungs- und Entwicklungs- sowie anderweitigen Daten selbstbestimmt umgehen können. Das heißt, die Erhebung, Speicherung, Verarbeitung und Nutzung von eigenen Daten sollte frei von Zugriffen, Beschränkungen oder Abhängigkeiten durch Dritte sein. Ansonsten besteht hier insbesondere die Gefahr, dass einerseits Daten der Organisation auch von Software-Anbietern zu eigenen Zwecken genutzt werden und andererseits eine Migration zu alternativen Anbietern nicht möglich ist. Damit verbundene Risiken sind Monopol-Bildungen am Markt, geschlossene Systeme oder nahezu knebelnde Lizenzverträge.

100%
Datensouveränität

Sicherheitsanforderung, mit denen die Hoheit bei der Organisation liegt

bestimmen, sodass Nachrichten, die eine gewisse Speicherdauer überschritten haben, automatisch von den Endgeräten oder Servern gelöscht werden. Daten werden so – insbesondere auf mobilen Endgeräten - nicht länger als notwendig vorgehalten und der Zugriff aufs Notwendige reduziert.

Ausschließlicher Serverstandort in Deutschland

Um etwaigen rechtlichen Ausnahmen in bestimmten Ländern aus dem Weg zu gehen, sollte die Organisation auf den Serverstandort Europa oder sogar Deutschland setzen – die einzige sichere Variante. Hiesige Datenschutz- und Datensicherheitsgesetze sorgen dafür, dass die Organisation allein rechtmäßiger Eigentümer der Daten ist.

Fernlöschen von Daten auf mobilen Endgeräten

Ob durch Diebstahl oder Verlust – kommen Endgeräte abhanden, sollte es möglich sein, per Fernzugriff einzelne Geräte oder Nutzer*innen zu sperren sowie etwaige Daten vom Gerät zu löschen. So lassen sich typische „Data Loss Prevention“-Szenarien einfach lösen. Auch erschweren es PIN-Codes, dass Unbefugte Zugang zur Anwendung über ein Endgerät erhalten.

Keine versteckten Analysen von Metadaten

Damit jeglicher Einfluss Dritter ausgeschlossen ist, sollte auch keine Analyse von Metadaten, Nutzerinformationen oder Kommunikation durch den Software-Anbieter stattfinden. Sollte der Anbieter Daten für den Betrieb der Lösung benötigen, muss er dies darlegen. Grundsätzlich gehören die Daten ausschließlich der Organisation selbst.

Professionelle Administration

Eine Kommunikationslösung für Organisationen sollte ein einfach zu bedienendes und professionelles Administrator-Portal beziehungsweise Dashboard bieten, um alle Nutzer und Daten

Lese-Tipp 3 ↓

Alle Hintergründe zum Dilemma mit US-Anbietern, lesen Sie auf unserem Blog!

MEHR ERFAHREN

100%

Datensouveränität

Sicherheitsanforderung, mit denen die Hoheit bei der Organisation liegt

einer Organisation jederzeit einfach und zentral steuern zu können. Hierzu zählen unter anderem die Benutzerverwaltung, Zugriffsverwaltung, Monitoring-Funktionen, unternehmensweite Richtlinien und Kommunikationsregeln.

Sicherer und steuerbarer App-Container

Die App eines Business Messengers sollte über einen eigenen sicheren Container verfügen, wo alle Nachrichten und Daten verschlüsselt gespeichert werden. Der App-Container sollte sich durch zahlreiche Richtlinien von der IT-Administration zentral konfigurieren und steuern lassen. Dadurch sind Unternehmensdaten auf Endgeräten bestmöglich geschützt und ein unkontrollierter Datenabfluss ausgeschlossen.

White Listing von Nutzer*innen

Gestattet es die Kommunikationslösung, ausgewählte Nutzer*innen, Teams und Geschäftsbereiche für die Nutzung freizuschalten, dann kontrolliert die Organisation den unternehmensweiten Einsatz des Tools und kann sicherstellen, dass nur autorisierte Mitarbeitende Zugriff haben.

Nutzer-Pooling

Lassen sich Nutzer*innen geschlossenen Bereichen (zum Beispiel Forschung und Entwicklung, Buchhaltung, Investment Banking) zuordnen, ermöglicht dies der Organisation, den Austausch von

100%
Datensouveränität

Sicherheitsanforderung, mit denen die Hoheit bei der Organisation liegt

vertraulichen Inhalten einzuschränken und Datenlecks zu verhindern.

Sichere Integration von Drittsystemen

Bei Anbindungen, Schnittstellen und APIs zu Drittanbietern gilt es vor allem sicherzustellen, dass der Datenzugriff und -austausch autorisiert ist. Es muss möglich sein den Datenzugriff jedes Drittsystems individuell zu konfigurieren und bei Bedarf jederzeit zu sperren. So kann ein Datenaustausch gesteuert erfolgen – ohne unkontrollierte Datenabflüsse.

Wer die Hoheit über seine Daten hat, muss auch die Verantwortung für deren Schutz und Sicherheit tragen – und das über die komplette Organisation und Infrastruktur hinweg und entlang der gesamten Lieferkette. Leider haben Unternehmen, deren Branche, Konkurrenten oder gar sie selbst Opfer von Cyberattacken geworden sind, noch immer nicht verinnerlicht, was sie in Sachen Cybersicherheit tun müssen. Das nachfolgende Kapitel klärt auf.

Es muss möglich sein den Datenzugriff jedes Drittsystems individuell zu konfigurieren und bei Bedarf jederzeit zu sperren. So kann ein Datenaustausch gesteuert erfolgen – ohne unkontrollierte Datenabflüsse.

100%
Cybersicherheit

Sicherheitsanforderungen zur Prävention von Cyberattacken

Das wirkungsvollste Argument dafür, das Thema Sicherheit bei jeder Software-Lösung mit einzubeziehen, ist die potenzielle Gefahr durch Cyberkriminelle. Der Bericht zur Lage der IT-Sicherheit in Deutschland 2022 des Bundesamts für Sicherheit in der Informationstechnik (BSI) bestätigt es: Die Zahl der Hackerangriff und Sicherheitsvorfälle im Bereich Cybersicherheit steigt rasant, und den wenigsten Organisationen ist bewusst, welche Risiken ihre IT-Entscheidungen wirklich bergen. [4]

Beispiele potenzieller Cybergefahren für bestimmte Branchen:

Polizei

z. B. Hackerangriffe zum Datenklau oder zur System-Lahmlegung

Gesundheits -wesen

z. B. Ransomware-Angriffe, die wichtige Systeme außer Betrieb setzen

Behörden & Ministerien authorities

z. B. Cyber-Angriffe zur Einsicht in Daten oder zur Beeinflussung kritischer Infrastrukturen

Banken & Versicherungen

z .B. Cyber-Attacken, die sensible Kunden- und Kontodaten abgreifen

Militär & Verteidigung

z. B. Cyber-Spionage- und -Sabotage

Logistik & Transport

z. B. Angriffe auf das Flot-tenmanagementsystem bei Gefahrguttranspor-ten, Verzö-gerung von Lieferketten

Versorgungs-unternehmen

z. B. Attacken auf Versorgungsnetze und Steuereinheiten, die die Versorgung unterbrechen

Produktion & Fertigung

z. B. Angriffe zur Wirtschaftsspionage

Einzelhandel

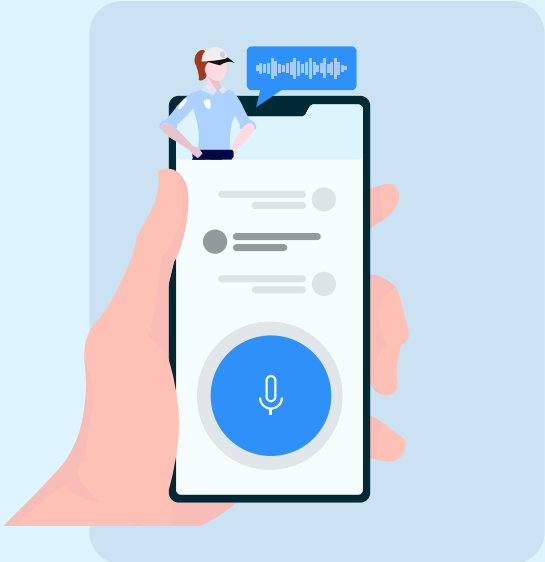
z. B. Cyber-Attacken auf Onlineshops, um Kunden- und Bezahldaten abzugreifen

Warum ist Cybersicher-heit so wichtig? [4]

Cybersicherheit beschreibt den Schutz von Systemen, Netzwerken und Anwendungen vor digitalen Angriffen. Diese Cyberattacken zielen zumeist auf den Zugriff, die Änderung oder die Zerstörung von Daten, das Erpressen von Geld oder das Stören von Prozessen. Cybersicherheit ist damit wichtigstes Gebot, um Informationen, Personen und andere Werte von Organisationen sowie diese selbst zu schützen.

100%
Cybersicherheit

Sicherheitsanforderungen zur Prävention von Cyberattacken



Aus technologischer Sicht sind demzufolge grundlegende Anforderungen zu erfüllen, um die Cybersicherheit zu gewährleisten. Dazu gehören die nachstehenden Aspekte:

- **Zero-Trust-Ansatz**
  Organisationen sind gut beraten, dem Zero-Trust-Ansatz zu folgen – das heißt, jeden internen wie externen Zugriff als potenzielle Gefahr und Angriff zu behandeln und in Sachen Authentifizierung auf Nummer sicher zu gehen. Daher sollte auch die Kommunikationslösung die Identitäts- und Rechteprüfung entsprechend umfassend abbilden und vor unberechtigten Zugriffen auf Apps, Geräten und Servern durch Nutzer, Bots oder Drittsysteme schützen. [5]

- **ISO-27001-Zertifizierung**
  Fällt die Entscheidung darauf, das Hosting dem Anbieter zu überlassen, gilt es, auf größtmögliche Sicherheit zu achten. Bewährt hat sich der Einsatz ISO-27001-zertifizierter Rechenzentren, welche neben standardisierten Sicherheitsprozessen auch eine verlässliche Infrastruktur, Netzanbindung, 24/7-Wachschutz, strenge Zugangskontrollen, Notfall-Absicherung und dergleichen bieten.

Lese-Tipp [5] ↓

Mehr darüber, wie Zero-Trust und Messenger-Kommunikation ineinandergreifen, lesen Sie online!

MEHR ERFAHREN

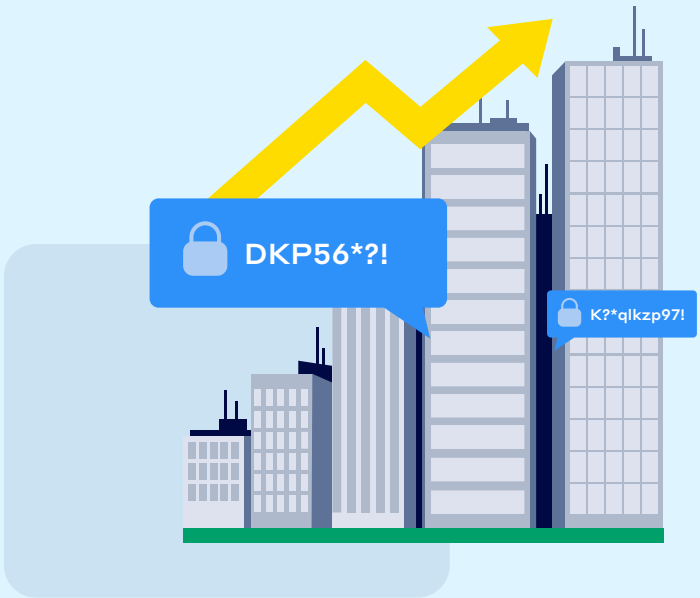
100%
Cybersicherheit

Sicherheitsanforderungen zur Prävention von Cyberattacken

Schutz der Infrastruktur und Netzwerke
Rechenzentren und Server sollten moderne Schutzmechanismen (z. B. Firewalls, Brandschutz und moderne Sicherheitssoftware) aufweisen und – strengstens bewacht – nur ausgewählten Personen den Zugriff gestatten. Die Sicherheitsrichtlinien des Anbieters sollten die Aufrechterhaltung der Schutzmaßnahmen gewährleisten.

Regelmäßige Sicherheitsanalysen
Interne und externe Audits mit Penetrationstests und Schwachstellenanalysen, die unter anderem typische Attacken simulieren, sollten in regelmäßigen Abständen beim Anbieter stattfinden. Nur so lässt sich die dauerhafte Funktionsfähigkeit der Schutzmaßnahmen und eine nachhaltige Sicherheit von Daten und Systemen garantieren.

Übertragungsverschlüsselung
Damit die Verbindung zwischen Anwendung und Servern einer Kommunikationslösung geschützt ist, sollte der Datenaustausch https-verschlüsselt erfolgen. Dabei sollten zufällige temporäre Schlüssel und gepinnte Zertifikate zum Einsatz kommen. Dadurch kann ein potenzieller Angreifer



100%
Cybersicherheit

Sicherheitsanforderungen zur Prävention von Cyberattacken

die Datenübertragung im Netzwerk im Nachhinein nicht entschlüsseln. Bei Unternehmen und Behörden empfehlen sich zudem VPN-Tunnel für den Transportkanal, die den Zugriff auf die eigene Infrastruktur absichern.

Verschlüsselung von Metadaten

Um Lauschangriffe oder „Man-in-the-middle"-Attacken zu verhindern, bei denen Angreifer häufig versuchen den https-Kanal zu kompromittieren, um sich zwischen Sender und Empfänger zu schalten und Informationen abzugreifen, gilt es die Metadaten zusätzlich vor der Übertragung zu verschlüsseln. Die Validierung und Entschlüsselung dieser Kommunikationspakete kann dann nur durch die Anwendung selbst und rechtmäßige Empfänger erfolgen. Somit sind auch die Metadaten gut geschützt.

Verschlüsselung von Nachrichten und Inhalten

Alle Nachrichten und digitalen Inhalte sollte der Sender darüber hinaus verschlüsseln und der Empfänger erst nach der Übertragung entschlüsseln. Während in manchen Fällen eine vollständige Ende-zu-Ende-Verschlüsselung notwendig ist, gibt es in der Geschäftswelt häufig Situationen in denen auch die Organisation – etwa aus Compliance-Gründen – Zugriff auf die Kommunikation ihrer Nutzer*innen benötigt. Wichtig ist eine durchgängige Verschlüsselung, bei der der Anbieter keinen Zugriff auf die Nachrichten und Inhalte hat.

Auch die Speicherung aller Daten – egal ob auf dem Smartphone, Tablet oder Desktop, auf dem Server in der Cloud oder On-Premises – sollte verschlüsselt erfolgen. Die jeweiligen Schlüssel hierfür sollten unter der Kontrolle der Organisation sein.

Verschlüsselte Datenspeicherung

Auch die Speicherung aller Daten – egal ob auf dem Smartphone, Tablet oder Desktop, auf dem Server in der Cloud oder On-Premises – sollte verschlüsselt erfolgen. Die jeweiligen Schlüssel hierfür sollten unter der Kontrolle der Organisation sein.

100%
Cybersicherheit

Sicherheitsanforderungen zur Prävention von Cyberattacken

- **Zwei-Faktor-Authentifizierung für Administratoren**
  Der Zugriff auf das Administrations-Portal sollte durch eine Zwei-Faktor-Authentifizierung abgesichert sein. Administratoren müssen ein Passwort und einen App-basierten zweiten Faktor eingeben, um auf das Administrations-Portal und vertrauliche Firmendaten zugreifen zu können.

- **Autorisierung von Endgeräten durch MDM/EMM**
  Durch Registrierungstoken und sichere App-Tunnel von MDM (Mobile Device Management)- und EMM (Enterprise Mobility Management)-Lösungen können Organisationen gewährleisten, dass ausschließlich autorisierte Geräte Zugriff auf die Anwendung und die Infrastruktur haben. Zudem gestattet eine Integration in das EMM der Organisation eine erweiterte Konfiguration der Anwendung – zum Beispiel bei der Festlegung von Regeln, die ein Teilen oder Kopieren von Nachrichten mit anderen Applikationen erlauben oder auch verhindern. [6]

Beim Schutz vor Cyberangriffen und Verlust von Daten stehen vor allem jene Informationen im Fokus, die für das Unternehmen einen hohen Wert besitzen. Dazu gehören oftmals auch personenbezogene Daten, die aus auch rechtlicher Sicht besonders zu schützen gilt. Welche Datenschutzanforderungen sich auf die Messenger-Kommunikation beziehen und wie sie sich erfüllen lassen, verrät Ihnen das folgende Kapitel.

Lese-Tipp [6] ↓

Wie Enterprise Mobility Management das sichere Messaging ergänzt, erfahren Sie auf unserem Blog!

MEHR ERFAHREN

100%
Datenschutz

Sicherheitsanforderungen zum Schutz personenbezogener Daten

Datenschutz ist eines der höchsten Güter unserer Zeit. Das im Grundrecht verankerte Recht auf informationelle Selbstbestimmung sichert jeder natürlichen Person zu, über die Art und Weise der Verarbeitung und Verwendung persönlicher Daten selbst entscheiden zu dürfen. Damit einhergehend gibt es konkrete gesetzliche Vorgaben, die dazu dienen, dieses Recht zu schützen. Verankert in der EU-Datenschutzgrundverordnung (DSGVO) sowie dem Bundesdatenschutzgesetz (BDSG) beinhalten sie konkrete Anforderungen an alle Organisationen, die personenbezogene Daten erheben, verarbeiten, speichern oder nutzen. [7]

DSGVO und deutsches Recht als Basis

Der Anbieter sollte Daten in Übereinstimmung mit den datenschutzrechtlichen Anforderungen der DSGVO sowie dem deutschen Recht verarbeiten. Ebenso sollte eine Verarbeitung von Daten einzig und allein nach ausdrücklicher Zustimmung erfolgen.

Datensparsamkeit und Datenvermeidung

Generell sollte ein Zugriff auf Daten durch einen Anbieter nur erfolgen, wenn es für die Bereitstellung des Dienstes notwendig ist. Insofern sollte der Anbieter nur auf personenbezogene Daten zugreifen, wenn es aus Sicherheits- oder Administrationsgründen absolut notwendig ist. Zudem sollten nicht mehr benötigte oder ältere Daten automatisch gelöscht werden. So lassen sich die DSGVO-Grundsätze der Datensparsamkeit und -vermeidung bestmöglich einhalten.

DSGVO-konforme Verträge

Es gilt, mit dem Anbieter ein Auftragsverarbeitungsvertrag der Lösung zu schließen, der alle Anforderungen der DGSVO erfüllt. Zudem sollte der Anbieter über eine gut auffindbare und leicht verständliche Datenschutzerklärung verfügen sowie Transparenz über alle Prozesse und Aktivitäten der Datenverarbeitung schaffen. [8]

Datenschutz vs. Datensicherheit – was ist der Unterschied? [7]

Datenschutz umfasst alle rechtlichen Aspekte im Hinblick auf die Erhebung, Verarbeitung und Verwertung personenbezogener Daten. Personendaten sind alle Informationen, die eine Person identifizieren oder identifizierbar machen. Datensicherheit hingegen befasst sich mit dem generellen Schutz von Daten – auch, aber nicht ausschließlich mit personenbezogenen Daten.

100%
Datenschutz

Sicherheitsanforderungen zum Schutz personenbezogener Daten

Anonymisierung und Verschlüsselung von Nutzerdaten

Die Kommunikationslösung sollte den Schutz personenbezogener Daten (z. B. IDs, Telefonnummern, E-Mail-Adressen und Passwörter) durch Anonymisierung und Verschlüsselung gewährleisten.

Mehrfach-Authentifizierung

Die Nutzer*innen der Lösung sollten sich über mehrere Stufen identifizieren lassen. Neben der Telefonnummer und der E-Mail-Adresse können dies auch IDs oder PINs als zweiter Faktor sein, die fortlaufend überprüft werden und so die Nutzer*innen zuverlässig authentifizieren. [9]

Keine komplizierten Einstellungen

Die Kommunikationslösung sollte im Idealfall für die sichere und vertrauliche Kommunikation im Team entwickelt sein und auf komplizierte Datenschutzeinstellungen verzichten. Datenaustausch und Kommunikation sollte per se immer datenschutzkonform und sicher sein.

Datenspeicherung auf Endgeräten

Es ist empfehlenswert, dass das Adressbuch mit allen Kontaktdaten nicht auf den Servern des Anbieters, sondern nur auf dem Endgerät des Nutzers gespeichert wird. Auch Nutzerdaten und Nachrichten sollten auf dem Endgerät verschlüsselt abgelegt werden, sodass die Daten der Organisation bestmöglich geschützt und getrennt von anderen Applikationen sind.

Sicherung und Löschung von Daten

Alle Daten sind regelmäßig und automatisch zu sichern. Dabei sollte der Backup redundant an mehreren Standorten erfolgen, um gegen Datenverlust gewappnet zu sein. Zudem sollten Daten nicht länger gespeichert werden, als es die Organisation

Lese-Tipp [8] ↓

Warum und wie Sie bei der Kommunikation keine Kompromisse in Sachen Datenschutz eingehen (sollten), verraten wir Ihnen in unserem Blog!

MEHR ERFAHREN

Privacy by Design und Privacy by Default – was ist damit gemeint? [9] ↓

Privacy by Design beschreibt die Einhaltung des Datenschutzes durch Technikgestaltung. Das heißt, dass jede Softwarelösung so konzipiert sein sollte, dass sie gesetzliche Vorgaben quasi „ab Werk“ umsetzt. Unter Privacy by Default versteht man starke datenschutzrechtliche Voreinstellungen als Standard, welche die Rechte betroffener Personen bestmöglich wahren.

100%
Datenschutz

Sicherheitsanforderungen zum Schutz personenbezogener Daten

wünscht. Idealerweise sind Inhalte und Nachrichten nach einem definierten Zeitraum zu löschen.

Neben den allgemeinen Anforderungen, sich als Organisation im Hinblick auf Datensouveränität und Datenschutz sicher aufzustellen und die Betriebs- sowie Cybersicherheit zu gewährleisten, sind auch Ansprüche von gesetzlicher Seite und Compliance-Vorgaben zu berücksichtigen. Was das konkret für bestimmte Branchen bedeutet, zeigt das folgende Kapitel.

Datenspeicherung auf EndgerätenEs ist empfehlenswert, dass das Adressbuch mit allen Kontaktdaten nicht auf den Servern des Anbieters, sondern nur auf dem Endgerät des Nutzers gespeichert wird.

100%

Revisionssicherheit und Compliance

Sicherheitsanforderungen, die aus rechtlicher Sicht zu erfüllen sind

Was bedeutet Compliance? [10]

Compliance bedeutet wörtlich übersetzt „Einhaltung". Gemeint ist hierbei die Erfüllung von ethischen, rechtlichen und gesetzlichen Anforderungen innerhalb einer Organisation durch diese selbst und ihre Mitarbeitenden. Es handelt sich also um Maßnahmen, die dazu dienen, den Organisationszweck rechtskonform zu erfüllen und (z. B. straf- sowie zivilrechtliche) Risiken zu minimieren.

Bestimmte Branchen sehen sich verschiedenen rechtlichen Anforderungen gegenüber – wie etwa einer Verschwiegenheitspflicht, notwendigen Risikobeurteilungen oder der erforderlichen Archivierung von Daten. Auch branchenübergreifende Gesetze wie etwa das Lieferkettengesetz und die Datenschutzgrundverordnung spielen hierbei eine Rolle. Damit einher gehen zumeist interne Ansprüche an das Verhalten der Organisationsmitglieder und Mitarbeitenden. Dies betrifft in Besonderem Maße auch die Kommunikation rund um die Arbeitsabläufe und somit die Nutzung von Kommunikationslösungen wie einen Business Messenger. [10]

Beispiele spezifischer Gesetze und Vorgaben für die Compliance:

Polizei
z. B. Einsatz-Dokumentation

Gesundheits-wesen
z. B. ärztliche Schweige-pflicht, Dokumen-tationspflicht

Behörden & Ministerien
z. B. Dokumentations-pflicht, Wahlgesetz

Banken & Versicherungen
z. B. Wertpapierhan-delsgesetz, MiFID-II, DORA

Militär & Verteidigung
z. B. Geheimhaltungs-pflicht, Sabotage-Abwehr

Logistik & Transport
z. B. Gefahrgut-beförderung, Export-kontrolle

Versorgungs-unternehmen
z. B. IT-Sicherheitsgesetz, KRITIS-Verordnung

Produktion & Fertigung
z. B. Umwelt- und Arbeits-schutz

Einzelhandel
z. B. Grundsätze des ehrbaren Kaufmanns

100%

Revisionssicherheit und Compliance

Sicherheitsanforderungen, die aus rechtlicher Sicht zu erfüllen sind

Die Anforderung, die Kommunikation über einen Messenger zu dokumentieren und revisionssicher zu archivieren, betrifft die Mehrheit aller Organisationen. Diese ergeben sich zumeist aus steuerrechtlichen und buchhalterischen Pflichten, gesetzlichen Vorgaben, ethischen Richtlinien oder der internen Compliance. Fakt ist insofern auch, dass Organisationen, die ihre geschäftliche Kommunikation nicht archivieren, mit rechtlichen Problemen rechnen sollten. Ebenso betrifft dies die Frage nach Zugriffsrechten für einzelne Organisationsmitglieder und -gruppen. Daher sind die nachfolgenden Punkte zwingend zu berücksichtigen.

- **Abbildung von Berechtigungen & Sicherheitsrichtlinien**
  Für ein organisationsweit sicheres Messaging bedarf es der Abbildung von Rollen und Berechtigungen im Rahmen eines dedizierten Zugriffsmanagements sowie durch granulare Sicherheits-, Datenschutz- und Compliance-Richtlinien, die Unternehmensdaten schützen und rechtliche Vorgaben wahren.

- **Archivierungsoptionen**
  Nachrichten und Daten der Organisationsmitglieder sollten sich einfach und verschlüsselt archivieren lassen. Die Definition der Archivierung sollte nach spezifischen Zeiträumen und Nutzungsgruppen oder Mandanten erfolgen können und durchsuchbar sein. Zudem sollte ein Zugriff auf das revisionssichere Archiv sowie dessen Durchsuchung nur autorisierten Personen (z. B. Datenschutzbeauftragten, internen Revisoren) möglich sein. [11]

- **Protokollierung**
  Für die zuverlässige Dokumentation aller Aktivitäten sind Audit Logs hilfreich, die ein chronologisches Protokoll erstellen. Damit lassen sich alle administrations-, aber auch compliance-relevanten Vorgänge aufzeichnen und bei Bedarf replizieren. Dazu sollten die Audit Logs durchsuchbar sein: Aktivitäten lassen

Lese-Tipp [11] ↓

Welche Vorgaben unter Umständen für eine revisionssichere Archivierung zu beachten sind, haben wir für Sie zusammengefasst!

MEHR ERFAHREN

100%

Revisionssicherheit und Compliance

Sicherheitsanforderungen, die aus rechtlicher Sicht zu erfüllen sind

sich bequem ermitteln und maschinelle Auswertungen ebenso einfach durchführen.

Revisor-Zugänge

Häufig muss die Erfüllung der Compliance- und gesetzlichen Vorgaben durch Revisoren oder externe Prüfer begutachtet werden. Deswegen ist ein Zugang zu den relevanten dokumentierten Daten – und nur zu diesen – wichtig und sollte sich ein Revisor-Zugang mit beschränkten Rechten für Prüfer, Auditoren oder Revisoren einrichten lassen. Dies unterstützt ein revisionssicheres Arbeiten und die Compliance, ohne dass damit unnötig Daten verteilt werden müssen.

Von Compliance und Revisionssicherheit über Datensouveränität und Cybersicherheit bis hin zum Datenschutz – für Geschäftsführung, IT und Datenschutzbeauftragte gibt es teilweise unterschiedliche, aber auch überschneidende Anforderungen hinsichtlich der sicheren Kommunikation innerhalb der Organisation. Um die passende Messaging-Lösung zu finden oder die eigenen Tools zu überprüfen, bringt die abschließende Checkliste noch einmal alle relevanten Aspekte auf den Punkt.

Für die zuverlässige Dokumentation aller Aktivitäten sind Audit Logs hilfreich, die ein chronologisches Protokoll erstellen. Damit lassen sich alle administrations-, aber auch compliance-relevanten Vorgänge aufzeichnen und bei Bedarf replizieren.

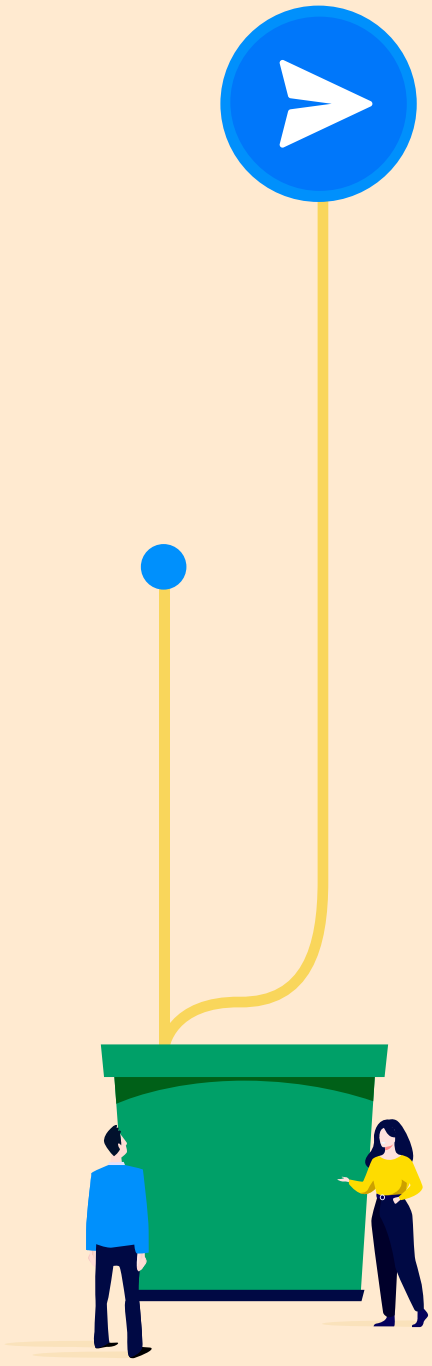
Checkliste von A bis Z: Sicher mit Ihrem Messenger?

Welche Sicherheitsanforderungen ein Messenger für eine zuverlässige und sichere Kommunikation innerhalb der Organisation erfüllen sollte, zeigt die folgende Übersicht – von A wie Abbildung von Berechtigungen bis Z wie Zwei-Faktor-Authentifizierung:

- Abbildung von Berechtigungen & Sicherheitsrichtlinien
- Anonymisierung und Verschlüsselung von Nutzerdaten
- Archivierungsoptionen
- Ausschließlicher Serverstandort in Deutschland
- Autorisierung von Endgeräten durch MDM/ EMM
- Datensparsamkeit und Datenvermeidung
- Datenspeicherung auf Endgeräten
- DSGVO und deutsches Recht als Basis
- DSGVO-konforme Verträge
- Fernlöschen von Daten auf mobilen Endgeräte
- Freie Hosting-Wahl
- Geringe Infrastrukturanforderungen
- Hohe Verfügbarkeit und Ausfallsicherheit
- ISO-27001-Zertifizierung
- Keine komplizierten Einstellungen
- Keine versteckten Analysen von Metadaten
- Leistungsfähigkeit und Verlässlichkeit
- Mehrfach-Authentifizierung
- Multi-Mandanten- und Multi-Domain-Fähigkeit
- Nutzer-Pooling
- Nutzungs-Statistiken
- Professionelle Administration
- Protokollierung
- Regelmäßige Sicherheitsanalysen
- Regeln für Datenspeicherungsfristen
- Revisor-Zugänge
- Schutz der Infrastruktur und Netzwerke
- Sichere Integration von Drittsystemen
- Sicherer und steuerbarer App-Container
- Sicherung und Löschung von Daten
- Skalierbarkeit
- Übertragungsverschlüsselung
- Verschlüsselte Datenspeicherung
- Verschlüsselung von Nachrichten und Inhalten
- Verschlüsselung von Metadaten
- Vollautomatisierter und sicherer Roll-out
- White Listing von Nutzer*innen
- Zentrale Administration von Nutzer*innen
- Zero-Trust-Ansatz
- Zwei-Faktor-Authentifizierung für Administratoren

Machen Sie jetzt den Check · mit Ihren geplanten oder bereits installierten Messenger!

Fazit



Wie jede andere Software muss sich auch eine Kommunikationslösung reibungslos in die IT-Landschaft einer Organisation integrieren. Dabei sind Sicherheitsanforderungen für Compliance, Betriebssicherheit, Datensouveränität, Cybersicherheit und Datenschutz essenzielle Aspekte, die eine reibungslose Funktionsweise gewährleisten und die Vertraulichkeit der Kommunikation über diese Lösung sicherstellen. Insbesondere ein Business Messenger, dessen besonderer Vorteil in der Verbindung aller Mitarbeitenden – ob im Büro, remote oder mobil tätig – liegt, muss über alle Endgeräte hinweg hundertprozentige Sicherheit bieten.

Damit schützen sich Organisationen vor potenziellen Cybergefahren, erfüllen alle rechtlichen Anforderungen an ihre Kommunikation und sorgen für den Schutz jedweder Daten – ob unternehmenskritisch oder personenbezogen. Dies festigt schon heute, aber auch langfristig betrachtet, die Zukunftsfähigkeit einer Organisation.

Über Teamwire

Die Teamwire GmbH hat sich mit der gleichnamigen Business Messenger App auf die sichere, einfache und schnelle Kommunikation über Text- und Sprachnachrichten sowie Videotelefonie spezialisiert. Das 2015 gegründete Unternehmen mit Hauptsitz in München hilft Unternehmen, Behörden, Blaulicht-Organisationen und dem Gesundheitswesen die Produktivität und Ergebnisse der mobilen Zusammenarbeit zu verbessern. Der Business Messenger bietet innovative Funktionen, die auf die Anwendungsfälle von Unternehmen mit vielen mobilen Arbeitskräften abgestimmt sind, und gewährleistet dabei eine professionelle Administration und höchste Sicherheitsanforderungen. Das Unternehmen erfüllt alle europäischen Datenschutzanforderungen und die DSGVO. Zahlreiche Kunden vertrauen auf Teamwire, darunter die Polizei, das Bundesministerium für Arbeit und Soziales, das Klinikum Chemnitz, Dataport und Vodafone.

teamwire.eu

Impressum

Herausgeber
Teamwire GmbH
Tittmoninger Straße 11
81679 München

teamwire.eu
E-mail: **info@teamwire.eu**

Geschäftsführung:
Tobias Stepan
Registergericht: Amtsgericht München
HRB 187102

Konzeption
Tobias Stepan, Teamwire GmbH, teamwire.eu
Katja Dreißig und Jennifer Köhler, Möller Horcher Kommunikation GmbH, moeller-horcher.de

Text
Jennifer Köhler, Möller Horcher Kommunikation GmbH, moeller-horcher.de

Layout & Grafik
Salva González, Pilar Sabogal, Teamwire GmbH, teamwire.eu

Version 1.0
Die Inhalte des Whitepapers wurden mit größter Sorgfalt erstellt. Für die Richtigkeit, Vollständigkeit und Aktualität können wir jedoch keine Gewähr übernehmen.