

Datenschutz und Sicherheit von Teamwire

Einleitung

Teamwire ist eine sichere und verschlüsselte Enterprise Messaging Lösung. Als deutsche Firma erfüllt Teamwire alle deutschen und europäischen Datenschutzanforderungen. Teamwire kann einfach administriert werden und gewährleistet unternehmensweite Sicherheitsrichtlinien. Die Lösung kann sowohl in der Cloud wie On-Premise installiert werden. Dieses Informationsblatt gibt eine Übersicht über alle Sicherheits- und Datenschutz-Features von Teamwire.

KOMPLETTE VERSCHLÜSSELUNG

Verschlüsselte Nachrichten

Alle Nachrichten und digitalen Inhalte werden automatisch vom Sender verschlüsselt, und erst nach der Übertragung vom Empfänger entschlüsselt (AES 256-bit und andere sichere Algorithmen).

Verschlüsselte Meta Data

Um gegen Lauschangriffe und „Man-in-the-middle“-Attacken zu schützen, werden alle Metadaten zusammen mit den verschlüsselten Nachrichten vor der Übertragung verschlüsselt (AES 256-bit). Nur die App und die Server können diese Datenpakete entschlüsseln.

Verschlüsselte Übertragung

Um die Verbindung zwischen der App und den Servern zu schützen, wird jeder Datenaustausch zusätzlich mit HTTPS verschlüsselt übertragen (TLS 256-bit mit „Perfect Forward Secrecy“).

Verschlüsselte Datenspeicherung

Teamwire nutzt modernste Technologie zur sicheren Datenspeicherung. Alle Nachrichten, digitalen Inhalte und Nutzerdaten werden auf den Servern verschlüsselt abgespeichert (AES 256-bit).

STARKER SCHUTZ DER PRIVATSPHÄRE

Anonymisierte Nutzerdaten

Der Schutz der Privatsphäre hat bei uns höchste Priorität. Teamwire anonymisiert persönliche Daten weitgehend und behandelt alle Daten absolut vertraulich.

Einweg-verschlüsselte Passwörter

Alle IDs, Telefonnummern, Emailadressen und Passwörter werden mit Einweg-Verschlüsselungs-Funktionen umgewandelt bevor sie abgespeichert werden (SHA-256 und andere sichere Algorithmen).

Mehrfach Authentifizierung

Teamwire-Nutzer werden über ihre Emailadresse und Telefonnummer authentifiziert bevor sie mit Kollegen und Teams kommunizieren können. Mehrere eindeutige IDs und Faktoren werden laufend überprüft, um einen Nutzer zu authentifizieren.

Schutz der firmeninternen Kommunikation

Teamwire wurde ausschließlich für die firmeninterne Kommunikation mit Kollegen und Teams entwickelt. Da keine Möglichkeit besteht Nachrichten öffentlich auszutauschen, bleibt die gesamte interne Kommunikation geschützt und vertraulich.

Keine komplizierten Einstellungen

Es gibt keine komplizierten Einstellungen zum Schutz der Privatsphäre: Ein Nutzer wählt die Empfänger einer Nachricht aus, und die Nachricht wird dann exklusiv an diese Kollegen gesendet. Einfacher geht es nicht.

Keine Speicherung des Adressbuchs

Alle Kontaktdaten werden mit Hashfunktionen anonymisiert (SHA-256), und nach dem Verbinden mit Kollegen sofort wieder von den Servern gelöscht. Teamwire speichert das Adressbuch der Nutzer NICHT ab.

SICHERE INFRASTRUKTUR

Private Cloud oder On-Premise Lösung

Unabhängig davon, welche Strategie ein Unternehmen für seine IT-Infrastruktur verfolgt, bietet Teamwire die passende Lösung: Kunden können Teamwire in unserer privaten Cloud hosten oder On-Premise auf firmeneigenen Servern installieren.

ISO-27001 zertifizierte Datenzentren

Alle Datenzentren von Teamwire sind ISO-27001 zertifiziert. Die Datenzentren bieten eine exzellente Netzanbindung, werden durch Werkschutzpersonal rund um die Uhr 7 Tage die Woche geschützt, sind videoüberwacht, zeichnen sich durch strenge Zugangskontrollen aus und sind selbst für Notfälle (z.B. Stromausfall) bestens ausgerüstet.

Umfassender Netzwerkschutz

Die Server liegen hinter robusten „Firewalls“, die nur ausgewählten Nutzern Zugriff

erlauben. Das Netzwerk von Teamwire wird dabei laufend überwacht und überprüft (24/7). Darüberhinaus führen wir regelmäßige Sicherheitsanalysen durch.

99,9% verfügbare Betriebszeit

Teamwire verwendet mehrere Server an verschiedenen Orten um eine möglichst hohe Verfügbarkeit sicherzustellen. Teamwire garantiert mindestens 99,9% verfügbare Betriebszeit.

Strenge Sicherheitsrichtlinien

Teamwire behandelt Daten absolut vertraulich und wendet strenge unternehmensweite Sicherheitsrichtlinien an, um einen Zugriff auf seine Infrastruktur, Datenzentren und Systeme einzuschränken bzw. zu verhindern.

Interne und externe Audits

Teamwire führt regelmäßig Audits inkl. Penetrationstests und Schwachstellenanalysen durch. Wir arbeiten auch mit Sicherheitsverbänden, Prüfungsfirmen und Hackern bei Sicherheitstests zusammen.

VOLLSTÄNDIGER DATENSCHUTZ

Datenspeicherung in Deutschland

Teamwire entspricht den Datenspeicherungsanforderungen von deutschen und europäischen Firmen vollständig. Alle Nutzerdaten, -nachrichten und -inhalte werden ausschließlich auf Servern in Deutschland gespeichert.

Deutsches Datenschutzrecht

Teamwire ist das Produkt einer deutschen Firma mit Hauptsitz in München, und erfüllt alle Auflagen des deutschen wie europäischen Datenschutzrechts.

Datensparsamkeit und Datenvermeidung

Teamwire verwendet für den Betrieb seiner Messaging Lösung so wenig Daten wie möglich, und auf personenbezogene Daten wird nur zugegriffen, wenn es aus Sicherheits- oder Administrationsgründen absolut notwendig ist.

Kontinuierliche Sicherung von Daten

Alle Daten werden synchron auf mehrere Server geschrieben, regelmäßig gesichert und verschlüsselt an verschiedenen Orten gespeichert.

Regelmäßige Löschung alter Daten

Daten werden nicht länger gespeichert als sie vom Kunden benötigt werden. Je nach Kundenanforderung, können zugestellte Nachrichten und ältere Inhalte regelmäßig und

automatisch von den Servern gelöscht werden.

Sichere Speicherung auf dem Endgerät

Die Nutzerdaten und Nachrichten werden auf dem Endgerät verschlüsselt gespeichert, um Unternehmensdaten zu schützen und zu trennen.

Sichere Integration und Anbindung

Teamwire hat die Anbindungen, Schnittstellen und APIs zu Drittanbietern selbst entwickelt. Teamwire kontrolliert alle mit diesen Lösungen ausgetauschten Daten vollständig und verhindert unkontrollierte Datenabflüsse.

PROFESSIONELLE IT-ADMINISTRATION

Administrations-Portal

Alle Nutzer einer Firma können über ein Administrations-Portal verwaltet werden. Der IT-Administrator kann Nutzer einladen, managen und den Zugriff von Mitarbeitern autorisieren bzw. sperren. Die Nutzerverwaltung erlaubt auch die Vorkonfigurierung der App und die Festlegung von Kommunikationsregeln.

Active Directory und LDAP Unterstützung

Teamwire bietet eine umfassend Integration in Active Directory und LDAP. Nutzer und auch Gruppen können leicht aus diesen Verzeichnissen importiert und laufend synchronisiert werden. Darüberhinaus können Veränderungen in diesen Verzeichnissen automatisch in Teamwire übernommen werden.

White Listing von Nutzern

Ausgewählte Nutzer, Teams und Geschäftsbereiche können für Teamwire freigeschalten werden. Damit kontrolliert die Firma den unternehmensweiten Einsatz von Teamwire und kann sicherstellen, dass nur autorisierte Mitarbeiter Zugriff auf Teamwire haben.

Pooling von Nutzern

Mitarbeiter können über das Administrations-Portal geschlossenen Bereichen zugeordnet werden (z.B. Forschung & Entwicklung, Buchhaltung, Investment Banking, usw.). Dies ermöglicht es einer Firma den Austausch von vertraulichen Inhalten einzuschränken und Datenlecks zu vermeiden.

Vorkonfigurierte Gruppen

Über das Administrations-Portal können Gruppen für Nutzer vorkonfiguriert werden. Diese Gruppen (z.B. Projektteams, Abteilungen, Unternehmenseinheiten, usw.) sind dann in der Teamwire App verfügbar, und erleichtern auch das "Onboarding" für die Nutzer.

Daten-Archivierung

Die Nachrichten und Daten der Nutzer einer Firma können über das Administrations-Portal archiviert werden. Die Archivierung kann für spezifische Zeiträume und Nutzergruppen erfolgen.

Multi-Domain Unterstützung

Teamwire unterstützt die Verwendung von mehreren Domains in einem Unternehmen. Mitarbeiter oder Organisationen mit verschiedenen Emaildomains können auf den selben Server geleitet werden. (Dies funktioniert sowohl für die Cloud- wie On-Premise-Lösung.)

Mandantenfähigkeit

Teamwire bietet eine moderne Mandantenfähigkeit. Ein Unternehmen kann einzelne Mandanten für unterschiedliche Tochtergesellschaften und Organisationseinheiten anlegen und verwalten. Außerdem kann ein Unternehmen Super-Administratoren bestimmen, die befugt sind, alle Mandanten zu verwalten.

MOBILE APPLICATION MANAGEMENT

Zugriff von Nutzern sperren

Der IT-Administrator kann problemlos den Zugriff eines Nutzers sperren, falls ein Mitarbeiter das Unternehmen verlässt oder dessen Endgerät gegebenenfalls kompromittiert wurde.

Daten „remote“ löschen

In möglichen „Data Loss Prevention“ Szenarien, wo das Endgerät gestohlen oder verloren wurde, kann der IT-Administrator alle Daten und Inhalte der App auf dem Endgerät „remote“ löschen.

Unternehmensweite Regeln

Es können unternehmensweite Regeln für alle Nutzer festgelegt werden, die die Verbreitung von Nachrichten via Copy&Paste oder das Versenden von digitalen Inhalten verhindern (z.B. Fotos, Ortsangaben, usw.).

Passcodes für Nutzer

Um eine zusätzliche Sicherheitsebene einzuziehen, kann der IT-Administrator für jeden Mitarbeiter einen PIN Passcode für den Zugriff auf die Teamwire App festlegen.

Sicherer App-Tunnel

Teamwire unterstützt sicheres App-Tunneln um den Zugriff auf das Firmennetzwerk zu steuern und zu schützen. Ein sicherer App-Tunnel verhindert den Zugriff von nicht autorisierten Geräten und kann in BYOD-Szenarien wichtig sein.

Registrierungs-Token

Der IT-Administrator kann einen Registrierungs-Token für die Endgeräte seiner Nutzer festlegen, und somit den Zugriff und die Nutzung von Teamwire auf nicht gemanagten Endgeräten verhindern.

Enterprise Mobility Management Integration

Teamwire ist voll in führende Enterprise Mobility Management Lösungen integriert (z.B. ist Teamwire ein Partner von MobileIron und von Airwatch). Die App kann problemlos unternehmensweit konfiguriert werden und gewährleistet die Umsetzung von internen Sicherheitsrichtlinien für mobile Endgeräte.

Über Teamwire

Teamwire ist eine schnelle, einfach zu benutzende und sichere Enterprise Messaging App. Teamwire verbessert die interne Kommunikation mit Kollegen und Teams, und hilft mittelständischen Unternehmen und Konzernen die Produktivität zu steigern. Nutzer können 1:1 und in Gruppen kommunizieren, und beliebige digitale Inhalte wie Termine, Dateien, Ortsangaben, Fotos, Video- und Sprachnachrichten, und vieles mehr in Echtzeit austauschen. Als deutsche Firma erfüllt Teamwire alle europäischen Datenschutzanforderungen. Die vollständig verschlüsselte Lösung kann einfach unternehmensweit administriert werden und gewährleistet firmeninterne Sicherheits-Richtlinien. Teamwire ist für alle mobilen Endgeräte und Desktop-Computer als "private Cloud" oder "On-Premise" Lösung verfügbar.

Weitere Informationen: <http://www.teamwire.eu>