Teamware GmbH und TeamFON GmbH Technische und organisatorische Maßnahmen (Art. 32 Abs. 1 DS-GVO)

Inhaltsverzeichnis

Alle technischen und organisatorischen Maßnahmen der Firma Teamware GmbH und TeamFON GmbH werden in einem Intranet in einem Information Security Management System (ISMS) revisionssicher dokumentiert und den Mitarbeitern zur Verfügung gestellt.

I. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1. Zutrittskontrolle

a. Büroräume

Gebäudesicherung durch zentrale Schließanlage.

Getrennte Sicherung der Büroeingangstüre durch elektronisch codierten Schlüssel (Transponder). Die Transponder sind personalisiert pro Mitarbeiter und bieten nur den Zugang zu relevanten Bürobereichen.

Absicherung der Büros mit einer Alarmanlage inkl. Brand-/Rauchmelde-Anlage mit Aufschaltung auf eine Sicherheitsfirma.

Zusätzliche Sicherung des Serverraums durch eine Zugangstüre und getrennte Zonen in der Alarmanlage.

Im Rahmen einer gesonderten Besucherregelung ist festgelegt, dass jeder Besucher in das Besucherbuch einzutragen ist.

b. Rechenzentrum

Gebäudesicherung durch Foto-ID-Zugangskarten mit PIN-Codes. Diese befinden sich an allen wichtigen Türen und werden ebenfalls zum Schutz bestimmter Gateway-Bereiche eingesetzt.

Sämtliche Außentüren sind alarm- /kamera- und videoüberwacht.

Zur Verifizierung der Person wird neben einer persönlichen Überprüfung im Eingangsbereich ebenfalls auf Handflächenscanner an wichtigen Zugangstüren zurückgegriffen. Das Zugangskontrollsystem überwacht und protokolliert alle Zugänge. Die Protokolle werden für 6 Monate aufbewahrt.

Zusätzlich werden die Serverschränke über eine getrennte Schließanlage gesperrt.

2. Zugangskontrolle

Vorgabe und Regelung zur Passwort-Sicherheit: Mindestlänge von 8 Zeichen mit einer guten Komplexität sowie eine Änderung alle 6 Monate.

Getrennte Passwörter und Zugriffe auf Live- und Entwicklungssystemen.

Automatische Bildschirmsperre mit Passwort-Aktivierung auf allen Arbeitsplätzen.

Getrennte Netzwerke (DMZ) für Arbeitsplätze, Telefone und einzelne Serverbereiche.

Remotezugang mit Netzwerkzugriff nur auf spezielle Arbeitsplätze mit VPN Einwahl. Hierfür werden vom normalen Login unabhängige Zugangsdaten benötigt: Benutzername, Passwort + Token für eine Zwei-Faktor-Authentifizierung.

Sicherung der Netzwerkzugriffe durch Security Appliances und Firewalls von den Herstellern Cisco und Sophos. Diese verwenden Packetfilter-Listen die ausschließlich vordefinierten IP

Verkehr erlauben. Policy-Verletzungen werden auf einem eigenen Logserver mitprotokolliert. Die entsprechenden Logfiles werden täglich gesichert.

3. Zugriffskontrolle

Jeder Mitarbeiter hat ein individuelles Login für seinen Arbeitsplatz und Server-Zugriff.

Trennung von sensiblen Daten durch getrennte Berechtigungsstufen und Zugriffsrechte für bestimmte Systeme. Hierzu zählen insbesondere folgende Systeme: Buchhaltungssystem, CRM System, Ticket-System, Telefon-Systeme und Wiki-System für die Dokumentation.

Checklisten für die Verarbeitung sensibler Daten wie beispielsweise Backup. Die Verarbeitung dieser sensiblen Daten erfolgt nur durch gesondert ernannte Mitarbeiter.

Die Backups werden verschlüsselt.

4. Trennungskontrolle

Es kommen getrennte Systeme zum Einsatz. Im Regelfall gibt es ein Entwicklungssystem, ein Staging System und Live-Systeme. Die Systeme werden mit unterschiedlichen Datenbanken betrieben. Die personenbezogenen Daten befinden sich nur auf Live-Systemen, auf welche die Entwickler keinen direkten Zugriff haben. Eine Dateninhaltsübertragung zwischen den Systemen findet nicht statt.

Die Mitarbeiter sind in Teams unterteilt. Jedes Team kann nur auf die für das jeweilige Team relevanten Daten zugreifen.

5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Soweit möglich werden personenbezogener Daten pseudonymisiert verarbeitet. Dies betrifft insbesondere die automatische Überwachung der Systeme.

II. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

1. Weitergabekontrolle

Der Zugriff auf Systeme wird nur mit verschlüsseltem Zugang gewährt. Dafür werden VPN-Verbindungen und zusätzlich verschlüsselte Zugänge über SSH genutzt.

Datenbackups die an externen Orten gelagert werden, sind verschlüsselt und es haben nur autorisierte Personen darauf Zugriff (z.B. Geschäftsführer).

Datenübertragungen erfolgen nur über gesicherte Zugänge wie HTTPS oder SFTP.

Daten auf Datenträgern werden von Teamware und TeamFON nicht verschickt. Ausgenommen hiervon sind öffentliche Daten wie Vertriebs- und Marketingunterlagen. Sollte uns ein Kunde Daten auf diesem Wege zukommen lassen wollen, wird dieser auf eine sichere Verschlüsselung hingewiesen.

2. Eingabekontrolle

Die Eingabe und Veränderung sensibler Daten für bestimmte Systeme wird protokoliert. Hierbei werden der Benutzer und der Zeitpunkt der Änderung erfasst. Hierzu zählen folgende

Systeme: Buchhaltungssystem, CRM System, Ticket-System und Wiki-System für die Dokumentation.

Alle Teamware und TeamFON-Mitarbeiter haben eine Verschwiegenheitsvereinbarung unterzeichnet. Es existieren für die Techniker Checklisten, die die periodische Wartung und Aktualisierung der jeweiligen Server und Software regeln. Außerdem werden alle Rechner automatisch mit Monitoring- und Auswertungs-Tools 24x7 überwacht.

Die Arbeitsplatzrechner werden mit aktueller Sicherheitssoftware auf dem neuesten Stand gehalten.

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1. Verfügbarkeitskontrolle

a. Büroräume

Für Entwicklungsserver kommt das gleiche Backup-Konzept wie für den Rechenzentrumbetrieb zum Einsatz. Zusätzlich gibt es ein zentrales Backup der einzelnen Arbeitsworkstations der Mitarbeiter.

Um auch bei einem Stromausfall den Service aufrecht zu erhalten sind einzelne Notfallarbeitsplätze für Mitarbeiter an einem System für unterbrechungsfreie Stromversorgung (USV) angeschlossen.

Der Serverraum für Entwicklungsserver ist ebenfalls an das USV System angeschlossen.

Die Notfall Dokumentation befindet sich zusätzlich in verschlüsselter Form und vor mechanischem Zugriff geschützt in den Privaträumen der beiden für die Technik verantwortlichen Geschäftsführer von Teamware und TeamFON.

b. Rechenzentrum

Das Rechenzentrum, das von Teamware und TeamFON genutzt wird, weist folgende Sicherheitsmerkmale auf:

Hardware-Sicherheit	Sicherheitsstrategie mit Authentication Biometrics und Videoüberwachung
Rund-um-die-Uhr- Zugang	Kundenzugang zu Colocation und Arbeitsbereichen 24 Stunden an 7 Tagen in der Woche
Stromversorgung	Redundante USV mit automatischer Übergabe an Diesel-Generator
Klimatische Raumbedingungen	Minimales Kondensierungs- und Überhitzungsrisiko durch Überwachung der Umgebungstemperatur
Internetleitungen	Redundante Zuführung der redundanten Glasfasertrassen zum Gateway

Gateway-Stromversorgung

Im Datacenter wird die USV-Leistung unter dem Doppelboden über eine drei phasige, am Boden befestigte Stromversorgungsleitung verteilt. Der Wechselstrom von der USV wird über einen mit Sicherungen geschützten, einphasigen Abzweig an die Wechselstromleiste in den einzelnen Schrank geleitet.

Unterbrechungsfreie Stromversorgung

Das Gateway ist anfänglich mit einer 400-V-USV mit nominal 400 kVA ausgestattet und kann bei Bedarf erweitert werden. Alle Verteilertafeln der USV sind mit doppelten Nullleitern ausgestattet. Ebenso verfügen alle USV Einspeiseleitungen über doppelte Nullleiter. Die USV wird von der mit der Wartung beauftragten Fachfirma einmal im Quartal gewartet und getestet. Das USV-System ist so ausgelegt, dass im Falle eines Stromausfalls das gesamte angeschlossene Equipment für mindestens 20 Minuten weiterbetrieben werden kann.

Notstromgenerator

Ein Notstromgenerator liefert bei Bedarf bis zu 100 % des Stroms für die Einrichtung. Passende Kontrollmechanismen sind vorgesehen, um Komponenten mit hohen Anlaufströmen wie etwa Motorlasten und Gleichrichter nacheinander zu starten. Der Generator hat eine Anlaufzeit von etwa 3 Minuten unter Volllast und wird einmal monatlich auf seine Funktionsfähigkeit überprüft und getestet. Der Kraftstofftank enthält genügend Kraftstoff für mehr als 7 Tage Betrieb des Generators bei voller Belastung sowie eine Reserve von 10 % für Testläufe.

Sprinkler-System

Bei dem Sprinklersystem handelt es sich um ein „Double-Interlocked Pre-Action Dry Charge System“. Dieses System bietet den besten Schutz gegen unbeabsichtigtes Austreten von Wasser aus den Sprinklern. Die Sprinklerleitungen sind nicht mit Wasser gefüllt, sondern enthalten Druckluft, die erst im Ernstfall entweicht und durch das Wasser ersetzt wird. Die Zuführung von Wasser in die Sprinklerleitungen erfolgt über ein zweistufiges System:

- Wenn die Rauchdetektoren, die ein Signal an die Brandalarmtafel senden und zusätzlich die Sprinkler aktiviert wurden, entweicht die Druckluft und das Pre Action-Ventil öffnet sich, so dass sich die Leitungen mit Wasser füllen.
- Die Sprinkler selbst sind gegen ungeplanten Wasseraustritt nochmals mit Schutzkappen versehen, so dass erst, wenn diese wegfallen, sich das Sprinklerwasser über den alarmierten Bereich verteilt.

Das „Pre Action-System“ ist mit dem Feuermeldesystem gekoppelt.

Feuermeldeanlage

Die Feuermeldeanlage erkennt Brände und signalisiert diese entsprechend, so dass das Personal die betroffenen Räumlichkeiten rechtzeitig verlassen kann. Darüber hinaus ist das Feueralarmsystem mit der Sprinkleranlage gekoppelt, so dass bei einem Alarm das „Pre-Action-Ventil“ der Sprinkleranlage automatisch aktiviert wird. Zur Aktivierung des „Pre-Action-Ventils“ müssen zwei Detektoren über Crosszoning oder Alarmüberprüfung ansprechen. Der erste Detektor veranlasst ein Alarmsignal zur Evakuierung des Personals. Der zweite Detektor aktiviert das Pre-Action-Ventil. In allen Colocation-Bereichen sind unterhalb der Decke und unter erhöhten Installationsebenen Rauchdetektoren installiert.

Die Rauchdetektoren in den Klimaanlagen sind ebenfalls mit der Feuermeldeanlage gekoppelt. Manuell können die Feuermeldeanlage und das Pre-Action-System auch über

Feuermelder aktiviert werden. In allen Bereichen sind Sirenen/Warnlampen zur Information umliegender Bereiche und Personen installiert.

Im Falle eines Alarmes werden automatisch entsprechende Einsatzkräfte alarmiert.

Klimaanlagen

Die Colocation-Fläche ist mit einer Unterboden-Klimaanlage ausgestattet. Die installierte Anlage ist für typische Computerraum-Anwendungen sowie Anforderungen mit unterschiedlichen Ebenen für einen voll genutzten Colocation-Bereich ausgelegt.

Die Eingangsklimatisierung beträgt 21 °C +/-2 °C, 50 % RH +/-20 %.

Datensicherung

Bei Teamware und TeamFON kommt ein zweistufiges Backup Verfahren zum Einsatz. Ein Server steuert die Backup Mechanismen. Für einen schnellen Datenzugriff werden die Daten auf Festplatten gespeichert. Erst in einem zweiten Schritt werden diese auf Bänder ausgelagert.

2. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Datensicherung auf Platte (Schritt 1)

Die Sicherung wird im ersten Schritt auf einen zentralen Backup Server auf Festplatten durchgeführt. Dieser befindet sich in einem räumlich getrennten Rechenzentrum. Die Sicherungsdaten werden auf dem Backup Server 7 Tage vorgehalten.

Datensicherung auf Band (Schritt 2)

In einem zweiten Schritt erfolgt die Sicherung auf Band. Die Verwaltung der Bänder erfolgt mit einem Strichcode Verfahren, sog. Barcode Labels. Die Vorhaltezeit auf Band beträgt 12 Monate. Der Aufbewahrungsort befindet sich im zweiten Rechenzentrum.

Verschlüsselung

Die Bänder werden durch die Software nach dem TEA block cypher standard mit einem 128 bit Key verschlüsselt.

Überwachung / Kontrolle

Die Überwachung des täglichen Backups erfolgt zweistufig: Der Backup Manager kontrolliert die erfolgten Backups und erfasst dies in einer Kontrollliste. Daneben werden die Backup-Server durch das Monitoring überwacht, ob die Backup Dateien der einzelnen Server aktuell sind. Der Kontrollplan wird revisionssicher in dem Wiki von Teamware / TeamFON geführt.

Rücksicherungsprotokolle

Um eine rasche Wiederherstellbarkeit sicherstellen zu können werden für alle Backups regelmäßig Wiederherstellungstests durchgeführt. Die regelmäßigen Wiederherstellungstests sowie die außerplanmäßig von Kunden oder internen Mitarbeitern angeforderten Rücksicherungen von Daten werden revisionssicher in dem Wiki-Verzeichnis von Teamware / TeamFON dokumentiert

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

1. Datenschutz-Management

Teamware und TeamFON haben eine Sicherheitszertifizierung nach ISO 27001.

Mit dem ISMS wird im Intranet eine zentrale Dokumentation aller Verfahrensanweisungen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für alle Mitarbeiter betrieben.

Im Rahmen der jährlichen Audits wird eine Überprüfung der Wirksamkeit Schutzmaßnahmen durchgeführt.

Alle Mitarbeiter werden in der Nutzung des ISMS, insbesondere zum Thema Datenschutz, jährlich geschult.

2. Incident-Response-Management

Verantwortlicher für das Incident Management ist Dr. Thomas Kupec, seine Stellvertreter sind Thomas Weiß und Holger Kluge.

Alle Sicherheitsvorfälle werden revisionssicher im JIRA dokumentiert und an den verantwortlichen Incident Manager gemeldet. Diese überprüfen gemeinsam mit dem Datenschutzbeauftragen von Teamware und TeamFON, Hrn. Florian Glas, ob eine Meldepflicht gegenüber Aufsichtsbehörden besteht. Der Prozess hierzu ist im ISMS für alle Mitarbeiter zugreifbar dokumentiert.

3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

4. Auftragskontrolle

Der Auftragsverarbeiter setzt nur dann Subunternehmer ein, wenn der Verantwortliche eine Beauftragung schriftlich genehmigt hat.

Subunternehmen werden explizit über den Datenschutz und die Sicherheitsrichtlinien von Teamware und TeamFON unterrichtet und sind zur Einhaltung dieser vertraglich verpflichtet.

Sicherheitsanforderungen an Lieferanten

Alle Lieferanten, die für den Betrieb erforderlich sind wurden auf folgende Punkte überprüft:

- 24x7 Notfall Hotline
- Hohe Verfügbarkeit, die durch ein Service-Level-Agreement (SLA) zugesichert wird
- Möglichst redundanter Betrieb in mehreren Rechenzentren
- Datensicherheit möglichst durch eine Zertifizierung bestätigt

Zertifikat

Prüfungsnorm **ISO/IEC 27001:2013**

Zertifikat-Registrier-Nr. **01 153 1401363/02**

Unternehmen: **TeamFON GmbH**
Stahlgruberring 11
81829 München
Deutschland

Geltungsbereich: TeamFON GmbH ist Anbieter der virtuellen Telefonanlage „TeamSIP Centrex“, erstellt VoIP Konzepte und entwickelt Software im Bereich VoIP.

SoA Version 23 vom 23.10.2017

Durch ein Audit wurde der Nachweis erbracht, dass die Forderungen der ISO/IEC 27001:2013 erfüllt sind.

Gültigkeit: Dieses Zertifikat ist nur gültig in Verbindung mit dem Hauptzertifikat vom 03.11.2017 bis 02.11.2020.

14.11.2017

TÜV Rheinland Cert GmbH
Am Grauen Stein · 51105 Köln

www.tuv.com

DAkkS Deutsche Akkreditierungsstelle D-ZM-16031-01-00

TÜVRheinland®
Genau. Richtig.