TeamViewer

Übersicht der technisch-organisatorischen Maßnahmen

Februar 2022

INHALT

1 Zugangskontrolle

1.1 Datenzentren

TeamViewer besitzt, mietet oder betreibt keine TeamViewer Server-Infrastruktur für seine Büros oder Produktionsumgebung. Die TeamViewer-Produktionsumgebung ist eine rein cloud-basierte Infrastruktur, die in Rechenzentren untergebracht ist, welche durch Drittanbieter betriebenen werden.

TeamViewer verfügt über Zugangskontrollmaßnahmen, die den unbefugten Zutritt zu Datenverarbeitungsanlagen verhindern sollen, in denen personenbezogene Daten gespeichert oder verarbeitet werden.

1.2 TeamViewer-Büros

Ausschließlich autorisierte Personen haben physischen Zugang zu Geländen, Gebäuden oder Räumen, in denen personenbezogene Daten verarbeitet werden. Die Einrichtungen von TeamViewer sind durch Schlüsselsysteme, Einbruchmeldeanlagen, Zugangskontrollmaßnahmen und aktives Schlüsselmanagement geschützt. Zugangsrechte werden autorisierten Personen auf individueller Basis gewährt, einschließlich Besuchern, die von autorisiertem Personal begleitet werden müssen. Mitarbeiter und Besucher sind verpflichtet, ihre Ausweise jederzeit sichtbar zu tragen, wenn sie sich in den Räumlichkeiten aufhalten.

2 System-Zugangs- und Zugriffskontrolle

TeamViewer stützt sich auf die folgenden Maßnahmen zur Systemzugriffskontrolle, um zu verhindern, dass unbefugte Personen Datenverarbeitungssysteme, in denen personenbezogene Daten gespeichert oder verarbeitet werden, nutzen können.

2.1 Netzwerk- und Hardwaresicherheit

Das TeamViewer-Firmennetzwerk ist durch Firewalls und Systeme zur Erkennung und anschließenden Beseitigung von Bedrohungen vor dem öffentlichen Netz geschützt. Es werden die auf dem neusten Stand befindende Antiviren-/Malware-Erkennungssoftware eingesetzt, um schädlichen Code zu erkennen, zu entfernen und vorzubeugen. Ein Sicherheits-Patch-Management ist implementiert und der Fernzugriff auf das TeamViewer-Unternehmensnetzwerk ist

durch starke Authentifizierungsmechanismen und ein Virtual Private Network (VPN) geschützt.

TeamViewer verwendet eine rollenbasierte Sicherheitsarchitektur und erfordert, dass Benutzer des Systems identifiziert und authentifiziert werden, bevor sie Systemressourcen nutzen können. Die Ressourcen werden durch systemeigene Sicherheits- und Zusatzsoftwareprodukte geschützt, die Benutzer identifizieren und authentifizieren die Zugriffsanfragen anhand der autorisierten Rollen der Benutzer in Zugriffskontrolllisten zu validieren. In Situationen, in denen unvereinbare Verantwortlichkeiten nicht getrennt werden können, implementiert TeamViewer die Überwachung einer oder mehrerer Verantwortlichkeiten. Die Überwachung muss von einem Vorgesetzten ohne Verantwortung für die Durchführung der kollidierenden Aktivitäten oder von Mitarbeitern einer separaten Abteilung durchgeführt werden.

Alle Ressourcen werden im Asset-Inventarisierungssystem verwaltet und jeder Ressource wird einen Verantwortlichen zugewiesen. Diese sind für die Genehmigung des Zugriffs auf die Ressource und für die Durchführung von Überprüfungen des Zugriffs nach Rolle verantwortlich.

Mitarbeiter melden sich im TeamViewer-Netzwerk mit einer Active Directory-Benutzer-ID und einem Passwort an. Die Benutzer müssen sich außerdem separat an allen Systemen oder Anwendungen anmelden, die nicht die geteilte Sign-On-Funktionalität von Active Directory nutzen. Die Passwörter müssen definierten Passwortstandards entsprechen und werden durch Parametereinstellungen im Active Directory erzwungen. Diese Einstellungen sind Teil der Konfigurationsstandards und zwingen die Benutzer, die Passwörter in einem definierten Intervall zu ändern. Benutzer-IDs werden nach einer bestimmten Anzahl von erfolglosen Anmeldeversuchen gesperrt, um den Zugriff auf System und Ressourcen zu unterbinden. Zusätzlich wird der Bildschirm von Benutzern nach einer definierten Zeit der Inaktivität, automatisch gesperrt.

Mitarbeiter, die von außerhalb des TeamViewer-Netzwerks auf das System zugreifen, müssen einen Virtual Private Network (VPN)-Tunnel und ein Zwei-Faktor-Authentifizierungssystem verwenden. Die Mitarbeiter erhalten bei ihrer Einstellung VPN-Zertifikate und der Zugang wird bei ihrem Austrittsgespräch deaktiviert.

TeamViewer-Mitarbeiter greifen über das Internet auf die Zwei-Faktor-Authentifizierungsdienste zu, indem sie die Secure Socket

Layer (SSL)-Funktionalität ihres Webbrowsers nutzen. Die Mitarbeiter geben zunächst eine gültige Benutzer-ID und ein Passwort ein, um Zugang zu den TeamViewer-Cloud-Ressourcen zu erhalten. Die Passwörter müssen den Anforderungen an die Passwortkonfiguration entsprechen, die auf den virtuellen Geräten unter Verwendung des virtuellen Server-Administrationskontos konfiguriert wurden. Virtuelle Geräte werden zunächst gemäß den TeamViewer-Konfigurationsstandards konfiguriert, aber diese Konfigurationsparameter können über das Administrationskonto des virtuellen Servers geändert werden.

TeamViewer unterhält ein sog. System and Operations Control (SOC), das rund um die Uhr wichtige Systeme und Warnmeldungen überwacht, um Sicherheitsvorfälle zu bewältigen. Diese Dienste werden auf eine konforme und datenschutzfreundliche Art und Weise betrieben und gewährleisten gleichzeitig eine Reaktion auf Bedrohungen, die dem Risikoniveau des Unternehmens angemessen ist.

TeamViewer-Mitarbeiter können sich über virtuelle Server-Administrationskonten bei ihren Systemen anmelden. Diese Administrationskonten verwenden ein zweistufiges, auf digitalen Zertifikaten basierendes Authentifizierungssystem.

Benutzer-IDs und Zugriffsregeln werden entsprechend der Rolle des jeweiligen Mitarbeiters festgelegt. Die Zugriffsregeln sind auf der Grundlage der definierten Rollen vordefiniert. Bei Änderungen an einer Position werden die zugehörigen Rechte und Zugriffsregeln entsprechend geändert.

Jährlich werden die Zugriffsrechte von den Teamleitern überprüft und mit der Stellenbeschreibung, den zu trennenden Aufgaben und den mit den Zugriffsrechten verbundenen Risiken abgeglichen.

Der Entzug von Rechten und Zugang sowie die Deaktivierung des Kontos im Falle des Austritts eines Mitarbeiters (“Offboarding”) oder im Falle eines Positionswechsels wird vom IT-Service Desk durchgeführt, um den Zugang des Mitarbeiters zu löschen bzw. die Zugangsrechte anzupassen.

Die Manager prüfen die Listen und tragen die erforderlichen Änderungen in den Ereignisverwaltungsdatensatz ein. Der Datensatz wird zur Bearbeitung an den Sicherheits-Helpdesk zurückgesandt. Der IT-Service-Desk-Manager identifiziert alle Einträge, die nicht innerhalb von zwei Wochen zurückgegeben werden, und setzt sich mit dem Manager in Verbindung. Im Rahmen dieses Prozesses überprüft der Information Security Officer (ISO) die Mitarbeiter mit

Zugang zu privilegierten Rollen und fordert Änderungen über das Verwaltungssystem an.

Nur autorisierte Personen können auf Systeme zugreifen, die personenbezogene Daten verarbeiten. TeamViewer verwendet mehrere Berechtigungsstufen bei der Gewährung des Zugangs zu Systemen. Alle Mitarbeiter greifen über ein personalisiertes Konto (Benutzer-ID) auf die Unternehmenssysteme von TeamViewer zu und haben nur Zugriff auf die Systeme, auf die sie zur Erfüllung ihrer Aufgaben zugreifen müssen. Berechtigungen und Privilegien werden regelmäßig überprüft. Ebenso überprüft werden Rechte für den Zugriff auf Systeme, wenn Mitarbeiter neue Rollen zugewiesen bekommen oder TeamViewer verlassen.

TeamViewer verfügt über eine Passwortrichtlinie, die die ordnungsgemäße Verwendung von Passwörtern regelt, einschließlich der Häufigkeit, mit der sie geändert werden müssen, der Mindestanforderungen und der Komplexität.

2.2 Einstellung (“Onboarding”) und Austritt (“Offboarding”) von Mitarbeitern

Bei der Einstellung werden die Mitarbeiter einer Position im Personalverwaltungssystem zugewiesen. 10 (zehn) Tage vor dem Startdatum des Mitarbeiters erstellt das HR-Team ein sog. “Onboarding”-Ticket, das die Benutzer-IDs des Mitarbeiters und die zu gewährenden Zugriffsrechte enthält. Das Ticket wird vom IT-Service-Desk verwendet, um Benutzer-IDs und Zugriffsregeln zu erstellen. Die Zugriffsregeln sind nach dem Minimalprinzip definiert (jeder Mitarbeiter erhält nur die Berechtigungen, die er/sie benötigt, um seine/ihre Aufgabe zu erfüllen). Darüber hinaus enthält das Ticketsystem eine Vorlage für Mitarbeiter, die ihre Position und die damit verbundenen Rechte wechseln, die innerhalb der bestehenden Zugriffsregelungen entsprechend geändert werden müssen.

Jährlich werden die Zugriffsrechte von den Teamleitern/innen überprüft, um festzustellen, ob diese widerrufen werden müssen. Bei der Bewertung der Zugriffsrechte berücksichtigen die Teamleiter die Stellenbeschreibung, die zu trennenden Aufgaben und die mit den Zugriffsrechten verbundenen Risiken.

Nach Kündigung des Arbeitsverhältnisses eines Mitarbeiters wird von der HR-Abteilung wiederum ein Ticket erstellt. Diese Tickets werden vom IT-Service Desk bearbeitet, um den Zugriff des Mitarbeiters in allen Systemen zu entfernen. Der IT-Service Desk

verwendet die Tickets, um Benutzer-IDs zu sperren und alle Zugriffsrollen von IDs zu löschen, die dem Mitarbeiter des Tickets gehören.

Die Listen der ehemaligen Mitarbeiter werden überprüft und die gewünschten Änderungen werden im Datensatz vermerkt. Der Datensatz wird zur Bearbeitung an den IT-Sicherheits-Helpdesk zurückgeleitet. Der IT-Service-Desk-Manager identifiziert alle Datensätze, die nicht innerhalb von zwei Wochen zurückgegeben werden, und setzt sich mit dem jeweiligen Teamleiter/in Verbindung. Als Teil dieses Prozesses überprüft der Information Security Officer (ISO) die Mitarbeiter mit Zugriff auf bestimmte (u.a. vertrauliche) Rollen und passt Änderungen über das System an.

2.3 Datenzugriffskontrolle

TeamViewer kontrolliert den Zugriff auf Systeme, die personenbezogene Daten enthalten, durch eine Mischung aus rollenbasierter Zugriffskontrolle (role-based access control, sog. RBAC) und Benutzerrechteverwaltung. Dadurch wird sichergestellt, dass der Zugriff auf und die Nutzung von Daten sowohl in Bezug auf die allgemeine Verarbeitung als auch in Bezug auf die Liste und den Umfang des Zugriffs für TeamViewer-Mitarbeiter minimiert wird. Diese Zugriffskontrollen variieren in Abhängigkeit von der Sensibilität der gespeicherten Daten und den betrieblichen Anforderungen.

2.4 Datentrennung

Netzwerke werden getrennt und segmentiert. Dies funktioniert im Rahmen von RBAC, um Risiken im Einklang mit fundierten Sicherheits- und Datenschutzpraktiken zu minimieren. So werden Daten für unterschiedliche Produkte/Zwecke, wenn möglich, getrennt verarbeitet, u.a. durch Trennung von Produktions- und Testumgebungen. Wo zweckdienlich werden die Daten getrennt verarbeitet, um eine unnötige Vermischung von Daten und eine Verarbeitung über den Zweck hinaus zu vermeiden.

2.5 Pseudonymisierung

TeamViewer setzt die Pseudonymisierung dort ein, wo sie ohne Beeinträchtigung der Effizienz der Prozesse angewendet werden kann und/oder wo sie zum Schutz der Daten im Falle einer notwendigen Offenlegung von Daten notwendig ist. Wo es im Rahmen

des Offenlegungsprozesses möglich ist, wird die Anonymisierung eingesetzt. Daten, die in pseudonymisierten Daten enthaltene Betroffenen identifizieren können, werden separat gespeichert und wenn möglich verschlüsselt.

TeamViewer verfügt über einen Prozess zur Bewertung der internen Datenweitergabe und verwendet Pseudonymisierung, um die Nutzung der personenbezogenen Daten für bestimmte Zwecke einzuschränken.

3 Maßnahmen zur Herstellung der Integrität

3.1 Weitergabekontrolle

Bei TeamViewer gibt es Weitergabekontrollen, die sicherstellen, dass die Daten während der Übertragung sicher sind und das Schutzlevel nicht unter einen Mindeststandard fällt, sobald sie den Perimeter verlassen.

Zu diesen Sicherheitsmaßnahmen gehören die Sicherung von Übertragungen mit SSL/TLS, https usw. und der Einsatz von VPNs im gesamten Unternehmen. TeamViewer unterhält Firewalls und andere Standardsicherheitssysteme, um den Betrieb und die Daten zu schützen.

Firewall-Systeme sind vorhanden, um nicht autorisierten eingehenden Netzwerkverkehr aus dem Internet zu filtern und jede Art von Netzwerkverbindung zu verweigern, die nicht ausdrücklich autorisiert ist. Die Network Address Translation (NAT)-Funktionalität wird verwendet, um interne IP-Adressen (Internet Protocol) zu verwalten. Der administrative Zugriff auf die Firewall ist auf autorisierte Mitarbeiter beschränkt.

3.2 Dateneingangsteuerung

TeamViewer hat Systeme im Einsatz, die protokollieren, wer auf personenbezogene Daten zugegriffen oder diese verändert hat, einschließlich der Verknüpfung solcher Kontrollen mit individuellen Accounts.

4 Datenverfügbarkeit und Belastbarkeit der Systeme

TeamViewer erstellt Backups von wichtigen Daten in Übereinstimmung mit gängiger Praxis und stellt sicher, dass diese Backups im Falle eines katastrophalen Ausfalls als zuverlässige Ausfallsicherung fungieren.

Die Kundendaten werden gesichert und von Mitarbeitern der Operations-Abteilung auf Vollständigkeit und Ausfälle überwacht. Im Falle eines Ausfalls führt die Operations-Abteilung eine Fehlerbehebung durch, um die Ursache zu identifizieren, und führt dann den Backup sofort oder als Teil des nächsten geplanten Backups erneut aus, je nach den vom Kunden in den dokumentierten Arbeitsanweisungen angegebenen Präferenzen.

Die Backup-Infrastruktur ist physisch in verschlossenen Schränken und/oder Käfigumgebungen innerhalb der Rechenzentren von Drittanbietern gesichert. Die Backup-Infrastruktur befindet sich in privaten Netzwerken, die logisch von anderen Netzwerken gesichert sind.

Es existieren Richtlinien und Verfahren zur Reaktion auf IT-Vorfälle, die das Personal bei der Meldung von sowie den entsprechenden Umgang mit solchen Vorfällen anleiten. Es gibt Verfahren, um Sicherheitsverletzungen im System und andere Vorfälle zu erkennen, zu melden und darauf zu reagieren. Es gibt Verfahren zur Reaktion auf Vorfälle, um diese im Netzwerk zu erkennen und darauf zu reagieren.

TeamViewer überwacht die Auslastung der physischen und computergestützten Infrastruktur sowohl intern als auch für Kunden, um sicherzustellen, dass die Dienstleistung den Service Level Agreements entspricht.

TeamViewer evaluiert den Bedarf an zusätzlicher Infrastrukturkapazität als Reaktion auf das Wachstum bestehender Kunden bzw. die Aufnahme neuer Kunden. Die Überwachung der Infrastrukturkapazität umfasst unter anderem folgendes:

- Rechenzentrumsfläche, Strom und Kühlung
- Plattenspeicher
- Bandspeicher
- Netzwerk-Bandbreite

TeamViewer hat einen Patch-Management-Prozess implementiert, um sicherzustellen, dass die vertraglich vereinbarten Kunden- und Infrastruktursysteme in Übereinstimmung mit den vom Hersteller empfohlenen Betriebssystem-Patches gepatcht werden. Kunden und TeamViewer-Systemverantwortliche überprüfen vorgeschlagene Betriebssystem-Patches, um festzustellen, ob die Patches angewendet werden.

TeamViewer ist dafür verantwortlich, das Risiko des Aufspielens oder Nichtaufspielens von Patches auf der Grundlage der Sicherheits- und

Verfügbarkeitsauswirkungen dieser Systeme und aller kritischen Anwendungen, die darauf gehostet werden, zu bestimmen. TeamViewer-Mitarbeiter überprüfen, ob alle Patches installiert wurden und ob gegebenenfalls ein Neustart durchgeführt wurde.

Redundanz ist in die Systeminfrastruktur eingebaut, die die Dienste des Rechenzentrums unterstützt, um sicherzustellen, dass es keinen einzelnen Ausfallpunkt (“Single Point of Failure”) gibt, der Firewalls, Router und Server umfasst. Wenn ein primäres System ausfällt, wird die redundante Hardware so konfiguriert, dass sie dessen Platz einnimmt.

Penetrationstests werden durchgeführt, um die Sicherheitslage eines Zielsystems oder einer Umgebung zu messen. Der beauftragter Drittanbieter verwendet eine von TeamViewer spezifizierte, branchenübliche Methodik für Penetrationstests. Der Ansatz des Drittanbieters beginnt mit einer Schwachstellenanalyse des Zielsystems, um festzustellen, welche Schwachstellen auf dem System vorhanden sind, die durch einen Penetrationstest ausgenutzt werden können, wobei ein verärgerter/betroffener Insider oder ein Angreifer simuliert wird, der sich internen Zugang zum Netzwerk verschafft hat.

Sobald die Schwachstellen identifiziert sind, versucht der Drittanbieter, die Schwachstellen auszunutzen, um festzustellen, ob ein unberechtigter Zugriff oder andere böswillige Aktivitäten möglich sind.

Penetrationstests umfassen Tests der Netzwerk- und Anwendungsebene sowie Tests der Kontrollen und Prozesse rund um die Netzwerke und Anwendungen und erfolgen sowohl von außen (externe Tests) als auch innerhalb des Netzwerks.

Schwachstellen-Scans werden wöchentlich von TeamViewer in Übereinstimmung mit den internen Richtlinien durchgeführt. Auf Anfrage des Kunden kann auch ein Schwachstellen-Scan durch einen Drittanbieter gemäß den TeamViewer-Richtlinien erfolgen. Der Drittanbieter verwendet Industriestandard-Scantechnologien und eine formelle, von TeamViewer spezifizierte Methodik. Diese Technologien sind so angepasst, dass sie die Infrastruktur und Software des Unternehmens auf effiziente Weise testen und gleichzeitig die mit dem aktiven Scannen verbundenen potenziellen Risiken minimieren.

Re-tests und On-Demand-Scans werden je nach Bedarf durchgeführt. Die Scans werden außerhalb der Hauptgeschäftszeiten durchgeführt.

Tools, die im TeamViewer-System installiert werden müssen, werden über den Change-Management-Prozess implementiert. Das Scannen wird mit genehmigten Scan-Vorlagen und mit aktivierten Optionen zur Bandbreiten-Drosselung durchgeführt.

Autorisierte Mitarbeiter können über das Internet mit Hilfe von VPN-Technologie auf das System zugreifen. Die Mitarbeiter werden durch ein token-basiertes Zwei-Faktor-Authentifizierungssystem authentifiziert.

5 Datenschutzmanagement

TeamViewer unterhält eine Vielzahl von Datenschutzrichtlinien und -verfahren, für die der Datenschutzbeauftragter (DSB) und das Management von TeamViewer letztlich verantwortlich sind. TeamViewer aktualisiert ständig seine Datenschutz- und Sicherheitsmaßnahmen im Einklang mit aktualisierten Richtlinien, Gesetzen und Best Practices. Dazu gehören regelmäßige Überprüfungen der Dokumentation von Verfahren, Schulungen sowie technischen und organisatorischen Maßnahmen, die Pflege und Erstellung von Verarbeitungsverzeichnisse und ggf. die Durchführung von Datenschutz-Folgenabschätzungen.

TeamViewer verfügt über Prozesse, Richtlinien und Verfahren, die die physische Sicherheit, den logischen Zugriff, den Computerbetrieb, die Änderungskontrolle und die Datenkommunikationsstandards beschreiben. Alle Mitarbeiter sind verpflichtet, dass sie sich an die TeamViewer-Richtlinien und -Verfahren halten, die definieren, wie Dienstleistungen erbracht werden sollen. Diese befinden sich im Intranet des Unternehmens und können von jedem TeamViewer-Mitarbeiter eingesehen werden.

Die Mitarbeiter werden regelmäßig datenschutzrechtlich geschult und auf Vertraulichkeit verpflichtet. TeamViewer führt regelmäßige (mindestens einmal jährlich) Awareness-Schulungen für Mitarbeiter durch, deren Häufigkeit sich jedoch je nach Bedarf erhöhen kann.

TeamViewer benennt pro Abteilung mindestens eine verantwortliche Person, die für die Einhaltung und Umsetzung der Vorgaben der Datenschutz-Grundverordnung (DS-GVO) verantwortlich ist. Alle verantwortlichen Datenschutz-Mitarbeiter verfügen mindestens über eine für ihren Arbeitsbereich relevante IAAP CIPP-Qualifikation.

Eine Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen wird mindestens jährlich durchgeführt. Datenschutz-Folgenabschätzungen werden dann durchgeführt, wenn es notwendig ist.

Es gibt eine formalisierte Richtlinie für die Bearbeitung von Anfragen von Betroffenen unter der DS-GVO.

Alle Mitarbeiter werden intern gem. Art. 32 Abs. 4 DS-GVO geschult und sind verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.

Nach Beendigung des Vertragsverhältnisses werden die Daten datenschutzkonform gelöscht und dabei die Grundsätze der Datenminimierung berücksichtigt.

5.1 Unterauftragsverarbeiter

TeamViewer schließt Auftragsverarbeitungsverträge (AVV) mit allen Unterauftragsverarbeiter von personenbezogenen Daten. Ferner stellt TeamViewer sicher, dass alle Unterauftragsverarbeiter die jeweils einschlägigen Standards für Sicherheit und Datenschutz erfüllen und, dass diese Anforderungen und Verpflichtungen als Teil des AVVs aufgenommen werden.

Im Falle einer langfristigen Zusammenarbeit erfolgt eine laufende Überprüfung des Unterauftragsverarbeiters und seines Schutzniveaus.

5.2 Incident Response Management

TeamViewer verfügt über Prozesse und Tools, um auf Sicherheits- und andere Vorfälle zu reagieren, darunter Firewalls, Anti-Malware-Systeme und die Zusammenarbeit zwischen dem DSB und dem Chief Information Security Officer (CISO).

Es gibt ein dokumentiertes Verfahren zur Erkennung und Meldung von Sicherheitsvorfällen sowie Datenverletzungen (insbesondere im Hinblick auf die Meldepflicht an die Aufsichtsbehörde) und ein dokumentiertes Verfahren zum Umgang mit Sicherheitsvorfällen. Insoweit Daten betroffen sind, die im Auftrag verarbeitet werden, stellt ein Prozess sicher, dass der Vorfall unverzüglich dem Auftraggeber, d.h. dem Verantwortlichen im Sinne der DS-GVO, gemeldet wird.

Sicherheitsvorfälle und Datenverletzungen werden dokumentiert und es gibt einen formalen Prozess mit zugewiesenen Verantwortlichkeiten für die Nachbearbeitung und Implementierung eventuell resultierender Maßnahmen.

6 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Personenbezogene Daten werden nur in dem Umfang erhoben und verarbeitet, der für den vorgeschriebenen Zweck erforderlich ist. Den

betroffenen Personen steht ein einfacher Weg offen, ihre Rechte auszuüben.

Bereits im Rahmen der Softwareentwicklung werden Grundsätze des Datenschutzes beachtet. Insbesondere sind die Mitarbeiter angehalten und geschult, technische und organisatorische Maßnahmen im Rahmen der Produktentwicklung umzusetzen, die die Einhaltung der Anforderungen der DS-GVO und speziell der Betroffenenrechte gewährleisten. Die Software wird grundsätzlich in der Art gestaltet, dass die Menge der erhobenen Daten sowie der Umfang der Verarbeitung auf das Erforderliche beschränkt ist. Insoweit verschiedene Einstellungsmöglichkeiten innerhalb der Software bestehen, ist im Auslieferungszustand immer die Einstellung gewählt, bei der die geringere Menge an personenbezogenen Daten verarbeitet wird.

In Bezug auf die Änderungskontrolle unterhält TeamViewer dokumentierte Richtlinien und Verfahren des Software Development Life Cycle (SDLC), um das Personal bei der Dokumentation und Implementierung von Anwendungs- und Infrastrukturänderungen anzuleiten. Zu den Änderungskontrollverfahren gehören: Änderungsanforderungs- und -einleitungsprozesse, Dokumentationsanforderungen, Entwicklungspraktiken, Qualitätssicherungs-Testanforderungen und erforderliche Genehmigungsverfahren.

Ein Ticketingsystem wird verwendet, um die Änderungen in der Anwendung und die Implementierung neuer Änderungen zu dokumentieren (sog. Änderungskontrollverfahren).

Qualitätssicherungsprüfungen und -ergebnisse werden dokumentiert und zusammen mit der entsprechenden Änderungsanforderung gepflegt. Entwicklung und Tests werden in einer Umgebung durchgeführt, die logisch von der Produktionsumgebung getrennt ist. Das Management genehmigt die Änderungen vor der Migration in die Produktionsumgebung und dokumentiert diese Genehmigungen im Ticketing-System. Versionskontrollsoftware wird eingesetzt, um Quellcodeversionen zu verwalten und Quellcode durch den Entwicklungsprozess in die Produktionsumgebung zu migrieren. Die Versionskontrollsoftware verwaltet eine Historie der Codeänderungen, um Rollback-Funktionen zu unterstützen, und verfolgt die Änderungen für die Entwickler.

Alle Infrastrukturänderungen an der Umgebung werden vom Change Advisory Board (CAB) geprüft und genehmigt. Das CAB besteht mindestens aus dem Leiter der "IT-Infrastruktur", dem Leiter der "Anwendungs- und Bedarfsverwaltung", einem Mitglied des IT-Sicherheitsteams und dem Antragsteller der Änderung. Dadurch wird sichergestellt, dass alle Änderungen überprüft werden und die Qualität der Implementierung erhalten bleibt.

TeamViewer Germany GmbH

Bahnhofsplatz 2

73033 Göppingen

Germany