Wir **schützen Ihre Daten** zuverlässig

Als deutsches Unternehmen sehen wir es als unsere Pflicht an, höchsten Anforderungen an die IT-Sicherheit gerecht zu werden. Der Schutz Ihrer Daten und Ihrer Privatsphäre ist uns äußerst wichtig. Durchgängige Verschlüsselung und Zwei-Faktor-Authentifizierung sind nur einige Maßnahmen, die wir dafür ergreifen. Doch wir tun noch mehr, um Ihre Arbeit mit TeamViewer so sicher wie möglich zu machen.

TeamViewer: **rundum sicher**

Die TeamViewer ID
Die TeamViewer ID ist eine einzigartige numerische ID, die jedem Gerät bei der Installation zugewiesen wird. Wie bei einer Telefonnummer, wählen Sie die ID an und erfragen anschließend das Passwort, um den Verbindungsaufbau zu authentifizieren.

Zertifizierte Sicherheit
Alle von TeamViewer verwendeten Rechenzentren sind nach ISO/IEC 27001 zertifiziert, der internationalen Norm für Informationssicherheitsmanagement. Mit der ISO 9001:2015 demonstriert TeamViewer zudem ein ganzheitliches Qualitätsmanagement.

Schutz vor Brute-Force-Attacken
Zur Abwehr von Brute-Force-Angriffen erhöht TeamViewer exponentiell die Wartezeit zwischen Verbindungsversuchen. Die Wartezeit wird erst nach der erfolgreichen Kennworteingabe zurückgesetzt.

Das TeamViewer Password
Dieses sechsstellige, zufallsgenerierte Kennwort wird im Fernsteuerungs-Tab Ihrer TeamViewer Anwendung angezeigt und ist für spontane Supportsitzungen gedacht. Es wird nach jedem Start von TeamViewer neu generiert – oder öfter, je nach Einstellung.

Secure Remote Password Protocol (SRP)
Für die Autorisierung und Passwort-Verschlüsselung wird das Secure Remote Password Protocol (SRP) verwendet: Das Passwort wird nie direkt gesendet und ausschließlich auf dem lokalen Rechner gespeichert.

Zwei-Faktor-Authentifizierung
Zusätzlich zu Ihrem Kennwort ist ein Sicherheitscode erforderlich, um sich an Ihrem TeamViewer Konto anzumelden. Der Code wird von einer App generiert.

Verschlüsselung
TeamViewer Verbindungen laufen über gesicherte Datenkanäle, die mit einem RSA-2048-Public/Private-Key-Exchange aufgebaut und mit 256-Bit-AES verschlüsselt sind. Diese Technik gilt nach heutigem Stand der Technik als vollständig sicher.

Conditional Access*
Steuern Sie die Nutzung und die Zugriffsrechte von TeamViewer in Ihrem gesamten Unternehmen über die Management Console.

**Verfügbar mit TeamViewer Tensor. Gemäß den allgemeinen Geschäftsbedingungen.*

AICPA SOC · A-LIGN HIPAA · südcert ISO 9001 · ISO ISO/IEC 27001

Protokolle und Datensicherheit

So kommen TeamViewer Verbindungen zustande

TeamViewer wählt die optimale Art der Verbindung: Nach dem Handshake über unsere Masterserver findet in 70 % der Fälle eine Direktverbindung über das User Datagram Protocol (UDP) oder das Transmission Control Protocol (TCP) statt, selbst hinter Standardgateways, Network-Address-Translation-Routern (NAT) und Firewalls. Die restlichen Verbindungen werden über unser hochredundantes Router-Netzwerk via TCP- oder HTTP-Tunneling geleitet. Sie müssen keinerlei Ports öffnen.

Verschlüsselung und Authentifizierung

TeamViewer Verbindungen laufen über gesicherte Datenkanäle: RSA-2048-Public/Private-Key-Exchange und 256-Bit-AES-Verschlüsselung. Diese Technik wird in vergleichbarer Form auch bei HTTPS/SSL eingesetzt und gilt nach heutigem Stand der Technik als sicher. Da der Private Key niemals den Client verlässt, ist durch dieses Verfahren technisch sichergestellt, dass zwischengeschaltete Computer im Internet Daten nicht dechiffrieren können. Das gilt auch für unsere eigenen Router: Nicht einmal TeamViewer als Betreiber des zentralen Rechenzentrums kann den Datenverkehr lesen.

Datenschutz und Compliance

Vertrauenswürdige Geräte (Trusted Devices)

Die Funktion „Vertrauenswürdige Geräte" bietet zusätzlichen Schutz für Ihr TeamViewer Konto: Sie müssen Geräte, von denen Sie sich zu erstem Mal einloggen, bei der ersten Anmeldung autorisieren und werden per E-Mail benachrichtigt.

Integritätsprüfung (Data Integrity)

Wir prüfen automatisch, ob Ihr TeamViewer Konto ungewöhnliches Verhalten zeigt: zum Beispiel Zugriff von einem ungewöhnlichen Standort aus, was darauf hindeuten könnte, dass das Konto kompromittiert wurde. In diesem Fall erhalten Sie von uns eine E-Mail zur Erstellung eines neuen Passworts.

Black- und Whitelist

Falls Sie bestimmte Kontakte daran hindern möchten, eine Verbindung zu Ihrem Computer aufzubauen, empfiehlt sich das Einrichten einer Blacklist. Richten Sie eine Whitelist ein, um ausschließlich bestimmten Konten oder IDs Zugriff zu erlauben.

ISO/IEC 27001

Alle von TeamViewer genutzten Rechenzentren sind zertifiziert nach ISO/IEC 27001, der internationalen Norm für Informationssicherheits-Managementsysteme und Sicherheitsverfahren.

ISO 9001:2015

Mit der Zertifizierung nach ISO 9001:2015 demonstriert TeamViewer ein ganzheitliches Qualitätsmanagement, absolute Kundenorientierung und kontinuierliche Verbesserung.

Datenschutzgrundverordnung (DSGVO)

TeamViewer ist ein weltweit agierendes Unternehmen, für das der Schutz personenbezogener Daten von Kunden und Mitarbeitern höchste Priorität hat. Weitere Informationen zum Datenschutz und zur DSGVO finden Sie auf der Seite „TeamViewer und die DSGVO" in unserer Knowledge Base.

Zertifiziert für Ihre Sicherheit: HIPAA, HITECH und SOC 2

TeamViewer ist zertifiziert nach HIPAA, HITECH und SOC 2 durch A-LIGN, ein US-amerikanisches Cybersicherheits- und Compliance-Unternehmen. HIPAA und HITECH gewährleisten die Vertraulichkeit und Sicherheit sensibler Daten.

SOC 2 ist ein Standard, gemäß dem Service-Organisationen Berichte zum Status bestimmter interner Kontrollparameter erstellen. Diese umfassen Sicherheit, Verfügbarkeit, Integrität der Verarbeitung, Vertraulichkeit und Datenschutz.

TeamViewer

TeamViewer Germany GmbH
Jahnstr. 30
73037 Göppingen

Bleiben Sie in Verbindung