SPECTRUM Hinweise

„Datensicherheit bei der von SPECTRUM eingesetzten Fernwartungssoftware TeamViewer™“

Zur Fernwartung auf Kundensystemen setzt SPECTRUM das Remote-Desktop-Tool TeamViewer™ ein. TeamViewer™ ist das weltweit am meisten genutzte Remote-Desktop-Tool mit über 30.000 Downloads pro Stunde. Derzeit gibt es über 1,8 Milliarden Live TeamViewer IDs, die auf das weltweit größte und schnellste Fernverbindungsnetzwerk zugreifen.

TeamViewer™ ist eine Fernwartungssoftware für Screen-Sharing, Videokonferenzen, Dateitransfer und VPN. Die Software arbeitet als Online-Dienst durch Firewalls und NAT sowie Proxy-Server hindurch. Die Software wurde 2006 durch die Göppinger TeamViewer GmbH erstellt. TeamViewer™ unterstützt Windows, macOS, Linux, Android, iOS, Blackberry und Windows Phone.

Die TeamViewer™-Infrastruktur ist nach ISO 27001 zertifiziert und vollständig HIPAA-konform (HIPAA = US-Sicherheitsrichtlinie nach dem Health Insurance Portability and Accountability Act) und entspricht den SOC2-Richtlinien (SOC = Service Organization Control nach dem amerikanischen Institut für Wirtschaftsprüfer AICPA).

Sicherheits-Übersicht:

- 256-bit AES Verschlüsselung
- Zwei-Faktor-Authentifizierung
- SOC2-zertifiziert und konform
- ISO 27001 Zertifizierung für Informationssicherheitsmanagement
- HIPAA-konform
- Brute-Force-Schutz
- Benutzer & IP Whitelisting
- Trusted Device Listen
- Erzwungenes Zurücksetzen des Kennworts

SPECTRUM verwendet für die TeamViewer-Fernwartung immer nur zufällig generierten Einmal-Passwort. Bei jedem Start des Fernwartungs-Clients wird ein neues Einmal-Passwort verwendet.

Sie starten die TeamViewer-Fernwartung über die SPECTRUM-Hompage **www.spectrum-news.de** über das am rechten Rand befindliche Icon:

Nachfolgend finden Sie die TeamViewer™-Sicherheitsinformationen.

Zielgruppe

Dieses Dokument richtet sich an professionelle Netzwerkadministratoren. Die Informationen in diesem Dokument sind technischer Art und sehr detailliert. Anhand dieser Informationen können sich IT-Profis bereits vor dem Einsatz von TeamViewer ein fundiertes Bild von der Softwaresicherheit machen. Gerne können Sie dieses Dokument auch Ihren Kunden weiterleiten, um eventuelle Sicherheitsbedenken auszuräumen.

Falls Sie sich selbst nicht zur Zielgruppe zählen, helfen Ihnen vielleicht dennoch die Softfacts im Abschnitt „Das Unternehmen / die Software“, um sich ein subjektives Bild zu machen.

Das Unternehmen / die Software

Über uns

Die TeamViewer GmbH wurde 2005 gegründet und hat Ihren Sitz im süddeutschen Göppingen (Nähe Stuttgart) mit weiteren Niederlassungen in Australien und den USA. Wir beschäftigen uns ausschließlich mit Entwicklung und Vertrieb von sicheren Systemen für die webbasierte Zusammenarbeit und Kommunikation. Ein rasanter Start und schnelles Wachstum haben zu über 200 Millionen Installationen der TeamViewer Software und Nutzern in fast allen Ländern der Erde geführt. Die Software ist in mehr als 30 Sprachen verfügbar.

Die Entwicklung findet ausschließlich in Deutschland statt. Auch Vertrieb und Support werden von Deutschland aus geleistet.

Unser Sicherheitsverständnis

TeamViewer wird weltweit millionenfach für den spontanen Support über das Internet, den Zugriff auf unbeaufsichtigte Server (z. B. Serverfernwartung) und für Online Meetings eingesetzt. Je nach Konfiguration von TeamViewer bedeutet dies, dass der entfernte Computer gesteuert werden kann, als säße man direkt davor. Ist der am entfernten Computer angemeldete Benutzer Windows-, Mac- oder Linux-Administrator, so erhält man also Administrator-Rechte am Computer.

Es ist offensichtlich, dass solch mächtige Funktionalität über das an und für sich unsichere Internet gegen verschiedenste Arten von Angriffen abgesichert werden muss. Tatsächlich dominiert das Thema Sicherheit bei uns alle anderen Entwicklungsziele – um den Zugriff auf Ihre Computer sicher zu gestalten und selbstverständlich auch um unsere ureigensten Interessen zu wahren: Denn nur einer sicheren Lösung vertrauen weltweit Millionen Anwender und nur eine sichere Lösung sichert langfristig unseren Unternehmenserfolg.

Qualitätsmanagement

Sicherheitsmanagement ist nach unserem Verständnis nicht ohne eingeführtes Qualitätsmanagementsystem denkbar. Die TeamViewer GmbH betreibt als einer der wenigen Anbieter am Markt ein zertifiziertes Qualitätssystem gemäß ISO 9001. Unser Qualitätsmanagement orientiert sich damit an international anerkannten Standards. Jährlich stellen wir uns externen Audits, in denen unser QM-System überprüft wird.

Externes Expertengutachten

Unsere Software TeamViewer wurde durch den Bundesverband der IT-Sachverständigen und Gutachter e.V. (BISG e.V.) mit dem Qualitätssiegel mit fünf Sternen (Maximalwert) ausgezeichnet. Die unabhängigen Sachverständigen des BISG e.V. prüfen Produkte qualifizierter Hersteller auf Qualitäts-, Sicherheits- und Serviceeigenschaften.

Sicherheitstechnische Prüfung

TeamViewer wurde der sicherheitstechnischen Prüfung der FIDUCIA IT AG (IT-Dienstleister im Finanzverbund Deutschland mit Rechenzentren für mehr als 800 Banken) unterzogen und für den Einsatz am Bankarbeitsplatz freigegeben.

Referenzen

Zum aktuellen Zeitpunkt ist TeamViewer auf über 200.000.000 Computern im Einsatz. Internationale Top-Unternehmen aus allen Branchen (inklusive hochsensibler Bereiche wie Banken, Finanzwirtschaft, Gesundheitswesen und Regierungswesen) setzen TeamViewer erfolgreich ein.

Wir laden Sie herzlich ein, unsere Referenzen-Seite im Internet aufzurufen und sich so vorab bereits einen Eindruck von der Akzeptanz unserer Lösung zu verschaffen. Sicher werden Sie zustimmen, dass die meisten dieser Unternehmen vermutlich ähnliche Sicherheits- und Verfügbarkeitsanforderungen hatten, bevor Sie sich schließlich nach intensiver Prüfung für TeamViewer entschieden haben. Damit Sie sich dennoch selbst einen Eindruck verschaffen können, finden Sie im Folgenden technische Details.

TeamViewer-Sitzung

Verbindungsaufbau und Verbindungsarten

TeamViewer ermittelt beim Aufbau einer Verbindung die optimale Verbindungsart. Nach dem Handshake über unsere Master-Server findet in 70% der Fälle (auch hinter Standard-Gateways, NAT und Firewalls) eine Direktverbindung über UDP oder TCP statt. Die restlichen Verbindungen werden über unser hochredundantes Router-Netzwerk via TCP oder http-Tunneling geleitet. Sie müssen also keinerlei Ports öffnen, um mit TeamViewer arbeiten zu können!

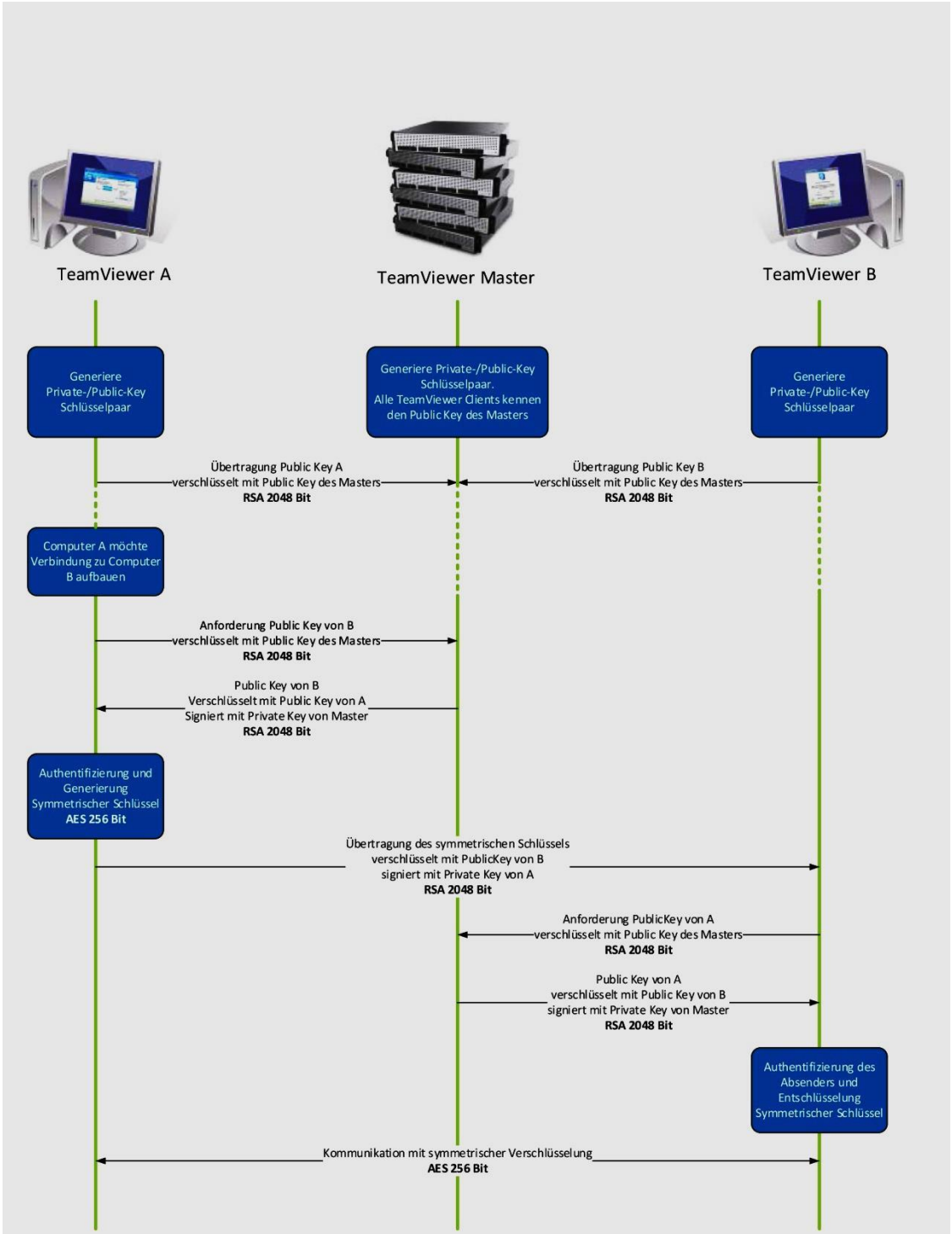
Wie später im Abschnitt „Verschlüsselung und Authentifizierung“ beschrieben, können auch wir als Betreiber der Routingserver den verschlüsselten Datenverkehr nicht einsehen.

Verschlüsselung und Authentifizierung

TeamViewer-Verbindungen laufen über komplett gesicherte Datenkanäle, die mit einem 2048 Bit RSA Public-/Private Key Exchange aufgebaut und mit 256 Bit AES verschlüsselt sind. Diese Technik wird in vergleichbarer Form auch bei https/SSL eingesetzt und gilt nach heutigem Stand der Technik als vollständig sicher. Da der Private Key niemals den Clientcomputer verlässt, ist durch dieses Verfahren technisch sichergestellt, dass zwischengeschaltete Computer im Internet den Datenstrom nicht entziffern können, das gilt somit auch für die TeamViewer Routingserver.

Jeder TeamViewer Client hat bereits den Public-Key unseres Masterclusters implementiert und kann so Nachrichten an den Mastercluster verschlüsseln bzw. dessen Signatur überprüfen. Die Public-Key-Infrastruktur verhindert effektiv „Man-in-the-middle-Attacken“. Das Kennwort wird trotz Verschlüsselung niemals direkt, sondern im Challenge-Response Verfahren übertragen und ist nur auf den lokalen Computern gespeichert.

Bei der Authentifizierung wird das Kennwort aufgrund der Verwendung des Secure Remote Password Protokolls (SRP) niemals direkt übertragen und es wird lediglich ein Passwort-Verifier auf dem lokalen Computer gespeichert.



TeamViewer-Verschlüsselung und Authentifizierung

Validierung von TeamViewer IDs

Die TeamViewer IDs werden direkt von TeamViewer automatisch anhand von diversen Hardware- und Softwaremerkmalen generiert. Die TeamViewer Server kontrollieren diese ID bei Verbindungen auf ihre Gültigkeit.

Brute-Force Schutz

Wenn Interessenten uns zur TeamViewer-Sicherheit befragen, spielt das Thema Verschlüsselung eine große Rolle. Verständlicherweise ist die Möglichkeit, dass Dritte eine Verbindung einsehen oder die TeamViewer-Zugangsdaten abgegriffen werden können, gefürchtet. In der Praxis sind es dann aber oft ganz primitive Angriffe, die am gefährlichsten sind.

Im Kontext der Computersicherheit ist ein Brute-Force Angriff meist der Versuch, ein Kennwort, welches den Zugriff auf eine Ressource schützt, durch Ausprobieren zu erraten. Mit der steigenden Rechenleistung handelsüblicher Computer wird der Zeitaufwand für das Ausprobieren auch längerer Kennwörter immer weiter reduziert.

Zur Abwehr von Brute-Force Angriffen erhöht TeamViewer exponentiell die Wartezeit zwischen Verbindungsversuchen. Für 24 Versuche werden so bereits 17 Stunden benötigt. Die Wartezeit für Verbindungsversuche wird erst nach der erfolgreichen Kennwort-Eingabe zurückgesetzt.

TeamViewer bietet seinen Kunden nicht nur Schutz vor Angriffen eines bestimmten Computers, sondern auch vor sogenannten Botnetz-Angriffen, bei denen versucht wird, von mehreren Computern aus auf eine spezielle TeamViewer ID zuzugreifen.

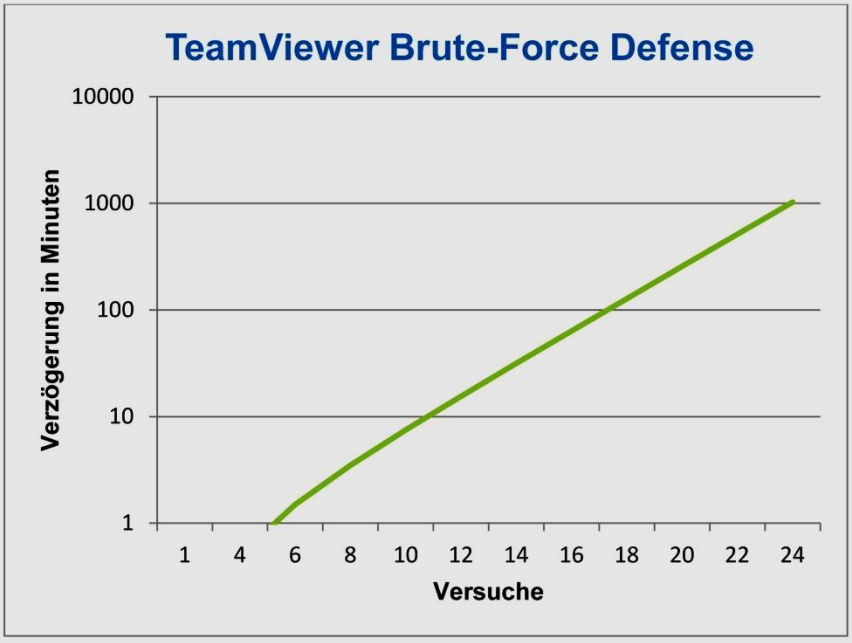


Diagramm: Benötigte Zeit für die Anzahl von Versuchen bei einem Brute-Force Angriff

Code Signing

Als zusätzliche Sicherheitsfunktion werden alle unsere Programme mittels VeriSign Code Signing signiert. Dadurch ist der Herausgeber der Software immer zuverlässig identifizierbar. Wird die Software nachträglich verändert, wird die digitale Signatur automatisch ungültig.

Datacenter & Backbone

Diese beiden Themen betreffen sowohl die Verfügbarkeit als auch die Sicherheit von TeamViewer. Die zentralen TeamViewer Server befinden sich innerhalb der Europäischen Union, in nach ISO 27001 zertifizierten Rechenzentren mit multiredundanter Carrier-Anbindung und redundanter Stromversorgung. Es wird ausschließlich Markenhardware eingesetzt.

Personenbezogene Zutrittsüberwachung, Videokameras, Bewegungsmelder, 24/7-Überwachung und Vor-Ort-Sicherheitspersonal gewährleisten, dass nur autorisiertes Personal Zugang zum Rechenzentrum hat und garantieren die bestmögliche Sicherheit für Hardware und Daten. An dem Single-Point-of-Entry zum Rechenzentrum findet eine ausführliche Personenüberprüfung und -identifikation statt.

TeamViewer-Konto

Die TeamViewer-Konten werden auf dedizierten TeamViewer Servern gehostet. Weitere Informationen zur Zutrittskontrolle entnehmen Sie bitte dem Abschnitt „Datacenter & Backbone“. Für Autorisierung und Passwortverschlüsselung wird das Secure Remote Password Protokoll (SRP), ein erweitertes passwortbasiertes Authentisierung- und Schlüsseleinigungsverfahren (PAKE) verwendet. Dadurch wird verhindert, dass ein Eindringling oder Man-In-The-Middle ausreichend Informationen erhält, um ein Passwort durch Brute-Force Angriffe zu erraten. Somit kann selbst mit schwachen Passwörtern eine hohe Sicherheit gewährleistet werden. Sensible Daten des TeamViewer-Kontos, z. B. Anmeldeinformationen für Cloud-Speicherdienste, werden mit AES/RSA 2048Bit verschlüsselt gespeichert.

Management Console

Die TeamViewer Management Console ist eine webbasierte Plattform, die dem Benutzermanagement, der Verbindungsprotokollierung und der Verwaltung der Computer & Kontakte dient. Sie wird in einem nach ISO-27001 zertifizierten Rechenzentrum gehostet. Die Datenübertragung wird durch das Verschlüsselungsprotokoll SSL (Secure Sockets Layer) verschlüsselt, dem Standard für sichere Internetverbindungen. Sensible Daten werden außerdem mit AES/RSA 2048 Bit verschlüsselt gespeichert. Für Autorisierung und Passwortverschlüsselung wird das Secure Remote Password Protokoll (SRP), ein erweitertes passwortbasiertes, gängiges und stabiles Authentisierung- und Schlüsseleinigungserfahren (PAKE) verwendet. Entsprechend der Datenschutzrichtlinie der Europäischen Union verbleiben die Daten innerhalb der EU.

Ein- und ausgehende Zugriffskontrolle

Sie können die Verbindungsmöglichkeiten von TeamViewer individuell konfigurieren. So können Sie beispielsweise Computer so einrichten, dass keine ein- oder ausgehenden Verbindungen (Fernsteuerung oder Meeting) möglich sind.

Die Beschränkung der Funktionalität auf die wirklich benötigten Funktionen bringt immer auch eine Beschränkung der möglichen Angriffspunkte mit sich.

Zwei-Faktor-Authentifizierung

Mit der Zwei-Faktor Authentifizierung unterstützt TeamViewer Unternehmen dabei, Ihre HIPAA und PCI-Anforderungen zu erfüllen. Die Zwei-Faktor-Authentifizierung bietet eine zusätzliche Sicherheitsebene zum Schutz vor unbefugtem Zugriff auf das TeamViewer-Konto. Zusätzlich zu seinem Passwort muss der User einen Code eingeben, um sich zu authentifizieren. Der Code wird mit einem zeitbasierten TOTP (time-based one-time password) Algorithmus erzeugt, dadurch hat der Code nur eine kurze, zeitlich begrenzte Gültigkeit.

Durch die Zwei-Faktor-Authentifizierung und die eingeschränkte Zugriffskontrolle mittels Whitelisting erfüllt TeamViewer alle notwendigen Kriterien für HIPAA und PCI Zertifizierungen.