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 ausliefern, um evtl. 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 hat Ihren Sitz im Süddeutschen Uhingen (Nähe Stuttgart) und wurde 2005 gegründet. Wir beschäftigen uns ausschließlich mit Entwicklung und Vertrieb von sicheren Systemen für die webbasierte Zusammenarbeit und Kommunikation. Ein rasanter Start und schnelles Wachstum haben in kurzer Zeit zu mehr als 10.000.000 Installationen der TeamViewer Software und Nutzern in über fünfzig Ländern der Erde geführt. Die Software ist zurzeit in 8 Sprachen verfügbar.

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

Die TeamViewer GmbH befindet sich in Privatbesitz und ist seit der Gründung profitabel.

Unser Sicherheitsverständnis

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

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 Service-eigenschaften.

Referenzen

Zum aktuellen Zeitpunkt (Juli / 2008) ist TeamViewer auf über 10.000.000 Rechnern im Einsatz. Internationale Top-Unternehmen aus allen Branchen (inklusive hochsensiblen Bereichen wie Banken/ Finanzwirtschaft) setzen TeamViewer erfolgreich ein.

Wir laden Sie herzlich ein, unsere Referenzen-Seite im Internet aufzurufen und sich so vorab schon mal einen Eindruck von der Akzeptanz unserer Lösung zu verschaffen. Sicher werden Sie zustimmen, dass die meisten dieser Unternehmen vermutliche 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 im Folgenden technische Details.

Aufbau und Ablauf einer TeamViewer-Sitzung

Verbindungsaufbau und Verbindungsarten.

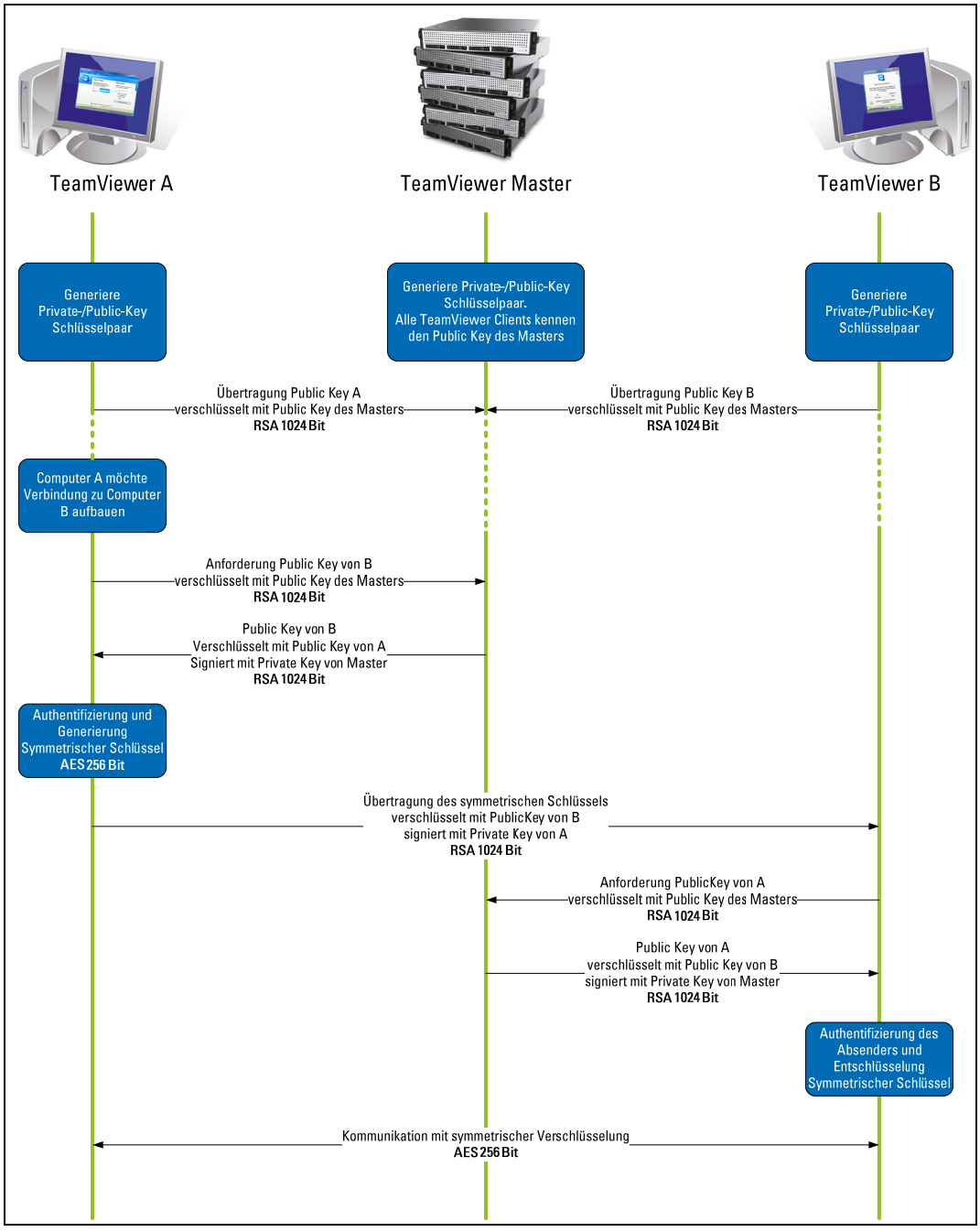
TeamViewer ermittelt beim Aufbau einer Verbindung die optimale Verbindungsart. Nach dem Handshake über unsere Master-Server findet in 70 % der Fälle (auch hinter Standard-Gateways, NAT und Firewalls) eine Direkt-verbindung über UDP oder TCP statt. Die restlichen Verbindungen werden über unser hochredundantes 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 arbeitet mit vollständiger Verschlüsselung auf Basis eines RSA Public-/Private Key Exchange und AES (256 Bit) Session Encoding. 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 Clientrechner verlässt, ist durch dieses Verfahren technisch sichergestellt, dass zwischengeschaltete Rechner im Internet den Datenstrom nicht entziffern können, das gilt somit auch für die TeamViewer Routingserver.

Jeder TeamViewer Client hat bereits den Public-Key des Masterclusters implementiert und kann so Nachrichten für den Master verschlüsseln bzw. die Signatur des Masters überprüfen. Die PKI 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 Rechnern gespeichert.



TeamViewer-Verschlüsselung und Authentifizierung

Validierung von TeamViewer IDs

Die TeamViewer IDs werden direkt von TeamViewer automatisch anhand von Hardware-Merkmalen generiert. Die TeamViewer Server kontrollieren diese ID bei jeder Verbindung auf Gültigkeit, so dass es nicht möglich ist, gefälschte IDs zu erzeugen und zu verwenden.

Schutz vor Brute-Force Angriffen

Wenn Interessenten uns zum Thema TeamViewer-Sicherheit befragen, werden wir regelmäßig zum Thema Verschlüsselung befragt. Verständlicherweise ist die Gefahr, dass Dritte eine Verbindung einsehen können 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 geschützte 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.

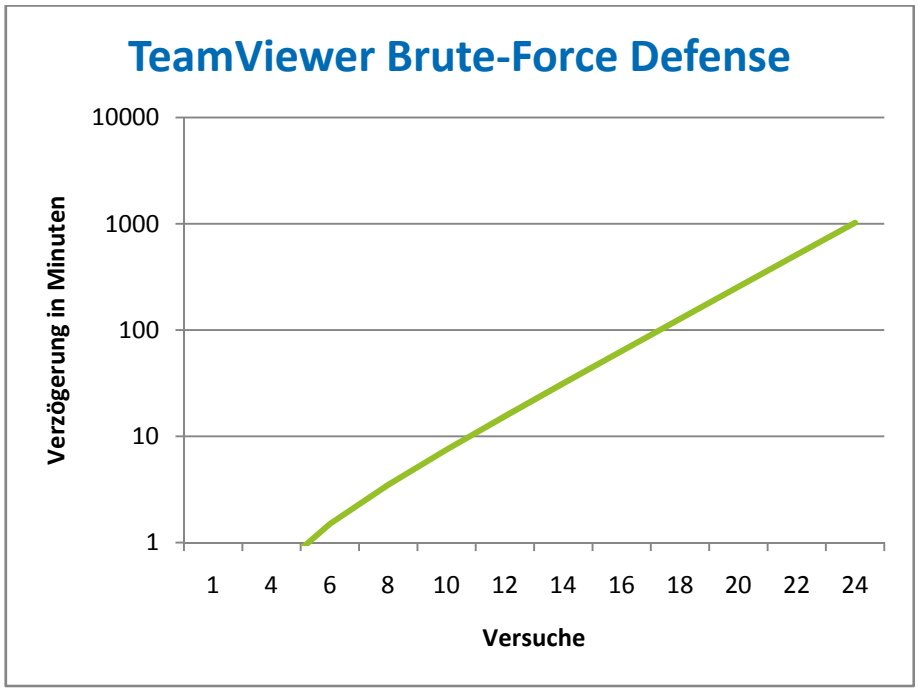


Diagramm: Benötigte Zeit für die Anzahl von n Versuchen bei einem Brute-Force Angriff.

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.
Sogar die selbst erstellten QuickSupport Custom Design Tools werden bei der Erstellung dynamisch signiert.

Datacenter & Backbone

Ein Thema für die Verfügbarkeit aber auch für die Sicherheit. Die zentralen TeamViewer Server befinden sich in einem hochmodernen Datacenter mit multiredundanter Carrier-Anbindung und redundanter Stromversorgung. Es wird ausschließlich Markenhardware (Cisco, Foundry, Juniper) eingesetzt.

Der Zugang zum Rechenzentrum ist nur über eine einzige Eingangsschleuse und nur nach Personen-überprüfung und –identifikation möglich. Kameraüberwachung, Einbruchsmeldung, 24/7 Überwachung und Vor-Ort-Sicherheitspersonal schützen unsere Server gegen Angriffe von innen.

Anwendungssicherheit in TeamViewer

Black- & Whitelist

Insbesondere wenn Sie TeamViewer auf Rechnern installieren, die unbeaufsichtigt gewartet werden sollen (also TeamViewer als Windows-Systemdienst installieren), kann es interessant sein, zusätzlich zu allen Sicherheits-mechanismen den Zugriff auf diesen Rechner auf bestimmte Clients einzuschränken.

Über die Whitelist-Funktion können Sie explizit angeben, welche TeamViewer IDs sich auf einen Rechner verbinden dürfen, über die Blacklist-Funktion bestimmte TeamViewer IDs sperren.

Kein Stealth-Mode

Es gibt keine TeamViewer-Funktion, die es ermöglicht, TeamViewer komplett unsichtbar im Hintergrund laufen zu lassen. Über ein Icon im Infobereich (system tray) ist TeamViewer auch dann sichtbar, wenn die Applikation als Windows-Systemdienst im Hintergrund läuft.

Nach dem Aufbau einer Verbindung ist immer ein kleines Control-Panel sichtbar – zur versteckten Über-wachung von Rechnern oder Mitarbeitern ist TeamViewer daher bewusst ungeeignet.

Kennwort-Schutz

Für den spontanen Kunden-Support generiert TeamViewer (TeamViewer QuickSupport) ein Sitzungskennwort (Einmal-Kennwort). Teilt Ihr Kunde Ihnen dieses Kennwort mit, so können Sie sich durch Eingabe von ID und Kennwort auf den Kundenrechner aufschalten. Beim Neustart von TeamViewer beim Kunden wird ein neues Sitzungskennwort generiert, so dass Sie die Rechner Ihrer Kunden nur erreichen können, wenn Sie explizit dazu eingeladen werden.

Beim Einsatz zur unbeaufsichtigten Fernwartung (z.B. von Servern) vergeben Sie ein individuelles festes Kennwort, das den Zugriff auf den Rechner schützt.

Zugriffskontrolle Ein- und Ausgehend

Sie können die Verbindungsmöglichkeiten von TeamViewer individuell konfigurieren. So können Sie beispielsweise einen Fernwartungsrechner oder Präsentationsrechner so einrichten, dass keine eingehenden Verbindungen möglich sind.

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

Weitere Fragen?

Bei weiteren Fragen zum Thema Sicherheit freuen wir uns jederzeit über Ihren Anruf: +49 (0) 7161 6069 250, bzw. Ihre E-Mail: support@teamviewer.com.

Kontakt

TeamViewer GmbH
Stuttgarter Str. 159
D-73066 Uhingen
service@teamviewer.com

Geschäftsführung: Dr. Tilo Rossmanith
Handelsregister: Ulm HRB 534075