TeamViewer Funktionsweise & Sicherheit

Aufbau und Ablauf einer TeamViewer-Sitzung

Verbindungsaufbau und Verbindungsarten

Die Fernwartungssoftware TeamViewer ermittelt beim Aufbau einer Verbindung die optimale Verbindungsart. Nach dem Handshake über den 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 ein hochredundantes Router-Netzwerk via TCP oder http-Tunneling geleitet. Es müssen also keinerlei Ports geöffnet werden, um mit TeamViewer arbeiten zu können!

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 unseres Masterclusters implementiert und kann so Nachrichten für jeden TeamViewer Master verschlüsseln bzw. die Signatur des Masters 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 Rechnern gespeichert.

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

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.

Code Signing

Als zusätzliche Sicherheitsfunktion werden alle 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

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 Personenüberprüfung und –identifikation möglich. Kameraüberwachung, Einbruchsmeldung, 24/7 Überwachung und Vor-Ort-Sicherheitspersonal schützen den Server gegen Angriffe von innen.

Anwendungssicherheit in TeamViewer

Black- & Whitelist

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 Überwachung 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 wir uns durch Eingabe von ID und Kennwort auf Ihren Kundenrechner aufschalten. Beim Neustart von TeamViewer wird ein neues Sitzungskennwort generiert, so dass ein Rechner nur erreicht werden kann, wenn explizit dazu eingeladen wird.

Ein- und ausgehende Zugriffskontrolle

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.

Der Text beruht auf Auszügen der Internetseite http://www.teamviewer.com/images/pdf/TeamViewer_Sicherheitsstatement.pdf vom 10.02.2011.