Informazioni sulla sicurezza TeamViewer

Gruppo target

Il presente documento è rivolto agli amministratori di rete professionali. Le informazioni ivi contenute sono di natura alquanto tecnica e molto dettagliata. Sulla base delle presenti informazioni, i professionisti IT avranno una visione dettagliata degli standard di sicurezza in TeamViewer e potranno superare qualsiasi incertezza prima del deployment del nostro software. Distribuite liberamente il presente documento ai clienti per mitigare qualsiasi preoccupazione relativa alla sicurezza.

Se ritenete di non appartenere al gruppo target, potrete comunque ottenere un'immagine chiara della serietà rivolta alla sicurezza dai dati qualitativi nella sezione L'azienda/Il software.

L'azienda/Il software

Chi siamo

TeamViewer GmbH è stata fondata nel 2005 e ha sede nella Germania meridionale, nelle città di Göppingen (vicino a Stoccarda), con consociate in Australia e negli Stati Uniti. Sviluppiamo e vendiamo in esclusiva sistemi di sicurezza per collaborazione su base web. In breve tempo, le nostre licenze Freemium hanno condotto a una rapida crescita, con oltre 200 milioni di utenti del software TeamViewer su oltre 1,4 miliardi di dispositivi in oltre 200 paesi nel mondo. Il software è disponibile in oltre 30 lingue.

La nostra comprensione della sicurezza

TeamViewer è utilizzato da oltre 30 milioni di persone ovunque in qualsiasi momento. Gli utenti forniscono supporto spontaneo su internet, accedono a computer privi di vigilanza (cioè assistenza in remoto per server) e ospitano riunioni online. In funzione della configurazione, potete utilizzare TeamViewer per il controllo remoto di un altro computer, come se vi foste seduti davanti. Se l'utente registrato sul computer remoto è un amministratore di Windows, Mac o Linux, a questa persona saranno concessi diritti di amministratore anche su tale computer.

Ovviamente, data la potenziale mancanza di sicurezza di Internet, questa importante funzionalità deve essere protetta dagli attacchi con grande attenzione. La questione della sicurezza domina infatti tutti i nostri obiettivi di sviluppo ed è un elemento che ci coinvolge e ci assorbe completamente in tutto quello che facciamo. Vogliamo assicurarvi un accesso al computer sicuro e proteggere i nostri stessi interessi: milioni di utenti nel mondo si fidano soltanto di una soluzione sicura, che è l'unica a garantire il successo a lungo termine della nostra azienda.

Valutazione di esperti esterni

Il nostro software, TeamViewer, ha ricevuto il sigillo di qualità a cinque stelle (valore massimo) dell'Associazione Federale degli Esperti e Revisori IT (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.), i cui revisori indipendenti controllano i prodotti di aziende qualificate accertandone qualità, sicurezza e caratteristiche di servizio.

Referenze

Attualmente, oltre 200 milioni di persone utilizzano TeamViewer e multinazionali di qualsiasi settore (tra cui settori altamente sensibili come bancario, finanziario, sanitario e governativo) ottengono risultati positivi.

Per una prima impressione sulle soluzioni proposte, vi invitiamo a valutare le nostre referenze su Internet. Scoprirete che presumibilmente molte altre aziende avevano esigenze analoghe di sicurezza e disponibilità prima di decidere - dopo un attento esame - di passare a TeamViewer. Nel seguito del documento riportiamo alcuni dettagli tecnici affinché possiate farvi un'idea.

Sessioni di TeamViewer

Creazione di una sessione e tipi di connessioni

Quando si stabilisce una sessione, TeamViewer determina il tipo di connessione ottimale. Dopo la comunicazione tra i nostri master server, nel 70% dei casi si stabilisce una connessione diretta via UDP o TCP (anche dietro gateway standard, NAT e firewall) e le altre connessioni sono instradate attraverso la rete del router altamente ridondante via TPC o https-tunnelling. Non è necessario aprire delle porte per lavorare con TeamViewer

Come descritto in seguito al paragrafo Codifica e autenticazione, neppure noi, in qualità di operatore di server di routing, possiamo leggere il traffico di dati criptati.

Codifica e autenticazione

TeamViewer Traffic è protetto con l'utilizzo di scambi con chiave pubblica/privata RSA e codifica di sessione AES (256 bit). Questa tecnologia è utilizzata in forma comparabile per http/SSL ed è ritenuta completamente sicura per gli standard odierni. Poiché la chiave privata non lascia mai il computer del cliente, questa procedura garantisce che i computer interconnessi - compresi i server di routing TeamViewer - non possano decifrare il flusso di dati.

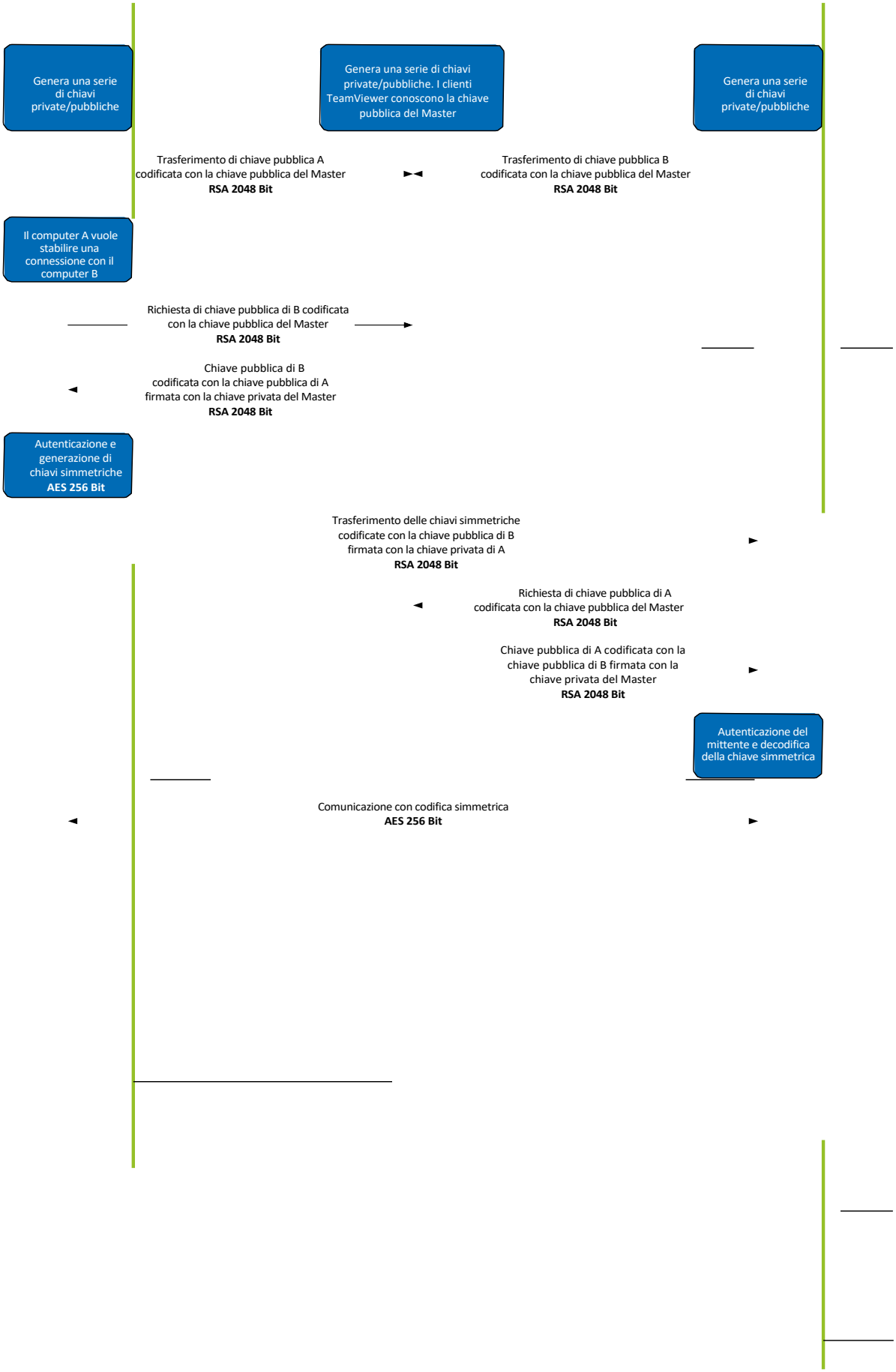
Ogni cliente TeamViewer ha già implementato la chiave pubblica del master cluster e può quindi codificare i messaggi al master cluster e controllare i messaggi firmati dal medesimo. La PKI (Public Key Infrastructure, infrastruttura a chiave pubblica) previene effettivamente attacchi man-in-the-middle. Nonostante la codifica, la password non è mai inviata direttamente, ma soltanto tramite una procedura di sfida-risposta e salvata solo su computer locale.

Durante l'autenticazione, la password non è mai trasferita direttamente in quanto si utilizza il protocollo Secure Remote Password (SRP). Sul computer locale è memorizzato soltanto un verificatore di password.

TeamViewer A

TeamViewer Master

TeamViewer B


Genera una serie di chiavi private/pubbliche
Genera una serie di chiavi private/pubbliche. I clienti TeamViewer conoscono la chiave pubblica del Master
Genera una serie di chiavi private/pubbliche
Trasferimento di chiave pubblica A codificata con la chiave pubblica del Master
RSA 2048 Bit
Trasferimento di chiave pubblica B codificata con la chiave pubblica del Master
RSA 2048 Bit
Il computer A vuole stabilire una connessione con il computer B
Richiesta di chiave pubblica di B codificata con la chiave pubblica del Master
RSA 2048 Bit
Chiave pubblica di B codificata con la chiave pubblica di A firmata con la chiave privata del Master
RSA 2048 Bit
Autenticazione e generazione di chiavi simmetriche
AES 256 Bit
Trasferimento delle chiavi simmetriche codificate con la chiave pubblica di B firmata con la chiave privata di A
RSA 2048 Bit
Richiesta di chiave pubblica di A codificata con la chiave pubblica del Master
RSA 2048 Bit
Chiave pubblica di A codificata con la chiave pubblica di B firmata con la chiave privata del Master
RSA 2048 Bit
Autenticazione del mittente e decodifica della chiave simmetrica
Comunicazione con codifica simmetrica
AES 256 Bit

Codifica e autenticazione TeamViewer

Convalida degli ID TeamViewer

Gli ID TeamViewer si basano su varie caratteristiche hardware e software e sono generati automaticamente da TeamViewer. I server TeamViewer controllano la validità di questi ID prima di qualsiasi connessione.

Protezione da forza bruta

I potenziali clienti che si informano sulla sicurezza di TeamViewer pongono regolarmente domande sulla codifica. Comprensibilmente, ciò che li spaventa maggiormente è il rischio che terzi possano monitorare la connessione o che i dati di accesso di TeamViewer siano sottratti. Tuttavia, in realtà, spesso gli attacchi più pericolosi sono alquanto primitivi.

Nell'ambito della sicurezza informatica, un attacco con forza bruta rappresenta un metodo empirico per indovinare una password che protegge una risorsa. Con la crescente potenza di calcolo dei computer standard, il tempo necessario per indovinare password lunghe si è ridotto sempre più.

Per la difesa dagli attacchi da forza bruta, TeamViewer aumenta in misura esponenziale il ritardo tra tentativi di connessione, rendendo quindi necessarie ben 17 ore per 24 tentativi. La latenza è ripristinata solo dopo il corretto inserimento della password corretta.

TeamViewer non solo ha attuato un meccanismo di protezione dei clienti contro gli attacchi da un singolo computer specifico, ma anche da più computer, noti come attacchi botnet, che tentano di accedere a un determinato ID TeamViewer.

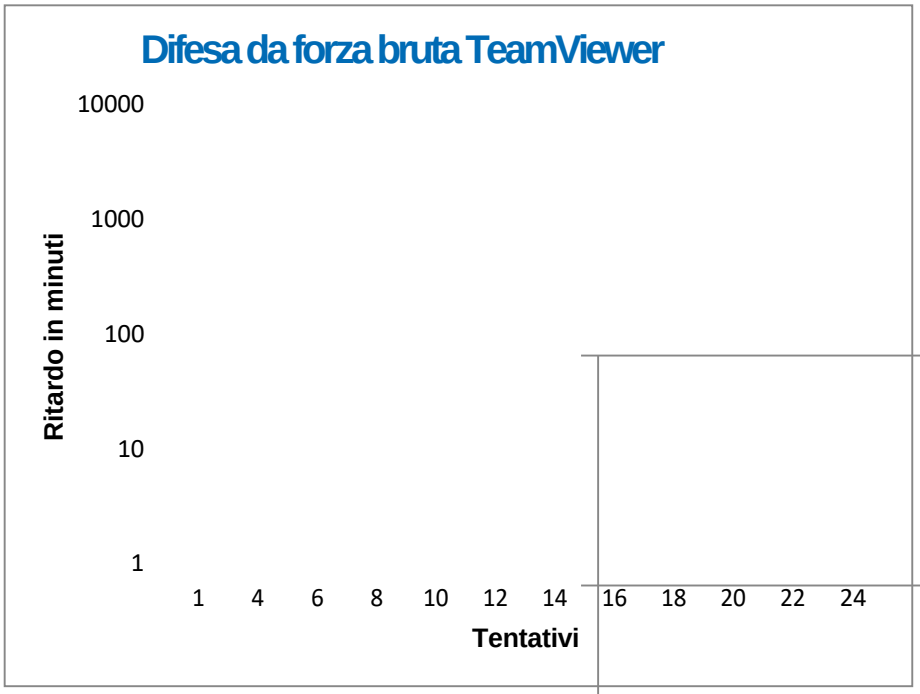


Diagramma: tempo trascorso dopo n tentativi di connessione durante un attacco con forza bruta

Firma del codice

Come funzione di sicurezza supplementare, tutti i nostri software sono sottoposti a VeriSign Code Signing, per individuare rapidamente l'autore del software. Se il software è stato modificato successivamente, la firma digitale è resa automaticamente non valida.

Data Center e backbone

Per fornire la massima sicurezza e disponibilità dei servizi, i server TeamViewer sono ubicati in data center conformi a ISO 27001 che influenzano connessioni di carrier multi-ridondanti e alimentazioni ridondanti. Inoltre, si utilizza soltanto l'hardware del nome del marchio allo stato dell'arte e i server che memorizzano dati sensibili sono ubicati in Germania o in Austria.

Con la certificazione ISO 27001, controllo accesso personale, sorveglianza con video camera, rilevatori di movimento, monitoraggio 24x7 e personale di sicurezza in loco garantiscono che l'accesso al data center sia consentito unicamente alle persone autorizzate e assicurano la massima sicurezza per hardware e dati. È previsto anche un controllo di identificazione dettagliato al singolo punto di accesso al data center.

Account TeamViewer

Gli account TeamViewer sono ospitati sui relativi server dedicati. Per informazioni sul controllo degli accessi, fate riferimento a Datacenter e a backbone sopra. Per autorizzazione e codifica password, si utilizza il protocollo Secure Remote Password (SRP), un protocollo aumentato di accordo con chiave autenticata da password (PAKE). Un infiltrato o man in the middle non può ottenere informazioni sufficienti a scoprire una password con forza bruta. Questo significa che si può ottenere un'elevata sicurezza persino utilizzando password scadenti. I dati sensibili nell'account TeamViewer, per esempio informazioni di login per lo storage del cloud, sono memorizzate con codifica a 2048 bit in AES/RSA.

Management Console

La TeamViewer Management Console è una piattaforma su base web per gestione utenti, report di connessione e gestione di computer e contatti, ospitata in data center conformi a HIPAA e certificati ISO-27001. Il trasferimento di dati avviene attraverso un canale sicuro utilizzando la codifica TSL (Transport Security Layer), lo standard per le connessioni di rete Internet sicure. Inoltre i dati sensibili sono memorizzati con codifica a 2048 bit AES/RSA. Per autorizzazione e codifica password, si utilizza il protocollo Secure Remote Password (SRP), un metodo di scambio chiavi e autenticazione solida e consolidata basata su password sicura, utilizzando un modulo a 2048 bit.

Impostazioni basate sulle politiche

Dall'interno della TeamViewer Management Console, gli utenti sono in grado di definire, distribuire e attuare politiche di impostazione per le installazioni dei software TeamViewer su dispositivi che appartengono specificatamente a loro. Le politiche di impostazione hanno la firma digitale dell'account che le ha generate, per garantire che l'unico l'account autorizzato ad assegnare una politica a un dispositivo sia quello a cui appartiene il dispositivo.

Sicurezza delle applicazioni in TeamViewer

Lista nera e lista bianca

In particolare, se si utilizza TeamViewer per la manutenzione di computer senza vigilanza (cioè TeamViewer è installato come servizio di Windows), può essere interessante l'opzione di sicurezza supplementare che prevede la restrizione dell'accesso a tali computer a una serie di clienti specifici.

La funzione lista bianca consente di indicare espressamente gli ID e/o gli account TeamViewer autorizzati ad accedere a un computer, mentre la funzione lista nera consente di bloccarli. È disponibile una lista bianca centrale nell'ambito delle impostazioni basate sulle politiche descritte sopra in “Management Console.”

Chat e codifica video

Le cronologie delle chat sono associate all'account TeamViewer e quindi codificate e memorizzate utilizzando la stessa sicurezza di codifica AES/RSA a 2048 descritta al paragrafo “Account TeamViewer”. I messaggi in chat e il traffico video sono codificati end-to-end tramite la codifica della sessione AES (256 bit).

Modalità stealth assente

Non esiste una funzione che consenta di eseguire TeamViewer completamente in background. Anche se l'applicazione è in esecuzione come servizio Windows in background, TeamViewer è sempre visibile tramite un'icona nella barra di sistema.

Dopo avere stabilito una connessione, è sempre visibile un piccolo pannello di controllo sopra la barra di sistema, che rende quindi TeamViewer chiaramente inadatto a monitorare computer o personale di nascosto.

Protezione con password

Per l'assistenza clienti autonoma, TeamViewer (TeamViewer QuickSupport) genera una password di sessione (valida una sola volta). Se il cliente vi comunica la password, potete connettervi al computer inserendo la sua ID e password. Dopo un riavvio di TeamViewer da parte del cliente, sarà generata una nuova password di sessione affinché possiate connettervi ai computer del cliente solo se invitati a farlo.

Nel deployment di TeamViewer per il supporto remoto senza vigilanza (per es. server), si imposta una password individuale e fissa che protegge l'accesso al computer.

Controllo accessi in entrata e in uscita

Potete configurare le singole modalità di connessione di TeamViewer, per esempio il supporto remoto o il computer delle riunioni in modo che non sia possibile alcuna connessione in entrata.

Ridurre la funzionalità alle caratteristiche effettivamente necessarie implica sempre una limitazione di eventuali punti deboli in potenziali attacchi.

Autenticazione a due fattori

TeamViewer assiste le aziende in base ai loro requisiti di conformità HIPAA e PCI. L'autenticazione a due fattori aggiunge un livello di sicurezza supplementare per proteggere gli account TeamViewer da accesso non autorizzato.

Oltre a nome utente e password, l'utente deve inserire un codice per l'autenticazione, generato dall'algoritmo della password a tempo valida una sola volta (TOTP). Il codice è quindi valido soltanto per un breve periodo di tempo.

Tramite autenticazione a due fattori e limitando l'accesso tramite una lista bianca, TeamViewer contribuisce a soddisfare tutti i criteri necessari alla certificazione HIPAA e PCI.

Test di sicurezza

L'infrastruttura e il software TeamViewer sono entrambi sottoposti a test di penetrazione su base regolare, svolti da aziende indipendenti specializzate in test di sicurezza.

Altre domande?

Per ulteriori chiarimenti o informazioni, potrete contattarci al numero +39 02 89 03 86 48, oppure inviare un'email a support@teamviewer.com.

Contatto

TeamViewer GmbH
Jahnstr. 30
D-73037 Göppingen
Germany
service@teamviewer.com