



Informazioni sulla sicurezza di TeamViewer

Utenti destinatari

Questo documento è diretto agli amministratori di rete professionisti. Le informazioni contenute nel presente documento sono di natura tecnica e particolareggiate. Grazie a queste informazioni, i professionisti IT hanno a disposizione, prima di installare TeamViewer, un'immagine dettagliata relativamente alla sicurezza del software. Non esitate a distribuire liberamente questo documento ai Vostri clienti per risolvere eventuali dubbi o quesiti riguardanti la sicurezza.

Qualora non Vi consideriate utenti destinatari del presente documento, le informazioni generali contenute nella sezione "La Società / il software" Vi aiuteranno ad ottenere una visione insieme del prodotto.

La Società / il software

Chi siamo

La Società TeamViewer GmbH ha sede nel sud della Germania, nella città di Göppingen (vicino a Stoccarda), ed è stata fondata nel 2005. La nostra attività è focalizzata in modo esclusivo sullo sviluppo e sulla vendita di sistemi sicuri per la collaborazione tramite web. Un rapido avviamento e la crescita dinamica hanno creato in breve tempo diversi milioni di installazioni del software TeamViewer, con utenti in oltre 200 paesi in tutto il mondo. Il software è attualmente disponibile in più di 30 lingue.

Il nostro concetto di sicurezza

TeamViewer è utilizzato milioni di volte nel mondo per fornire un supporto immediato via Internet, oppure per accedere ai computer non presidiati (ad es. teleassistenza ai server). A seconda della configurazione di TeamViewer, ciò significa che il computer remoto può essere controllato come se si fosse seduti davanti ad esso. All'utente amministratore di Windows, Linux o di Mac, che ha avuto accesso al computer remoto, saranno assegnati i diritti di amministratore anche sulla postazione remota.

È evidente che una funzionalità di tale portata, nella potenziale carenza di sicurezza di Internet, deve essere protetta in diversi modi contro eventuali attacchi. L'aspetto della sicurezza prevale infatti su tutti gli altri nostri obiettivi di sviluppo, per consentire all'utente di accedere al proprio computer in sicurezza e salvaguardare inoltre i nostri propri interessi: milioni di utenti in tutto il mondo si affideranno solamente ad una soluzione sicura e soltanto una soluzione sicura garantirà alla nostra attività aziendale un successo di lungo termine.

Gestione della qualità

È nostra convinzione che la gestione della sicurezza sia inconcepibile senza una consolidata gestione della qualità. TeamViewer GmbH è uno dei pochi fornitori sul mercato ad applicare la gestione della qualità certificata secondo la norma ISO 9001. La nostra gestione della qualità segue gli standard riconosciuti a livello internazionale. Il nostro sistema QM (gestione qualità) è rivisto da revisori esterni su base annuale.



Valutazione dei tecnici qualificati esterni

Al software TeamViewer è stato conferito il sigillo di qualità a cinque stelle (valore massimo) dalla Associazione Federale dei Tecnici e Revisori IT (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.). I revisori indipendenti di BISG e.V. ispezionano i prodotti dei produttori qualificati per quanto riguarda la qualità, la sicurezza e il grado di eccellenza del servizio.



Ispezione relativa alla sicurezza

TeamViewer è stato sottoposto ad un'ispezione relativa alla sicurezza dalle società tedesche FIDUCIA IT AG e GAD eG (entrambi sono operatori nell'ambito dei centri di elaborazione dati per circa 1200 banche tedesche), ed è stato approvato per l'utilizzo sulle stazioni di lavoro delle banche.



Referenze

Attualmente TeamViewer è utilizzato su oltre 100.000.000 computer. Società internazionali ai massimi livelli, in tutti i settori industriali (inclusi i settori estremamente sensibili, come le banche ed altre istituzioni finanziarie), utilizzano TeamViewer con successo.

Vi invitiamo a consultare le nostre referenze su Internet per farvi un'idea dell'approvazione ottenuta dalla nostra soluzione. Converrete sicuramente che la maggior parte delle aziende aveva presumibilmente degli analoghi requisiti di sicurezza e disponibilità prima di scegliere, in seguito ad un attento esame, TeamViewer. Per potervi fare un'opinione personale, nei paragrafi seguenti sono descritti alcuni dettagli tecnici.

Creazione e funzionamento di una sessione di TeamViewer

Creazione di una sessione e tipi di connessioni.

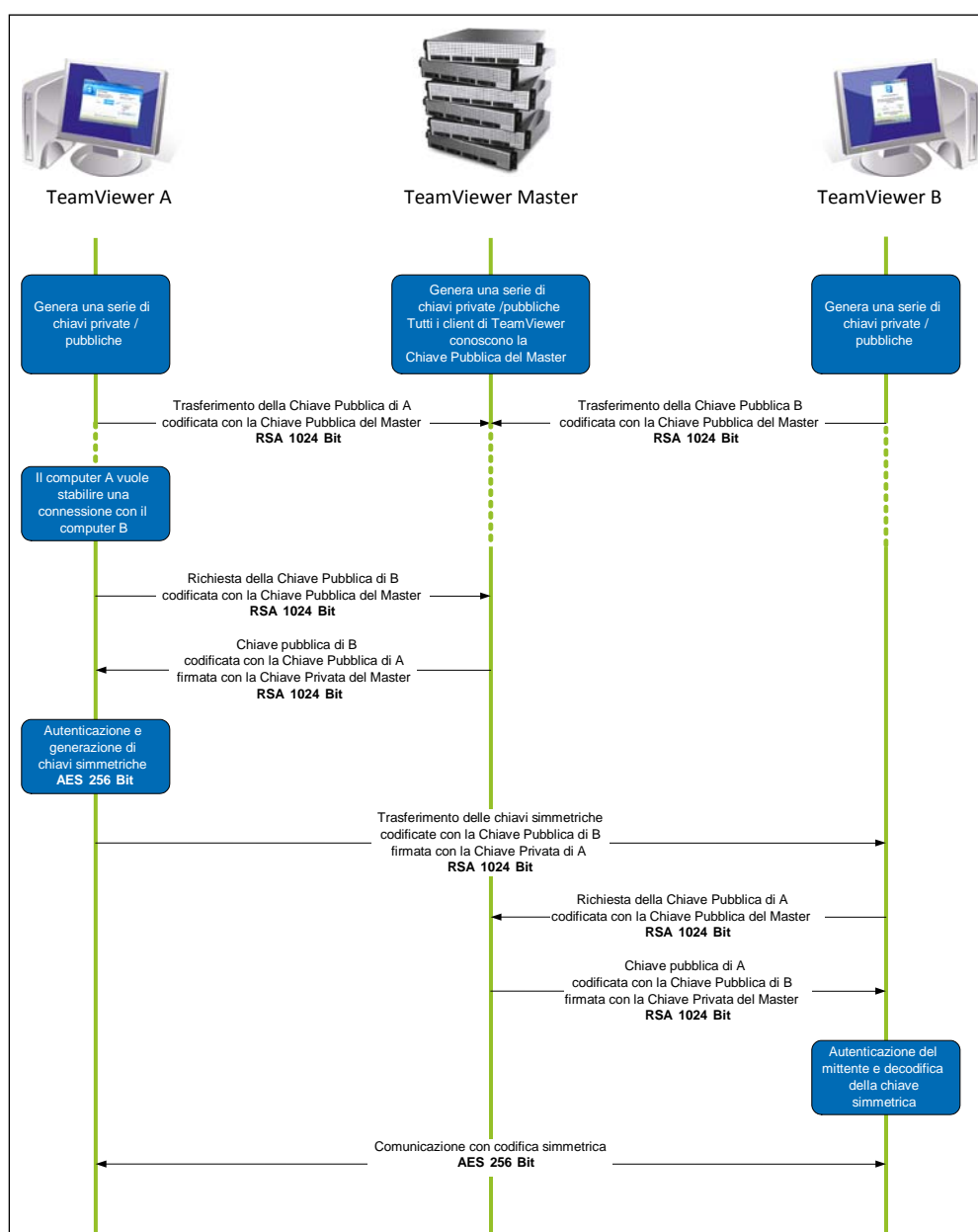
Quando si crea una sessione, TeamViewer stabilisce il tipo ottimale di connessione. Dopo il processo di "handshaking" eseguito attraverso i nostri server master, nel 70% dei casi viene instaurata una connessione tramite UDP oppure TCP (anche dietro a gateway, NAT e firewall standard). Le restanti connessioni sono instradate tramite la nostra rete di router ad alta ridondanza, via TCP oppure http tunnelling. Non occorre aprire alcuna porta per operare con TeamViewer!

Come descritto più avanti nel paragrafo "Crittografia e autenticazione", nemmeno noi, in qualità di operatori dei server di instradamento, possiamo leggere il traffico di dati crittografati.

Crittografia e autenticazione

TeamViewer funziona con una crittografia completa basata sullo scambio di chiave pubblica/privata RSA e con la codifica di sessione AES (256 Bit). Questa tecnologia è utilizzata, in una forma paragonabile, per https/SSL, e può essere considerata completamente sicura secondo gli standard attuali. Poiché la chiave privata non lascia mai il computer client, questa procedura assicura che i computer interconnessi, inclusi i server di instradamento di TeamViewer, non possano decifrare il flusso di dati.

Ciascun client di TeamViewer ha già costruito la chiave pubblica del cluster master, ed è quindi in grado rispettivamente di crittografare i messaggi per il server master e di verificare la firma del master. La PKI (Public Key Infrastructure - infrastruttura a chiave pubblica) previene efficacemente la condizione di "Man-in-the-middle-attacks" (attacchi dell'uomo in mezzo). Nonostante la crittografia, la password non viene mai inviata direttamente, bensì solamente attraverso una procedura di domanda-risposta ed è salvata solamente sul computer locale.



Crittografia e autenticazione di TeamViewer

Convalida degli ID di TeamViewer

Gli ID di TeamViewer sono generati automaticamente dallo stesso TeamViewer, in base a caratteristiche hardware. I server di TeamViewer controllano la validità dell'ID prima di qualsiasi connessione, rendendo così impossibile la generazione e l'utilizzo di ID falsi.

Protezione contro il metodo "forza bruta"

Se i potenziali clienti pongono dei quesiti sulla sicurezza di TeamViewer, di norma questi riguardano la crittografia. Comprensibilmente, i maggiori timori sono costituiti dal rischio che terzi possano riuscire ad entrare nella connessione, oppure che i dati di accesso a TeamViewer siano intercettati. In realtà, gli attacchi più pericolosi sono spesso quelli più semplici.

Nell'ambito della sicurezza dei computer, gli attacchi con il metodo di "brute force" sono rappresentati da frequenti tentativi di indovinare una password di protezione di una risorsa sicura tramite prova ed errore. Con la crescente potenza di calcolo dei computer standard, il tempo richiesto per indovinare anche le password più lunghe si è andato sempre più riducendo.

Come difesa contro il metodo di "brute force", TeamViewer aumenta in modo esponenziale la latenza tra i tentativi di connessione. Per 24 tentativi impiega già 17 ore. La latenza viene azzerata solamente dopo l'inserimento della password corretta.

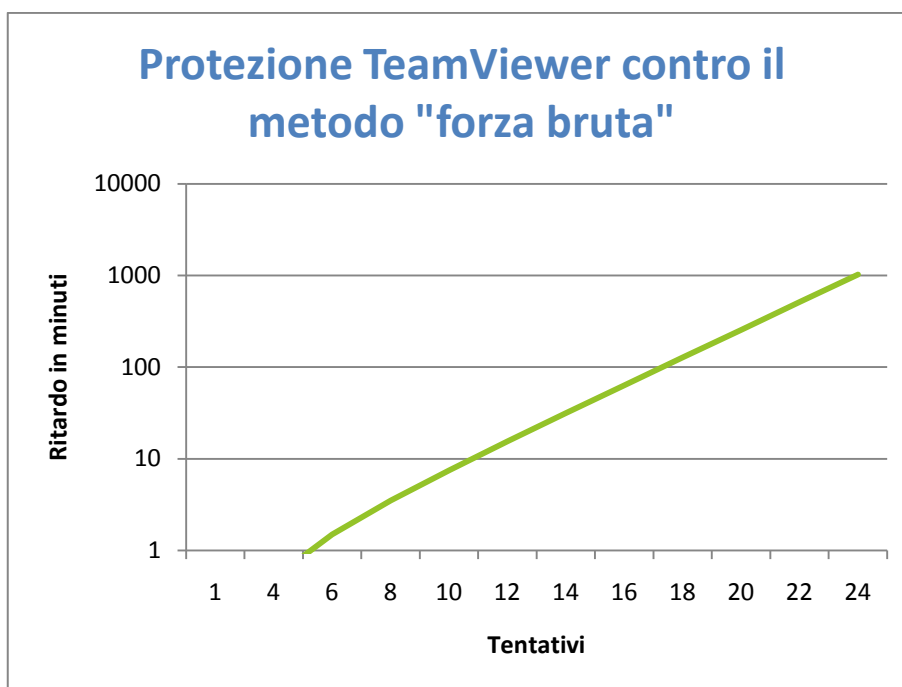


Grafico: Tempo trascorso dopo N tentativi di connessione durante un attacco con il metodo di forza bruta

Firma del codice

Con un'ulteriore funzionalità di sicurezza, tutto il nostro software viene firmato tramite la Firma del Codice di VeriSign. Grazie a questo metodo, l'autore del software può essere sempre identificato in modo affidabile. Se il software viene modificato, la firma digitale diventa, di conseguenza, automaticamente non più valida. Persino i moduli personalizzabili di TeamViewer sono firmati dinamicamente durante la sua generazione.

Data center e backbone

Questi due argomenti riguardano la disponibilità e la sicurezza. Gli server centrale di TeamViewer sono situati in un modernissimo centro dati dotato di connessioni con portante multiplo ridondante e ridondante alimentazione di energia elettrica. Viene utilizzato esclusivamente un hardware di marca (Cisco, Foundry, Juniper).

L'accesso al centro dati è possibile solamente dopo un approfondito controllo d'identità tramite una porta ad entrata singola. Il sistema CCTV, la rilevazione di incursioni, la sorveglianza 24 ore su 24 e 7 giorni su 7, unitamente al personale di sicurezza on-site, proteggono internamente i nostri server dagli attacchi.

Sicurezza dell'applicazione in TeamViewer

Funzione di blacklist e whitelist

Specialmente quando TeamViewer è utilizzato per la manutenzione di computer non presidiati (ad es. TeamViewer è installato come un servizio di Windows), può essere importante, in aggiunta a tutti gli altri meccanismi di sicurezza, vietare l'accesso di determinati client ai computer suddetti.

Con la funzione di whitelist si può specificare esplicitamente quali ID di TeamViewer sono autorizzati ad accedere al computer in questione, mentre con la funzione di blacklist è possibile bloccare determinati ID di TeamViewer.

Nessuna modalità nascosta

Non esiste alcuna funzione che consenta a TeamViewer di funzionare integralmente in background. Anche se l'applicazione sta funzionando come un servizio di Windows in background, TeamViewer è sempre visibile grazie ad un'icona sulla barra di sistema.

Una volta stabilita la connessione, è sempre visibile un piccolo pannello di controllo, situato sopra alla barra di sistema: ciò significa che TeamViewer è deliberatamente non idoneo al monitoraggio nascosto di computer o di dipendenti.

Protezione della password

Per l'assistenza immediata al cliente, TeamViewer (TeamViewer QuickSupport) genera una password di sessione (password monouso). Se il Vostro cliente Vi comunica la sua password, potete collegarvi al computer del cliente inserendone l'ID e password. Dopo un riavvio eseguito da parte del cliente, sarà generata una nuova password di sessione e potrete quindi raggiungere i computer del Vostro cliente solamente se sarete invitati a farlo.

Quando si installa TeamViewer per la teleassistenza di computer non presidiati (ad es. dei server), si configura una password personale fissa che protegge l'accesso a questo computer.

Controllo dell'accesso in entrata e in uscita

Le modalità di connessione di TeamViewer possono essere configurate individualmente. Si può quindi configurare, ad esempio, il proprio computer di teleassistenza o di presentazione in modo da impedire le connessioni in entrata.

Limitare le funzionalità a quelle effettivamente necessarie significa sempre restringere i possibili punti deboli per evitare potenziali attacchi.

Ulteriori domande?

Per qualsiasi ulteriore informazione potete contattarci ai seguenti numeri di telefono: +39 02 89 03 86 48, oppure all'indirizzo e-mail: support@teamviewer.com.

Contatti

TeamViewer GmbH
Kuhnbergstr. 16
D-73037 Göppingen
Germany
service@teamviewer.com

Registro delle Imprese: Ulm HRB 534075