Informații privind securitatea TeamViewer

Grupul țintă

Acest document este pentru administratori de rețele profesioniști. Informațiile din acest document sunt tehnice și foarte detaliate. Pe baza acestor informații, profesioniștii IT vor dobândi o imagine detaliată a standardelor de securitate din cadrul TeamViewer și se vor soluționa orice îngrijorări înainte de a implementa software-ul nostru. Puteți distribui acest document clienților dvs. pentru a oferi informații care să soluționeze orice posibile îngrijorări legate de securitate.

Dacă nu vă considerați a fi parte din grupul țintă, informațiile de bază din secțiunea Compania/Software-ul vă vor ajuta să obțineți o imagine clară privind modul serios în care abordăm securitatea.

Compania/Software-ul

Despre noi

TeamViewer GmbH a fost înființată în 2005 și este bazată în Sudul Germaniei, în Göppingen (în apropiere de Stuttgart), cu filiale în Australia și Statele Unite. Dezvoltăm și comercializăm exclusiv sisteme securizate pentru colaborare pe bază de web. Într-un scurt interval de timp, programul nostru de licențiere de tip Freemium a dus la o dezvoltare rapidă, cu peste 200 de milioane de utilizatori ai software-ului TeamViewer pe mai mult de 1,4 miliarde de dispozitive, în peste 200 de țări din întreaga lume. Software-ul este disponibil în mai mult de 30 de limbi.

Conceptul nostru de securitate

TeamViewer este utilizată de mai mult de 30 de milioane de utilizatori la orice moment al zilei. Acești utilizatori oferă asistență spontană pe internet, accesând computere fără utilizator (de ex. asistență de la distanță pentru servere) și pentru găzduirea de ședințe online. În funcție de configurație, TeamViewer poate fi utilizat pentru a controla de la distanță un alt computer, ca și cum ați sta la acesta. Dacă utilizatorul conectat la un computer la distanță este un administrator de Windows, Mac sau Linux, această persoană va primi drepturi de administrator și pe computerul respectiv.

Este clar că o funcționalitate atât de puternică care acționează în mediul online potențial nesigur trebuie protejată corespunzător împotriva atacurilor. De fapt, subiectul securității domină toate obiectivele noastre de dezvoltare și este ceva ce noi folosim în tot ceea ce facem. Dorim să asigurăm faptul că accesul la computerul dvs. este sigur și să protejăm interesele dvs.: milioane de utilizatori din întreaga lume au încredere numai într-o soluție sigură și numai o soluție sigură asigură succesul nostru pe termen lung ca întreprindere.

Evaluarea de către experți externi

Software-ul nostru, TeamViewer, a primit scorul de cinci stele (valoarea maximă) din partea Asociației Federale de Experți și Evaluatori IT (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.). Evaluatorii independenți ai BISG e.V. inspectează produsele producătorilor calificați pentru calitate, securitate și caracteristicile serviciului.

Referințe

În prezent, TeamViewer este utilizat de peste 200 de milioane de utilizatori. Companii internaționale de top din tot felul de industrii (inclusiv sectoare foarte sensibile precum cel bancar, finanțe, sănătate și administrație publică) utilizează cu succes TeamViewer.

Vă invităm să consultați referințele noastre disponibile peste tot pe internet, pentru a dobândi o primă impresie legată de recepția soluției noastre. Veți afla că probabil cele mai multe societăți aveau cerințe de securitate și disponibiltate similare înainte de a opta - după o examinare detaliată - pentru TeamViewer. Pentru a vă forma propria impresie, aveți detalii tehnice în restul documentului.

Sesiunile TeamViewer

Crearea unei sesiuni și tipuri de conexiuni

La stabilirea unei sesiune, TeamViewer determină tipul de conexiune optim. După efectuarea handshake-ului prin serverele noastre master, se stabilește o conexiune directă prin UDP sau TCP în 70% din toate cazurile (chiar și în spatele gateway-urilor, NAT-uri și paravanelor de protecție standard). Restul conexiunilor sunt rutate prin rețeaua noastră de router foarte redundantă prin TCP sau https-tunnelling. Nu trebuie să deschideți porturi pentru a lucra cu TeamViewer

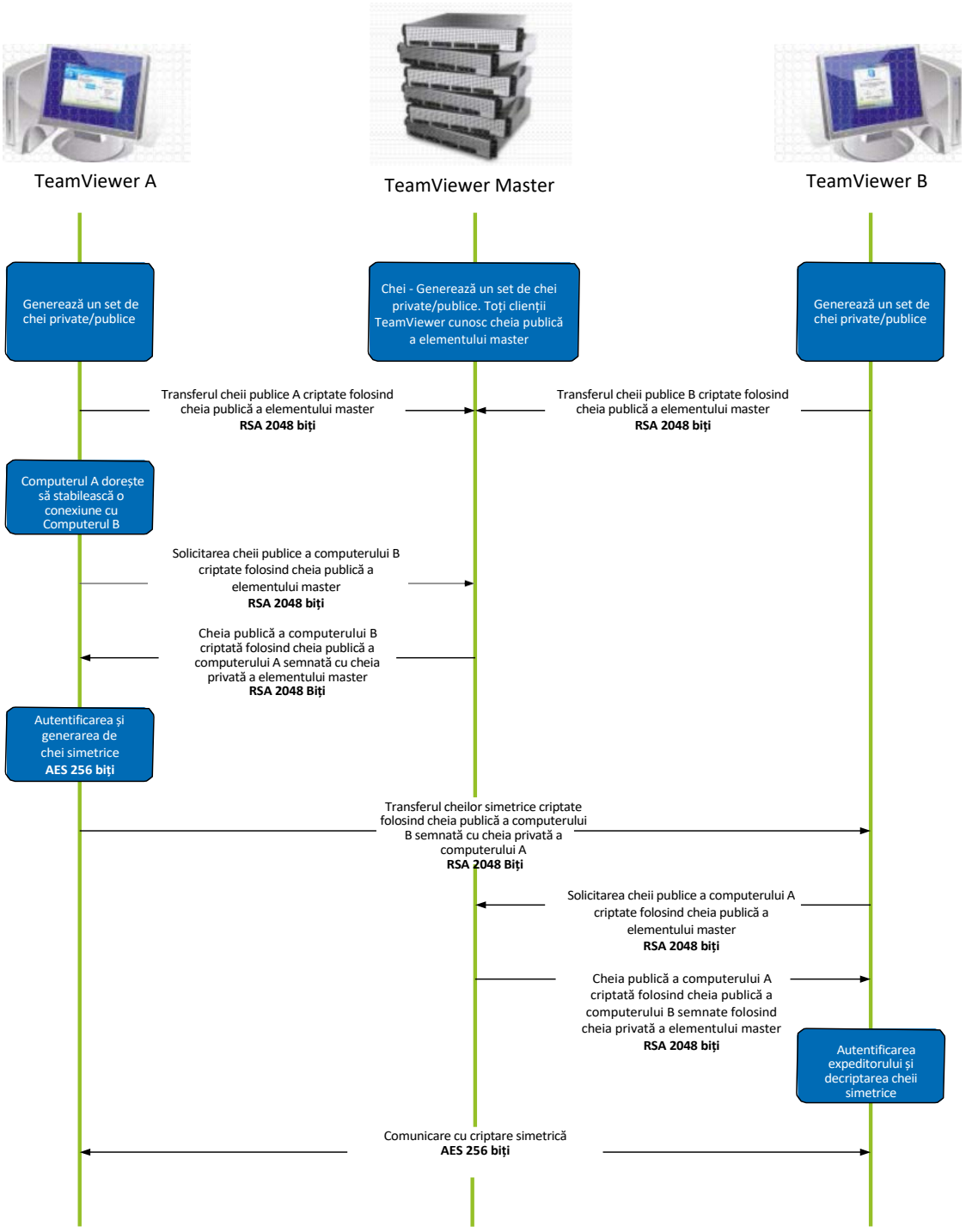
Astfel cum este descris în paragraful Criptarea și autentificarea, nici măcar noi, operatorii serverelor de rutare, nu putem citi traficul de date criptat.

Criptarea și autentificarea

Traficul TeamViewer este securizat folosind interschimbare de chei RSA publice/private și criptare de sesiune AES (256 biți). Această tehnologie este utilizată într-o formă comparabilă pentru http/SSL și este considerată sigură conform normelor actuale. Deoarece cheia privată nu părăsește niciodată computerul client, această procedură asigură faptul că computerele interconectate - inclusiv serverele de rutare TeamViewer - nu pot descifra fluxul de date.

Fiecare client TeamViewer are deja implementată cheia publică a clusterului master și așadar poate cripta mesaje către clusterul master și verificat mesaje semnate de acesta. PKI-ul (Infrastructura pentru chei publice) împiedică în mod eficientă atacurile de tipul man-in-the-middle. În ciuda criptării, parola nu este trimisă niciodată în mod direct, ci numai printr-o procedură interogare-răspuns și este salvată numai pe computerul local.

În timpul autentificării, parola nu este transferată niciodată în mod direct deoarece se utilizează protocolul Secure Remote Password (SRP). Numai un verificator de parolă este stocat pe computerul local.



Criptarea și autentificarea TeamViewer

Validarea ID-urilor TeamViewer

ID-urile TeamViewer sunt bazate pe diferite caracteristici hardware și software și sunt generate în mod automat de TeamViewer. Serverele TeamViewer verifică validitatea acestor ID-uri înainte de fiecare conexiune.

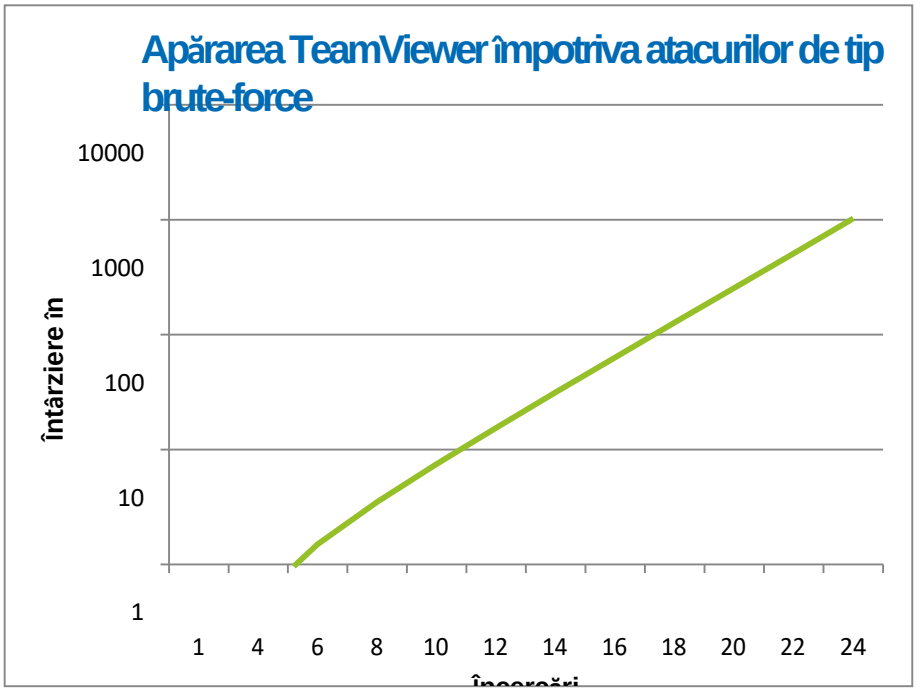
Protecție brute-force

Clienții potențiali care pun întrebări privind securitatea TeamViewer întreabă de obicei despre criptare. Evident, riscul că o parte terță ar putea monitoriza conexiunea sua că datele de acces la TeamViewer sunt urmărite reprezintă temerile cele mai mari. Cu toate acestea, realitatea este că aceste atacuri relativ primitive sunt adeseori cele mai periculoase.

În contextul securității computerelor, un atac de tip brute-force este o metodă de încercare repetată de a ghici o parolă care protejează o resursă. Datorită puterii de calcul tot mai mare a computerelor standard, timpul necesar pentru ghicirea parolelor lungi a fost redus tot mai mult.

Ca apărare împotriva atacurilor de tip brute-force, TeamViewer mărește exponențial întârzierea dintre încercările de conectare. Așadar, pentru 24 de încercări pot fi necesare până și 17 ore. Timpul de așteptare este resetat numai după introducerea cu succes a parolei corecte.

TeamViewer are implementat un mecanism pentru a-și proteja clienții împotriva atacurilor provenite de la un singur computer sau de la mai multe computere, atacuri numite atacuri de tip botnet, care încearcă să acceseze un ID TeamViewer specific.



Diagramă: Timp parcurs după n încercări de conectare în timpul unui atac de tip brute force

Semnarea codului

Ca funcție de securitate suplimentară, toate aplicațiile noastre software sunt semnate prin Semnare de cod VeriSign. Astfel, partea care a publicat software-ul este întotdeauna identificabilă. Dacă software-ul a fost modificat ulterior, semnătura digitală devine în mod automat nevalidă.

Centrele de date și elementele de susținere

Pentru a furniza cea mai bună securitate și disponibilitate posibilă a serviciilor TeamViewer, toate serverele TeamViewer sunt situate în centre de date care sunt în conformitate cu ISO 27001 și care gestionează conexiuni purtătoare cu redundanță multiplă și surse de alimentare redundante. De asemenea, se utilizează numai componente hardware de mărci de la nivelul actual al tehnologiei. Suplimentar, toate serverele care stochează date sensibile sunt situate în Germania sau Austria.

Certificarea ISO 27001 înseamnă că măsuri precum controlul accesului, supraveghere prin camere video, detectoare de mișcare, monitorizare non-stop și personal de securitate la fața locului asigură faptul că accesul la centrul de date este acordat numai persoanelor autorizate și garantează cea mai bună securitate posibilă pentru componente hardware și date. De asemenea, există o verificare detaliată a identității la singurul punct de intrare al centrului de date.

Contul TeamViewer

Conturile TeamViewer sunt găzduite pe servere TeamViewer dedicate. Pentru informații privind controlul accesului, consultați secțiunea Centrele de date și elementele de susținere de mai sus. Pentru autorizarea și criptarea parolei se utilizează protocolul Secure Remote Password (SRP), un protocol de acord de cheie autentificat prin parolă (PAKE) augmentat. O persoană infiltrată sau un intermediar nu poate obține informații suficiente pentru a putea ghici prin metode brute-force o parolă. Acest lucru înseamnă că se poate obține securitate semnificativă chiar și folosind parole simple. Date sensibile din contul TeamViewer, de exemplu informații de autentificare la stocarea pe cloud, sunt stocate prin criptare AES/RSA pe 2048 biți.

Management Console

TeamViewer Management Console este o platformă bazată pe web pentru managementul utilizatorilor, raportarea conexiunilor și gestionarea Computerelor și contactelor. Aceasta este găzduită în centre de date cu certificare ISO-27001 și în conformitate cu HIPAA. Toate transferurile de date sunt printr-un canal securizat care utilizează criptare TSL (Transport Security Layer), standardul pentru conexiuni de rețele de internet securizate. Datele sensibile sunt stocate suplimentare prin criptare AES/RSA pe 2048 biți. Pentru autorizarea și criptarea parolei, se utilizează Secure Remote Password protocol (SRP). SRP este o metodă bine stabilită, robustă, securizată pe bază de parolă, de autentificare și interschimbare de chei folosind un modul pe 2048 biți.

Setări bazate pe politici

Din TeamViewer Management Console, utilizatorii pot defini, distribui și implementa politici de setări pentru instalările de software TeamViewer pe dispozitive care aparțin în mod specific lor. Politicile de setări sunt

semnate digital de contul care le-a generat. Acest lucru asigură faptul că singurul cont care poate aloca o politică unui dispozitiv este contul la care aparține dispozitivul.

Securitatea aplicațiiilor în TeamViewer

Listă de elemente interzise și listă de elemente permise

În mod deosebit, dacă TeamViewer este utilizat pentru menținerea de computere fără utilizator (cu alte cuvinte, TeamViewer este instalat ca serviciu Windows), poate fi de interes opțiunea de securitate suplimentară de restricționare a accesului la aceste computere la un număr de clienți specifici.

Cu funcția de listă de elemente permise puteți indica în mod explicit care ID-uri TeamViewer și/sau conturi TeamViewer pot accesa un computer. Cu funcția de listă de elemente interzise, puteți bloca anumite ID-uri TeamViewer și conturi TeamViewer. O listă centrală de elemente permise este disponibilă ca parte din „setările bazate pe politici" descrise mai sus în secțiunea „Management Console."

Criptare chat și video

Istoricurile de chat sunt asociate contului dvs. TeamViewer și sunt așadar criptate și stocate folosind aceeași securitate de criptare AES/RSA pe 2048 biți descrisă în secțiunea Contul TeamViewer. Toate mesajele de chat și traficul video sunt criptate de la capăt la capăt folosind criptare prin sesiune AER (256 biți).

Nu există mod Stealth

Nu există o funcție care să vă permită să rulați TeamViewer complet în fundal. Chiar dacă aplicația rulează ca serviciu Windows în fundal, TeamViewer este întotdeauna vizibilă prin intermediul unei pictograme din bara de sistem.

Întotdeauna după stabilirea unei conexiuni este vizibil un panou de control mic deasupra barei de sistem. Așadar, TeamViewer este în mod intenționat nepotrivită pentru monitorizarea pe ascuns a computerelor sau a angajaților.

Protejarea parolelor

Pentru asistență spontană pentru clienți, TeamViewer (TeamViewer QuickSupport) generează o parolă de sesiune (o parolă care expiră după o singură utilizare). Dacă aflați parola de la clientul dvs., puteți să vă conectați la computerul acestuia introducând ID-ul și parola sa. După o repornire a TeamViewer pe partea clientului, se va genera o nouă parolă de sesiune astfel încât să vă puteți conecta la computerele clientului dvs. numai dacă sunteți invitați să efectuați acest lucru.

La implementarea TeamViewer pentru asistență de la distanță fără utilizator (de ex. pentru servere), setați o parolă individuală, fixă, care securizează accesul la computer.

Controlul accesului de intrare și ieșire

Puteți configura individual modurile de conectare ale TeamViewer. De exemplu, puteți configura computerul de asistență la distanță sau computerul de ședință astfel încât să nu fie posibile conexiuni de intrare.

Limitarea funcționalității la funcțiile necesare cu adevărat înseamnă întotdeauna limitarea punctelor slabe posibile pentru potențiale atacuri.

Autentificarea pe două niveluri

TeamViewer asistă societățile cu cerințele de conformitate legate de HIPAA și PCI. Autentificarea pe două niveluri adaugă un strat de securitate suplimentar pentru protejarea conturilor TeamViewer împotriva accesului neautorizat.

Pe lângă numele de utilizator și parolă, utilizatorul trebuie să introducă un cod pentru a se autentifica. Acest cod este generat prin algoritmul time-based one-time password (TOTP). Așadar codul este valid numai o scurtă perioadă de timp.

Prin autentificarea pe două niveluri și limitarea accesului prin funcția de listă cu elemente aprobate, TeamViewer asistă la îndeplinirea tuturor criteriilor necesare pentru certificarea HIPAA și PCI.

Testarea securității

Atât infrastructura TeamViewer cât și software-ul TeamViewer sunt supuse unor testări de penetrare în mod regulat. Testările sunt efectuate de societăți independente, specializate pe testarea securității.

Aveți întrebări suplimentare?

Pentru întrebări sau informații suplimentare, contactați-ne la (SUA) +1 (800) 951 4573 și (Regatul Unit) +44 (0) 2080 997 265 sau trimiteți-ne e-mail la support@teamviewer.com.

Contact

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