TeamViewer säkerhetsinformation

Målgrupp

Detta dokument riktar sig till professionella nätverksadministratörer. Informationen i detta dokument är relativt teknisk och mycket detaljerad. Baserat på denna information, får IT-specialister en detaljerad bild av TeamViewers säkerhetsstandard och all frågor kan redas ut innan vår programvara används. Tveka inte att distribuera detta dokument till dina kunder för att klargöra eventuella säkerhetsfrågor.

Om du inte anser dig tillhöra målgruppen så kommer mjuka fakta i delen Företaget / programvaran ändå att hjälpa dig att få en klar överblick över hur vi tar säkerheten på allvar.

Företaget / programvaran

Om oss

TeamViewer GmbH grundades 2005 och är baserat i södra Tyskland, i staden Göppingen (nära Stuttgart), med dotterbolag i Australien och i USA. Vi utvecklar och säljer uteslutande säkra system för webbaserat samarbete. Inom en kort tidsperiod har vår Freemium-licensiering lett till snabb tillväxt, med mer än 200 miljoner användare av programvaran TeamViewer på mer än 1,4 miljarder enheter, i mer än 200 länder runt om i världen. Programvaran finns tillgänglig på mer än 30 språk.

Säkerhet enligt oss

TeamViewer används av mer än 30 miljoner användare vid varje given tidpunkt, vilken dag som helst. Dessa användare tillhandahåller spontan support över internet genom åtkomst till obevakade datorer (dvs fjärrsupport för servrar) och är värdar för online-möten. Beroende på konfigurationen kan TeamViewer användas för att fjärrstyra en annan dator, som om du satt direkt framför den. Om användaren som är inloggad på en fjärrdator är en Windows-, Mac- eller Linux-administratör så kommer den här personen att beviljas administratörsrättigheter på den datorn också.

Självklart måste en sådan kraftfull funktionalitet över det potentiellt osäkra internet, skyddas mot angrepp med stor noggrannhet. Säkerhet är de facto ämnet som dominerar alla våra utvecklingsmål och är någonting vi alltid har i tankarna, vad vi än gör. Vi vill säkerställa att tillgången till din dator är säker, och även skydda våra egna intressen. Miljontals användare världen över litar endast på säkra lösningar, och endast en säker lösning försäkrar långsiktig framgång för oss som företag.

Utvärdering av extern expert

Vår programvara, TeamViewer, har tilldelats en femstjärnig kvalitetsstämpel (högsta betyg) av Federal Association of IT Experts and Reviwers (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.). De oberoende granskarna från BISG e.V. kontrollerar produkter från kvalificerade producenter i avseende på kvalitet, säkerhet och serviceegenskaper.

Referenser

För närvarande används TeamViewer av mer än 200 miljoner användare. Internationella toppföretag från alla typer av branscher (däribland så känsliga sektorer som banksektorn, finanssektorn, hälsovårdssektorn och myndigheter) använder framgångsrikt TeamViewer.

Vi inbjuder dig att ta en titt på våra referenser som finns över hela internet, för att få ett första intryck av godkännandet av vår lösning. Du kommer förmodligen att upptäcka att de flesta andra företag hade liknande säkerhets- och tillgänglighetskrav innan de - efter intensiv efterforskning - slutligen bestämde sig för TeamViewer. Titta dock igenom den tekniska informationen i resten av det här dokumentet för att bilda dig en egen uppfattning.

TeamViewer-sessioner

Att skapa en session och typer av anslutningar

Vid upprättandet av en session avgör TeamViewer den optimala typen av anslutning. Efter handskakningen genom våra huvudservrar, etableras i 70% av alla fall en direktanslutning via UDP eller TCP (även bakom standardgateways, NAT-routrar och brandväggar). Resten av anslutningarna dirigeras genom vårt mycket redundanta routernätverk via TCP eller https-tunnlar. Du behöver inte öppna några portar för att arbeta med TeamViewer

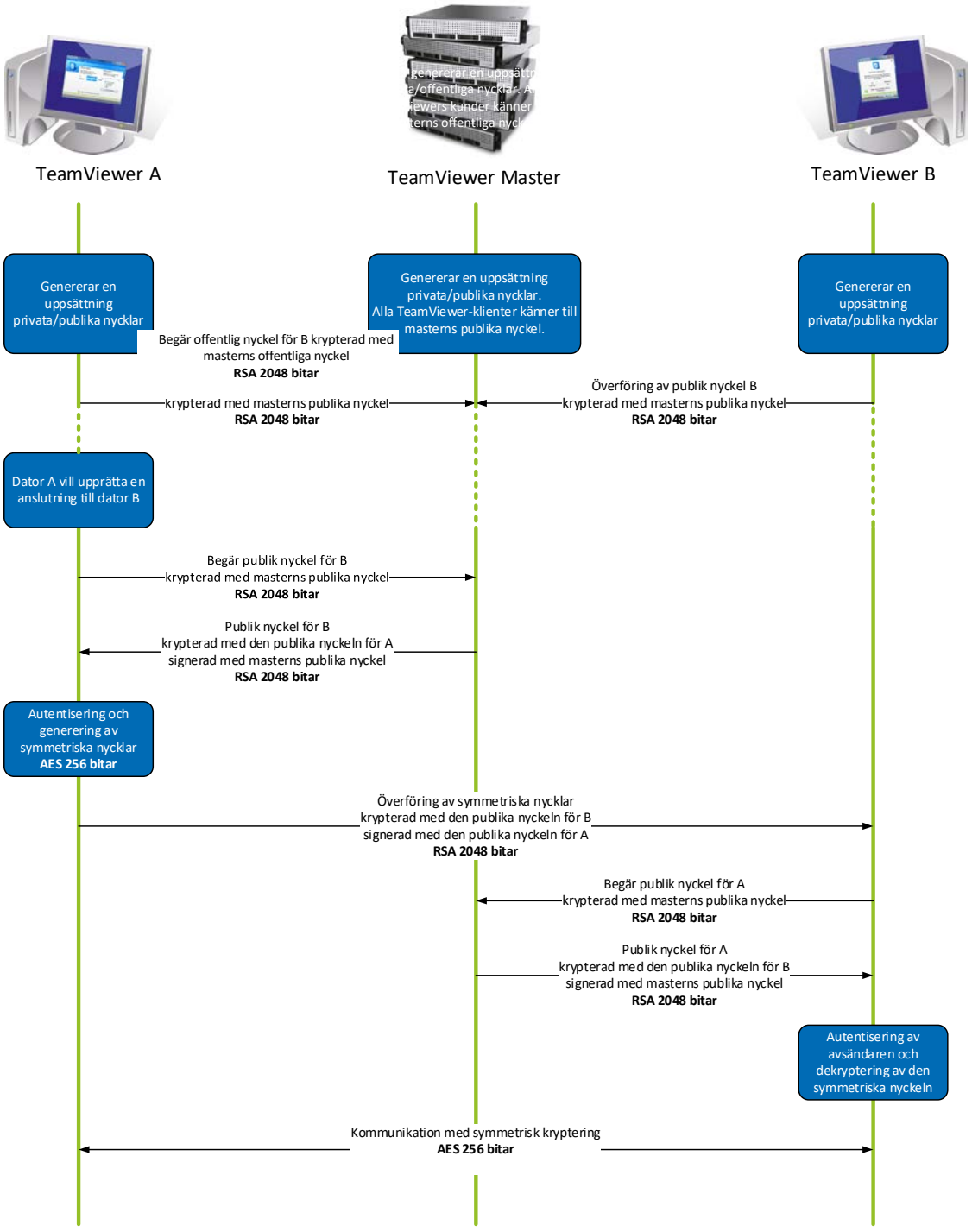
Som senare beskrivs i paragrafen ”Kryptering och autentisering”, kan inte ens vi, som tillhandahåller routingservrarna, läsa den krypterade datatrafiken.

Kryptering och autentisering

TeamViewers trafik säkras genom användning av offentligt/privat nyckelutbyte RSA och sessionskryptering AES (256 bitars). Den här tekniken används i en jämförbar form för https/SSL och betraktas som helt säker enligt dagens standard. Eftersom den privata nyckeln aldrig lämnar kundens dator, säkerställer den här proceduren att anslutna datorer - inklusive TeamViewers routingservrar - inte kan dechiffrera dataflödet.

Varje TeamViewer-kund har redan implementerat mastergruppens offentliga nyckel och kan därför kryptera meddelanden till mastergruppen och kontrollera meddelanden som den har signerat. PKI (Public Key Infrastructure) förebygger effektivt man-i-mitten-attacker. Trots krypteringen, skickas lösenordet aldrig direkt, utan bara genom ett förfarande med kontrollfrågor och svar, och sparas endast på den lokala datorn.

Under autentisering överförs lösenordet aldrig direkt eftersom protokollet Secure Remote Password (SRP) används. Endast en lösenordsverifierare lagras på den lokala datorn.



TeamViewer kryptering och autentisering

Validering av TeamViewer-ID:n

TeamViewer-ID:n är baserade på olika hård- och programvaruegenskaper och genereras automatiskt av TeamViewer. TeamViewers servrar kontrollerar giltigheten av dessa ID:n innan varje anslutning.

Brute force-skydd

Potentiella kunder som frågar om TeamViewers säkerhet frågar ofta om kryptering. Det är förståeligt att risken för att en tredje part kan övervaka anslutningen eller att TeamViewers åtkomstdata avlyssnas, är vad de är mest rädda för. I verkligheten är dock relativt primitiva attacker ofta de farligaste.

I datasäkerhetssammanhang är en brute-force-attack en trial-and-error-metod för att gissa ett lösenord som skyddar en resurs. I och med standarddatorernas ökade datorkraft, har den tid som behövs för att gissa långa lösenord, minskats allt mer.

Som ett försvar mot brute force-attacker ökar TeamViewer exponentiellt fördröjningen mellan anslutningsförsöken. 24 försök kan därför ta upp till 17 timmar. Latensen återställs endast efter att korrekt lösenord anges.

TeamViewer har inte bara en mekanism för att skydda sina kunder från attacker från en specifik dator utan också från flera datorer, kända som botnet-attacker, som försöker komma åt ett visst TeamViewer-ID.

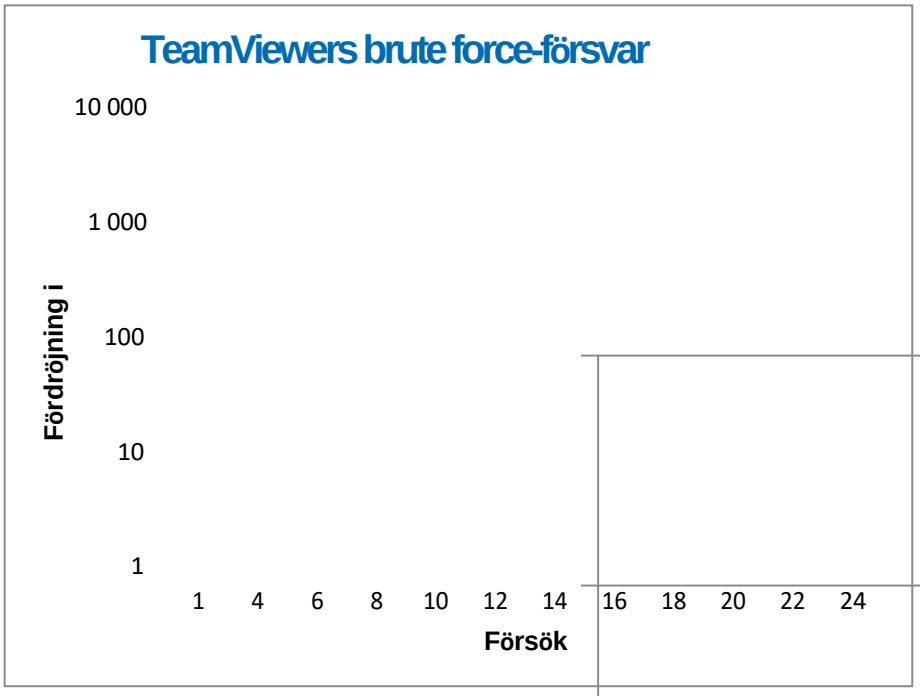


Diagram: Tid som förflutit efter n anslutningsförsök under en brute force-attack

Kodsignering

Som en extra säkerhetsfunktion är all vår programvara signerad via VeriSign-kodsignering. På detta sätt är utgivaren av programvaran alltid lätt att identifiera. Om programvaran har ändrats i efterhand blir den digitala signaturen automatiskt ogiltig.

Datacenter & stamnät

För att kunna erbjuda TeamViewers tjänster till bästa möjliga säkerhet och tillgänglighet är alla TeamViewers servrar lokaliserade i ISO 27001-certifierade datacenter och utnyttjar flerredundanta operatörsförbindelser och redundant strömförsörjning. Därtill används endast toppmoderna hårdvarumärken. Dessutom ligger alla servrar som lagrar känslig data, i Tyskland eller Österrike.

Att vara ISO 27001-certifierad innebär personlig åtkomstkontroll, videoövervakning, rörelsedetektorer, övervakning dygnet runt och säkerhetspersonal på plats som säkerställer att tillgång till datacentret endast beviljas auktoriserade personer och garanterar bästa möjliga säkerhet för hårdvara och data. Det sker även en noggrann identifieringskontroll vid data centrets enda ingång.

TeamViewer-konto

TeamViewer-konton finns på särskilda TeamViewer-servrar. För information angående åtkomstkontroll, var god se Datacenter & stamnät ovan. För auktorisering och lösenordskryptering används SRP-protokoll (Secure Remote Password), ett förbättratpassword-authenticated key agreement, ett så kallat PAKE-protokoll. En infiltratör eller man-i-mitten-attack kan inte komma åt tillräckligt mycket information för att kunna brute force-gissa ett lösenord. Detta betyder att hög säkerhet även kan uppnås vid användning av svaga lösenord. Känslig data inom TeamViewer-kontot, till exempel inloggningsinformation till molnlagring, lagras med AES/RSA 2048 bitars kryptering.

Systemhanteringskontroll

TeamViewers systemhanteringskontroll är en webbaserad plattform för användarhantering, anslutningsrapportering och hantering av datorer och kontakter. Den drivs från ISO-27001 certifierade, HIPAA-kompatibla datacentra. All dataöverföring sker genom en säker kanal med TSL (Transport Security Layer) kryptering, standarden för säkra nätverksanslutningar på internet. Känslig data lagras dessutom med AES/RSA 2048 bitars kryptering. För auktorisering och lösenordskryptering används SRP (Secure Remote Password) protokoll. SRP är en väletablerad, robust och säker metod för lösenordsbaserad autentisering och nyckelutbyte, som använder 2048 bitars modul.

Policybaserade inställningar

Inifrån TeamViewers systemhanteringskontroll kan användare definiera, distribuera och genomdriva inställningspolicyer för TeamViewers mjukvaruinstalleringar på enheter som specifikt tillhör dem. Inställningspolicyer signeras digitalt av det konto som genererade dem. Detta säkerställer att det enda kontot som tillåts tilldela en enhet en policy är det konto enheten tillhör.

Programsäkerhet i TeamViewer

Svartlista och vitlista

I synnerhet om TeamViewer används för att underhålla obemannade datorer (dvs. om TeamViewer är installerad som en Windows-tjänst), så kan det vara ett intressant säkerhetsalternativ att endast ge ett antal specifika kunder tillgång till dessa datorer.

Med vitlistefunktionen kan du uttryckligen ange vilka TeamViewer-ID:n och/eller TeamViewer-konton som får tillgång till en dator. Med svartlistefunktionen kan du blockera vissa TeamViewer-ID:n och TeamViewer-konton. En central vitlista finns tillgänglig som en del av de ”policybaserade inställningar” som beskrivs ovan under ”Systemhanteringskontroll”.

Chatt- och videokryptering

Chatthistorik associeras med ditt TeamViewer-konto och krypteras därför och lagras genom att använda samma AES/RSA-2048 bitars säkerhetskryptering som beskrivs under rubriken ”TeamViewer-konto”. Alla chattmeddelanden och all videotrafik är end-to-end krypterad med AES (256 bitars) sessionskryptering.

Inget dolt läge

Det finns ingen funktion som låter dig köra TeamViewer helt i bakgrunden. Även om programmet körs som en Windows-tjänst i bakgrunden, så är TeamViewer alltid synligt som en ikon i systemfältet.

När en anslutning har etablerats finns det alltid en liten kontrollpanel synlig ovanför systemfältet. Därför är TeamViewer med avsikt olämpligt för att i hemlighet övervaka datorer eller anställda.

Lösenordsskydd

För spontan kundsupport genererar TeamViewer (TeamViewer QuickSupport) ett sessionslösenord (engångslösenord). Om din kund ger dig sitt lösenord så kan du ansluta till kundens dator genom att ange kundens ID och lösenord. Efter en omstart av TeamViewer på kundens sida så genereras ett nytt sessionslösenord så att du endast kan ansluta till din kunds dator om du blir inbjuden att göra det.

När du använder TeamViewer för obevakad fjärrsupport (t.ex. av servrar) ställer du in ett individuellt, fast lösenord som säkrar tillgång till datorn.

Inkommande och utgående tillgångskontroll

Du kan konfigurera TeamViewers anslutningslägen individuellt. Du kan exempelvis konfigurera din dator för fjärrsupport eller möten på så sätt att inga inkommande anslutningar är möjliga.

Att begränsa funktionaliteten till de funktioner som faktiskt behövs betyder att man begränsar möjliga svaga punkter för potentiella attacker.

Tvåfaktorautentisering

TeamViewer hjälper företag att möta HIPAA- och PCI-krav. Tvåfaktorautentisering ger ett extra säkerhetslager för att skydda TeamViewer-konton från obehörig åtkomst.

Utöver både användarnamn och lösenord måste användaren ange en kod för autentisering. Denna kod genereras via algoritmen TOTP för tidsbaserade engångslösenord. Därför är koden endast giltig under en kort tidsperiod.

Tvåfaktorsautentisering och begränsande tillgång genom vitlistning hjälper TeamViewer att uppfylla alla nödvändiga kriterier för HIPAA och PCI-certifiering.

Säkerhetstestning

Både TeamViewers infrastruktur och TeamViewers programvara utsätts regelbundet för penetrationstester. Testen utförs av oberoende företag, specialiserade på säkerhetstestning.

Övriga frågor?

För övriga frågor eller information kontakta oss gärna på 08 52 507 085 eller skicka ett e-postmeddelande till support@teamviewer.com.

Kontakt

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