TeamViewer sikkerhedsinformation

Målgruppe

Dette dokument henvender sig til professionelle netværksadministratorer. Oplysningerne i dokumentet er relativt tekniske og meget detaljerede. Ud fra oplysningerne vil man som IT-professionel få et detaljeret billede af sikkerhedsstandarderne hos TeamViewer, og alle bekymringer vil være afklaret, inden man tager vores software i brug. Du er velkommen til at dele dokumentet med dine kunder, så eventuelle bekymringer vedrørende sikkerheden kan imødegås.

Hvis du ikke mener, du er i målgruppen, kan du stadig få hjælp fra vores "soft facts" i afsnittet "Virksomheden / softwaren", hvor du kan få et klart indtryk af, hvordan vi tager sikkerheden alvorligt.

Virksomheden / softwaren

Om os

TeamViewer GmbH er grundlagt i 2005 og har hjemme i det sydlige Tyskland i byen Göppingen (tæt ved Stuttgart) med repræsentationer i Australien og USA. Vi udvikler og sælger sikkerhedssystemer til webbaseret samarbejde. I løbet af ganske kort tid har vores Freemium-licensmodel givet en kraftig vækst – med mere end 200 millioner brugere af TeamViewer-softwaren på mere end 1,4 milliarder enheder i mere end 200 lande rundt omkring i verden. Softwaren findes på mere end 30 sprog.

Vores tilgang til sikkerhed

TeamViewer anvendes af mere end 30 millioner brugere på et givent tidspunkt på en hvilken som helst dag. Disse brugere leverer spontan support over internettet – via adgang til computere uden opsyn (dvs. fjernsupport til servere) og i form af online-møder. Afhængigt af konfigurationen kan TeamViewer anvendes til fjernstyring af en anden computer – som om man sad direkte foran den. Hvis brugeren, der er logget på en fjerncomputer, er en Windows-, Mac- eller Linux-administrator, vil denne person have administratorrettigheder også på denne computer.

Det er klart, at en så magtfuld funktionalitet via det potentielt usikre internet skal beskyttes omhyggeligt mod angreb. Og temaet sikkerhed er faktisk dominerende i alle vores udviklingsmål, og det er noget, vi lever og ånder for i alt, hvad vi gør.Vi ønsker at sikre, at adgangen til din computer er sikker samt at beskytte vores egne interesser: Millioner af brugere verden over har kun tillid til en sikker løsning, og kun en sikker løsning giver os forretningsmæssig succes på den lange bane.

Ekstern ekspertbedømmelse

Vores software, TeamViewer, har fået fem kvalitetsstjerner (det højest mulige antal) af den tyske sammenslutning af IT-eksperter og -bedømmere (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.). De uafhængige bedømmere i BISG e.V. vurderer produkter fra kvalificerede producenter i forhold til deres kvalitet, sikkerhed og serviceegenskaber.

Referencer

TeamViewer har i dag mere end 200 millioner brugere. Internationale toporganisationer fra alle brancher (inkl. de meget følsomme såsom bank-, finans- og sundhedssektoren og myndigheder) anvender TeamViewer med succes.

Tag gerne et kig på vores referencer rundt omkring på internettet, så du kan danne dig et billede af, hvordan vores løsninger anvendes. Du vil opdage, at formentlig de fleste andre virksomheder havde lignende sikkerheds- og tilgængelighedskrav, inden de – efter intensive undersøgelser – endelig besluttede sig for TeamViewer. Resten af dokumentet indeholder tekniske detaljer, der kan bidrage til dit indtryk af løsningerne.

TeamViewer-sessions

At oprette en session og typer af forbindelser

Under etableringen af en session afgør TeamViewer, hvilken type forbindelse der er den mest optimale. Efter et handshake via vores master-servere etableres en direkte forbindelse via UDP eller TCP i 70 % af tilfældene (endda efter standardgateways, NAT's og firewalls). Resten af forbindelserne dirigeres gennem vores højredundante routernetværk via TCP eller https-tunnellering. Du behøver ikke åbne nogen porte for at arbejde med TeamViewer

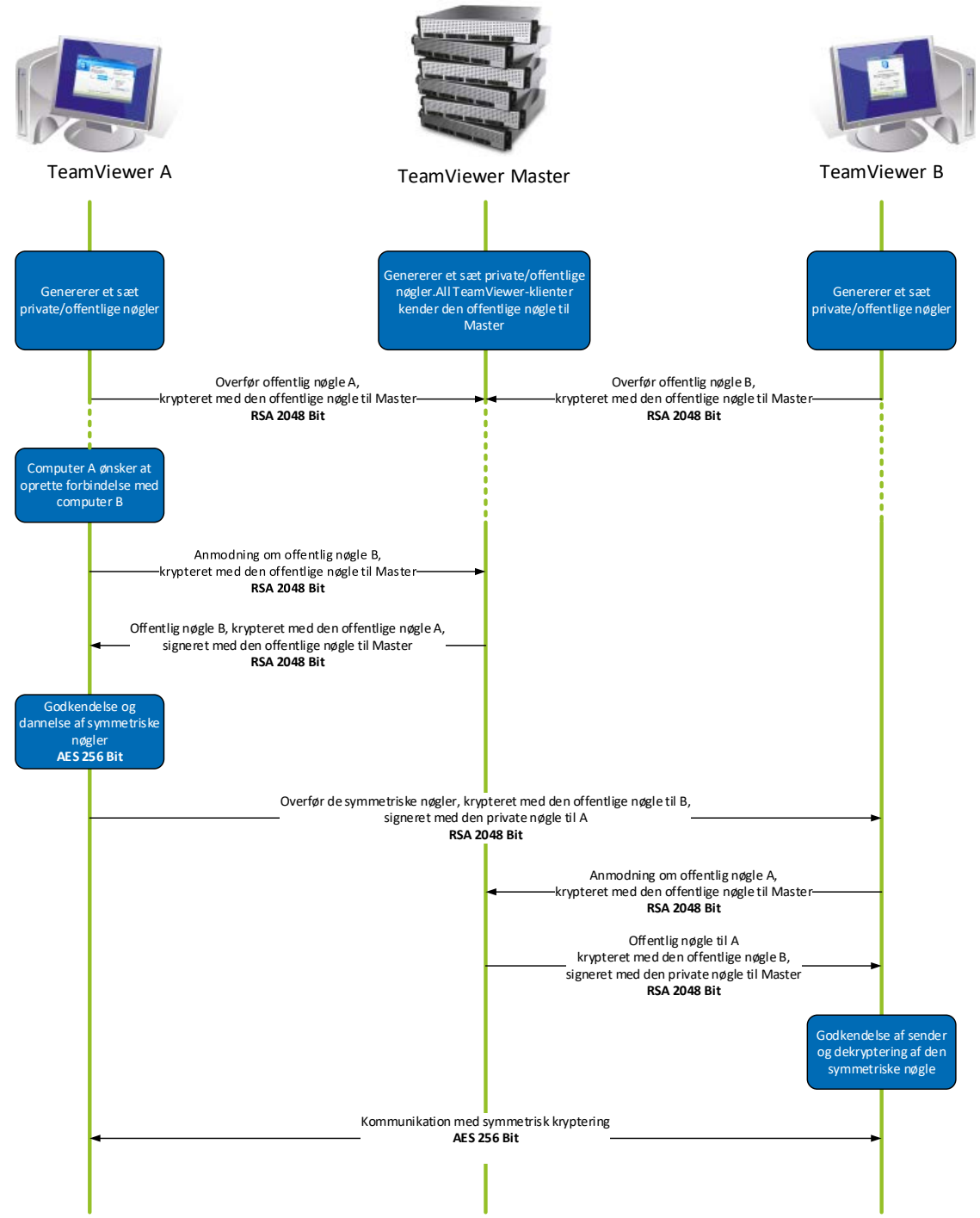
Som det beskrives senere under Kryptering og autentificering, kan ikke engang vi, operatørerne bag de dirigerende servere, læse den krypterede datatrafik.

Kryptering og autentificering

TeamViewer-trafik sikres ved hjælp af RSA offentlig/privat nøgleudveksling og AES (256 bit) sessions-kryptering. Denne teknologi anvendes på lignende vis til http/SSL og anses som værende fuldstændig sikker ud fra dagens standarder. Eftersom den private nøgle aldrig forlader klient-computeren, sikrer denne procedure, at indbyrdes forbundne computere, inkl. de TeamViewer-dirigerende servere, ikke kan dechifrere datastrømmen.

Hver TeamViewer-klient har allerede implementeret den offentlige nøgle fra master clusteren, og vedkommende kan dermed kryptere beskeder til master clusteren og kontrollere beskeder signeret af denne. PKI'en (Public Key Infrastructure) forhindrer effektivt man-in-the-middle-angreb. Trods krypteringen sendes passwordet aldrig direkte men derimod via en challenge-response-procedure, og den gemmes kun på den lokale computer.

I løbet af autentificeringen overføres passwordet aldrig direkte, fordi Secure Remote Password (SRP) protokollen anvendes. Der gemmes kun en password-verifier på den lokale computer.



TeamViewer-kryptering og autentificering

Validering af TeamViewer-ID'er

TeamViewer-ID'er er baseret på forskellige hardware- og software-egenskaber og genereres automatisk af TeamViewer. TeamViewer-serverne kontrollerer validiteten af disse ID'er inden alle forbindelser.

Brute-force-beskyttelse

Potentielle kunder, der spørger ind til sikkerheden ved TeamViewer, nævner ofte kryptering. Det er forståeligt nok, og den største frygt er risikoen for, at tredjepart kan overvåge forbindelsen, eller at TeamViewer-adgangsoplysningerne aflures. Men i virkeligheden er det ofte de relativt primitive angreb, der er de mest farlige.

I forbindelse med computersikkerhed findes de såkaldte brute-force-angreb, hvor et password forsøges afluret ved at prøve sig frem. Med den voksende computerkraft i standardcomputere i dag er den tid, det tager at gætte lange passwords, blevet reduceret markant.

Som et forsvar mod brute-force-angreb øger TeamViewer forsinkelsen mellem forbindelsesforsøgene eksponentielt. Det tager således intet mindre end 17 timer at foretage 24 forsøg. Ventetiden nulstilles først, når det korrekte password er afgivet.

TeamViewer har ikke alene en mekanisme til at beskytte kunderne mod angreb fra en specifik computer, men også fra flere computere, kendt som "botnet"-angreb, der forsøger at opnå adgang til en specifik TeamViewer-ID.

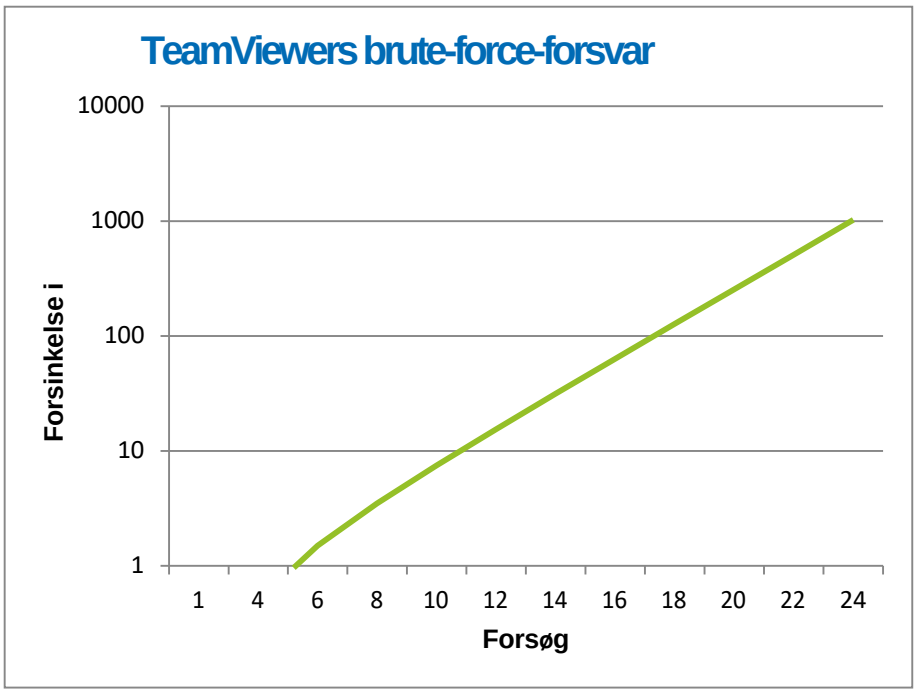


Diagram: Tid gået efter n forbindelsesforsøg under et brute-force-angreb

Kodesignering

Som en ekstra sikkerhedsfeature signeres al vores software ved hjælp af VeriSign Code Signing. På den måde er det altid nemt at identificere softwarens udgiver. Hvis softwaren er blevet ændret efterfølgende, bliver den digitale signatur automatisk ugyldig.

Datacentre & backbone

For at levere den bedst mulige sikkerhed og tilgængelighed for TeamViewers services er alle TeamViewer-servere placeret i datacentre, der overholder ISO 27001 og benytter sig af multiredundante carrier-forbindelser og redundante strømforsyninger. Desuden er det kun state-of-the-art-hardware fra anerkendte leverandører, der anvendes. Og alle servere med følsomme data er placeret i Tyskland eller Østrig.

ISO 27001-certifikatet indebærer personlig adgangskontrol, videokameraovervågning, bevægelsesdetektorer, 24/7-overvågning og sikkerhedspersonale på stedet, ligesom der kun gives adgang til datacenteret til autoriserede personer – det er en garant for den højest mulige sikkerhed for hardware og data. Der er også et udførligt ID-tjek ved hvert eneste adgangspunkt til datacenteret.

TeamViewer-konti

TeamViewer-konti hostes på særlige TeamViewer-servere. Information om adgangskontrol findes i afsnittet "Datacenter & backbone" ovenfor. Der anvendes en Secure Remote Password-protokol (SRP) – en forstærket password-key-agreement protocol (PAKE) – til autentificeringen og password-krypteringen. En infiltrator eller "man in the middle" kan ikke indhente tilstrækkelig information til at brute-force-gætte et password. Det vil sige, at høj sikkerhed kan opnås selv med svage passwords. Følsomme data på TeamViewer-kontoen, for eksempel cloud-gemte login-informationer, er gemt med AES/RSA 2048 bit-kryptering.

Management Console

TeamViewers Management Console er en webbaseret platform til brugerstyring, forbindelsesrapportering og styring af computere og kontakter. Den hostes i datacentre, der er ISO-27001-certificerede og overholder HIPAA-standarden. Al dataoverførsel sker via en sikker kanal med brug af TSL (Transport Security Layer) kryptering – standarden for sikre internetnetværksforbindelser. Følsomme data gemmes desuden med AES/RSA 2048 bit-kryptering. Til autentificeringen og password-krypteringen anvendes en Secure Remote Password-protokol (SRP). SRP er en veletableret og robust metode til sikkert-password-baseret autentificering og nøgleudveksling, der anvender 2048 bit-modulus.

Policy-baserede indstillinger

Fra TeamViewers managementkonsol kan brugerne definere, distribuere og effektuere indstillingspolicies for TeamViewer-software-installationerne på enheder, der tilhører specifikt dem. Indstillingspolicies signeres digitalt af den konto, der har genereret dem. Dette sikrer, at den eneste konto med tilladelse til at tildele en policy til en enhed, er den konto, som enheden tilhører.

Applikationssikkerhed hos TeamViewer

Sort- og hvidliste

Især hvis TeamViewer anvendes til servicearbejde på computere uden opsyn (dvs. at TeamViewer er installeret som en Windows-service), kan det være relevant med en ekstra sikkerhedsmulighed for at begrænse adgangen til disse computere til udvalgte klienter.

Med hvidliste-funktionen kan du eksplicit angive, hvilke TeamViewer-ID'er og/eller TeamViewer-konti der skal have adgang til computeren. Med sortliste-funktionen kan du blokere bestemte TeamViewer ID'er og TeamViewer-konti. En central hvidliste er tilgængelig som led i de "policy-baserede indstillinger", der er beskrevet foroven under “Management Console.”

Chat- og videokryptering

Chathistorikken er forbundet med din TeamViewer-konto og er derfor krypteret og gemt ved hjælp af samme AES/RSA 2048 bit-krypteringssikkerhed som beskrevet under "TeamViewer-konti". Alle chatbeskeder og al videotrafik krypteres ende-til-ende med AES (256 bit)-sessions-kryptering.

Ingen Stealth Mode

Der er ingen funktion, der gør det muligt for dig at have TeamViewer kørende fuldstændigt i baggrunden. Selv hvis applikationen kører som en Windows-service i baggrunden, er TeamViewer altid synlig i form af et ikon i systembakken.

Når forbindelsen er etableret, er et lille kontrolpanel altid synligt over systembakken. Derfor er TeamViewer bevidst gjort uanvendelig for skjult overvågning af computere eller medarbejdere.

Password-beskyttelse

Til den spontane kundesupport genererer TeamViewer (TeamViewer QuickSupport) et sessions-password (engangs-password). Hvis dine kunder fortæller dig deres password, kan du tilslutte dig deres computer ved at indtaste deres ID og password. Efter en genstart af TeamViewer hos kunden genereres et nyt sessions-password, så du kun kan tilslutte dig din kundes computer, hvis du inviteres.

Når du anvender TeamViewer til fjernsupport uden opsyn (f.eks. af servere), definerer du et individuelt, fast password, hvilket sørger for adgang til computeren.

Indgående og udgående adgangskontrol

Du kan konfigurere TeamViewers forbindelsesmåder individuelt. Du kan f.eks. indstille din fjernsupport eller mødecomputer på en måde, så ingen indgående forbindelser er mulige.

Ved at begrænse funktionaliteten til de features, der rent faktisk er brug for, begrænser man de potentielle svage punkter over for mulige angreb.

.

Tofaktor-autentificering

TeamViewer hjælper virksomheder med at leve op til deres HIPAA- og PCI-krav. Tofaktor-autentificering tilføjer et ekstra sikkerhedslag til at beskytte TeamViewer-konti mod uautoriseret adgang

Ud over brugernavn og password skal brugeren indtaste en kode for at autentificere sig. Denne kode er genereret via algoritmen til det tidsbaserede engangs-password (TOTP). Derfor er koden kun gyldig i et kort tidsrum.

Via tofaktor-autentificeringen og adgangsbegrænsningen i form af hvidlistning hjælper TeamViewer til at overholde alle nødvendige krav til HIPAA- og PCI-certificeringen.

Sikkerhedstest

Både TeamViewers infrastruktur og TeamViewer-softwaren gennemgår regelmæssigt penetrationstests. Disse tests udføres af uafhængige virksomheder, der er specialiseret i sikkerhedstests.

Yderligere spørgsmål?

Har du spørgsmål eller brug for information, kan du kontakte os på +45 6991 8655 eller sende en e-mail til support@teamviewer.com.

Kontakt

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