TeamViewer beveiligingsinformatie

Doelgroep

Dit document is bestemd voor professionele netwerkbeheerders. De informatie in dit document is van nogal technische aard en zeer gedetailleerd. Op basis van deze informatie kunnen IT-professionals een gedetailleerd beeld van de softwarebeveiliging krijgen, voordat TeamViewer wordt ingezet. Het staat u vrij om dit document onder uw klanten te verspreiden om mogelijke bezorgdheid wat betreft beveiliging weg te nemen.

Als u van mening bent dat u niet tot de doelgroep behoort, dan zullen de eenvoudige feiten in het deel "Het bedrijf / de software" u toch helpen om een beeld te krijgen.

Het bedrijf / de software

Over ons

TeamViewer GmbH werd opgericht in 2005 en is gevestigd in het zuiden van Duitsland, in Göppingen (in de buurt van Stuttgart), met dochtermaatschappijen in Australië en de VS. Wij ontwikkelen en verkopen uitsluitend veilige systemen voor een webgebaseerde samenwerking. Binnen zeer korte tijd hebben een snelle start en groei ertoe geleid dat de TeamViewer software meer dan 200 miljoen keer is geïnstalleerd door gebruikers in meer dan 200 landen wereldwijd. De software is verkrijgbaar in meer dan 30 talen.

De software wordt uitsluitend in Duitsland ontwikkeld.

Dit verstaan wij onder beveiliging

TeamViewer wordt over de hele wereld miljoenen keren gebruikt voor het leveren van spontane support via internet, voor toegang tot onbeheerde computers (bijv. support op afstand voor servers) en voor het organiseren van online-meetings. Afhankelijk van de configuratie kan TeamViewer worden gebruikt om op afstand een andere computer te bedienen alsof u er zelf voor zit. Als de gebruiker die bij een externe computer is aangemeld een Windows, Mac of Linux administrator is, zal deze persoon ook administratorrechten op die computer krijgen.

Het spreekt voor zich dat een dergelijk krachtige functionaliteit via het potentieel onveilige internet op verschillende manieren moet worden beveiligd tegen aanvallen. Het is zelfs zo dat beveiliging de belangrijkste plaats inneemt bij al onze ontwikkelingsdoelen, zowel om toegang tot uw computer veilig te maken, als om onze eigen belangen te beschermen: miljoenen gebruikers over de hele wereld vertrouwen alleen een veilige oplossing, en alleen een veilige oplossing garandeert ons zakelijke succes op lange termijn.

Kwaliteitsmanagement

Naar onze mening is beveiligingsmanagement ondenkbaar zonder een erkend kwaliteitsmanagementsysteem. TeamViewer GmbH is één van de weinige aanbieders op de markt die volgens een gecertificeerd kwaliteitsmanagementsysteem in overeenstemming met ISO 9001 werkt. Ons kwaliteitsmanagement volgt internationaal erkende standaarden. Wij laten ons kwaliteitsmanagementsysteem jaarlijks beoordelen door externe audits.

Externe beoordeling door experts

Aan onze software, TeamViewer, is een vijf-sterren kwaliteitskeurmerk (hoogste score) toegekend door de bond van IT-experts en adviseurs in de Bondsrepubliek Duitsland (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.). De onafhankelijke experts/adviseurs van de BISG e.V. inspecteren producten van gekwalificeerde producenten op hun kwaliteits-, beveiligings- en service-eigenschappen.

Beveiligingsgerelateerde inspectie

TeamViewer is onderworpen aan beveiligingsgerelateerde inspecties door FIDUCIA IT AG (een beheerder van gegevensverwerkingscentra voor ca. 800 Duitse banken) en is goedgekeurd voor gebruik op werkstations in banken.

Referenties

Momenteel wordt TeamViewer gebruikt op meer dan 200.000.000 computers. Internationale topbedrijven in alle bedrijfstakken (waaronder zeer gevoelige sectoren als het bank- en geldwezen, gezondheidszorg en overheid) maken met succes gebruik van TeamViewer.

Wij nodigen u uit om eens naar onze referenties op internet te kijken, om een eerste indruk te krijgen van de acceptatie van onze oplossing. U zult het er zeker mee eens zijn dat de meeste van deze bedrijven soortgelijke eisen m.b.t. beveiliging en beschikbaarheid hadden, voordat zij - na een uitgebreid onderzoek - uiteindelijk kozen voor TeamViewer. Om toch uw eigen indruk te kunnen vormen, vindt u in de volgende hoofdstukken enkele technische details.

TeamViewer sessies

Opzetten van een sessie en verbindingstypes

Bij het tot stand brengen van een sessie bepaalt TeamViewer het optimale verbindingstype. Na de handshake via onze masterservers wordt in 70% van alle gevallen een directe verbinding via UDP of TCP tot stand gebracht (zelfs achter standaard gateways, NAT's en firewalls). De rest van de verbindingen wordt langs ons zeer redundant uitgevoerde routernetwerk doorgestuurd via TCP of http-tunnels. U hoeft geen poorten te openen om met TeamViewer te werken!

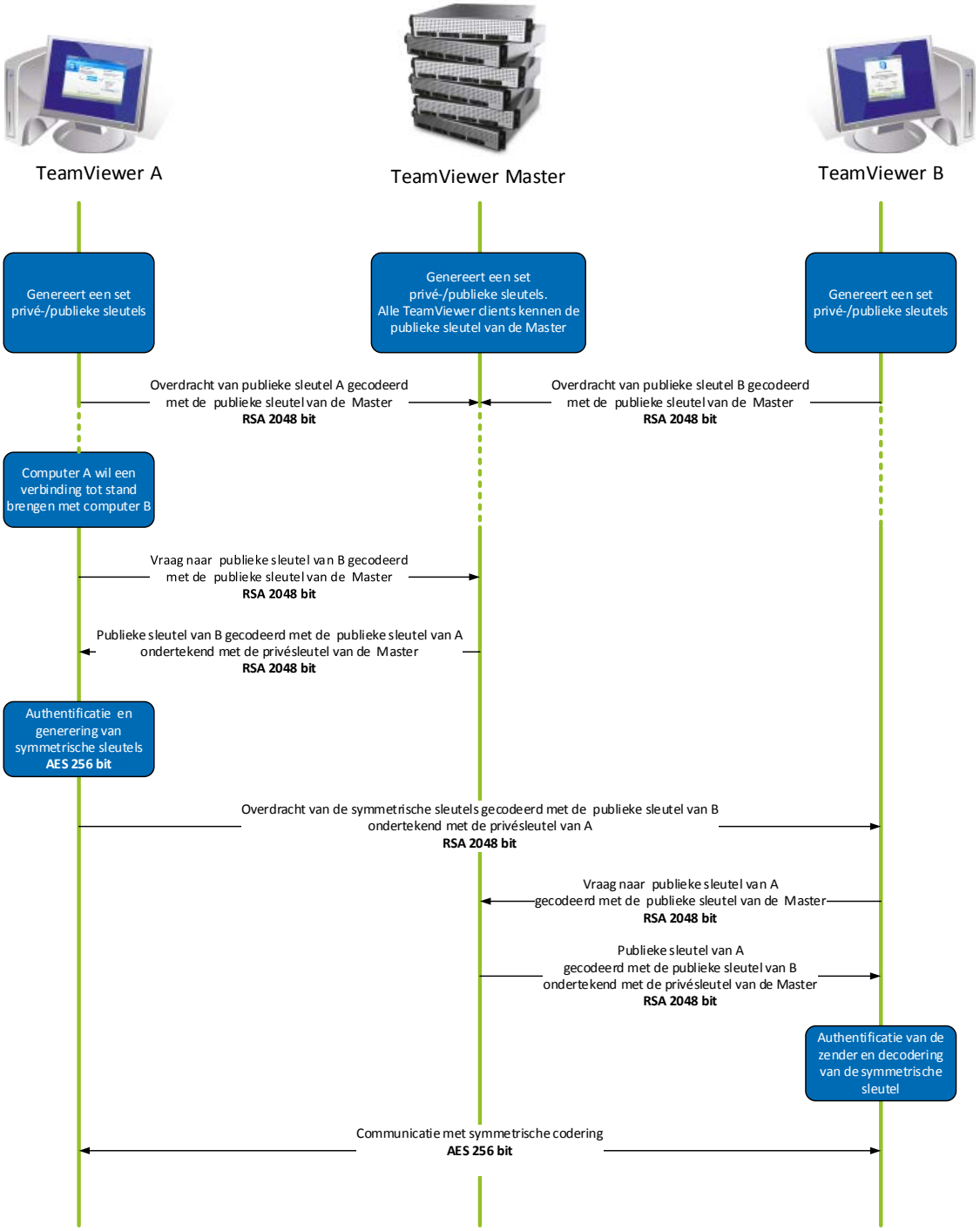
Zoals hieronder beschreven in het hoofdstuk "Codering en authenticatie", kunnen zelfs wij als operators van de routingservers het gecodeerde dataverkeer niet lezen.

Codering en authenticatie

TeamViewer dataverkeer wordt beveiligd met behulp van RSA sleuteluitwisseling (publiek/privé) en AES (256 bit) sessiecodering. Deze technologie wordt in een vergelijkbare vorm gebruikt voor https/SSL en wordt volgens de huidige standaarden als volledig veilig beschouwd. Aangezien de privésleutel (geheime sleutel) nooit de client computer verlaat, garandeert deze procedure dat onderling verbonden computers - waaronder de routingservers van TeamViewer - de datastroom niet kunnen decoderen.

In elke TeamViewer client is de publieke sleutel van het hoofdcluster al geïmplementeerd en de client kan zo berichten aan het hoofdcluster coderen en berichten die hiermee ondertekend zijn, controleren. De PKI (Public Key Infrastructure) voorkomt doeltreffend "man-in-the-middle-aanvallen". Ondanks de codering wordt het wachtwoord nooit rechtstreeks verzonden, maar alleen via een procedure met vraag en antwoord, en wordt het alleen op de lokale computer opgeslagen.

Tijdens authenticatie wordt het wachtwoord nooit rechtstreeks overgebracht, omdat het Secure Remote Password (SRP) protocol wordt gebruikt. Er is alleen een wachtwoordcontrole op de lokale computer opgeslagen.



TeamViewer codering en authentificatie

Validatie van TeamViewer-ID's

TeamViewer ID's zijn gebaseerd op diverse hardware- en softwarekenmerken en worden automatisch gegenereerd door TeamViewer. De TeamViewer servers controleren vóór elke verbinding de geldigheid van deze ID's.

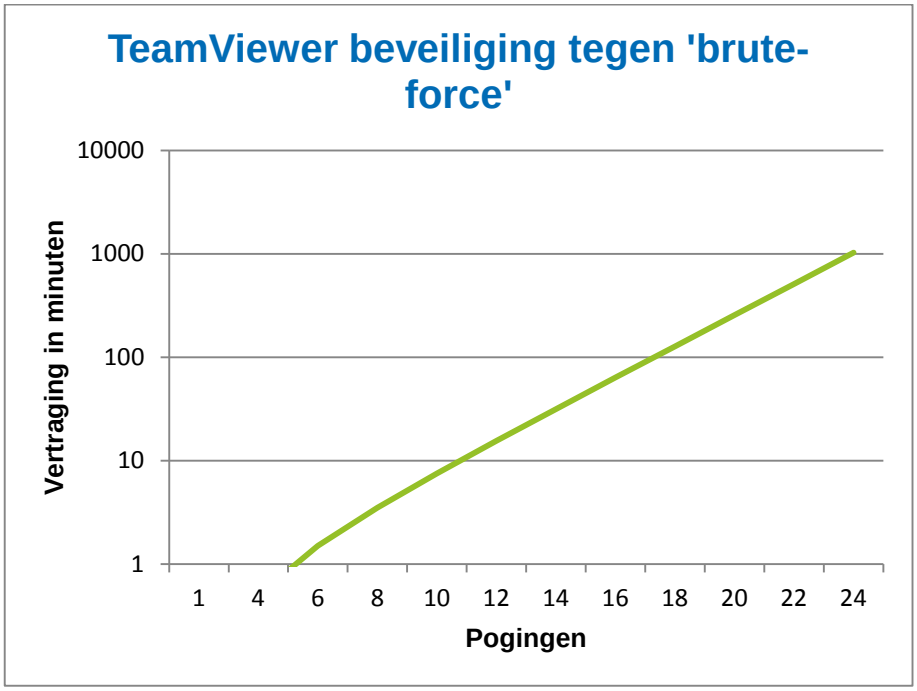
Beveiliging tegen 'brute-force'

Toekomstige klanten die informeren naar de beveiliging van TeamViewer hebben regelmatig vragen over codering. Het is begrijpelijk dat men het meest bang is voor het risico dat een derde de verbinding zou kunnen monitoren of dat de toegangsgegevens van TeamViewer worden onderschept. In werkelijkheid zijn het echter de primitieve aanvallen die vaak het gevaarlijkst zijn.

In verband met computerbeveiliging is een 'brute-force'-aanval een methode waarbij botweg alle mogelijke opties worden uitgeprobeerd om een wachtwoord te achterhalen dat een bron beveiligt. Door de steeds toenemende rekenkracht van standaard computers is de tijd die nodig is om lange wachtwoorden te achterhalen, aanzienlijk verminderd.

Als een verdediging tegen 'brute-force'-aanvallen vergroot TeamViewer de wachttijd (latency) tussen verbindingspogingen exponentieel. Zo is er wel 17 uur nodig voor 24 pogingen. De wachttijd wordt alleen teruggezet, nadat met succes het juiste wachtwoord is ingevoerd.

TeamViewer heeft niet alleen een mechanisme geïntegreerd om zijn klanten tegen aanvallen vanaf één bepaalde computer te beveiligen, maar ook vanaf meerdere computers, bekend als botnet-aanvallen, die toegang proberen te krijgen tot één bepaalde TeamViewer-ID.



Grafiek: Tijd die is verstreken na n verbindingspogingen tijdens een 'brute-force'-aanval

Code-ondertekening

Als een extra beveiligingsfunctie wordt al onze software ondertekend via VeriSign Code Signing. Op deze manier kan de uitgever van de software altijd gemakkelijk worden geïdentificeerd. Als de software later is gewijzigd, wordt de digitale handtekening automatisch ongeldig.

Datacentrum en backbone

Deze twee onderwerpen hebben betrekking op de beschikbaarheid en de beveiliging van TeamViewer. De centrale TeamViewer servers bevinden zich in de Europese Unie in ISO 27001-gecertificeerde datacentra met multi-redundante carrier-verbindingen en redundante stroomvoorzieningen. Er wordt uitsluitend gebruik gemaakt van hardware van bekende merken.

Persoonlijke toegangscontrole, videocameratoezicht, bewegingsdetectors, 24/7 monitoring en beveiligingspersoneel op locatie zorgen ervoor dat toegang tot het datacentrum alleen wordt verleend aan geautoriseerde personen en garanderen de best mogelijke beveiliging voor hardware en data. Er is ook een uitgebreide identificatiecontrole bij de centrale toegang tot het datacentrum.

TeamViewer-account

Speciaal toegewezen TeamViewer servers dienen als host voor TeamViewer-accounts. Zie voor informatie over toegangscontrole het bovenstaande hoofdstuk "datacentrum en backbone". Voor autorisatie en wachtwoordcodering wordt het Secure Remote Password (SRP) protocol, een uitgebreid 'password-authenticated key agreement' (PAKE) protocol, gebruikt. Een infiltrant of 'man in the middle' kan niet voldoende informatie krijgen om via een 'brute-force'-aanval een wachtwoord te achterhalen. Dit betekent dat zelfs bij het gebruik van zwakke wachtwoorden een sterke beveiliging kan worden verkregen. Gevoelige gegevens binnen het TeamViewer-account, bijvoorbeeld aanmeldingsgegevens voor cloudopslag, worden met behulp van AES/RSA 2048 bitcodering opgeslagen.

Management Console

De TeamViewer Management Console is een webgebaseerd platform voor gebruikersbeheer, verbindingsrapporten en beheer van Computers & Contacten. Hiervoor dienen ISO 27001-gecertificeerde datacentra die voldoen aan HIPAA-eisen, als host. De gegevensoverdracht vindt plaats via een veilig kanaal met SSL (Secure Sockets Layer) codering, de standaard voor veilige internetverbindingen. Gevoelige gegevens worden bovendien met behulp van AES/RSA 2048 bitcodering opgeslagen. Voor autorisatie en wachtwoordcodering wordt het Secure Remote Password (SRP) protocol gebruikt. SRP is een bewezen, robuuste, veilige, op wachtwoorden gebaseerde authentificatie- en sleuteluitwisselingsmethode die gebruik maakt van 2048-bitmodulus.

Op richtlijnen gebaseerde instellingen

Vanuit de TeamViewer Management Console kunnen gebruikers specifiek bij apparaten horende instellingen definiëren, distribueren en afdwingen voor de TeamViewer software-installaties. Instellingen

worden digitaal ondertekend door het account dat deze heeft gegenereerd. Dit garandeert dat het enige account dat een richtlijn aan een apparaat mag toewijzen, het account is waartoe het apparaat behoort.

Toepassingsbeveiliging in TeamViewer

Zwarte en witte lijst

Vooral als TeamViewer wordt gebruikt voor het onderhoud van onbeheerde computers (d.w.z. TeamViewer wordt als een Windows-service geïnstalleerd), kan de extra beveiligingsoptie de toegang tot deze computers beperken tot het aantal aangegeven clients.

Met de functie 'witte lijst' kunt u expliciet aangeven welke TeamViewer-ID's en/of TeamViewer-accounts toegang mogen hebben tot een computer. Met de functie 'zwarte lijst' kunt u bepaalde TeamViewer-ID's en TeamViewer-accounts blokkeren. Een centrale witte lijst is beschikbaar als onderdeel van de 'op richtlijnen gebaseerde instellingen' die hierboven onder "Management Console" zijn beschreven.

Chat- en videocodering

Chatgeschiedenissen zijn verbonden met uw TeamViewer-account en worden daarom gecodeerd en opgeslagen met behulp van dezelfde AES/RSA 2048 bitcoderingsbeveiliging als beschreven onder "TeamViewer-acccount". Alle chatberichten en al het videoverkeer worden end-to-end gecodeerd met behulp van AES (256 bit) sessiecodering.

Geen Stealth-modus

Er is geen functie die u in staat stelt om TeamViewer helemaal op de achtergrond uit te voeren. Zelfs als de toepassing wordt uitgevoerd als een Windows-service op de achtergrond, is TeamViewer altijd zichtbaar door middel van een pictogram in het systeemvak.

Na het tot stand brengen van een verbinding is er altijd een klein controlevenster zichtbaar boven het systeemvak. Zodoende is TeamViewer opzettelijk ongeschikt voor het heimelijk monitoren van computers of werknemers.

Wachtwoordbeveiliging

Voor spontane support aan klanten genereert TeamViewer (TeamViewer QuickSupport) een sessiewachtwoord (eenmalig wachtwoord). Als uw klant u zijn wachtwoord meedeelt, dan kunt u verbinding maken met zijn computer door zijn ID en wachtwoord in te voeren. Na een herstart van TeamViewer bij de klant wordt een nieuw sessiewachtwoord gegenereerd, zodat u alleen verbinding kunt maken met computers van uw klant als u wordt uitgenodigd om dit te doen.

Bij het inzetten van TeamViewer voor onbeheerde support op afstand (bijv. van servers) stelt u een individueel, vast wachtwoord in dat de toegang tot de computer beveiligt.

Inkomende en uitgaande toegangscontrole

U kunt de verbindingsmodi van TeamViewer individueel configureren. U kunt bijvoorbeeld uw computer voor support op afstand of meetings zodanig configureren dat geen inkomende verbindingen mogelijk zijn.

Het beperken van de functionaliteit tot die functies die echt nodig zijn, betekent altijd het beperken van mogelijke zwakke punten voor potentiële aanvallen.

Tweeledige authenticatiemethode

TeamViewer helpt bedrijven te voldoen aan HIPAA- en PCI-eisen. De tweeledige authenticatiemethode voegt een extra beveiligingslaag toe om TeamViewer-accounts te beveiligen tegen toegang door onbevoegden. Naast zowel gebruikersnaam als wachtwoord moet de gebruiker een code invoeren om de authentificatie uit te voeren. Deze code wordt gegenereerd via het TOTP-algoritme (eenmalig wachtwoord op basis van tijd). Zodoende is de code slechts gedurende een korte tijd geldig.

Door middel van de tweeledige authentificatiemethode en het beperken van de toegang door middel van witte lijsten helpt TeamViewer om te voldoen aan alle noodzakelijke criteria voor HIPAA- en PCI-certificering.

Nog vragen?

Neem bij verdere vragen of voor meer informatie contact op met (NL) +31 (0)858880136 en (BE) +32 (0)28088659, of stuur een e-mail naar support@teamviewer.com.

Contact

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