TeamViewer Informatie over beveiliging

Doelgroep

Dit document is gericht op professionele netwerkbeheerders. De informatie in dit document is van nogal technische aard en zeer gedetailleerd. Aan de hand van deze informatie kunnen IT-professionals zich een gedetailleerd beeld vormen van de beveiligingsstandaarden van TeamViewer, en worden eventuele vragen beantwoord voordat ze onze software in gebruik nemen. Verspreid dit document gerust onder uw klanten om eventuele bezorgdheid over de beveiliging weg te nemen.

Als u denkt dat u zelf geen deel uitmaakt van de doelgroep, geven de feiten in de sectie Het bedrijf/de Software u evengoed een duidelijk beeld over hoe we beveiliging serieus nemen.

Het bedrijf/de software

Over ons

TeamViewer GmbH is opgericht in 2005 en is gevestigd in zuid Duitsland, in de stad Göppingen (in de buurt van Stuttgart), met dochterondernemingen in Australië en de Verenigde Staten. We ontwikkelen en verkopen uitsluitend veilige systemen voor samenwerking via het web. Binnen een kort tijdsbestek heeft onze Freemium-licentiëring tot een snelle groei geleid, met meer dan 200 miljoen gebruikers van de TeamViewer-software op meer dan 1,4 miljard apparaten, in meer dan 200 landen wereldwijd. De software is in ruim 30 talen verkrijgbaar.

Ons begrip van beveiliging

TeamViewer wordt gebruikt door meer dan 30 miljoen gebruikers op elk willekeurig tijdstip van de dag. Deze gebruikers leveren spontane ondersteuning via internet, benaderen computers die zonder toezicht draaien (ofwel externe ondersteuning voor servers) en voor het hosten van online-vergaderingen. Afhankelijk van de configuratie kan TeamViewer worden gebruikt om een andere computer op afstand te bedienen, alsof u daar recht voor zit. Als de gebruiker die op de externe computer is aangemeld een Windows-, Mac- of Linux-beheerder is, krijgt deze persoon ook beheerdersrechten op die computer.

Het is duidelijk dat zulke krachtige mogelijkheden over het potentieel onveilige internet heel zorgvuldig moeten worden beschermd tegen aanvallen. In feite domineert het onderwerp beveiliging al onze ontwikkelingsdoelen en is het iets waarmee we bij alles wat we doen intens omgaan. We willen er voor zorgen dat de toegang tot uw computer veilig is en we willen onze eigen belangen beschermen: miljoenen gebruikers wereldwijd vertrouwen alleen een veilige oplossing, en alleen een veilige oplossing maakt ons succes als bedrijf op de lange termijn mogelijk.

Beoordeling door externe experts

Aan onze software, TeamViewer, is een vijfsterren-kwaliteitszegel (maximum wqaarde) toegewezen door de federale bond van IT-expertes en beoordelers (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.). De onafhankelijke beoordelers van de BISG e.V. inspecteren producten van gekwalificeerde producenten op kwaliteit, beveiliging en onderhoudskenmerken.

Referenties

Op dit moment wordt TeamViewer door meer dan 200 miljoen gebruikers toegepast. Internationale topbedrijven vanuit allerlei branches (waaronder zulke zeer gevoelige sectoren zoals bankieren, financiën, gezondheidszorg en overheid) gebruiken TeamViewer met veel succes.

We nodigen u uit om eens te kijken naar onze referenties die overal op internet te vinden zijn, om een eerste indruk te krijgen van de acceptatie van onze oplossing. U zult merken dat waarschijnlijk de meeste andere bedrijven gelijksoortige eisen over beveiliging en beschikbaarheid hadden voordat ze - na een intensief onderzoek - uiteindelijk kozen voor TeamViewer. Maar om zelf een indruk te vormen, kunt u een aantal technische details in de rest van dit document vinden.

TeamViewer-sessies

Een sessie opzetten en soorten verbindingen

Bij het opzetten van een sessie stelt TeamViewer het optimale type verbinding vast. Na de handshake via onze master servers wordt in 70 % van alle gevallen een rechtstreekse verbinding opgezet via UDP of TCP (ook achter standaard gateways, NATs en firewalls). De rest van de verbindingen worden via ons zeer redundante routernetwerk gerouteerd over TCP of https-tunneling. U hoeft geen poorten te openen om met TeamViewer te kunnen werken

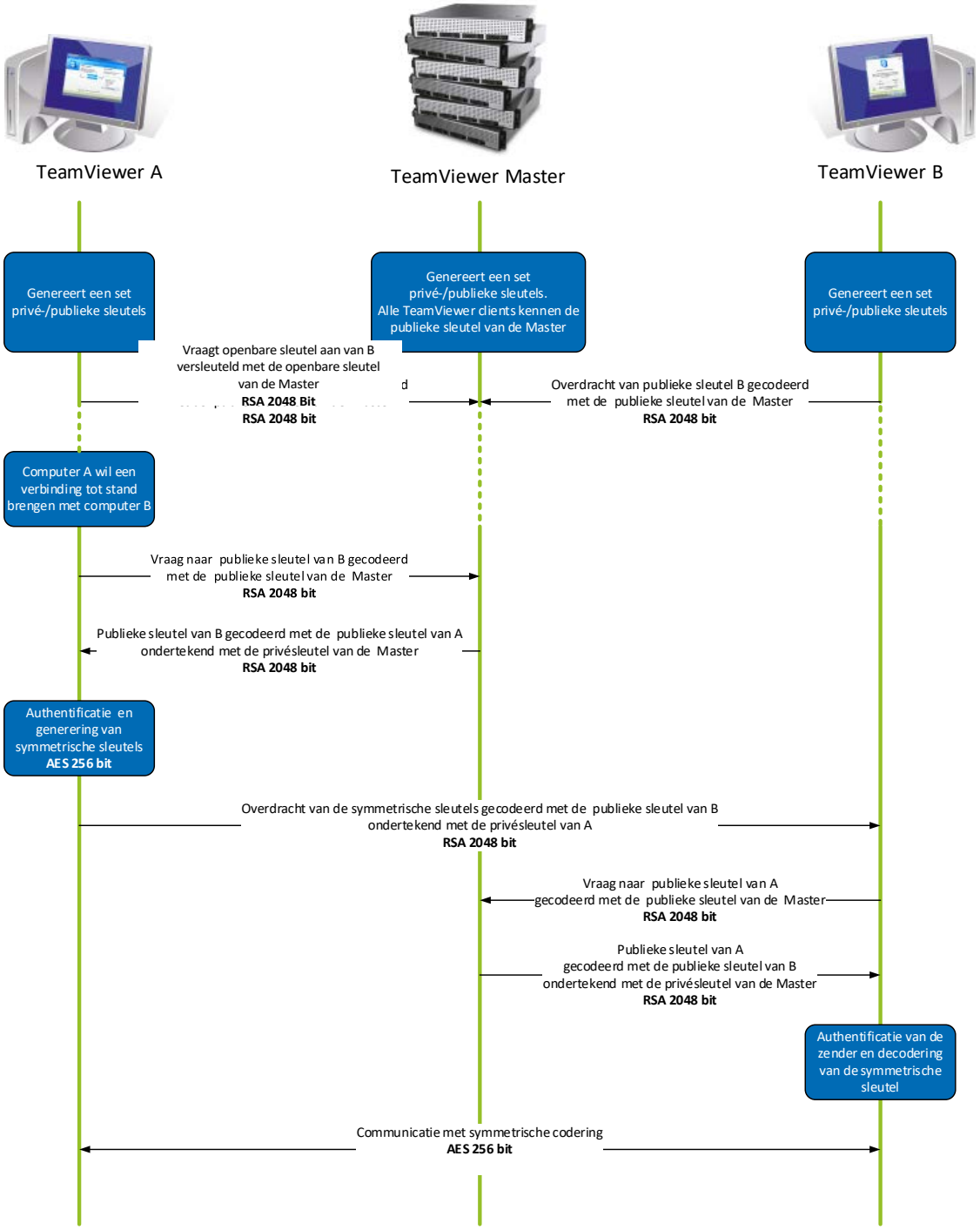
Zoals hieronder wordt beschreven in de paragraaf Versleuteling en authenticatie kunnen zelfs wij, als bedieners van de routerende servers, het versleutelde gegevensverkeer niet lezen.

Versleuteling en authenticatie

Het verkeer van TeamViewer wordt beveiligd met de uitwisseling van publieke en privé RSC-sleutels en met AES (256 bit) sessieversleuteling. Deze technologie wordt op vergelijkbare wijze gebruikt voor http/SSL en dit wordt als volledig veilig beschouwd volgens de hedendaagse standaarden. Omdat de privésleutel de client computer nooit verlaat, zorgt deze procedure er voor dat onderling verbonden computers - waaronder de TeamViewer routeringsservers - de gegevensstroom niet kunnen ontcijferen.

Elke TeamViewer-client heeft de openbare sleutel van de master cluster reeds geïmplementeerd en kan daarom berichten naar de master cluster versleutelen en berichten controleren die daarmee zijn ondertekend. De PKI (Public Key Infrastructure) voorkomt op effectieve wijze man-in-the-middle-aanvallen. Ondanks de versleuteling wordt het wachtwoord nooit rechtstreeks verzonden, maar alleen via een uitdaging-antwoord-procedure, en wordt dit alleen op de lokale computer opgeslagen.

Tijdens authenticatie wordt het wachtwoord nooit rechtstreeks overgedragen omdat gebruik wordt gemaakt van het Secure Remote Password (SRP) protocol. Op de lokale computer wordt alleen een wachtwoordcontroleur opgeslagen.



TeamViewer versleuteling en authenticatie

Validatie van TeamViewer IDs

TeamViewer IDs zijn gebaseerd op verschillende kenmerken van hardware en software en worden automatisch gegenereerd door TeamViewer. De TeamViewer-servers controleren voor elke verbinding de geldigheid van deze IDs.

Brutekracht-bescherming

Mogelijke klanten die informeren naar de beveiliging van TeamViewer hebben regelmatig vragen over versleuteling. Het is begrijpelijk dat men vooral bang is dat derden de verbinding kunnen volgen of dat de toegansgegevens voor TeamViewer worden afgetapt. Maar de realiteit is dat nogal primitieve aanvallen vaak de gevaarlijkste zijn.

Binnen de context van computerbeveiliging is een brutekracht-aanval een trial-en-error-methode om een wachtwoord te raden dat een resource beschermt. Met de toenemende computerkracht van standaardcomputers is de tijd die nodig is om lange wachtwoorden te raden, aanzienlijk afgenomen.

Ter beveiliging tegen brutekracht-aanvallen vergroot TeamViewer de tijd tussen verbindingspogingen exponentieel. Daardoor duren 24 pogingen 17 uur. De latentie wordt pas teruggezet nadat het juiste wachtwoord is ingevoerd.

TeamViewer beschikt niet alleen over een mechanisme ter bescherming van de klanten tegen aanvallen op een specifieke computer, maar ook vanaf meerdere computers, ofwel botnet-aanvallen, die proberen om een specifiek TeamViewer-id te benaderen.

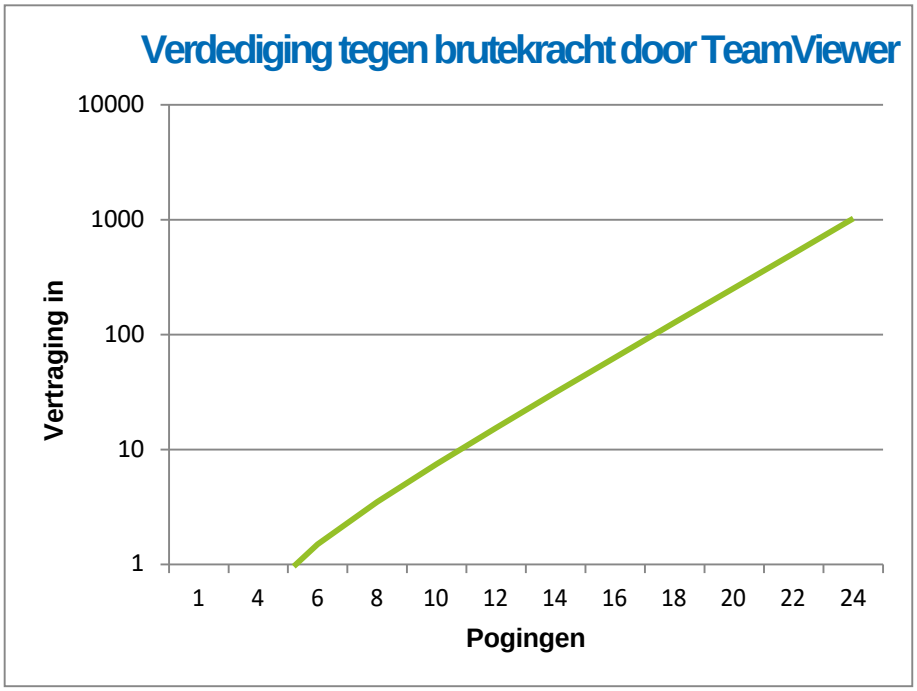


Diagram: Tijd verlopen na n verbindingspogingen tijdens een brutekracht-aanval

Code Signing

Als extra beveiligingsmaatregel is al onze software ondertekend via VeriSign Code Signing. Op deze manier is de uitgever van de software altijd snel identificeerbaar. Als de software achteraf is gewijzigd, dan wordt de digitale handtekening automatisch ongeldig.

Datacentra en backbone

Om te zorgen voor de best mogelijke beveiliging en beschikbaarheid van de TeamViewer-diensten zijn alle TeamViewer-servers geplaatst in datacentra die voldoen aan ISO 27001 en maken ze gebruik van multiredundante carrier-verbindingen en redundante voedingen. Verder wordt alleen state-of-the-art merkhardware gebruikt. Daarnaast zijn alle servers waarop gevoelige informatie wordt opgeslagen, in Duitsland of Oostenrijk geplaatst.

ISO 27001-gecertificeerd zijn houdt in dat persoonlijke toegangscontrole, bewaking met videocamera's, bewegingsdetectoren, 24x7 bewaking en beveiligingspersoneel op locatie er voor zorgen dat toegang tot het datacentrum alleen mogelijk is voor geautoriseerde personen en een garantie vormen voor de best mogelijke beveiliging van hardware en gegevens. Tevens wordt een uitgebeide identiteitscontrole verricht op het enkele toegangspunt van het datacentrum.

TeamViewer-account

TeamViewer-accounts worden gehost op speciale TeamViewer-servers. Zie voor informatie over toegangscontrole Datacentra en backbone hierboven. Voor authenticatie en wachtwoordversleuteling wordt het Secure Remote Password protocol (SRP), een uitgebreid password-authenticated key agreement (PAKE) protocol, gebruikt. Een infiltrator of man-in-the-middle kan nooit voldoende informatie verkrijgen om met brute kracht een wachtwoord te raden. Dat betekent dat een stevige beveiliging tevens kan worden verkregen met zwakken wachtwoorden. Gevoelige gegevens binnen een TeamViewer-account, bijvoorbeeld aanmeldinformatie voor de cloud-opslag, wordt AES/RSA 2048 bit versleuteld opgeslagen.

Management Console

De TeamViewer Management Console is een op het web gebaseerd platform voor gebruikersbeheer, verbindingsrapportage en het beheer van computers en contacten. Dit wordt gehost in ISO-27001 gecertificeerde, aan HIPAA voldoende datacentra. Alle gegevensoverdracht vindt plaats via een veilig kanaal met TSL (Transport Security Layer)-versleuteling, de standaard voor beveiligde internetverbindingen. Daarnast wordt gevoelige informatie AES/RSA 2048 bit versleuteld opgeslagen. Voor authenticatie en wachtwoordversleuteling wordt Secure Remote Password protocol (SRP) gebruikt. SRP is een gevestigde, robuuste, veilige op wachtwoorden gebaseerde methode voor authenticatieen uitwisselen van sleutels met 2048 bit modulus.

Op beleiden gebaseerde instellingen

Vanuit de TeamViewer Management Console kunnen gebruikers instelbeleiden definiëren, distribueren, en opleggen voor de TeamViewer software-installaties op apparaten die hun specifieke eigendom zijn. Instelbeleiden worden digitaal ondertekend doro de account die deze heeft gegenereerd. Dit zorgt er voor dat de enige account die toestemming heeft om een beleid toe te wijzen aan een apparaat, de account is waartoe het apparaat behoort.

Toepassingsbeveiliging in TeamViewer

Black- & Whitelist

Met name als TeamViewer wordt gebruikt voor het onderhoud van computers die zonder toezicht draaien (bijvoorbeeld TeamViewer is geïnstalleerd als een Windows-service) kan de extra beveiligingsoptie om toegang tot deze computers te beperken tot een aantal specifieke clients van belang zijn.

Met de whitelist-functie kunt u expliciet aangeven welke TeamViewer-id's en/of TeamViewer-accounts toegang tot een computer mogen hebben. Met de blacklist-functie kunt u bepaalde TeamViewer-IDs en TeamViewer-accounts blokkeren. Een centrale whitelist is beschikbaar als onderdeel van de hierboven onder "Managementconsole" beschreven beleidsgebaseerde instellingen.

Chat- en videoversleuteling

Chatgeschiedenissen zijn gekoppeld aan uw TeamViewer-account en deze worden daarom versleuteld en opgeslagen met dezelfde AES/RSA 2048 bits versleuteling als beschreven onder "TeamViewer-account". Alle chatberichten en het videoverkeer worden end-to-end versleuteld met AES (256 bit) sessieversleuteling.

Geen stealth-modus

Er is geen functie waarmee u TeamViewer volledig op de achtergrond kunt laten draaien. Ook als de toepassing als Windows-service op de achtergrond draait, is TeamViewer altijd zichtbaar via een pictogram in het systeemvak.

Nadat een verbinding is opgezet, is boven het systeemvak altijd een klein bedieningspaneel zichtbaar. Daarom is TeamViewer met opzet ongeschikt voor het stiekem bewaken van computers of medewerkers.

Wachtwoordbeveiliging

Voor spontane klantondersteuning genereert TeamViewer (TeamViewer QuickSupport) een sessiewachtwoord (eenmalig wachtwoord). Als de klant u het wachtwoord doorgeeft, kunt u met diens computer verbinding maken door diens ID en wachtwoord in te voeren. Nadat TeamViewer bij de klant opnieuw is gestart, wordt een nieuw sessiewachtwoord gegenereerd zodat u alleen verbinding kunt maken met de computers van de klant als u daartoe wordt uitgenodigd.

Bij gebruik van TeamViewer voor externe ondersteuning zonder verdere begeleiding (bijvoorbeeld van servers) stelt u een individueel vast wachtwoord in dat de toegang tot de computer afschermt.

Regeling van binnenkomende en uitgaande toegang

U kunt de verbindingsmodi van TeamViwer individueel instellen. U kunt bijvoorbeeld de computer voor externe ondersteuning of vergaderen zo instellen dat binnenkomende verbindingen niet mogelijk zijn.

Het beperken van de werking van functies die feitelijk nodig zijn, betekent altijd het beperken van mogelijke zwakke punten voor mogelijke aanvallen.

Dubbele authenticatie

TeamViewer helpt bedrijven bij het voldoen aan HIPAA en PCI. Dubbele authenticatie voegt een extra beveiligingslaag toe ter bescherming van TeamViewer-accounts tegen ongeautoriseerde toegang.

In aanvulling op gebruikersnaam en wachtwoord moet de gebruiker een code invoeren om te kunnen authenticeren. Deze code wordt gegenereerd via het op tijd gebaseerde eenmalige wachtwoord (TOTP)-algoritme. Daarom is de code slechts zeer kort geldig.

Via dubbele authenticatie en beperken van toegang door middel van whitelisting helpt TeamViewer bij het voldoen aan alle noodzakelijke criteria voor HIPAA- en PCI-certificatie.

Beveiliging testen

Zowel de TeamViewer-infrastructuur als de TeamViewer-software worden regelmatig onderworpen aan penetratietests. De tests worden uitgevoerd door onafhankelijke bedrijven, die gespecialiseerd zijn in het testen van de beveiliging.

Meer vragen?

Neem voor meer vragen of informatie gerust contact met ons op onder (NL) +31 (0)858880136 en (BE) +32 (0)28088659 of stuur een e-mail aan support@teamviewer.com.

Contact

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