TeamViewer turvallisuustietoja

Kohderyhmä

Tämä asiakirja on tarkoitettu verkkoja hallinnoiville ammattilaisille. Tämän asiakirjan tiedot ovat jokseenkin teknillisiä ja hyvin yksityiskohtaisia. Näiden tietojen perusteella tietotekniikan ammattilaiset saavat yksityiskohtaisen kuvan Teamviewerin turvallisuusstandardreista, ja he voivat ennakoida tilanteita ennen ohjelmistomme lataamista. Ole hyvä ja jaa tämä asiakirja asiakkaillesi, jotta kaikki mahdolliset turvallisuuskysymykset ratkeavat.

Jollet kuulu kohderyhmään, katso osaan yritys / ohjelma antaa sinulle selkeän käsityksen turvallisuuteen liittyvistä tottumuksistamme.

Yritys / ohjelma

Meistä

TeamViewer GmbH perustettiin 2005. Se sijaitsee Etelä-Saksassa, Göppingenin kaupungissa (Stuttgartin lähellä), ja sillä on tytäryhtiöitä Australiassa ja USA:ssa. Kehitämme ja myymme vain turvallisia järjestelmiä verkkoyhteistyöhön. Freemiumin lisensiointi on noussut nopeaan kasvuun lyhyellä aikavälillä. TeamViewerillä on yli 200 miljoonaa käyttäjää yli 1,4 miljardilla laitteella yli 200 maassa ympäri maailman. Ohjelma on saatavilla yli 30 kielellä.

Turvallisuuskuvamme

TeamViewerillä on joka hetki yli 30 miljoonaa käyttäjää. Nämä käyttäjät antavat nopeasti tukea verkon kautta, käyttäen vartioimattomia tietokoneita (esim. palvelimia) kauko-ohjauksella ja isännöimällä verkkotapaamisia. Konfiguroinnista riippuen, TeamViewerillä voi kauko-ohjata toista tietokonetta, aivan kuin istuisit sen edessä. Jos etätietokone, jolle on kirjauduttu on Windows-, Mac- tai Linux-hallinnoitsija, voi hän antaa hallinnointioikeuksia myös etätietokoneella.

Tuollaisia oikeuksia on syytä turvata erityisellä tarkkaavaisuudella. Turvallisuuden aihe on sydäntämme lähellä. Haluamme sinun tietokoneesi olevan turvallinen. Tämä on myös oman etumme mukaista, koska miljoonat asiakkaat luottavat pidemmällä aikavälillä vain turvalliseen ratkaisuun.

Ulkoisten asiantuntijoiden arviointi

Saksan IT-asiantuntijoiden ja tarkastajien liitto (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.) on palkinnut ohjelmamme TeamViewer viiden tähden laatusinetillä (korkein arvo). BSIG:n riippumattomat tarkastajat tutkivat ammattilaisten tuotteiden laatua, turvallisuutta ja palveluominaisuuksia.

Suositukset

TeamViewerillä on nyt yli 200 miljoonaa käyttäjää. Kansainväliset huippuyritykset eri aloilta (mm. arkaluontoisilta pankki-, rahoitus-, terveydenhoito- ja viranomais-) käyttävät TeamVieweriä menestyksellä.

Suosittelemme tarkastamaan suosituksiamme verkosta. Tuotteemme on saanut paljon arvostusta. Useilla yrityksillä on ollutsamansuuntaisia turvallisuuteen ja yhteyksiin liittyviä tarpeita, ja he päätyivät lopulta TeamViewerin käyttäjiksi. Saat ensivaikutelman tuotteestamme tästä asiakirjasta.

TeamViewer-tapaamiset

Tapaamisen aloittaminen ja yhteystyypit

Kun alat tapaamisen, TeamViewer määrittää parhaan yhteystyypin. Kättelyn jälkeen käytetään suoraa UDP- tai TCP-yhteyttä 70% tapauksista (myös tavanomaisten käytävien, NAT-osoitteenmuutosten ja palomuurien takaa). Loput yhteydet reititetään hyvin turvatun verkostomme ja TCP:n tai https-tunneloinnin kautta. TeamViewerin käyttöön ei tarvitse avata portteja

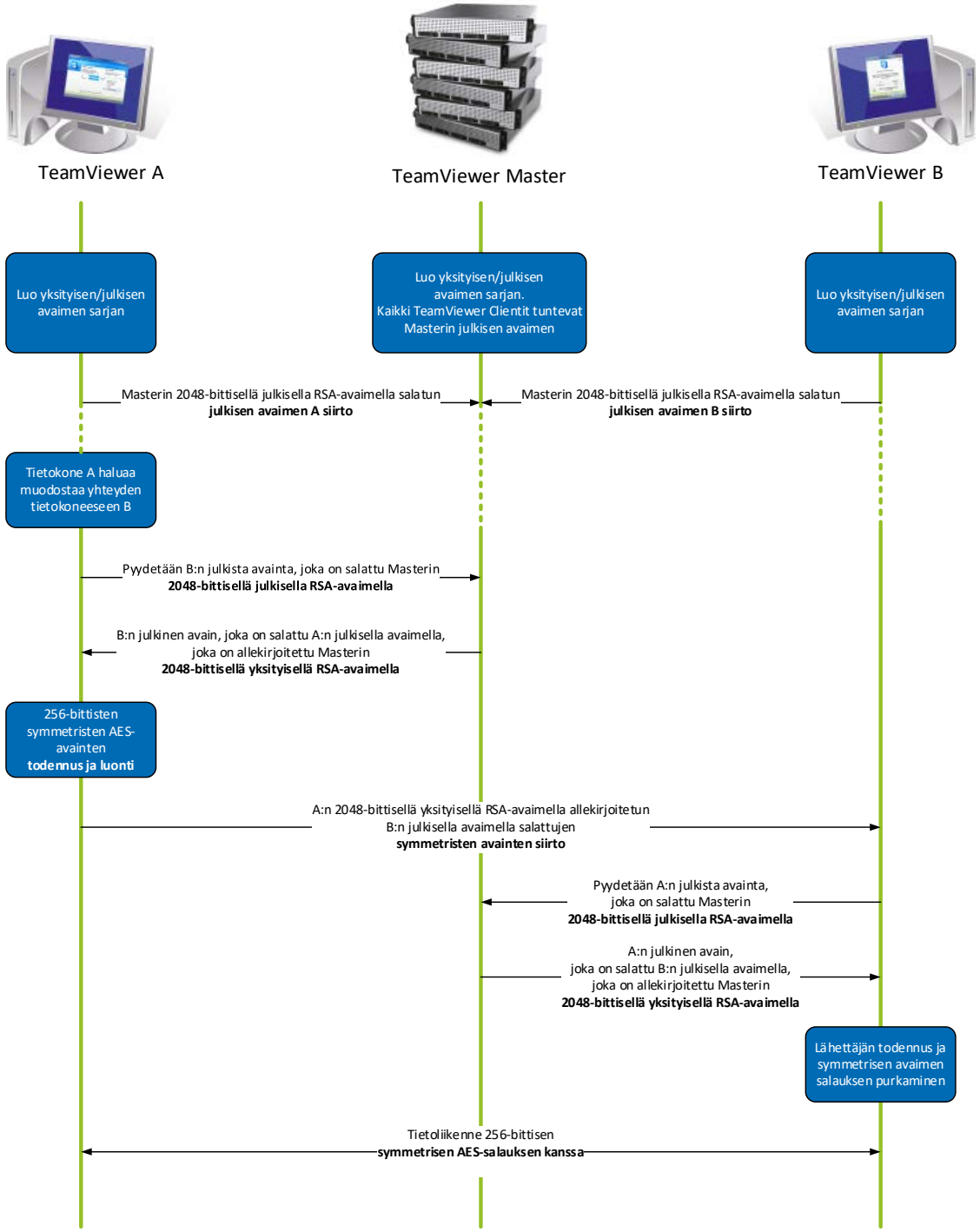
Salausta ja todennusta koskevassa osassa alla kerromme, ettemme itsekään kykene lukemaan salattua tietoliikennettä.

Salaus ja todennus

TeamViewer Traffic varmistetaan RSA julkisen/yksityisen avaimen vaihdolla ja AES (256 bit) salauksella. Tätä teknologiaa käytetään verrattavassa muodossa http/SSL:ssä ja sitä pidetään nykyään täysin turvallisena. Koska yksityinen avain ei koskaan lähde asiakkaan tietokoneelta, tämä menettely takaa, etteivät yhdistetyt tietokoneet - edes TeamViewerin reitittävät palvelimet - kykene lukemaan tietovirtaa.

Kukin TeamViewerin asiakas on jo saanut pääjoukon julkisen avaimen ja voi siksi salata viestejä pääjoukolle ja tarkastaa sen allekirjoittamia viestejä. PKI (Public Key Infrastructure) estää mies-välissä-hyökkäykset. Salauksesta huolimatta salasanaa ei koskaan lähetetä suoraan, vaan vain ehdollisella menettelyllä, ja se tallennetaan vain paikalliselle tietokoneelle.

Todennuksen aikana salasanaa ei koskaan siirretä suoraan, koska käytössä on SRP (Secure Remote Password)-protokolla. Vain salasanan vahvistin tallennetaan paikalliselle tietokoneelle.



TeamViewer salaus ja todennus

TeamViewerin tunnusten vahvistaminen

TeamViewrin tunnukset perustuvat eri kaluston ja ohjelmiston ominaisuuksiin ja ne luodaan automaattisesti TeamViewerissä. TeamViewerin palvelimet vahvistavat tunnukset ennen jokaista yhdistämistä.

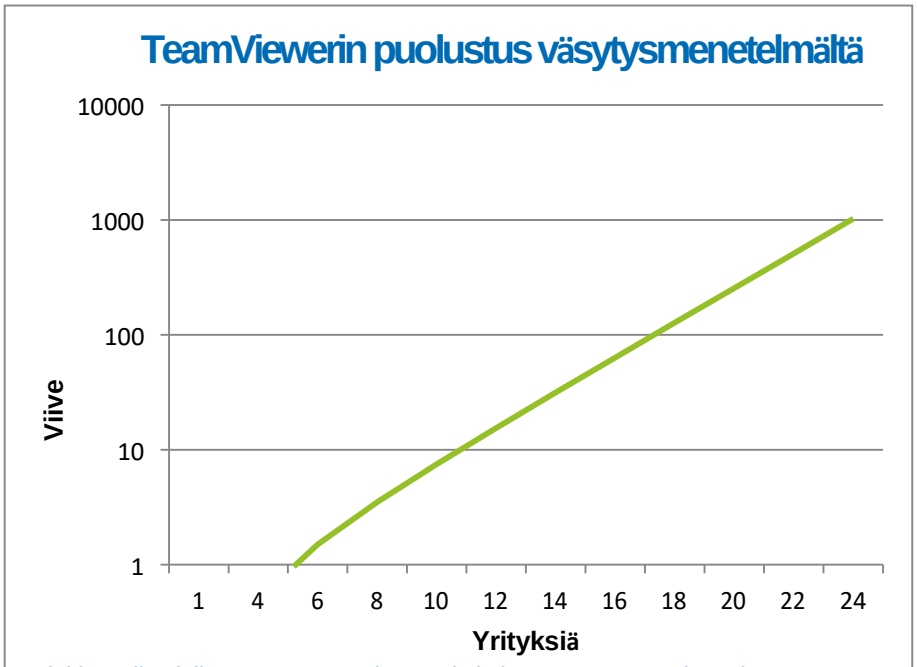
Suoja väsytysmenetelmältä

Mahdolliset TeamViewerin asiakkaat usein kysyvät salauksesta. Ymmärrettävästi eniten pelätään, että ulkopuoliset pääsevät vahtimaan tai tallentamaan TeamViewerissä kulkevia tietoja. Todellisuudessa alkukantaisimmat hyökkäykset ovat yleensä vaarallisimpia.

Väsytysmenetelmällä pyritään arvaamaan suojaava salasana. Tietokoneiden tehon kasvaessa on pitkien salasanojen arvaamiseen tarvittava aika vähentynyt.

TeamViewer nostaa jatkuvasti aikavälejä yhteysyritysten välillä väsytysmenetelmää estääkseen. Se voi siis viedä jopa 17 tuntia 24 yritykselle. Hidastus lopetetaan vasta, kun oikea salasana on annettu.

TeamViewerillä on välineet asiakkaidensa suojelemiseksi tietyltä tai usealta tietokoneelta (”botnet”) tulevilta, tiettyä TeamViewer-tunnusta tavoittelevilta hyökkäyksiltä.



Taulukko: Viive jälkeen n määrän yhteysyrityksiä väsytysmenetelmää käyttäen

Koodien suojeleminen

Lisää turvallisuutta tuo kaikkien ohjelmiemme suojelu VeriSignillä (VeriSign Code Signing). Tämän ansiosta ohjelmiston julkaisija on aina helppo tunnistaa. Digitaalinen allekirjoitus menettää automaattisesti pätevyytensä, jos ohjelmaa on muutettu jälkikäteen.

Palvelinkeskukset & selkäranka

Turvallisuuden takaamiseksi sijaitsevat kaikki TeamViewerin palvelimet palvelinkeskuksissa, jotka noudattavat ISO 27001, ja joissa on erityisesti varayhteyksin turvatut yhteydet ja virtalähteet. Lisäksi käytämme uusinta laadukasta kalustoa. Kaikki arkaluontoisia tietoja varastoivat palvelimet sijaisevat Saksassa ja Itävallassa.

ISO 27001 vaatii henkilöiden pääsyn rajoitusta, videokameravalvontaa, liiketunnistimia, 24x7 valvontaa ja paikalla vahtivaa turvallisuushenkilökuntaa. Näin varmistetaan, että palvelinkeskukselle pääsevät vain valtuutetut henkilöt. Näin voimme taata parhaan mahdollisen turvallisuuden kalustolle ja tiedoille. Tulijoiden henkilöllisyys tarkastetaan ainoalla sisäänkäynnillä palvelinkeskuksella.

TeamViewer-tili

TeamViewerin tilit isännöidään erityisillä TeamViewerin palvelimilla. Katso tietoja pääsyrajoituksista kohdasta Palvelinkeskukset & selkäranka yllä. Todennukseen ja salasanojen salaukseen käytetään SRP (Secure Remote Password protocol), joka on laajennus salasanojen vahvistussopimus (PAKE) -protokollasta. Soluttautuja tai mies välissä ei voi kerätä kylliksi tietoja kyetäkseen salasanan arvaamiseen väsytysmenetelmällä. Näin saadaan vahva turvallisuus jopa käytettäessä heikkojasalasanoja. Arkaluontoiset tiedot TeamViewer-tilillä, kuten kirjautumistiedot pilveen, tallennetaan ES/RSA 2048 bitin salauksella.

Hallintakonsoli

TeamViewerin hallintakonsoli on verkkopohjainen alusta käyttöhallinnalle, yhteysraportoinnille ja tietokoneiden ja kontaktien hallinnoille. Se isännöidään ISO-27001:n ja HIPAA:n mukaisissa palvelinkeskuksissa. Kaikki tiedonsiirrot tunneloidaan turvallisesti käyttäen TSL (Transport Security Layer) -salausta, joka on norminmukainen turvallisille verkkoyhteyksille. Arkaluontoiset tiedot tallennetaan lisäksi AES/RSA 2048 bitin salauksella. Todennukseen ja salasanojen salaukseen käytetään SRP:tä (Secure Remote Password protocol). SRP on tunnustettu, toimiva ja varma salasana-pohjainen todennus-ja avainten vaihdon menetelmä, joka käyttää 2048 bitin modulilla.

Käytäntökohtaiset asetukset

TeamViewering hallintakonsolista käyttäjät voivat määrittää, jakaa ja käyttää asetuskäytäntöjä TeamViewerin ohjelmien asennuksille heidän omilla laitteillaan. Asetuskäytännöt ovat niitä luoneiden tilien digitaalisesti allekirjoittamia. Tämä takaa, että laitetta koskevat käytännöt voi asetella vain siihen kuuluvalta tililtä.

Sovellusten turvallisuus TeamViewerissä

Kiellettyjen ja pääsijöiden listat

Lisäturvallisuus rajaamalla pääsyn tietyille asiakkaille on tarpeen varsinkin, jos TeamVieweriä käytetään vartioimattomien tietokoneiden huoltoon (jolloin TeamViewer on asennettu Windows-palveluna).

Pääsylista-toiminnolla voit nimenomaisesti tarkentaa, mitkä TeamViewer-tunnukset ja/tai -tilit saavat pääsyn tietokoneelle. Kiellettyjen lista-toiminnolla voit estää tiettyjen TeamViewer-tunnusten ja -tilien pääsyn. Keskeinen pääsijälista on tarjolla ”käytäntökohtaisten asetusten” osana, ja sitä kuvataan yllä kohdassa ”Hallintakonsoli.”

Chatti- ja video-salaus

TeamViewer-tiliisi liittyy chatti-historioita, jotka salataan ja tallennetaan käyttäen samaa AES/RSA 2048 bitin salausta, jota kuvattiin yllä osassa ”TeamViewer-tili”. Kaikki chatti- ja video-liikenne on salattu päästä päähän käyttäen AES (256 bit) salausta.

Peittelemätön tila

TeamVieweriä ei millään toiminnolla voi käyttää pelkästään taustalla. TeamViewer näkyy aina vähintään kuvakkeena ilmaisinalueella, vaikka sen edessä pidettäisiinkin toista ikkunaa auki.

Yhteyden muodostuttua pieni ohjauspaneeli näkyy aina ilmaisinalueella. Näin tietokoneiden ja työntekijöiden salainen tarkkailu on TeamViewerillä tahallaan tehty vaikeaksi.

Salasanan suoja

Nopealle asiakaspalvelulle TeamViewer (TeamViewer QuickSupport) luo (kertakäyttöisen) salasanan. Jos asiakas antaa salasanansa, voit yhdistää sillä ja hänen tunnuksellaan hänen tietokoneeseensa. Kun TeamViewer on resetoitu asiakkaan puolella, uusi salasana luodaan, jotta voit asiakkaan pyynnöstä yhdistää hänen tietokoneisiinsa.

Kun otat TeamViewerin kauko-ohjattavaan käyttöön vartioimattomassa kohteessa (esim. palvelimeen), luot yksittäisen pysyvän salasanan, jolla takaat tietokoneelle pääsyn.

Sisääntulevan ja ulosmenevän pääsyn ohjaus

Voit konfiguroida yhteydet TeamVieweriin yksilöllisesti. Esimerkiksi voit konfiguroida etätukesi tai yhteystietokoneen siten, ettei sisääntulevia yhteyksiä sallita lainkaan.

Toiminnallisuuden rajaus tarvittuihin ominaisuuksiin vähentää hyökkäysten riskiä.

Kahden tekijän todennus

TeamViewer auttaa yrityksiä noudattamaan HIPAA ja PCI. Kahden tekijän todennus lisää turvallisuutta TeamViewerin tilien suojaamiseksi ulkopuolisilta.

Todennus vaatiii käyttäjänimen ja salasanan lisäksi koodin. Koodi luodaan ajoitetulla yhdenkertaisella (TOTO) algoritmilla. Koodi käy siksi vain lyhyen aikaa.

Kahden tekijän todennuksella ja suljetun pääsijälistan laatimisella TeamViewer auttaa HIPAA- ja PCI-sertifikaation saavuttamista.

Turvallisuuden kokeileminen

TeamViewerin infrastruktuuria ja ohjelmistoa kokeillaan tasaisin aikavälein. Kokeilut suorittavat erillisetyritykset, jotka erikoistuvat turvallisuuden kokeilemiseen.

Lisää kysyttävää?

Jos sinulla on lisää kysyttävää, ole hyvä ja soita meille +358 (0) 9 4241 9398 tai lähetä sähköpostia osoitteeseen support@teamviewer.com.

Yhteystiedot

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