„TeamViewer“ saugos informacija

Tikslinė grupė

Šis dokumentas skirtas profesionaliems tinklo administratoriams. Dokumente pateikta informacija yra ganėtinai techninio pobūdžio ir labai išsami. Remdamiesi šia informacija, IT profesionalai susidarys išsamų vaizdą apie „TeamViewer“ saugos standartus ir, prieš diegdami mūsų programinę įrangą, išspręs visus susirūpinimą keliančius dalykus. Galite laisvai platinti šį dokumentą savo klientams, kad palengvintumėte visų galimų su saugumu susijusių klausimų svarstymą.

Jei ir nemanote, kad priklausote tikslinei grupei, skyriuje „Bendrovė / programinė įranga“ pateiktos bendrosios žinios padės jums susidaryti aiškų vaizdą, kaip rimtai traktuojame saugumą.

Bendrovė / programinė įranga

Apie mus

„TeamViewer GmbH“ įsteigta 2005 metais. Ji įkurta Vokietijos pietuose, Gepingene (netoli Štutgarto), turi filialus Australijoje ir Jungtinėse Valstijose. Mes kuriame ir parduodame išimtinai tik saugos sistemas, skirtas bendradarbiauti internetu. Per trumpą laikotarpį mūsų „Freemium“ licencijavimas leido sparčiai išaugti ir pasiekti daugiau kaip 200 milijonų „TeamViewer“ grupių valdymo programos naudotojų, įdiegusių ją į daugiau kaip 1,4 milijardo įrenginių, pasklidusių po daugiau kaip 200 šalių visame pasaulyje. Programinė įranga prieinama daugiau kaip 30 kalbų.

Kaip mes suprantame saugumą?

„TeamViewer“ bet kuriuo paros metu naudojasi daugiau kaip 30 milijonų naudotojų. Kai tik prireikia, šie naudotojai teikia pagalbą internetu, jungdamiesi prie be žmogaus paliekamų veikti kompiuterių (t. y. atlikdami nuotolinę serverių priežiūrą) ir organizuodami internetinius susirinkimus. Atsižvelgiant į konfigūraciją, „TeamViewer“ gali būti naudojamas nuotoliniu būdu valdyti kitą kompiuterį taip, tarsi jūs patys sėdėtumėte tiesiai priešais jį. Jei prie nuotolinio kompiuterio prisijungęs naudotojas yra „Windows“, „Mac“ arba „Linux“ administratorius, šiam asmeniui bus suteiktos ir to kompiuterio administratoriaus teisės.

Aišku, kad potencialiai nesaugiu internetu veikiančios tokios galingos funkcijos turi būti itin kruopščiai apsaugotos nuo atakų. Iš tiesų saugumo tema dominuoja tarp visų mūsų projektavimo tikslų ir yra tai, kuo mes gyvename ir kvėpuojame, atlikdami visas savo užduotis. Mes norime užtikrinti, kad prieiga prie jūsų kompiuterio būtų saugi, ir apsaugoti savo pačių interesus: milijonai naudotojų visame pasaulyje pasitikės tik saugiu sprendimu ir tik saugus sprendimas užtikrins ilgalaikę mūsų verslo sėkmę.

Išorinių ekspertų vertinimas

Mūsų programinei įrangai „TeamViewer“ Federacinė IT ekspertų ir apžvalgininkų asociacija (*Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.*) suteikė penkių žvaigždučių kokybės ženklą (aukščiausią įvertinimą). Nepriklausomi *BISG e.V.* apžvalgininkai tikrina kvalifikuotų gamintojų produktų kokybę, saugumą ir veikimo charakteristikas.

Nuorodos

Šiuo metu „TeamViewer“ grupių valdymo programa naudojasi daugiau kaip 200 milijonų naudotojų. Pirmaujančios tarptautinės visų ūkio šakų (įskaitant tokius ypač jautrius sektorius kaip bankininkystė, finansai, sveikatos apsauga ir vyriausybinės institucijos) bendrovės sėkmingai naudojasi „TeamViewer“.

Kviečiame pažvelgti į mūsų po visą internetą surastus šaltinius, kad susidarytumėte pirmąjį įspūdį apie tai, koks priimtinas yra mūsų sprendimas. Pamatysite, kad tikriausiai dauguma kitų bendrovių kėlė panašius saugumo ir patikimumo reikalavimus, kol po intensyvios analizės pagaliau pasirinko „TeamViewer“. O kad susidarytumėte įspūdį, likusioje šio dokumento dalyje susipažinkite su kai kuriais techniniais duomenimis.

„TeamViewer“ seansai

Kaip sukurti seansą ir ryšių tipus?

Kai inicijuojamas seansas, „TeamViewer“ nustato optimalų ryšio tipą. Kai patvirtinama iš mūsų pagrindinių serverių, 70 proc. visų atvejų nustatomas tiesioginis sujungimas naudojantis UDP arba TCP (netgi už standartinių šliuzų, NAT ir užkardų). Likę sujungimai siunčiami per mūsų didelio perteklumo maršruto parinktuvų tinklą naudojantis TCP arba https tuneliavimu. Kad galėtumėte dirbti su „TeamViewer“, jums nereikės atverti kokių nors prievadų.

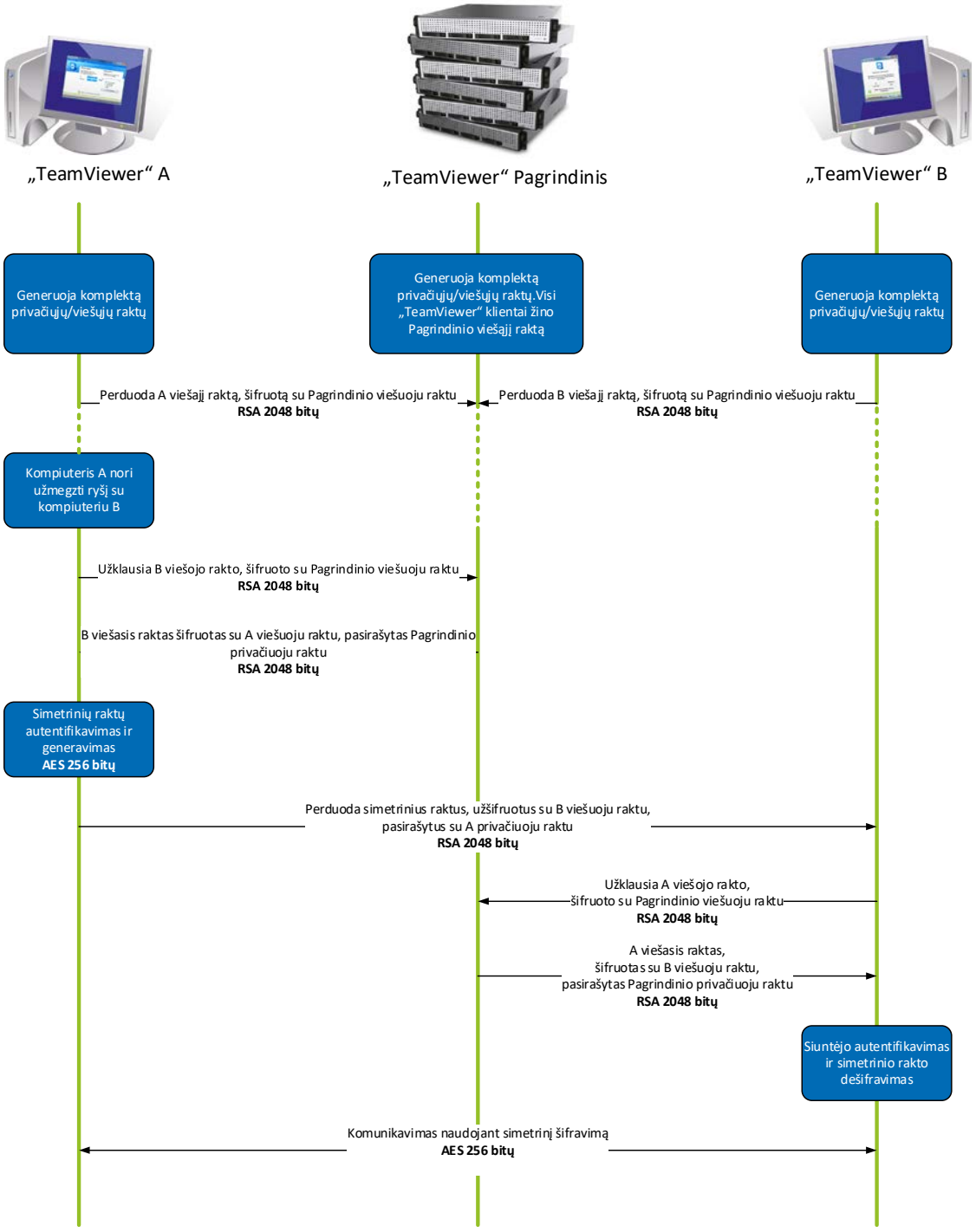
Kaip aprašyta toliau dalyje „Šifravimas ir tapatybės nustatymas“, net ir mes, kaip siuntimo serverių operatoriai, negalime perskaityti šifruotų duomenų srauto.

Šifravimas ir tapatybės nustatymas

„TeamViewer“ srautui apsaugoti naudojami RSA viešųjų / privačiųjų raktų mainai ir AES (256 bitų) seanso šifravimas. Ši technologija naudojama http / SSL prilyginama forma ir pagal šiandienius standartus laikoma visiškai saugia. Kadangi privatusis raktas iš kliento kompiuterio niekaip nėra siunčiamas, šia procedūra užtikrinama, kad tarpiniuose kompiuteriuose – įskaitant „TeamViewer“ siuntimo serverius – nebūtų galima iššifruoti duomenų srauto.

Kiekvienas „TeamViewer“ klientas jau turi įdiegtą viešąjį pagrindinio blokinio raktą ir taip gali šifruoti į pagrindinį blokinį siunčiamus pranešimus, tikrinti jo pasirašytus pranešimus. PKI (angl. *Public Key Infrastructure* – viešųjų raktų infrastruktūra) efektyviai apsaugo nuo įsiterpusio įsibrovėlio atakų. Šifravimo slaptažodis niekada nesiunčiamas tiesiogiai, o tik taikant patvirtinimo–atsakymo (angl. *challenge-response*) procedūrą, ir saugomas tik vietiniame kompiuteryje.

Nustatant tapatybę slaptažodis niekada neperduodamas tiesiogiai, nes naudojamas saugaus nuotolinio slaptažodžio (angl. *Secure Remote Password*, SRP) protokolas. Vietiniame kompiuteryje saugomas tik slaptažodžio tikrintuvas.



„TeamViewer“ šifravimas ir tapatybės nustatymas

„TeamViewer“ identifikatorių tikrinimas

„TeamViewer“ identifikatoriai pagrįsti įvairiomis aparatinės ir programinės įrangos charakteristikomis ir yra automatiškai generuojami „TeamViewer“. Prieš kiekvienąkart sujungiant „TeamViewer“ serveriuose tikrinamas šių identifikatorių tinkamumas.

Apsauga jėgos metodu

Būsimieji klientai, kurie teiraujasi apie „TeamViewer“ saugumą, reguliariai klausia apie šifravimą. Suprantama, pavojus, kad trečioji šalis galėtų stebėti sujungimą arba kad gali būti perimti „TeamViewer“ prieigos duomenys, gąsdina labiausiai. Tačiau tikrovė yra tokia, kad dažnai pavojingiausios būna gana primityvios atakos.

Kompiuterinės saugos kontekste jėgos metodo ataka yra bandymų ir klaidų metodas siekiant atspėti išteklius saugantį slaptažodį. Auganti standartinių kompiuterių skaičiavimo galia vis trumpina laiką, kurio reikia ilgiems slaptažodžiams atspėti.

Kaip apsaugą nuo atakų jėgos metodu „TeamViewer“ eksponentiškai ilgina laukimą tarp prisijungimo bandymų. Taip 24 bandymams prireiks net 17 valandų. Ši delsa anuliuojama tik sėkmingai įvedus teisingą slaptažodį.

„TeamViewer“ geba ne tik apsaugoti savo klientus nuo atakų iš vieno konkretaus kompiuterio, bet ir nuo daugybės kompiuterių. Tokios atakos vadinamos botų tinklo atakomis, jomis mėginama pasiekti vieną tam tikrą „TeamViewer“ identifikatorių.

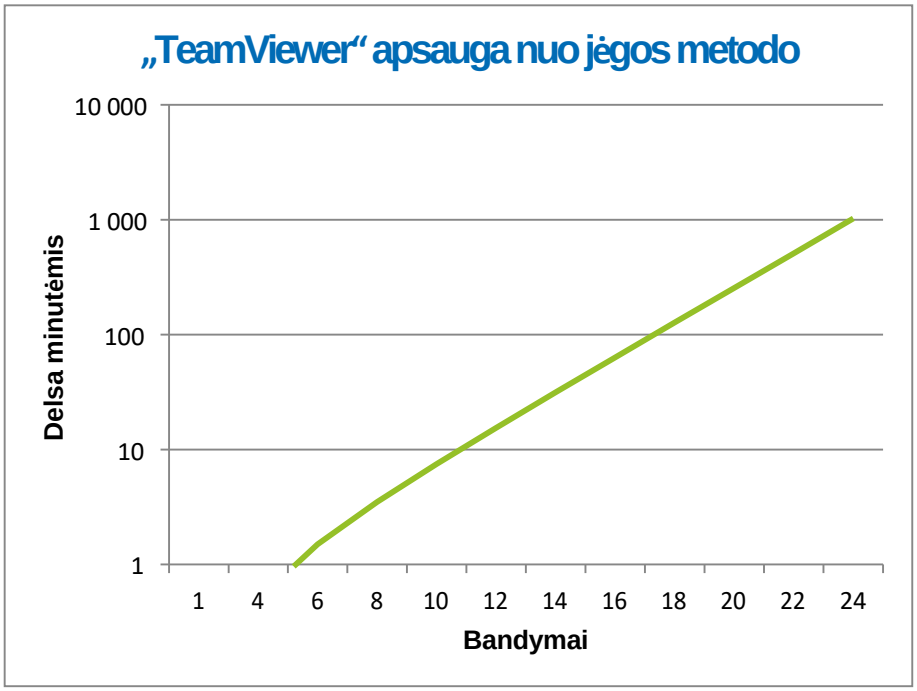


Diagrama: Laikas, praeinantis po n prisijungimo bandymų vykstant atakai jėgos metodu

Pasirašytas kodas

Kaip papildoma saugumo priemonė, visa mūsų programinė įranga pasirašyta „VeriSign Code Signing“ kodo parašu. Taip šios programinės įrangos leidėją visuomet paprasta identifikuoti. Jei programinė įranga vėliau pakeičiama, skaitmeninis parašas automatiškai tampa negaliojantis.

Duomenų centrai ir pagrindinis tinklas

Kad užtikrintų geriausią įmanomą „TeamViewer“ paslaugų saugumą ir patikimumą, visi „TeamViewer“ serveriai įrengti su ISO 27001 suderintuose duomenų centruose, turinčiuose daug kartų perteklinius sujungimus su perdavimo terpe ir perteklinius maitinimo šaltinius. Be to, naudojama tik moderniausia pripažintų gamintojų aparatinė įranga. Ir dar – visi serveriai, kuriuose saugomi jautrūs duomenys, yra įrengti Vokietijoje arba Austrijoje.

Suteiktas ISO 27001 sertifikatas reiškia, kad tai, jog prieiga prie duomenų centro būtų suteikta tik įgaliotiesiems asmenims ir būtų garantuojamas geriausias įmanomas aparatūros ir duomenų saugumas, yra užtikrinama asmeninės prieigos valdymu, stebėjimu vaizdo kameromis, judesio detektoriais, 24 x 7 stebėjimu ir vietoje dirbančio saugos personalo veikla. Be to, prie vienintelio įėjimo į duomenų centrą punkto vykdoma išsami identifikacinė patikra.

„TeamViewer“ paskyra

„TeamViewer“ paskyros laikomos tam skirtuose „TeamViewer“ serveriuose. Informaciją apie prieigos valdymą rasite ankstesniame skyriuje „Duomenų centrai ir pagrindinis tinklas“. Prieigai suteikti ir slaptažodžiams šifruoti naudojamas saugaus nuotolinio slaptažodžio (angl. *Secure Remote Password*, SRP) protokolas – tai išplėstas slaptažodžiu patvirtintos sutarties dėl rakto naudojimo (angl. *password-authenticated key agreement*, PAKE) protokolas. Įsilaužėlis arba įsiterpęs įsibrovėlis negali surinkti pakankamai informacijos, kad sugebėtų jėgos metodu atspėti slaptažodį. Tai reiškia, kad patikimą saugumą galima pasiekti net ir naudojant silpnus slaptažodžius. Jautrūs „TeamViewer“ paskyros duomenys, pavyzdžiui, registravimosi prie debesijos saugyklos informacija, saugomi šifruoti AES / RSA 2 048 bitų algoritmu.

Valdymo terminalas

„TeamViewer“ valdymo terminalas yra internetinė platforma, skirta valdyti naudotojams, teikti ataskaitoms apie ryšį ir administruoti kompiuteriams ir kontaktams. Jis laikomas pagal ISO-27001 sertifikuotuose, su HIPAA suderinamuose duomenų centruose. Visas duomenų perdavimas vyksta saugiu kanalu naudojant TSL (angl. *Transport Security Layer* – perdavimo saugos lygmens) šifravimą, standartinį saugiems interneto tinklo ryšiams. Be to, jautrūs duomenys saugomi šifruoti AES / RSA 2 048 bitų algoritmu. Prieigai ir slaptažodžių šifravimui naudojamas saugaus nuotolinio slaptažodžio (SRP) protokolas. SRP yra gerai organizuotas, atsparus, saugus slaptažodžiais pagrįstas tapatybės nustatymo ir apsikeitimo raktais metodas, kuriam naudojamas 2 048 bitų modulis.

Strategija pagrįstos nuostatos

„TeamViewer“ valdymo terminale naudotojai gali apibrėžti, platinti ir įgyvendinti nuostatų strategijas konkrečiai jiems priklausančiuose įrenginiuose įdiegtai „TeamViewer“ programinei įrangai. Nuostatų strategijos skaitmeniniu būdu pasirašomos jas sugeneravusios paskyros. Taip užtikrinama, kad vienintelė paskyra, iš kurios leidžiama priskirti įrenginiui strategiją, būtų paskyra, kuriai tas įrenginys priklauso.

„TeamViewer“ programos saugumas

Juodasis ir baltasis sąrašai

Konkrečiu atveju, jei „TeamViewer“ naudojamas prižiūrėti be žmogaus buvimo paliekamiems veikti kompiuteriams (t. y. „TeamViewer“ įdiegiamas kaip „Windows“ tarnyba), gali būti įdomi papildoma saugumo parinktis, kuria prieiga prie šių kompiuterių apribojama keletu specifinių klientų.

Naudojantis baltojo sąrašo funkcija galima tiksliai nurodyti, kuriems „TeamViewer“ identifikatoriams ir (arba) kurioms „TeamViewer“ paskyroms leidžiama prieiga prie kompiuterio. Juodojo sąrašo funkcija galima blokuoti tam tikrus „TeamViewer“ identifikatorius ir tam tikras „TeamViewer“ paskyras. Centrinis baltasis sąrašas prieinamas kaip strategija pagrįstų nuostatų, aprašytų ankstesniame skyriuje „Valdymo terminalas“, dalis.

Pokalbių ir vaizdo šifravimas

Pokalbių istorija yra susieta su jūsų „TeamViewer“ paskyra, todėl šifruojama ir saugoma naudojant tą pačią AES / RSA 2 048 bitų šifravimo apsaugą, aprašytą skyriuje „TeamViewer“ paskyra“. Visos pokalbio žinutės ir vaizdo srautas šifruojami visoje linijoje naudojant AES (256 bitų) seanso šifravimą.

Nėra paslėpto režimo

Nėra funkcijos, kuria būtų leidžiama „TeamViewer“ veikti visiškai foniniu režimu. Net jei programa veikia fone kaip „Windows“ tarnyba, „TeamViewer“ visuomet matoma kaip piktograma sistemos dėkle.

Užmezgus ryšį, mažas valdymo skydelis visuomet matomas virš sistemos dėklo. Taip „TeamViewer“ specialiai padaryta netinkama slapta stebėti kompiuteriams ar darbuotojams.

Apsauga slaptažodžiu

Nenumatytai prireikus suteikti pagalbą klientui, „TeamViewer“ („TeamViewer QuickSupport“) generuojamas seanso slaptažodis (vienkartinis slaptažodis). Jei jūsų klientas pasakys jums savo slaptažodį, galėsite prisijungti prie jo kompiuterio įvedę jo identifikatorių ir slaptažodį. Kliento pusėje paleidus „TeamViewer“ iš naujo, bus sugeneruotas naujas seanso slaptažodis, taigi prisijungti prie savo kliento kompiuterių galėsite tik tuomet, kai būsite pakviesti tai padaryti.

Kai „TeamViewer“ diegiama be žmogaus veikiančių nuotolinių kompiuterių (pvz., serverių) priežiūrai, nustatomas individualus fiksuotas slaptažodis, kuriuo apsaugoma prieiga prie to kompiuterio.

Gaunamosios ir išsiunčiamosios prieigos valdymas

Galima individualiai konfigūruoti „TeamViewer“ ryšio režimus. Pavyzdžiui, nuotolinei pagalbai arba susirinkimams skirtą kompiuterį galima sukonfigūruoti taip, kad gaunamieji ryšiai būtų negalimi.

Kai funkcijos apribojamos šiomis iš tikrųjų būtinomis priemonėmis, tai reiškia, kad apribojami galbūt silpni prieš potencialias atakas taškai.

Dviejų dalių tapatumo nustatymas

„TeamViewer“ padeda bendrovėms, kuriose keliami atitikties HIPAA ir PCI reikalavimai. Dviejų dalių tapatumo nustatymu įtraukiamas papildomas saugumo lygmuo, saugantis „TeamViewer“ paskyras nuo nesankcionuotosios prieigos.

Kad patvirtintų tapatybę, greta naudotojo vardo ir slaptažodžio naudotojas turi įvesti kodą. Šis kodas generuojamas taikant terminuoto vienkartinio slaptažodžio (angl. *time-based one-time password*, TOTP) algoritmą. Todėl toks kodas galioja tik trumpą laiko tarpą.

Taikanti dviejų dalių tapatumo nustatymą ir baltaisiais sąrašais ribojanti prieigą, „TeamViewer“ padeda tenkinti visus būtinus HIPAA ir PCI sertifikavimo kriterijus.

Saugumo bandymai

Tiek su „TeamViewer“ infrastruktūra, tiek su „TeamViewer“ programine įranga reguliariai atliekami prasiskverbimo bandymai. Šiuos bandymus atlieka nepriklausomos bendrovės, kurių specializacija – vykdyti saugumo bandymus.

Ar kilo daugiau klausimų?

Užduoti klausimų ar paprašyti informacijos galite kreipdamiesi į+49 (0) 7161 60692 50
arba išsiuntę el. laišką adresu support@teamviewer.com.

Kontaktai

„TeamViewer GmbH“
Jahnstr. 30
D-73037 Gepingenas
Vokietija
service@teamviewer.com