Bezbednosne informacije za TeamViewer

Ciljna grupa

Ovaj dokument je namenjen za profesionalne administratore mreže. Informacije u ovom dokumentu su krajnje tehničke prirode i veoma su detaljne. Na osnovu ovih informacija IT stručnjaci dobijaju detaljnu sliku bezbednosnih standarda u programu TeamViewer, a sve nedoumice se rešavaju pre instalacije našeg softvera. Slobodno delite ovaj dokument klijentima da biste ublažili sve moguće nedoumice po pitanju bezbednosti.

Ako ne smatrate da ste deo ciljne grupe, činjenice o softveru u odeljku Kompanija /softver i dalje će vam biti od pomoći da steknete jasan uvid u to koliko ozbiljno pristupamo pitanju bezbednosti.

Kompanija/softver

O nama

TeamViewer GmbH osnovan je 2005. godine i ima sedište u južnoj Nemačkoj, u gradu Gepingenu (blizu Štutgarta), sa podružnicama u Australiji i Sjedinjenim Državama. Isključivo razvijamo i prodajemo bezbednosne sisteme za saradnju bazirane na mreži. U kratkom vremenskom roku naše izdavanje licenci Freemium dovelo je do brzog rasta, sa više od 200 miliona korisnika softvera TeamViewer na više od 1,4 milijarde uređaja, u više od 200 zemalja širom planete. Softver je dostupan na više od 30 jezika.

Naše poimanje bezbednosti

TeamViewer koristi više od 30 miliona korisnika u svakom trenutku u toku dana. Ovi korisnici spontano pružaju podršku putem interneta, pristupajući računarima bez nadzora (npr. daljinska podrška za servere) i organizujući onlajn sastanke. U zavisnosti od konfiguracije TeamViewer može da se koristi za daljinsko upravljanje drugim računarom, kao da sedite direktno ispred njega. Ako je korisnik koji je prijavljen na udaljenom računaru administrator za Windows, Mac ili Linux, ovoj osobi će biti odobrena prava administratora i na tom računaru.

Jasno je da tako snažna funkcionalnost nad potencijalno nebezbednom internetu mora da se zaštiti od napada uz ozbiljan nadzor. Zapravo, tema bezbednosti dominira nad svim našim razvojnim ciljevima i to je nešto po čijem principu živimo i dišemo u svemu što radimo. Želimo da zagarantujemo da pristup vašem računaru bude bezbedan i da zaštitimo svoje interese: milioni korisnika širom sveta veruju jedino bezbednom rešenju, a samo bezbedno rešenje garantuje naš dugoročni uspeh kao kompanije.

Eksterna procena stručnjaka

Našem softveru, TeamViewer, dodeljen je pečat za kvalitet od pet zvezdica (maksimalna vrednost) od strane Federalnog udruženja IT stručnjaka i revizora (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.). Nezavisni revizori udruženja BISG e.V. pregledaju proizvode kvalifikovanih proizvođača po pitanju karakteristika koje se tiču kvaliteta, bezbednosti i usluge.

Reference

Trenutno TeamViewer koristi više od 200 miliona korisnika. Vodeće međunarodne korporacije iz svih industrijskih oblasti (uključujući i izuzetno osetljive sektore, poput bankarstva, finansija, zdravstvene nege i vlade) uspešno koriste TeamViewer.

Pozivamo vas da pogledate naše reference koje se mogu naći svuda na internetu da biste stekli prvi utisak po pitanju prihvatanja našeg rešenja. Uvidećete da je verovatno većina drugih kompanija imala slične zahteve po pitanju bezbednosti i dostupnosti pre nego što su se – nakon intenzivne istrage – konačno odlučili za TeamViewer. Ipak, da biste stekli sopstveni utisak, pronađite neke tehničke detalje u preostalom delu ovog dokumenta.

Sesije programa TeamViewer

Kreiranje sesije i vrste povezivanja

Prilikom uspostavljanja sesije TeamViewer odlučuje koja je idealna vrsta povezivanja. Nakon rukovanja putem našeg glavnog servera, direktno povezivanje putem UDP ili TCP uspostavlja se u 70% svih slučajeva (čak i iza standardnih mrežnih prolaza, NAT-ova i zaštitnih zidova). Preostala povezivanja se sprovode kroz našu izuzetno pouzdanu mrežu za preusmeravanje putem TCP ili https tunela. Ne morate da otvarate nijedan priključak da biste radili u programu TeamViewer

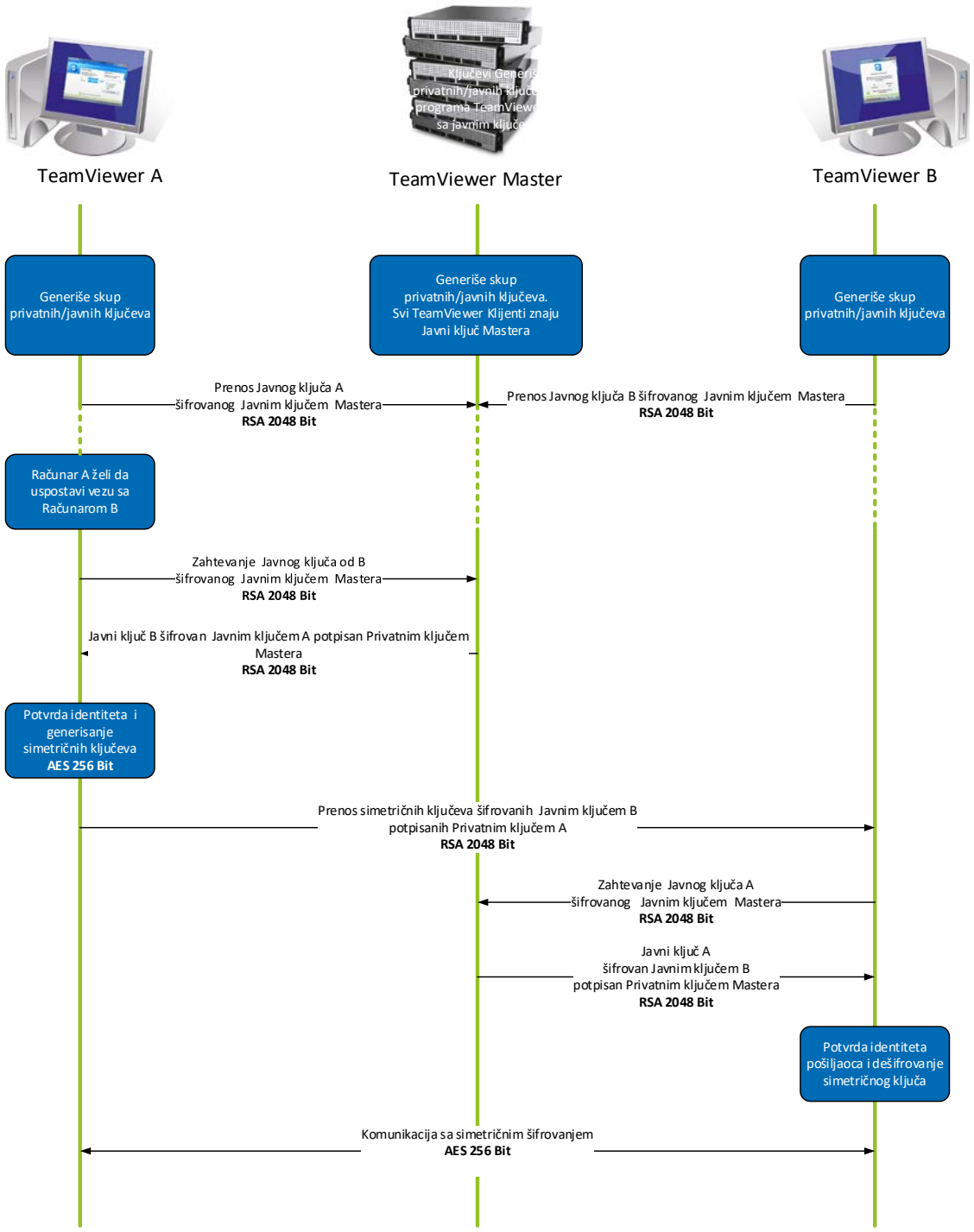
Kako je dalje opisano u odeljku Šifriranje i provera identiteta, čak ni mi, kao operatori servera za usmeravanje, ne možemo da očitamo saobraćaj šifriranih podataka.

Šifriranje i provera identiteta

Saobraćaj putem programa TeamViewer obezbeđen je korišćenjem razmene RSA javnog/privatnog ključa i AES (256-bitnog) šifriranja sesije. Ova tehnologija se koristi u uporednom obliku za http/SSL i smatra se da je potpuno bezbedna na osnovu današnjih standarda. Kako privatni ključ nikada ne napušta računar klijenta, ova procedura garantuje da međusobno povezani računari – uključujući servere za usmeravanje programa TeamViewer – ne mogu da dešifruju protok podataka.

Svaki klijent programa TeamViewer već je implementirao javni ključ glavne grupe i stoga može da šifruje poruke upućene glavnoj grupi i da proveri poruke sa njenim potpisom. PKI (infrastruktura javnog ključa) efikasno sprečava napade u koje je uključeno neko lice. Uprkos šifriranju lozinka se nikada ne šalje direktno već putem procedure koja uključuje „izazov” i „odgovor” i čuva se samo na lokalnom računaru.

Tokom provere identiteta lozinka se nikada direktno ne šalje jer se primenjuje protokol za bezbednosnu daljinsku lozinku (SRP). Samo proverena lozinka se skladišti na lokalnom računaru.



šifriranje i provera identiteta u programu TeamViewer

Potvrđivanje ID-jeva programa TeamViewer

ID-jevi programa TeamViewer zasnivaju se na karakteristikama hardvera i softvera i automatski ih generiše TeamViewer. Serveri programa TeamViewer proveravaju ispravnost ovih ID-jeva pre svakog povezivanja.

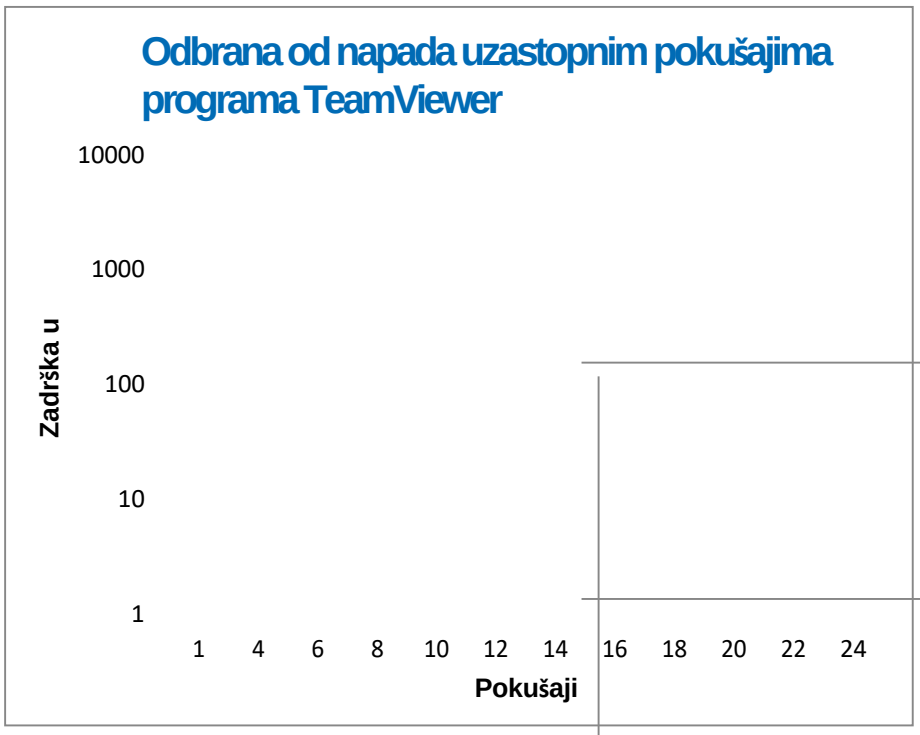
Zaštita od napada uzastopnim pokušavanjem

Potencijalni klijenti koji se interesuju za bezbednost programa TeamViewer redovno se raspituju o šifriranju. Razumljivo je da je ono čega se najviše plaše opasnost od toga da treća strana može da nadgleda povezivanje ili da pristupni podaci programa TeamViewer budu kompromitovani. Međutim, u praksi su krajnje primitivni napadi često i najopasniji.

U kontekstu bezbednosti računara, *brute-force* napad je metoda po principu pokušaja i greške sa ciljem nagađanja lozinke koja štiti neki resurs. Uz sve veću moć izračunavanja standardnih računara vreme koje je potrebno da se pogodi dugačka lozinka postaje sve kraće.

Kao zaštita od napada uzastopnim pokušajima TeamViewer neprekidno produžava zadršku između pokušaja povezivanja. Stoga je potrebno čak 17 sati za 24 pokušaja. Kašnjenje se resetuje tek nakon uspešnog unošenja tačne lozinke.

TeamViewer ne samo da ima na raspolaganju mehanizam za zaštitu klijenata od napada sa jednog konkretnog računara, već i sa više računara, koji su poznati i kao *botnet* napadi, kojima se pokušava pristup jednom određenom ID-u programa TeamViewer.



Grafikon: Vreme proteklo od n pokušaja povezivanja tokom napada uzastopnim pokušajima

Potpisivanje koda

Kao dodatno bezbednosno svojstvo, naš celokupan softver se potpisuje putem potpisivanja koda VeriSign. Na taj način izdavač softvera se uvek jednostavno identifikuje. Ako se softver naknadno izmeni, digitalni potpis automatski postaje nevažeći.

Centri za podatke i kičma

Da bi se omogućila najbolja moguća bezbednost i dostupnost usluga programa TeamViewer, svi serveri programa TeamViewer smešteni su u centrima za podatke koji su u skladu sa standardom ISO 27001 i maksimalno koriste povezivanja putem višestruko pouzdanih nosača i pouzdana napajanja. Uz to, koriste se samo najmoderniji brendovi hardvera. Uz to, svi serveri koji skladište delikatne podatke smešteni su u Nemačkoj ili Austriji.

Usklađenost sa standardom ISO 27001 podrazumeva da lični pristup upravljanju, nadzor video kamerom, detektori pokreta, nadzor tokom 24 časa 7 dana u nedelji i bezbednosno osoblje na lokaciji garantuju da se pristup centru za podatke odobrava isključivo ovlašćenim licima uz zagarantovanu najbolju moguću bezbednost hardvera i podataka. Postoji i detaljna provera identiteta pri pojedinačnoj tački pristupa centra za podatke.

Nalog TeamViewer

Nalozi TeamViewer uskladišteni su na namenskim serverima TeamViewer. Za informacije po pitanju kontrole pristupa pogledajte gorenavedeni odeljak Centar za podatke i kičma. Za davanje dozvole i šifriranje lozinke, primenjuje se protokol za bezbednu daljinsku lozinku (SRB), prošireni protokol za slaganje ključa sa proverom lozinke (PAKE). Napadač ili lice koje posreduje ne može da dobije dovoljno informacija da bi mogao da pogodi lozinku uzastopnim pokušajima. To znači da se snažna bezbednost može postići čak i korišćenjem slabih lozinki. Delikatni podaci u sklopu TeamViewer naloga, na primer skladištenje informacija za prijavu na računarskom oblaku, skladište se AES/RSA 2048-bitnim šifriranjem.

Konzola za upravljanje

Konzola za upravljanje TeamViewer je veb-platforma za upravljanje korisnika, izveštavanje o povezivanju i upravljanje računarima i kontaktima. Skladišti se u centrima za podatke koji su u skladu sa standardom ISO-27001 i HIPAA. Celokupan prenos podataka obavlja se putem bezbednog kanala korišćenjem TSL (bezbednosnog sloja za transport) šifriranja, standarda za bezbedna povezivanja mreže sa internetom. Delikatni podaci se zatim skladište šifrirani pomoću AES/RSA 2048-bitnog šifriranja. Za dobijanje dozvole i šifriranje lozinke primenjuje se protokol za bezbednu daljinsku lozinku (SRP). SRP je dobro uspostavljena, snažna, bezbedna metoda za proveru identiteta na osnovu lozinke i razmene ključa koja koristi 2048-bitni modulus.

Podešavanja na osnovu pravila

Iz TeamViewer konzole za upravljanje korisnici mogu da definišu, distribuiraju i sprovode pravila za podešavanje za instalacije softvera TeamViewer na uređajima koji posebno pripadaju njima. Pravila podešavanja nose digitalni potpis naloga koji ih je generisao. To osigurava da je jedini nalog sa dozvolom za dodeljivanje pravila uređaju nalog kome uređaj pripada.

Bezbednost aplikacija i TeamViewer-u

Crna i bela lista

Naročito u slučaju da se TeamViewer koristi za održavanje računara bez nadzora (tj. TeamViewer je instaliran kao Windows servis), dodatna opcija bezbednosti za ograničavanje pristupa ovim računarima na određeni broj specifičnih klijenta može biti interesantna.

Uz funkciju bele liste možete isključivo da naznačite koji TeamViewer ID-jevi i/ili koji TeamViewer nalozi imaju pravo da pristupe računaru. Uz funkciju crne liste, možete da blokirate određene TeamViewer ID-jeve i TeamViewer naloge. Centralna bela lista je dostupna kao deo „podešavanja na osnovu pravila" koja su opisana iznad u odeljku „Konzola za upravljanje".

Ćaskanje i video šifriranje

Istorije ćaskanja su povezane sa vašim TeamViewer nalogom i stoga se šifriraju i skladište koristeći istu 2048-bitnu bezbednost šifriranja AES/RSA kao što je opisano u odeljku „TeamViewer nalog". Sve poruke ćaskanja i video saobraćaj se šifriraju u potpunosti koristeći AES (256-bitno) šifriranje sesije.

Nema nevidljivog režima

Nema funkcije koja vam omogućava da TeamViewer radi u potpunosti u pozatini. Čak i ako aplikacija radi kao Windows servis u pozadini, TeamViewer je uvek vidljiv putem ikonice na sistemskoj paleti.

Nakon upostavljanja veze uvek postoji mala kontrolna tabla iznad sistemske palete. Stoga, TeamViewer predviđeno nije pogodan za tajni nadzor računara ili zaposlenih.

Zaštita lozinkom

Za spontanu korisničku podršku TeamViewer (TeamViewer QuickSupport) generiše lozinku za sesiju (jednokratna lozinka). Ako vam korisnik kaže svoju lozinku, možete da se povežete sa njegovim/njenim računarom unošenjem njihovog ID-ja i lozinke. Nakon restartovanja TeamViewer-a na strani korisnika, generisaće se nova lozinka za sesiju tako da se samo vi možete povezati sa računarom korisnika ako ste pozvani.

Prilikom instalacije programa TeamViewer za nenadgledanu daljinsku podršku (npr. za servere), podešavate pojedinačnu, nepromenljivu lozinku koja omogućava pristup računaru.

Kontrola dolaznog i odlaznog pristupa

Pojedinačno možete da podesite režime veze za TeamViewer. Na primer, možete da podesite svoj računar za daljinsku podršku ili sastanke tako da dolazne veze nisu moguće.

Ograničavanje funkcija na funkcije koje su stvarno potrebne podrazumeva ograničavanje mogućih slabih tačaka za potencijalne napade.

Provera identiteta uz dva faktora

TeamViewer pomaže kompanijama u zadovoljavanju zahteva za usklađenost sa HIPAA i PCI. Provera identiteta uz dva faktora donosi dodatni nivo bezbednosti za zaštitu TeamViewer naloga od neovlašćenog pristupa.

Pored korisničkog imena i lozinke, korisnik mora da unese šifru da bi potvrdio identitet. Ova šifra se generiše putem vremenskog algoritma za jednokratnu lozinku (TOTP). Stoga, šifra važi samo kratak vremenski period.

Putem provere identiteta uz dva faktora i ograničavanje pristupa putem bele liste, TeamViewer pruža pomoć kod zadovoljavanja svih potrebnih kriterijuma za sertifikate HIPAA i PCI.

Bezbednosno testiranje

I infrastruktura TeamViewer-a i softver TeamViewer podležu testovima penetracije na redovnoj bazi. Testove obavljaju nezavisne kompanije specijalizovane za bezbednosno testiranje.

Dodatna pitanja?

Za dodatna pitanja ili informacije slobodno nam se obratite putem telefona 0800 190 302
ili pošaljite e-pismo na support@teamviewer.com.

Kontakt

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