Informacije o sigurnosti za TeamViewer

Ciljna skupina

Ovaj dokument namijenjen je profesionalnim mrežnim administratorima. Informacije u ovom dokumentu tehničke su prirode i vrlo su podrobne. Na temelju ovih informacija informatički profesionalci dobit će detaljnu sliku o sigurnosnim standardima TeamViewera i razriješit će im se bilo kakve dvojbe prije uporabe našeg softvera. Slobodno podijelite ovaj dokument svojim kupcima kako biste olakšali bilo kakve moguće brige u vezi sa sigurnosti.

Ako se ne smatrate dijelom ciljne skupine, meke činjenice u odjeljku Tvrtka/softver ipak će vam pomoći u dobivanju jasne slike o tome da sigurnost doživljavamo ozbiljno.

Tvrtka/softver

O nama

Tvrtka TeamViewer GmbH osnovana je 2005. godine i smještena je u južnoj Njemačkoj, u gradu Göppingenu (u blizini Stuttgarta), s podružnicama u Australiji i SAD-u. Razvijamo i prodajemo isključivo sigurne sustave za suradnju na webu. U kratko vrijeme naše licenciranje Freemium dovelo je do brzog rasta, s više od 200 milijuna korisnika softvera TeamViewer na više od 1,4 milijarde uređaja u više od 200 zemalja diljem svijeta. Softver je dostupan u više od 30 jezika.

Naše razumijevanje sigurnosti

TeamViewer upotrebljava više od 30 milijuna korisnika u bilo kojem trenutku svakog dana. Ti korisnici pružaju spontanu podršku putem interneta, pristupajući računalima bez nadzora (tj. daljinsku podršku za poslužitelje) i za udomljavanje sastanaka na mreži. Ovisno o konfiguraciji, TeamViewer može se upotrebljavati za daljinsko upravljanje drugog računala, kao da sjedite ispred njega. Ako je korisnik koji je prijavljen na udaljeno računalo administrator Windowsa, Maca ili Linuxa, toj osobi dodijelit će se administratorska prava i na tom računalu.

Jasno je da takva moćna funkcionalnost na potencijalno nesigurnom internetu mora biti zaštićena od napada s velikom pažnjom. Tema sigurnosti zapravo dominira svim našim razvojnim ciljevima i mi je živimo i dišemo u svemu što radimo. Želimo osigurati da je pristup vašem računalu siguran i želimo zaštiti svoje interese: milijuni korisnika diljem svijeta vjeruju samo sigurnom rješenju i samo sigurno rješenje osigurava dugoročni uspjeh našeg poslovanja.

Vanjska stručna procjena

Našem softveru, TeamVieweru, Savezna udruga stručnjaka i revizora informatičke tehnologije (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.) dodijelila je pečat kvalitete od pet zvjezdica (maksimalna vrijednost). Nezavisni revizori udruge BISG e.V. pregledavaju proizvode kvalificiranih proizvođača i ispituju njihovu kvalitetu, sigurnost i značajke usluge.

Reference

Trenutačno više od 200 milijuna korisnika upotrebljava TeamViewer. Međunarodne vodeće korporacije iz svih vrsta industrija (uključujući toliko visoko osjetljive sektore poput bankarstva, financija, zdravstva i vlade) uspješno upotrebljavaju TeamViewer.

Pozivamo vas da provjerite naše reference diljem čitavog interneta kako biste dobili prvi dojam o prihvatljivosti našeg rješenja. Vidjet ćete da su vjerojatno većina drugih tvrtki imale slične zahtjeve sigurnosti i dostupnosti prije nego što su se - nakon intenzivne provjere - naposljetku odlučile za TeamViewer. Međutim, kako biste oblikovali vlastiti dojam, provjerite tehničke pojedinosti u ostatku ovog dokumenta.

Sesije u TeamVieweru

Izrada sesije i vrste povezivanja

Prilikom upostavljanja sesije TeamViewer određuje optimalnu vrstu povezivanja. Nakon rukovanja kroz naše glavne poslužitelje uspostavlja se izravna veza putem UDP-a ili TCP-a u 70 % svih slučajeva (čak i iza standardnih pristupnika, NAT-ova i vatrozida). Ostatak veza usmjeren je kroz našu visoko redundantnu mrežu usmjerivača putem TCP-a ili https-tuneliranja. Ne morate otvarati nikakve priključke za rad s programom TeamViewer

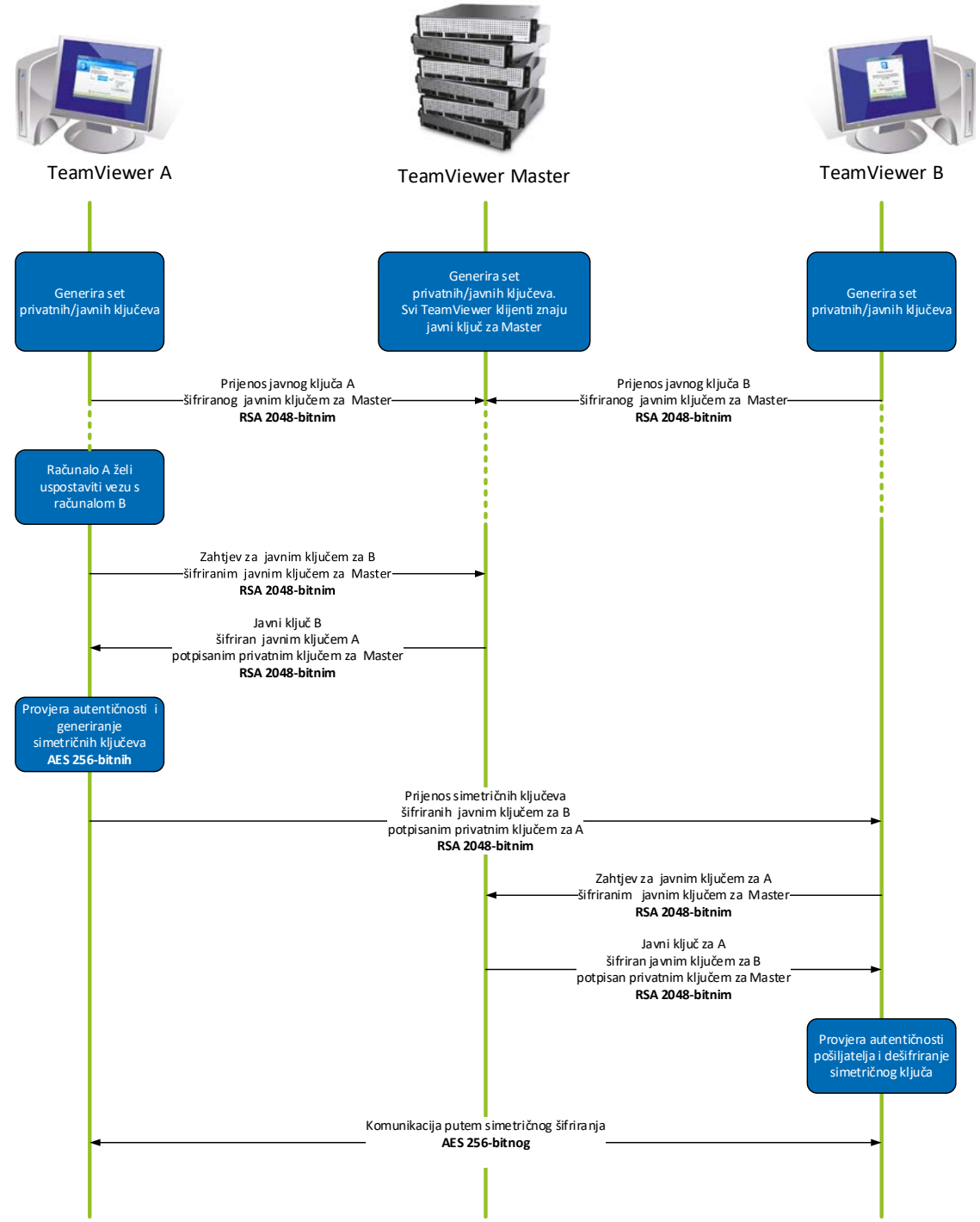
Kako je kasnije opisano u paragrafu Šifriranje i provjera autentičnosti, čak ni mi, rukovatelji poslužitelja za usmjeravanje, ne možemo čitati šifrirani podatkovni promet.

Šifriranje i provjera autentičnosti

Promet TeamViewera osiguran je pomoću RSA-razmjene javnog/privatnog ključa i šifriranjem sesije AES (256-bitnim). Ta tehnologija upotrebljava se u usporedivom obliku za http/SSL i smatra se potpuno sigurnom prema suvremenim standardima. Budući da privatni ključ nikad ne napušta računalo klijenta, ovaj postupak osigurava da međusobno povezana računala - uključujući poslužitelje za usmjeravanje TeamViewera - ne mogu dešifrirati tok podataka.

Svaki TeamViewerov klijent već je implementirao javni ključ glavnog klastera i stoga može šifrirati poruke upućene glavnom klasteru i provjeriti poruke koji glavni klaster potpisuje. PKI (infrastruktura javnog ključa) učinkovito sprječava napade posrednika. Usprkos šifriranju, lozinka se nikad ne šalje izravno, već samo kroz postupak upita i odgovora te se sprema isključivo na lokalno računalo.

Tijekom provjere autentičnosti, lozinka se nikad ne prenosi izravno jer se upotrebljava protokol sigurne udaljene lozinke (SRP). Samo alat za provjeru lozinke pohranjuje se na lokalnom računalu.



Šifriranje i provjera autentičnosti TeamViewera

Provjera valjanosti identifikacija TeamViewera

Identifikacije TeamViewera temelje se na različitim hardverskim i softverskim značajkama i TeamViewer ih automatski generira. TeamViewerovi poslužitelji provjeravaju valjanost tih identifikacija prije svakog povezivanja.

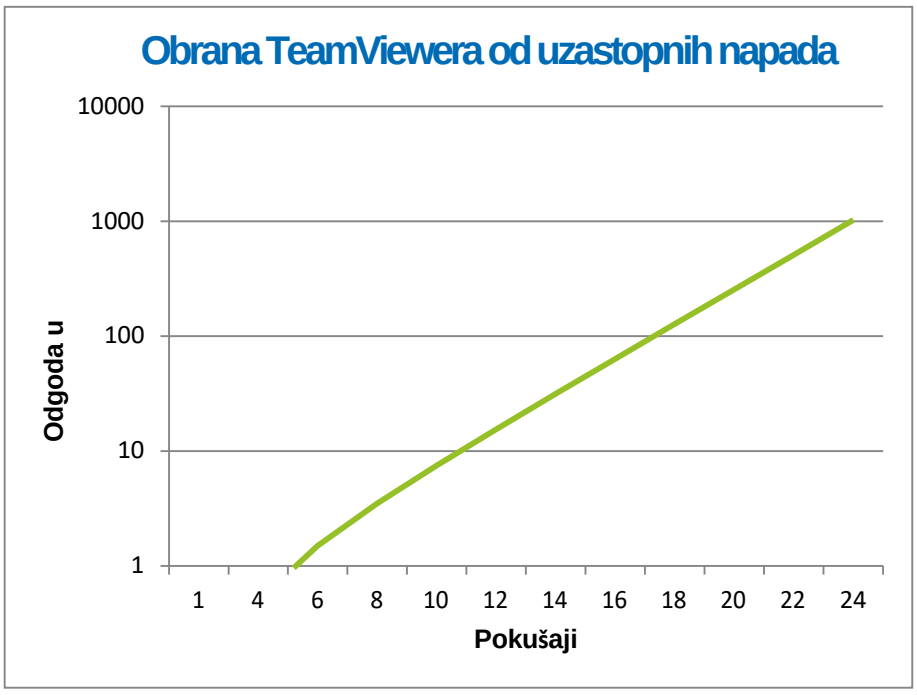
Zaštita od napada uzastopnim pokušajima (brute force)

Potencijalni kupci koji se raspituju o sigurnosti TeamViewera redovito pitaju za šifriranje. Razumljivo, najveći strah je od opasnosti da bi treća strana mogla nadgledati vezu ili kopirati pristupne podatke za TeamViewer. Međutim, u stvarnosti su prilično primitivno napadi često najopasniji.

U kontekstu računalne sigurnosti, napad metodom brute force je metoda pokušaja i pogreške za pogađanje lozinke koja štiti resurs. S rastućom računalnom moći standardnih računala vrijeme potrebno za pogađanje dugačkih lozinki sve se više smanjuje.

Kao obrana od napada uzastopnim pokušajima, TeamViewer eksponencijalno povećava odgodu između pokušaja povezivanja. Zato je potrebno čak do 17 sati za 24 pokušaja. Latencija se resetira tek nakon uspješnog unosa ispravne lozinke.

TeamViewer nema spreman samo mehanizam za zaštitu svojih kupaca od napada s jednog određenog računala, već i s višestrukih računala, od takozvanih napada botneta, koji pokušavaju pristupiti jednoj određenoj identifikaciji TeamViewera.



Grafikon: Proteklo vrijeme nakon n pokušaja povezivanja tijekom napada brute force

Potpisivanje koda

Kao dodatna sigurnosna značajka, sav naš softver potpisan je putem potpisivanja koda VeriSign. Na taj način izdavač softvera uvijek se može lako prepoznati. Ako je softver naknadno promijenjen, digitalni potpis automatski postaje nevažeći.

Podatkovni centri i glavna mreža

Kako bi se pružila najbolja moguća sigurnost i dostupnost usluga TeamViewera, svi TeamViewerovi poslužitelji smješteni su u podatkovnim centrima koji ispunjavaju uvjete standarda ISO 27001 i iskorištavaju višestruko redundantnih veza s mrežom i redundantnih napajanja. Osim toga, upotrebljava se samo najsuvremeniji hardver poznatih proizvođača. Nadalje, svi poslužitelji koji pohranjuju osjetljive podatke smješteni su u Njemačkoj ili Austriji.

Certifikat ISO 27001 znači da osobna kontrola pristupa, videonadzor, detektori kretanja, neprekidni nadzor i sigurnosno osoblje na lokaciji osiguravaju da se pristup podatkovnom centru omogućuje samo ovlaštenim osobama i jamče najbolju moguću sigurnost za hardver i podatke. Također postoji podrobna provjera identifikacije na pojedinačnoj točki ulaza u podatkovni centar.

Račun za TeamViewer

Računi za TeamViewer smješteni su na posvećenim poslužiteljima. Za informacije o upravljanju pristupom pogledajte gore navedenu točku Podatkovni centar i glavna mreža. Za provjeru autentičnosti i šifriranje lozinke upotrebljava se protokol sigurne udaljene lozinke (SRP), poboljšani protokol za razmjenu ključeva potvrđenu lozinkom (PAKE). Uljez ili posrednik ne može dobiti dovoljno informacija kako bi mogao pogoditi lozinku metodom brute force. To znači da se velika sigurnost može ostvariti i pomoću slabih lozinki. Osjetljivi podaci unutar računa za TeamViewer, na primjer informacije za prijavu u pohranu u oblaku, pohranjuju se šifrirani 2048-bitnom vrstom AES/RSA.

Upravljačka konzola

Upravljačka konzola TeamViewera je platforma na webu za upravljanje korisnicima, izvješćivanje o vezi i upravljanje računalima i kontaktima. Smještena je u podatkovnim centrima koji ispunjavaju uvjete standarda ISO-27001 i HIPAA. Sav prijenos podataka odvija se kroz siguran kanal pomoću šifriranja TSL (transportni sloj sigurnosti), što je standard za sigurne internetske mrežne veze. Nadalje, osjetljivi podaci pohranjuju se šifrirani 2048-bitnom vrstom AES/RSA. Za potvrdu autentičnosti i šifriranje lozinke upotrebljava se protokol sigurne udaljene lozinke (SRP). SRP je dobro uspostavljena, robusna i sigurna metoda provjere autentičnosti na temelju lozinke i metoda razmjene ključeva pomoću 2048-bitnog modula.

Postavke na temelju police

Iz upravljačke konzole TeamViewera korisnici mogu definirati, distribuirati i provoditi police postavki za softverske instalacije TeamViewera na uređajima čiji su isključivi vlasnici. Police postavki digitalno potpisuje račun koji ih je generirao. To osigurava da je jedini račun s dozvolom za dodjelu police uređaju račun kojem uređaj pripada.

Sigurnost aplikacija u TeamVieweru

Crni i bijeli popis

Osobito ako se TeamViewer upotrebljava za održavanje računala bez nadzora (tj. ako je TeamViewer instaliran kao usluga Windowsa), dodatna sigurnosna opcija za ograničavanje pristupa tim računalima na nekoliko određenih klijenata može biti od interesa.

S funkcijom bijelog popisa možete izričito navesti kojim identifikacijama i/ili računima za TeamViewer je dozvoljen pristup određenom računalu. S funkcijom crnog popisa možete blokirati određene identifikacije i račune za TeamViewer. Središnji bijeli popis dostupan je kao dio „postavki na temelju police“ opisanih u gore navedenoj točki „Upravljačka konzola“.

Šifriranje čavrljanja i videa

Povijesti čavrljanja povezane su s vašim računom za TeamViewer i stoga su šifrirane i pohranjene pomoću iste sigurnosti 2048-bitnog šifriranja AES/RDA koja je opisana pod točkom „Račun za TeamViewer“. Sve poruke čavrljanja i videopromet sveobuhvatno su šifrirani pomoćuAES-šifriranja sesija (256-bitnog).

Nema nevidljivog načina rada

Ne postoji funkcija koja vam omogućuje rad TeamViewera potpuno u pozadini. Čak i ako aplikacija radi kao usluga Windowsa u pozadini, TeamViewer uvijek je vidljiv pomoću ikone u paleti sustava.

Nakon uspostavljanja veze uvijek postoji mala upravljačka ploča vidljiva iznad palete sustava. Zato je TeamViewer namjerno neprikladan za prikriveno praćenje računala ili zaposlenika.

Zaštita lozinkom

Za spontanu korisničku podršku TeamViewer (TeamViewer Quick Support) generira lozinku sesije (jednokratnu lozinku). Ako vam kupac kaže svoju lozinku, možete se povezati s njihovim računalom tako da unesete njihovu identifikaciju i lozinku. Nakon što kupac ponovno pokrene TeamViewer generirat će se nova lozinka sesije tako da se možete povezati s računalom kupca samo ako vas kupac pozove.

Ako upotrebljavate TeamViewer za udaljenu podršku bez nadzora (npr. poslužitelja), postavljate pojedinačnu fiksnu lozinku koja osigurava pristup računalu.

Ulazno i izlazno upravljanje pristupom

Možete pojedinačno konfigurirati načine povezivanja za TeamViewer. Primjerice, možete konfigurirati računalo za daljinsku podršku ili sastanak na način u kojem nikakve dolazne veze nisu moguće.

Ograničavanje funkcionalnosti na stvarno potrebne značajke uvijek znači ograničavanje mogućih slabih točki za potencijalne napade.

Dvostruka provjera autentičnosti

TeamViewer pomaže tvrtkama s ispunjavanjem uvjeta HIPAA i PCI. Dvostruka provjera autentičnosti pruža dodatni sigurnosni sloj za zaštitu računa TeamViewera od neovlaštenog pristupa.

Osim korisničkog imena i lozinke, korisnik mora unijeti i šifru za potvrdu autentičnosti. Ta šifra generira se putem algoritma za jednokratnu lozinku na temelju vremena (TOTP). Šifra je stoga važeća samo za kratko vremensko razdoblje.

Kroz dvostruku provjeru autentičnosti i ograničavanje pristupa pomoću bijelog popisa TeamViewer pomaže u ispunjavanju svih potrebnih uvjeta za certifikate HIPAA i PCI.

Ispitivanje sigurnosti

Infrastruktura i softver TeamViewer redovito se ispituju penetracijskim testovima. Testove provode nezavisne tvrtke specijalizirane za ispitivanje sigurnosti.

Dodatna pitanja?

Za dodatna pitanja ili informacije slobodno nam se javite na brojeve telefona +385 (0) 1 777 6281 ili pošaljite e-poruku na adresu support@teamviewer.com.

Kontakt

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