TeamViewer biztonsági információk

Célcsoport

Ez a dokumentum hálózati rendszergazdák számára íródott. A dokumentumban szereplő információk inkább műszaki jellegűek és nagyon részletesek. Ezen információk alapján az informatikai szakemberek a szoftver telepítése előtt részletes képet kaphatnak a TeamViewer biztonsági szabványairól, melyek minden aggályt eloszlatnak. Kérjük, juttassa el a dokumentumot az ügyfeleknek is, hogy ezzel is enyhítse az esetleges biztonsági aggályokat.

Ha úgy véli, hogy nem tartozik a célcsoportba, az A Vállalat / a Szoftver című fejezetben olvasható közvetett előnyök/adatok jóvoltából világos képet kaphat arról, hogy mennyire komolyan vesszük a biztonságot.

A Vállalat / a Szoftver

Rólunk

A TeamViewer GmbH 2005-ben alakult a Németország déli részén fekvő Göppingenben (Stuttgart közelében), leányvállalatai Ausztráliában és az Egyesült Államokban találhatók. Kizárólag webalapú együttműködéshez fejlesztünk és árusítunk biztonsági rendszereket. Freemium licencünk jóvoltából rövid időn belül gyors növekedésnek indultunk, a TeamViewer szoftver jelenleg több mint 200 millió felhasználóval rendelkezik, akik több mint 1,4 milliárd eszközön, világszerte több mint 200 országban használják azt. A szoftver több mint 30 nyelven érhető el.

Ahogy mi értelmezzük a biztonságot

A TeamViewert mindennap több mint 30 millióan használják világszerte azzal a céllal, hogy spontán támogatást nyújtsanak az interneten keresztül felügyelet nélküli számítógépek elérésével (pl. szerverek távfelügyeletével), és hogy online megbeszéléseket szervezzenek. A TeamViewer konfigurációtól függően másik számítógép távoli irányítására is használható úgy, mintha közvetlenül előtte ülne a felhasználó. Ha a távoli számítógépre bejelentkezett felhasználó Windows, Mac vagy Linux rendszergazda, a másik számítógépen is rendszergazdai jogai lesznek.

Világos, hogy a potenciálisan nem biztonságos interneten keresztül megvalósított ilyen erőteljes funkcionalitást nagy körültekintéssel kell védeni a támadásokkal szemben. Fejlesztési céljainkat alapvetően a biztonság dominálja. Ezt éljük meg, bármibe is fogunk, ezt lélegezzük be és ki. Szeretnénk, ha biztonságosan zajlana a hozzáférés az Ön számítógépéhez, és saját érdekeinket is védjük: világszerte felhasználók milliói csak biztonságos megoldásban bíznak, és csak biztonságos megoldás biztosíthatja hosszú távú üzleti sikerünket.

Külső szakértői értékelés

Szoftverünk, a TeamViewer ötcsillagos minőség pecsétet kapott (ez a maximális érték) az Informatikai Szakértők és Kritikusok Államszövetségi Szövetségétől (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.). A BISG e.V. független kritikusai minősített szolgáltatók termékeit vizsgálják minőség, biztonság és a szolgáltatási jellemzők szempontjából.

Referenciák

A TeamViewer jelenleg több mint 200 millió felhasználóval rendelkezik. Nemzetközi csúcsvállalatok használják sikerrel a TeamViewert különböző területekről (olyan érzékeny ágazatok is, mint a bankok, a pénzügyi, egészségügyi és kormányzati szektor).

Vessen egy pillantást az interneten is megtalálható referenciáinkra, hogy első benyomást szerezzen megoldásunk elfogadottságáról. Látni fogja, hogy a legtöbb, nagyrészt feltehetően hasonló biztonsági és rendelkezésre állási követelményekkel rendelkező hasonló cég is – alapos vizsgálat után – végül a TeamViewer mellett döntött. A saját benyomás kialakításához a dokumentum további részében technikai részleteket is talál.

TeamViewer munkamenetek

Munkamenet létrehozása és kapcsolattípusok

Munkamenet létrehozásakor a TeamViewer meghatározza az optimális kapcsolattípust. A főszervereinken keresztül történő egyeztetés után az esetek 70%-ában létrejön egy UDP vagy TCP alapú közvetlen kapcsolat (akár még normál átjárók, NAT-ok és tűzfalak mögött is). A többi kapcsolat magas szinten redundáns útválasztó hálózatunkon keresztül TCP protokoll vagy https-tunnelling technikával épül fel. A TeamViewer használatához nem kell megnyitni semmilyen portot

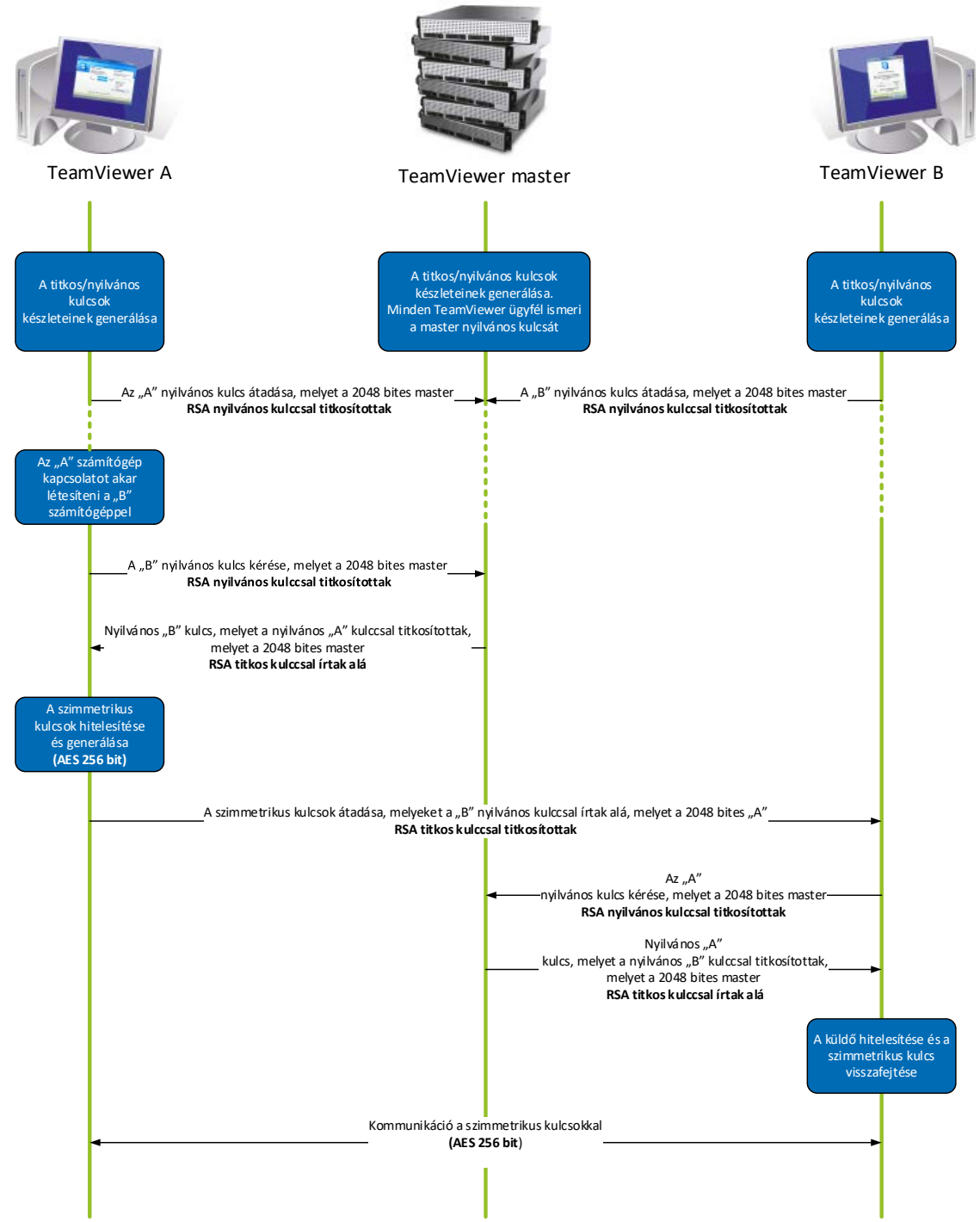
Mint később a Titkosítás és hitelesítés című fejezetben leírjuk, sem mi nem tudjuk, sem az útválasztó szerverek kezelői nem képesek olvasni a titkosított adatforgalmat.

Titkosítás és hitelesítés

A TeamViewer adatforgalmát RSA nyilvános/személyes kulcscsere és AES (256 bites) munkamenet-titkosítás biztosítja. Ezt a technológiát használja összehasonlítható formában a http/SSL is, és a mai szabványok alapján teljesen biztonságosnak tekinthető. Mivel a személyes kulcs soha nem hagyja el a kliens számítógépet, az eljárás jóvoltából az összekapcsolt számítógépek – beleértve a TeamViewer útválasztó szervereit is – nem képesek visszafejteni az adatfolyamot.

A TeamViewer klienseken már telepítve van a főklaszter nyilvános kulcsa, ezért képesek titkosítani a főklaszternek küldött üzeneteket, valamint ellenőrizni az általa aláírtakat. A PKI (Public Key Infrastructure) hatékonyan akadályozza a közbeékelődéses támadásokat. A titkosítás ellenére a jelszó nem közvetlenül, hanem kérdés-válasz eljárással kerül elküldésre, és csak a helyi számítógépen tárolódik.

A hitelesítés során a jelszó az SRP (Secure Remote Password) protokoll miatt soha nem kerül átadásra közvetlenül. A helyi számítógép csak a jelszóhitelesítőt tárolja.



TeamViewer titkosítás és hitelesítés

A TeamViewer azonosítók érvényesítése

A TeamViewer azonosítókat, melyek alapját különböző hardver- és szoftverjellemzőik képezik, a TeamViewer hozza létre automatikusan, a TeamViewer szerverek pedig minden kapcsolat létrehozása előtt ellenőrzik ezeket az azonosítókat.

„Nyers erővel” végzett támadások (brute-force) elleni védelem

A TeamViewer biztonságáról érdeklődő leendő vásárlók rendszeresen tesznek fel kérdéseket a titkosítással kapcsolatban, ami teljesen érthető. Attól tartanak leginkább, hogy egy külső fél monitorozhatja a kapcsolatot, vagy lehallgathatja a TeamViewer hozzáférési adatait. A valóság azonban az, hogy gyakran a meglehetősen primitív támadások a legveszélyesebbek.

A számítógép-biztonság kontextusában a nyers erővel végzett támadás többszöri próbálkozást jelent az erőforrást védő jelszó kitalálására. A normál számítógépek egyre nagyobb számítási teljesítménye jóvoltából a hosszú jelszavak kitalálásához szükséges idő folyamatosan csökken.

A nyers erővel végzett támadások elleni védekezésként a TeamViewer exponenciálisan növeli a kapcsolódási kísérletek közötti késleltetést, így 24 kísérlet akár 17 órán át is tarthat, a látencia pedig csak a helyes jelszó megadása után áll vissza alaphelyzetre.

A TeamViewer nem csak egy adott számítógépről érkező támadások ellen védi ügyfeleit, a védelmi mechanizmus adott TeamViewer-azonosító elérését célzó több számítógépről érkező, ismertebb nevén botnet támadásokat is képes elhárítani.

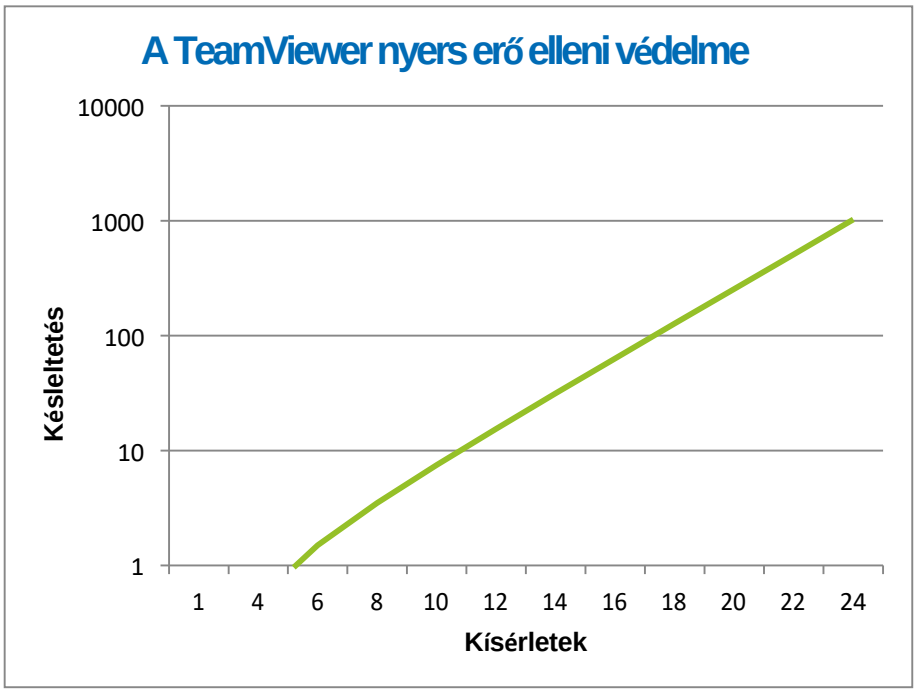


Diagram: Nyers erővel végzett támadás során n csatlakozási kísérlet után eltelt idő

Kódaláírás

Kiegészítő biztonsági funkcióként összes szoftverünk aláírása VeriSign kódaláíráson keresztül történik, ily módon a szoftver közzétevője mindig könnyen azonosítható. Ha a szoftver később megváltozik, a digitális aláírás automatikusan érvénytelenné válik.

Adatközpontok és gerincrendszer

A TeamViewer szolgáltatások lehető legmagasabb szintű biztonsága és rendelkezésre állása érdekében a TeamViewer szerverek ISO 27001 tanúsítású adatközpontokban működnek, többszörösen redundáns szolgáltatói kapcsolatokkal és redundáns tápegységekkel biztosítva, emellett kizárólag a legnagyobb márkanevek alatt futó hardvereket használjuk. Minden érzékeny adatokat tároló szerver Németországban és Ausztriában található.

Az ISO 27001 minősítés azt jelenti, hogy beléptetőrendszer, videokamerás megfigyelés, mozgásérzékelők, folyamatos monitorozás és helyszíni biztonsági személyzet garantálja a lehető legnagyobb biztonságot a hardver és az adatok számára, és hogy az adatközpontban csak engedéllyel rendelkező személyek tartózkodhassanak. Az adatközpont egyetlen beviteli pontján emellett részletes azonosító ellenőrzés történik.

TeamViewer fiók

A TeamViewer fiókokat dedikált szerverek tárolják. A hozzáférés-szabályozással kapcsolatos információkért olvassa el a fenti Adatközpontok és gerincrendszer című fejezetet. Azonosításra és jelszó titkosításra SRP (Secure Remote Password) rendszert, egy kibővített, jelszóval hitelesített kulcscsere (PAKE) protokollt használunk. A beszivárgó vagy köztes támadó nem juthat elegendő információhoz ahhoz, hogy nyers erővel végzett találgatással rájöhessen a jelszóra. Ez azt jelenti, hogy még gyenge jelszó esetén is erős biztonság garantálható. A TeamViewer fiókban tárolt érzékeny adatok, például a felhő tároló bejelentkezési adatai 2048 bites AES/RSA titkosítással vannak ellátva.

Kezelőkonzol

A TeamViewer kezelőkonzol a felhasználók kezelésére, kapcsolatjelentésre, valamint a számítógépek és partnerek kezelésére szolgáló webes platform. A platform ISO-27001 tanúsítvánnyal rendelkező, HIPAA-kompatibilis adatközpontokon fut. Az összes adatátvitel TSL (Transport Security Layer) titkosítású biztonságos csatornán keresztül történik, ami a biztonságos internetes hálózati kapcsolatok szabványos megoldása. Az érzékeny adatok emellett 2048 bites AES/RSA titkosítással is el vannak látva. Azonosításra és a jelszó titkosítására SRP (Secure Remote Password) rendszert használunk. Az SRP egy jól működő, robusztus, biztonságos jelszóalapú hitelesítési és kulcscseremódszer, mely 2048 bites modulust használ.

Házirend alapú beállítások

A felhasználók a TeamViewer kezelőkonzolon belül meghatározhatják, terjeszthetik és hatályba léptethetik a TeamViewer szoftvertelepítések beállítási házirendjeit a kifejezetten hozzájuk tartozó eszközökön. A beállítási házirendek az őket létrehozó fiók digitális aláírásával vannak ellátva, ezáltal csak az a fiók rendelhet házirendet az adott eszközhöz, amelyikhez az eszköz tartozik.

Alkalmazásokkal kapcsolatos biztonság a TeamViewerben

Tiltó- és engedélyezési lista

Különösen akkor, ha a TeamViewert felügyelet nélküli számítógépek karbantartására használják (azaz a TeamViewer Windows-szolgáltatásként került telepítésre), kiegészítő biztonsági lehetőségként az ilyen számítógépekhez való hozzáférés korlátozása sok ügyfél érdeklődésére számot tarthat.

Az engedélyezési lista funkcióval kifejezetten megadható, hogy mely TeamViewer azonosítók és/vagy TeamViewer fiókok férhetnek hozzá adott számítógéphez. A tiltólista funkcióval adott TeamViewer azonosítók és TeamViewer fiókok blokkolhatók. Egy központi engedélyezési lista a fent a „Kezelőkonzol” fejezetben ismertetett „házirend alapú beállítások” részeként elérhető.

Chat- és videótitkosítás

A chat-előzmények a TeamViewer fiókhoz társulnak, így ugyanazzal a 2048 bites AES/RSA titkosítással vannak biztosítva, amit a „TeamViewer fiók” cím alatt ismertettünk. Az összes chat-üzenet és videóforgalom végponttól végpontig AES (256 bites) munkamenet-titkosítással közlekedik.

Nincs rejtett üzemmód

Nincs olyan funkció, amely lehetővé teszi, hogy a TeamViewer teljesen a háttérben fusson. A TeamViewer a rendszertálcán látható ikon képében akkor is látható, ha az alkalmazás Windows-szolgáltatás részeként a háttérben fut.

A kapcsolat létrejötte után a rendszertálca fölött mindig látható marad egy kis vezérlőpult, hogy a TeamViewert szándékosan alkalmatlanná tegyük számítógépek vagy alkalmazottak rejtett megfigyelésére.

Jelszavas védelem

A spontán ügyfélszolgálat érdekében a TeamViewer (TeamViewer QuickSupport) munkamenetjelszót (egyszeri jelszót) hoz létre. Ha ügyfele megmondja jelszavát, az ő azonosítójával és jelszavával rácsatlakozhat a számítógépére. Az ügyfél oldalán a TeamViewer újraindítása után új munkamenetjelszó jön létre, így Ön csak akkor tud rácsatlakozni ügyfele számítógépére, ha erre felkérést kap tőle.

Ha a TeamViewer felügyelet nélküli távoli támogatáshoz lett telepítve (pl. szerver felügyelete), a számítógéphez való hozzáférés biztosítására egyéni fix jelszó állítható be.

Bejövő és kimenő hozzáférés szabályozása

A TeamViewer kapcsolódási módjai egyedileg konfigurálhatók. Például beállíthatja távtámogatásra vagy értekezletre használt számítógépét úgy is, hogy ne fogadhasson bejövő kapcsolatokat.

Az ilyen funkciók működésének korlátozása mindig azt jelenti, hogy a potenciális támadásoknak kitett gyenge pontok száma is csökken.

Kéttényezős hitelesítés

A TeamViewer segíti a vállalatokat HIPAA és PCI megfelelőségi követelményeik teljesítésében. A kéttényezős hitelesítés egy további biztonsági réteggel egészíti ki a TeamViewer fiókok védelmét a jogosulatlan hozzáféréssel szemben.

A felhasználónak a felhasználónév és a jelszó mellett egy kódot is meg kell adnia a belépéshez. Ezt a kódot az idő alapú egyszeri jelszó (TOTP) algoritmus hozza létre, így az csak rövid ideig érvényes.

A kéttényezős hitelesítés és a hozzáférés engedélyezési lista alapú korlátozása révén a TeamViewer az értekezlet támogatásának minden HIPAA és PCI minősítési követelményét teljesíti.

Biztonsági tesztelés

A TeamViewer infrastruktúra és a TeamViewer szoftver egyaránt rendszeresen átesik behatolási teszteken. A teszteket biztonsági tesztelésre szakosodott független társaságok végzik.

További kérdései vannak?

További kérdéseit felteheti és információkat kérhet az +36 1 808 8428 telefonszámon vagy e-mailben a support@teamviewer.com címen.

Kapcsolat

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