TeamViewer — informacje dotyczące bezpieczeństwa

Grupa docelowa

Niniejszy dokument jest przeznaczony dla administratorów sieci. Informacje w nim zamieszczone mają charakter techniczny i szczegółowy. Na ich podstawie pracownicy działu IT będą mogli w dokładny sposób poznać standardy bezpieczeństwa TeamViewer i uzyskać pełne informacje o oprogramowaniu przed jego wprowadzeniem. Zalecamy przekazanie niniejszego dokumentu klientom, aby także oni mogli poznać informacje dotyczące bezpieczeństwa.

Nawet jeśli nie uważacie się Państwo za docelowych odbiorców niniejszego dokumentu, warto przeczytać informacje zamieszczone w części „Firma i oprogramowanie” — dzięki nim dowiecie się, jak ważne jest dla nas bezpieczeństwo.

Firma i oprogramowanie

Informacje o firmie

Firma TeamViewer GmbH została założona w roku 2005. Jej siedziba znajduje się w południowych Niemczech, w mieście Göppingen obok Stuttgartu. Posiadamy oddziały w Australii oraz Stanach Zjednoczonych. Zajmujemy się opracowywaniem i sprzedażą bezpiecznych systemów do zdalnej współpracy. W krótkim czasie nasze licencje udostępniane na zasadzie Freemium pozwoliły nam na szybki rozwój: z oprogramowania TeamViewer korzysta ponad 200 milionów użytkowników, zostało ono zainstalowane na ponad 1,4 miliardzie urządzeń w ponad 200 krajach. Oprogramowanie jest dostępne w ponad 30 wersjach językowych.

Nasza koncepcja bezpieczeństwa

Z oprogramowania TeamViewer korzysta ponad 30 milionów użytkowników na całym świecie. Świadczą oni usługi wsparcia on-line, mogą uzyskać zdalny dostęp do komputerów (zdalne wsparcie dla serwerów), oraz mogą organizować konferencje poprzez sieć. Zależnie od konfiguracji oprogramowanie TeamViewer może służyć do zdalnego zarządzania innym komputerem. Jeśli użytkownik zalogowany na komputerze zdalnym jest administratorem systemu Windows, Mac lub Linux, otrzyma on prawa administratora także na tym komputerze.

Tak zaawansowane możliwości wykorzystywane w niebezpiecznym środowisku jakim jest Internet wymagają stosowania zabezpieczeń przed atakami. Aspekt bezpieczeństwa jest traktowany priorytetowo w naszym procesie rozwojowym. Naszym celem jest zapewnienie bezpieczeństwa komputerów oraz ochrona milionów użytkowników na całym świecie, którzy zaufali naszym rozwiązaniom. Wierzymy, że bezpieczeństwo jest kluczem do długoterminowego sukcesu w biznesie.

Ocena zewnętrznych ekspertów

Nasze oprogramowanie — TeamViewer —otrzymało maksymalną ocenę pięciu gwiazdek przyznaną przez federalną organizację ekspertów i kontrolerów IT (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.). Niezależni kontrolerzy BISG e.V. sprawdzają produkty kwalifikowanych producentów pod kątem jakości, bezpieczeństwa oraz charakterystyki działania.

Referencje

Obecnie oprogramowanie TeamViewer jest wykorzystywane przez ponad 200 milionów użytkowników. Jest ono z powodzeniem używane przez największe międzynarodowe korporacje działające w takich wymagających branżach jak bankowość, finanse, opieka zdrowotna oraz organizacje rządowe.

Zachęcamy do zapoznania się z naszymi referencjami w Internecie — pozwoli to wstępnie poznać nasze rozwiązanie. Warto zwrócić uwagę, że wiele różnych firm o podobnych wymaganiach dotyczących bezpieczeństwa i dostępności, po przeprowadzeniu dokładnych analiz, wybrało oprogramowanie TeamViewer. Aby dowiedzieć się więcej, prosimy także zapoznać się z danymi technicznymi zamieszczonymi w dalszej części niniejszego dokumentu.

Sesje TeamViewer

Tworzenie sesji i typy połączeń

Na etapie tworzenia sesji oprogramowanie TeamViewer określi optymalny typ połączenia. Po ustaleniu parametrów transmisji danych (handshake) w 70% przypadków zostanie nawiązane połączenie bezpośrednie UDP lub TCP (nawet w przypadku standardowych bram, translacji NAT i zapór sieciowych). Pozostała część połączeń jest kierowana przez sieć o wysokiej redundancji z wykorzystaniem protokołu tunelującego TCP lub https. Do pracy z oprogramowaniem TeamViewer nie wymaga się otwierania portów

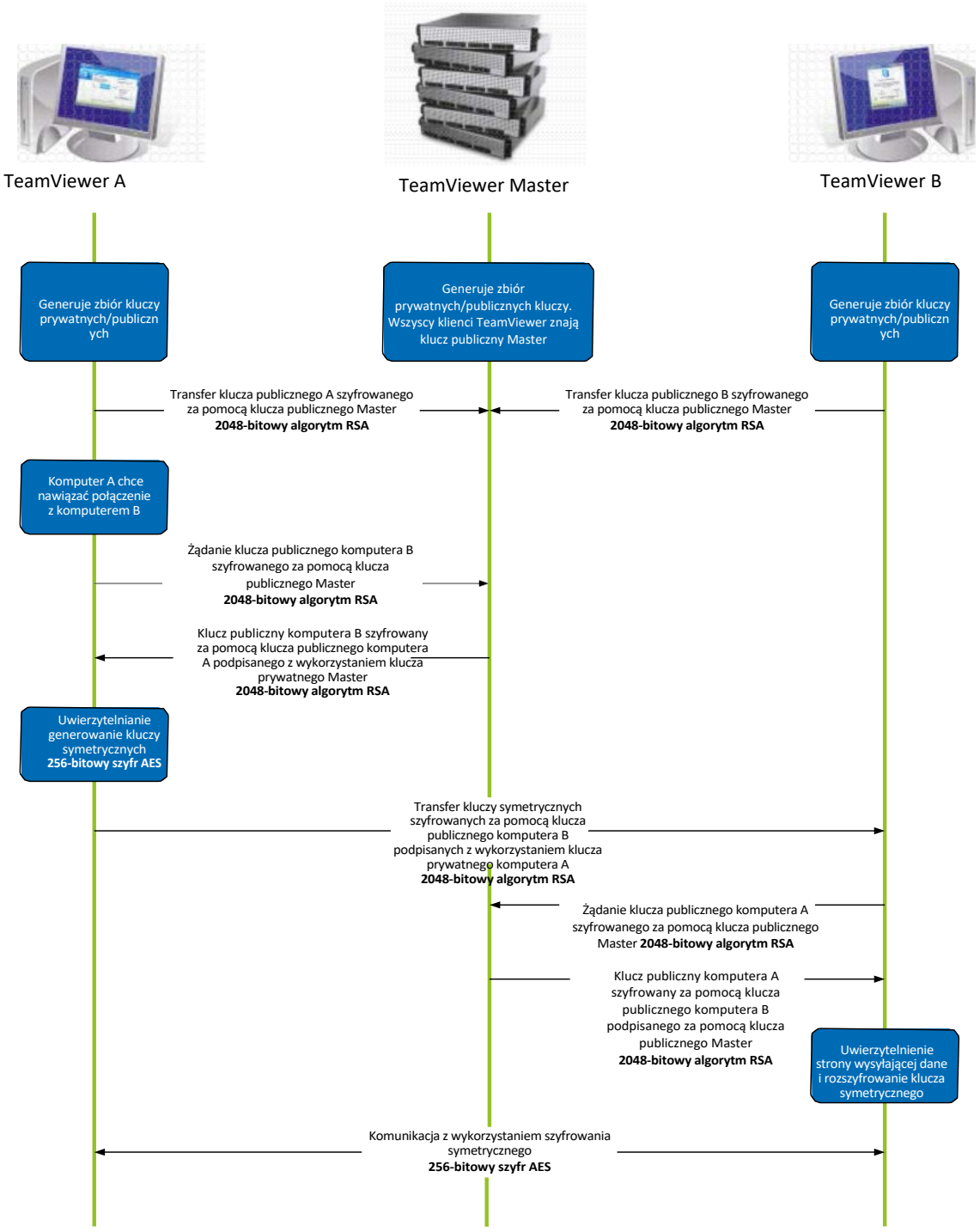
Zgodnie z informacjami zamieszczonymi w części „Szyfrowanie i uwierzytelnianie", nawet my (jako operatorzy serwerów routujących) nie mamy dostępu do zaszyfrowanych danych.

Szyfrowanie i uwierzytelnianie

Dane przesyłane przez oprogramowanie TeamViewer są szyfrowane za pomocą metody RSA z wykorzystaniem klucza publicznego/prywatnego oraz 256-bitowego szyfru AES. Ta technologia jest wykorzystywana przez protokół http/SSL i jest obecnie uważana za całkowicie bezpieczną. Ponieważ klucz prywatny nie jest wysyłany z komputera klienta, procedura ta zapewnia, że połączone komputery (włącznie z serwerami routującymi TeamViewer) nie są w stanie rozszyfrować strumienia danych.

Każdy klient TeamViewer posiada zaimplementowany klucz publiczny klastra głównego, dzięki czemu może szyfrować komunikaty wysyłane do niego i sprawdzać komunikaty przez niego podpisywane. PKI (infrastruktura kluczy publicznych) w skuteczny sposób zapobiega atakom typu „man-in-the-middle". Pomimo szyfrowania hasło nie jest wysyłane bezpośrednio, ale z wykorzystaniem procedury odpowiedzi na wezwanie i jest zapisywanie jedynie w komputerze lokalnym.

Podczas uwierzytelniania hasło nie jest przesyłane bezpośrednio — wykorzystywany jest protokół Secure Remote Password (SRP). Lokalnie przechowywany jest jedynie weryfikator haseł.



TeamViewer — szyfrowanie i uwierzytelnianie

Walidacja identyfikatorów TeamViewer

Identyfikatory TeamViewer bazują na różnych charakterystykach sprzętowych i programowych oraz są automatycznie generowane przez oprogramowanie TeamViewer. Przed każdym nawiązaniem połączenia serwery TeamViewer sprawdzają ważność tych identyfikatorów.

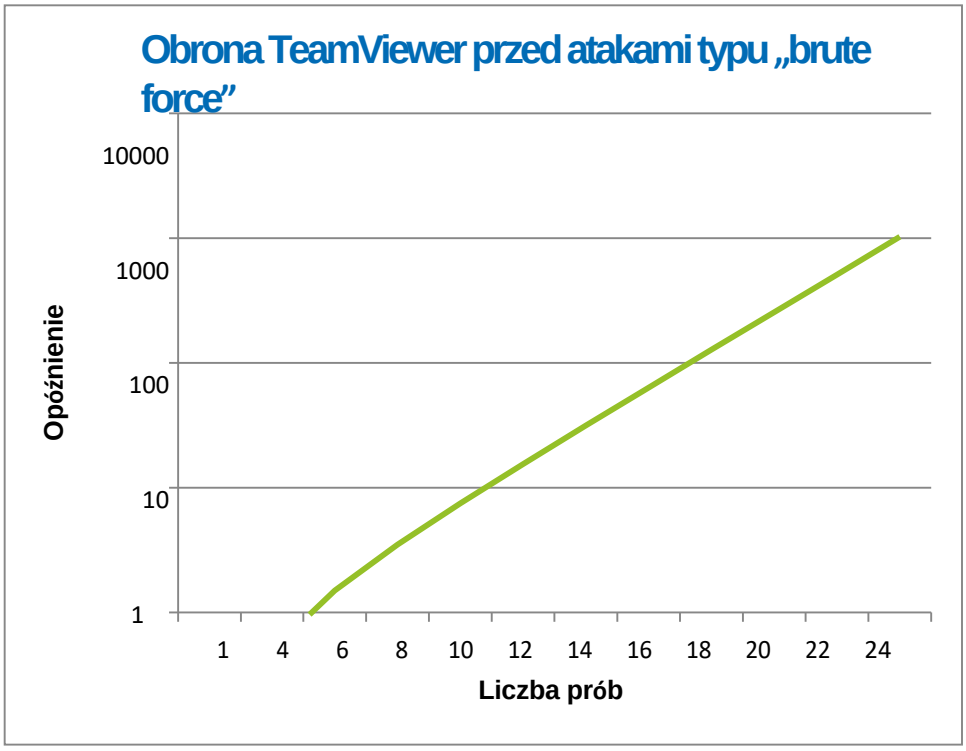
Zabezpieczenie przed atakami typu „brute force”

Potencjalni klienci zainteresowani oprogramowaniem TeamViewer często zainteresowani są szyfrowaniem. Najczęściej obawiają się oni ryzyka monitorowania połączenia przez strony trzecie lub wycieku danych dostępu do oprogramowania TeamViewer. W rzeczywistości często największe zagrożenie jest spowodowane przez stosunkowo prymitywne metody ataków.

W kontekście bezpieczeństwa komputerów ataki typu „brute force” polegają na metodzie prób i błędów w celu odgadnięcia hasła chroniącego dany zasób. Wraz ze wzrostem mocy obliczeniowej typowych komputerów czas wymagany na odgadnięcie długich haseł uległ znacznemu skróceniu.

Zabezpieczeniem przed tego typu atakami zapewnianym przez oprogramowanie TeamViewer jest zwiększenie odstępu czasowego między próbami połączenia. 24 próby nawiązania połączenia zajmują aż 17 godzin. Czas oczekiwania zostanie skasowany tylko po wprowadzeniu prawidłowego hasła.

Oprogramowanie TeamViewer posiada mechanizm chroniący użytkowników przed atakami przeprowadzanymi z jednego lub kilku komputerów (tzw. ataki „botnet”), których celem jest uzyskanie dostępu do komputera z określonym identyfikatorem TeamViewer.



Wykres: opóźnienie po n próbach połączenia podczas ataku typu „brute force”

Podpisywanie kodem (Code Signing)

Jako dodatkowe zabezpieczenie nasze oprogramowanie jest podpisywane kodem VeriSign Code Signing. Pozwala to na identyfikację producenta oprogramowania. Jeśli do oprogramowania wprowadzono zmiany, podpis cyfrowy będzie automatycznie rozpoznawany jako nieprawidłowy.

Centra danych i sieci szkieletowe

Aby zapewnić najwyższy poziom bezpieczeństwa oraz dostępność usług TeamViewer, wszystkie serwery TeamViewer znajdują się w centrach danych zgodnych z normą ISO 27001 i wykorzystują połączenia o wielokrotnej redundancji oraz są zasilane za pomocą nadmiarowych źródeł zasilania. Ponadto korzystamy jedynie ze sprzętu czołowych producentów. Wszystkie serwery przechowujące ważne dane znajdują się w Niemczech lub Austrii.

Certyfikat ISO 27001 oznacza, że centrum danych jest objęte kontrolą dostępu, nadzorem wideo, a ponadto stosujemy w nich detektory ruchu oraz system monitorowania działający w trybie 24x7. Dostęp do centrum danych jest udzielany tylko upoważnionym pracownikom — takie rozwiązania gwarantują najwyższy poziom bezpieczeństwa sprzętu i danych. Każde wejście do centrum danych podlega szczegółowej kontroli tożsamości.

Konto TeamViewer

Dane kont TeamViewer są przechowywane w dedykowanych serwerach. Więcej informacji dotyczących kontroli dostępu zamieszczono w części „Centra danych i sieci szkieletowe” powyżej. Na potrzeby uwierzytelniania i szyfrowania haseł korzystamy z protokołu Secure Remote Password (SRP), rozszerzonego protokołu wymiany kluczy (PAKE). Infiltrator lub osoba przeprowadzająca atak typu „man in the middle” nie może uzyskać wystarczającej liczby informacji do odgadnięcia hasła na podstawie ataku typu „brute force”. Oznacza to, że nawet słabe hasła mogą zapewnić wysoki poziom bezpieczeństwa. Ważne dane przechowywane w koncie TeamViewer , takie jak dane logowania do chmury, są szyfrowane 2048-bitowym algorytmem AES/RSA.

Platforma Management Console

TeamViewer Management Console jest internetową platformą służącą do zarządzania użytkownikami, zgłaszania połączeń i zarządzania komputerami i danymi kontaktowymi. Platforma ta działa z wykorzystaniem centrów danych zgodnych z normą ISO-27001 i ustawą HIPAA. Transfer wszystkich danych odbywa się przez bezpieczny kanał z szyfrowaniem TSL (Transport Security Layer) — jest to standard w zakresie bezpieczeństwa połączeń sieciowych. Przechowywane ważne dane są dodatkowo szyfrowane 2048-bitowym algorytmem AES/RSA. Na potrzeby uwierzytelniania i szyfrowania haseł korzystamy z protokołu Secure Remote Password (SRP). SRP jest uznanym, pewnym i bezpiecznym sposobem uwierzytelniania i sposobem wymiany kluczy za pomocą algorytmu 2048-bitowego.

Ustawienia dotyczące zasad

Z poziomu platformy TeamViewer Management Console użytkownicy mogą definiować, udostępniać i wdrażać zasady dotyczące oprogramowania TeamViewer zainstalowanego na urządzeniach należących do nich. Zasady są podpisywane cyfrowo z poziomu konta, z którego zostały wygenerowane. Dzięki temu zasady można przypisywać do danego urządzenia jedynie z konta należącego do niego.

TeamViewer a bezpieczeństwo aplikacji

Czarna lista i biała lista

Jeśli oprogramowanie TeamViewer będzie wykorzystywane do konserwacji komputerów bez nadzoru (np. gdy oprogramowanie TeamViewer działa jako usługa systemu Windows), użytkownicy mogą wymagać dodatkowych opcji zabezpieczeń pozwalających na ograniczenie dostępu do takich komputerów.

Dzięki funkcji białej listy można określić, które identyfikatory i/lub konta TeamViewer mogą uzyskiwać dostęp do danego komputera. Czarna lista umożliwia natomiast blokowanie wybranych identyfikatorów i kont TeamViewer. Centralna biała lista jest udostępniana w ramach ustawień dotyczących zasad, które opisano w części „Platforma Management Console" powyżej.

Szyfrowanie historii czatu i wideo

Historia czatu powiązana z danym kontem TeamViewer jest szyfrowana i przechowywana z wykorzystaniem 2048-bitowego algorytmu AES/RSA, zgodnie z informacjami zamieszczonymi w części „Konto TeamViewer". Wszystkie wiadomości przesyłane poprzez czat są szyfrowane za pomocą 256-bitowej metody szyfrowania.

Brak trybu niewidzialności

Nie wprowadziliśmy funkcji pozwalającej na działanie oprogramowania TeamViewer całkowicie w tle. Nawet jeśli aplikacja TeamViewer działa jako usługa systemu Windows w tle, jej ikona będzie zawsze widoczna na pasku zadań.

Po ustanowieniu połączenia nad paskiem zadań widoczny będzie także niewielki panel sterowania. Z tego względu oprogramowanie TeamViewer w celowy sposób zostało pozbawione możliwości ukrytego monitorowania komputerów lub pracowników.

Ochrona hasłem

Na potrzeby wsparcia TeamViewer (TeamViewer QuickSupport) generuje jednorazowe hasło dla sesji. Jeśli klient poda własne hasło, można połączyć się z jego komputerem, wprowadzając odpowiedni identyfikator oraz hasło. Po ponownym uruchomieniu oprogramowania TeamViewer po stronie klienta zostanie wygenerowane nowe hasło dla sesji, co uniemożliwi ponowne połączenie się z komputerem klienta bez podania przez niego hasła.

W przypadku udostępniania oprogramowania TeamViewer na potrzeby wsparcia zdalnego bez nadzoru (np. związanego z serwerami), ustanawiane jest indywidualne stałe hasło, które zabezpiecza dostęp do komputera.

Kontrola połączeń przychodzących i wychodzących

Istnieje możliwość indywidualnego skonfigurowania trybów połączeń oprogramowania TeamViewer. Przykładowo komputer, z którego będzie świadczona usługa wsparcia lub konferencji, można skonfigurować tak, by wykluczyć połączenia przychodzące.

Ograniczenie dostępu jedynie do wymaganych funkcji pozwala na zmniejszenie liczby elementów narażonych na potencjalny atak.

Uwierzytelnianie dwupoziomowe

Oprogramowanie TeamViewer pozwala firmom na spełnienie wymogów zgodności z HIPAA oraz PCI. Uwierzytelnianie dwupoziomowe zapewnia dodatkową warstwę bezpieczeństwa, które chroni konta TeamViewer przed niepowołanym dostępem.

Oprócz nazwy oraz hasła użytkownik musi wprowadzić kod uwierzytelniający. Jest to jednorazowy kod generowany na zasadzie algorytmu TOTP. Jest on zatem ważny jedynie przez ograniczony czas.

Uwierzytelnianie dwupoziomowe oraz ograniczenie dostępu za pomocą białej listy powodują, że oprogramowanie TeamViewer spełnia wszystkie kryteria związane z certyfikatami HIPAA i PCI.

Testowanie funkcji zabezpieczeń

Zarówno infrastruktura, jak i oprogramowanie TeamViewer, są poddawane regularnym testom na penetrację. Testy te są przeprowadzane przez niezależne firmy specjalizujące się w testach zabezpieczeń.

Dalsze informacje

Aby dowiedzieć się więcej, prosimy o kontakt pod numerem +48 (0) 22 398 34 83) lub wysłanie wiadomości pod adres support@teamviewer.com.

Informacje kontaktowe

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