Informasi Keamanan TeamViewer

Grup Sasaran

Dokumen ini ditujukan kepada administrator jaringan profesional. Informasi dalam dokumen ini merupakan keterangan yang bersifat agak teknis dan sangat terperinci. Berdasarkan informasi ini, profesional TI akan menerima gambaran terperinci tentang standar keamanan pada TeamViewer, dan setiap kekhawatiran akan dipecahkan sebelum menggunakan perangkat lunak kami. Jangan ragu-ragu untuk mendistribusikan dokumen ini kepada para pelanggan Anda untuk mengurangi setiap kekhawatiran keamanan yang mungkin ada.

Jika Anda tidak mempertimbangkan diri sendiri menjadi bagian dari grup sasaran, fakta lunak dalam bagian Perusahaan / Perangkat Lunak akan tetap membantu Anda mendapatkan gambaran jelas tentang cara kami menangani keamanan secara serius.

Perusahaan / Perangkat Lunak

Tentang kami

TeamViewer GmbH ditemukan pada tahun 2005 dan berbasis di Jerman selatan, di kota Göppingen (dekat Stuttgart), dengan kantor cabang di Australia dan Amerika Serikat. Kami secara eksklusif mengembangkan dan menjual sistem yang aman untuk kolaborasi berbasis web. Dalam rentang waktu singkat, lisensi Freemium kami telah memandu pertumbuhan sangat cepat, dengan lebih dari 200 juta pengguna perangkat lunak TeamViewer pada lebih dari 1,4 miliar perangkat, di lebih dari 200 negara di penjuru dunia. Perangkat lunak tersedia di lebih dari 30 bahasa.

Pemahaman Kami tentang Keamanan

TeamViewer digunakan oleh lebih dari 30 juta pengguna di setiap titik yang diberikan setiap hari. Para pengguna ini memberikan dukungan spontan melalui internet, dengan mengakses komputer yang tidak dihadiri (yaitu dukungan jarak jauh untuk server) dan untuk menyelenggarakan rapat online. Tergantung pada konfigurasinya, TeamViewer dapat digunakan untuk mengontrol komputer lain secara jarak jauh, seolah-olah Anda sedang duduk langsung di depannya. Jika pengguna yang masuk ke komputer jarak jauh adalah administrator Windows, Mac atau Linux, orang ini juga akan diberikan hak administrator di komputer tersebut.

Sudah jelas bahwa fungsi kuat tersebut melalui Internet yang berpotensi tidak aman harus dilindungi dari serangan dengan inspeksi menyeluruh. Faktanya, topik tentang keamanan mendominasi semua tujuan pengembangan kami dan merupakan sesuatu yang senantiasa kita temui dan bahas dalam kehidupan sehari-hari. Kami ingin memastikan akses ke komputer Anda aman dan untuk melindungi kepentingan kami sendiri: jutaan pengguna di seluruh dunia hanya percaya pada solusi yang aman, dan hanya solusi aman yang menjamin kesuksesan jangka panjang sebagai sebuah bisnis.

Penilaian Ahli Eksternal

Perangkat lunak kami, TeamViewer, telah mendapatkan penghargaan segel mutu lima-bintang (nilai maksimum) oleh Asosiasi Federal Ahli dan Peninjau TI (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.). Para peninjau independen dari BISG e.V. memeriksa produk dari produser yang memenuhi syarat atas mutu, keamanan, dan karakteristik layanan mereka.

Referensi

Saat ini, TeamViewer digunakan oleh lebih dari 200 juta pengguna. Korporasi teratas internasional dari semua jenis industri (termasuk sektor yang sangat sensitif seperti perbankan, keuangan, perawatan kesehatan, dan pemerintah) berhasil menggunakan TeamViewer.

Kami mengundang Anda untuk melihat referensi kami yang ditemukan di Internet, untuk mendapatkan kesan pertama tentang penerimaan solusi kami. Anda akan menemukan bahwa sebagian besar perusahaan lain memiliki persyaratan keamanan dan ketersediaan yang serupa sebelum mereka - setelah pengujian intensif - akhirnya memutuskan memilih TeamViewer. Untuk membentuk kesan yang kuat, harap cari beberapa detail teknis di bagian lain dokumen ini.

Sesi TeamViewer

Membuat Sesi dan Tipe Koneksi

Saat membentuk sebuah sesi, TeamViewer akan menentukan tipe koneksi yang optimal. Setelah sambutan melalui server master kami, koneksi langsung via UDP atau TCP akan dibentuk dalam 70% dari semua kondisi (meskipun di belakang gateway, NAT, dan firewall standar). Sisa koneksi akan dirutekan melalui jaringan router redundan via TCP atau penerowongan https (https-tunnelling). Anda tidak harus membuka porta apa pun untuk bekerja dengan TeamViewer

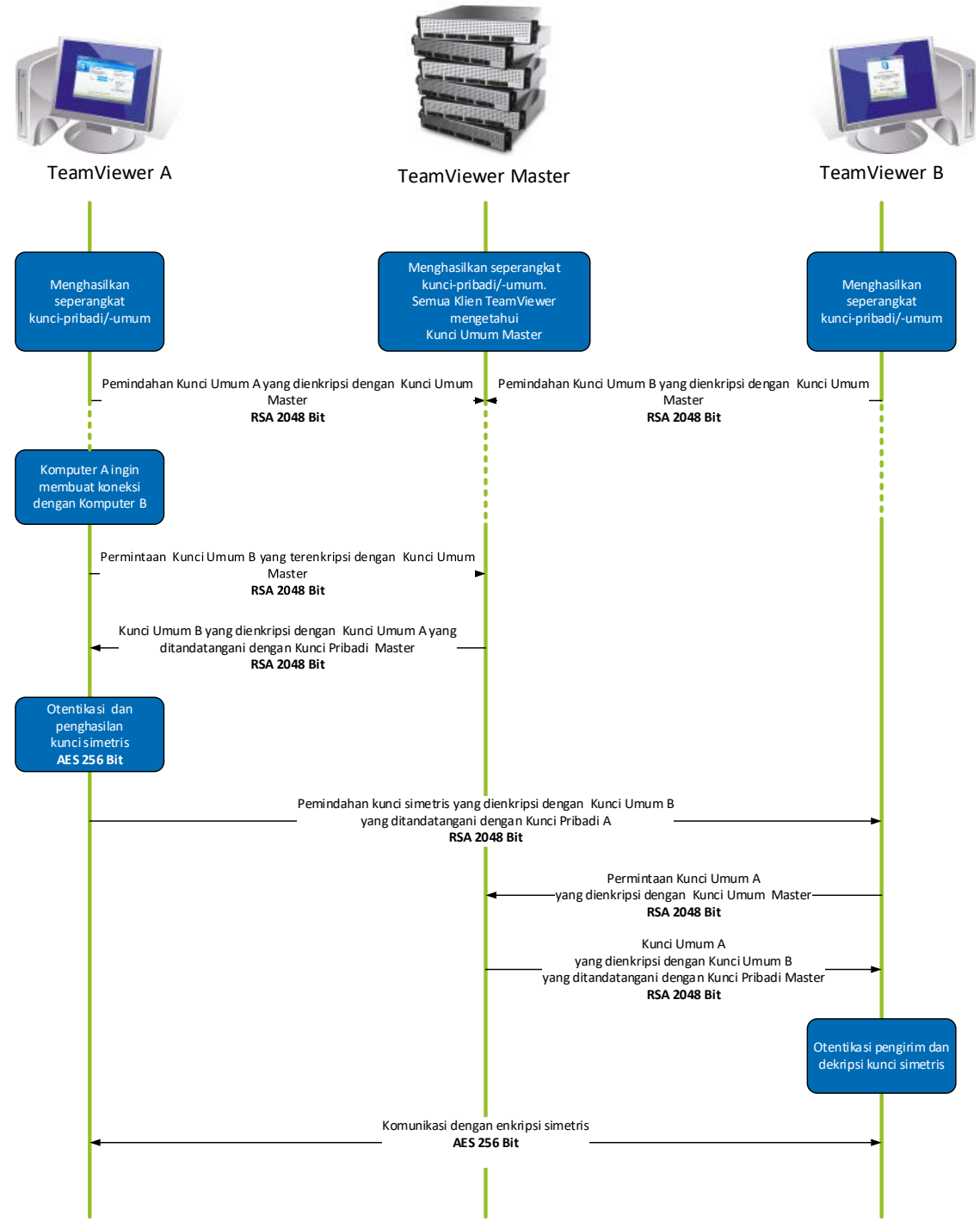
Seperti yang akan dijelaskan lebih lanjut dalam paragraf Enkripsi dan Autentikasi, tidak saja kami, sebagai operator server perutean, dapat membaca lalu lintas data yang terenkripsi.

Enkripsi dan Autentikasi

Lalu Lintas TeamViewer diamankan menggunakan pertukaran kode publik/pribadi RSA dan enkripsi sesi AES (256 bit). Teknologi ini digunakan dalam bentuk yang dapat dibandingkan untuk http/SSL dan dipertimbangkan benar-benar aman sesuai standar yang berlaku. Dikarenakan kode pribadi tidak pernah meninggalkan komputer klien, prosedur ini menjamin bahwa komputer yang terhubung satu sama lain - termasuk server perutean TeamViewer - tidak dapat menguraikan aliran data.

Setiap klien TeamViewer telah menerapkan kode publik dari cluster master, sehingga mengenkripsikan pesan ke cluster master dan memeriksa pesan yang tandatangani olehnya. PKI (Public Key Infrastructure) secara efektif melindungi serangan penyadapan (MITM/Man-in-the-Middle). Walaupun ada enkripsi, kata sandi tidak pernah dikirim secara langsung, namun hanya melalui prosedur respons tantangan, dan hanya disimpan di komputer lokal.

Selama autentikasi, kata sandi tidak pernah ditransfer secara langsung karena protokol Kata Sandi Jarak Jauh Aman (Secure Remote Password -SRP) digunakan. Hanya pemverifikasi kata sandi yang disimpan di komputer lokal.



Enkripsi dan autentikasi TeamViewer

Validasi ID TeamViewer

ID TeamViewer didasarkan pada berbagai karakteristik perangkat keras dan perangkat lunak dan dibuat secara otomatis oleh TeamViewer. Server TeamViewer memeriksa validitas ID ini sebelum setiap koneksi.

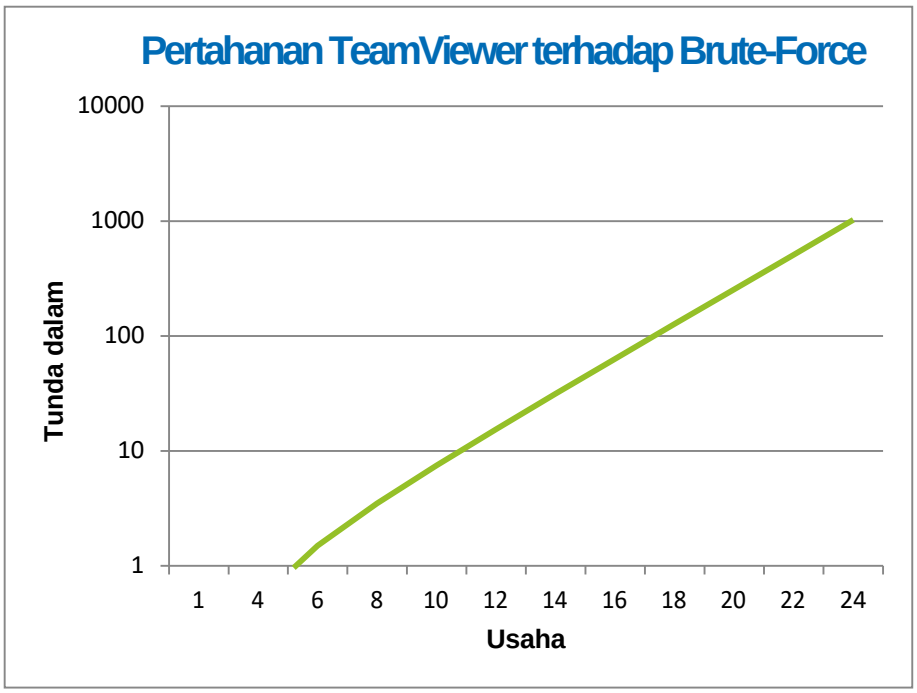
Proteksi terhadap Brute-Force (serangan brutal)

Pelanggan prospektif yang menanyakan tentang keamanan TeamViewer secara teratur meminta enkripsi ini. Dapat dipahami bahwa risiko yang paling dikhawatirkan adalah jika pihak ketiga dapat memantau koneksi atau jika data akses TeamViewer akan digunakan. Akan tetapi, realitasnya adalah bahwa serangan yang agak primitif seringkali merupakan serangan paling berbahaya.

Dalam konteks keamanan komputer, serangan brutal (brute-force) adalah metode uji coba untuk menebak kata sandi yang melindungi sumber data. Dengan daya komputasi yang meningkat dari komputer standar, waktu yang diperlukan untuk menebak kata sandi panjang telah sangat berkurang.

Sebagai pertahanan terhadap serangan brutal, TeamViewer meningkatkan penundaan usaha antar koneksi secara eksponen. Jadi, usaha ini perlu waktu selama 17 jam untuk 24 usaha. Latensi ini hanya berhasil direset setelah memasukkan kata sandi yang benar.

TeamViewer tidak hanya memiliki mekanisme untuk melindungi pelanggannya dari serangan satu komputer spesifik, namun juga dari beberapa komputer, yang dikenal sebagai serangan Botnet, yang mencoba mengakses satu ID TeamViewer khusus.



Grafik: Waktu yang dilewati setelah usaha koneksi selama serangan Brute Force

Penandatanganan Kode

Sebagai fitur keamanan tambahan, semua perangkat lunak kami ditandatangani via Penandatanganan Kode VeriSign. Dengan cara ini, penerbit perangkat lunak selalu dapat siap diidentifikasi. Jika kemudian perangkat lunak berubah, tanda tangan digital akan otomatis menjadi tidak valid.

Pusat Data & Tulang Punggung

Untuk memberikan keamanan terbaik dan ketersediaan layanan TeamViewer, semua server TeamViewer dilokasikan di pusat data center yang sesuai dengan ISO 27001, dan mengungkit koneksi pembawa multi-redundan dan pemasok daya redundan. Selanjutnya, hanya perangkat keras dengan merek paling mutakhir yang digunakan. Selain itu, semua server yang menyimpan data sensitif dilokasikan di Jerman atau Austria.

Memiliki status tersertifikasi ISO 27001 berarti bahwa kontrol akses pribadi, pengawasan kamera video, detektor gerakan, pemantauan 24x7 dan staf keamanan di lokasi memastikan akses ke pusat data hanya diberikan kepada orang-orang yang sah dan menjamin keamanan terbaik untuk perangkat keras dan data. Juga ada pemeriksaan identifikasi terperinci di titik entri tunggal ke pusat data.

Akun TeamViewer

Akun TeamViewer diselenggarakan di server TeamViewer khusus. Untuk informasi tentang kontrol akses, harap merujuk ke Pusat Data & Tulang Punggung di atas. Untuk otorisasi dan enkripsi kata sandi, protokol Secure Remote Password (SRP), protokol perjanjian kode yang disahkan kata sandi (PAKE) digunakan. Seorang infiltrator atau orang di posisi tengah tidak dapat memperoleh cukup informasi untuk dapat menebak kata sandi secara brutal. Hal ini berarti bahwa keamanan yang kuat bahkan dapat diperoleh menggunakan kata sandi lemah. Data sensitif dalam akun TeamViewer, misalnya informasi masuk penyimpanan cloud, disimpan dengan AES/RSA 2048 bit terenkripsi.

Konsol Manajemen

Konsol Manajemen TeamViewer adalah platform berbasis web untuk manajemen pengguna, pelaporan koneksi dan pengelolaan Komputer & Kontak. Fitur ini diselenggarakan dengan tersertifikasi ISO-27001, pusat data yang sesuai dengan HIPAA. Semua transfer data melalui saluran aman menggunakan enkripsi TSL (Transport Security Layer), standar untuk koneksi jaringan Internet yang aman. Data sensitif selanjutnya akan disimpan dengan AES/RSA 2048 bit terenkripsi. Untuk otorisasi dan enkripsi kata sandi, digunakan protokol Secure Remote Password (SRP). SRP adalah autentikasi berbasis kata sandi yang aman, kuat, dan stabil dan metode pertukaran kode menggunakan modulus 2048 bit.

Pengaturan Berbasis Kebijakan

Dari dalam Konsol Manajemen TeamViewer, para pengguna dapat menetapkan, mendistribusikan, dan melaksanakan kebijakan pengaturan untuk pemasangan perangkat lunak TeamViewer di berbagai perangkat terutama yang termasuk milik mereka. Kebijakan pengaturan ditandatangani secara digital oleh akun yang membuat kebijakan tersebut. Hal ini memastikan bahwa hanya akun yang diizinkan untuk menetapkan kebijakan ke perangkat adalah akun pemilik perangkat tersebut.

Keamanan Aplikasi dalam TeamViewer

Daftar Hitam & Putih

Khususnya jika TeamViewer digunakan untuk mengelola komputer yang tidak dihadiri (yaitu TeamViewer dipasang sebagai layanan Windows), opsi keamanan tambahan untuk membatasi akses ke komputer ini kepada sejumlah klien spesifik dapat menjadi salah satu perhatian.

Dengan fungsi daftar putih, Anda dapat mengindikasikan secara eksplisit ID TeamViewer dan/atau akun TeamViewer yang diizinkan untuk mengakses komputer. Dengan fungsi daftar hitam, Anda dapat memblokir ID TeamViewer dan akun TeamViewer tertentu. Daftar putih sentral tersedia sebagai bagian dari “pengaturan berbasis kebijakan” yang dijelaskan di atas pada “Konsol Manajemen.”

Enkripsi Obrolan dan Video

Riwayat obrolan terkait dengan akun TeamViewer Anda dan oleh karena itu dienkripsi dan disimpan menggunakan keamanan enkripsi AES/RSA 2048 bit yang sama seperti yang dijelaskan di bagian “Akun TeamViewer”. Semua lalu lintas pesan obrolan dan video dienkripsi ujung-ke-ujung menggunakan enkripsi sesi AES (256 bit).

Tidak Ada Mode Sembunyi

Tidak ada fungsi yang memungkinkan Anda membiarkan TeamViewer beroperasi sepenuhnya di latar belakang. Meskipun jika aplikasi beroperasi sebagai layanan Windows di latar belakang, TeamViewer selalu terlihat dengan adanya ikon di baki sistem.

Setelah koneksi terbentuk, akan selalu ada panel kontrol kecil yang terlihat di atas baki sistem. Dengan demikian, TeamViewer tidak sesuai untuk secara sengaja memantau komputer atau karyawan dengan diam-diam.

Perlindungan Kata Sandi

Untuk dukungan pelanggan spontan, TeamViewer (TeamViewer QuickSupport) membuat kata sandi sesi (kata sandi satu waktu). Jika pelanggan Anda memberi tahu kata sandinya kepada Anda, Anda dapat terhubung ke mereka dengan memasukkan ID dan kata sandi mereka. Setelah memulai ulang TeamViewer di lokasi pelanggan, kata sandi sesi yang baru akan dibuat sehingga Anda hanya dapat tersambung ke komputer pelanggan jika Anda diundang untuk melakukannya.

Saat menggunakan TeamViewer untuk dukungan jarak jauh yang tidak dihadiri (misalnya di beberapa server), Anda mengatur satu kata sandi tetap terpisah, yang mengamankan akses ke komputer itu.

Kontrol Akses Masuk dan Keluar

Anda dapat mengonfigurasikan mode koneksi TeamViewer secara terpisah. Misalnya, Anda dapat mengonfigurasikan dukungan jarak jauh atau komputer rapat dalam suatu cara di mana koneksi masuk tidak dimungkinkan.

Membatasi fungsi pada fitur yang sebetulnya diperlukan tersebut berarti membatasi kemungkinan titik lemah untuk serangan potensial.

Dua Autentikasi Faktor

TeamViewer membantu banyak perusahaan dengan persyaratan yang sesuai dengan HIPAA dan PCI. Autentikasi dua faktor menambah lapisan keamanan tambahan untuk melindungi akun TeamViewer dari akses yang tidak sah.

Sebagai tambahan untuk nama pengguna dan kata sandi, pengguna harus memasukkan kode untuk dapat disahkan. Kode ini dibuat via algoritma kata sandi satu waktu berbasis waktu (TOTP). Oleh karena itu, kode ini hanya valid untuk jangka waktu singkat.

Melalui autentikasi dua faktor dan membatasi akses dengan daftar putih, TeamViewer membantu dalam memenuhi semua kriteria penting untuk sertifikasi HIPAA dan PCI.

Pengujian Keamanan

Infrastruktur TeamViewer dan Perangkat Lunak TeamViewer tunduk pada uji penetrasi pada basis reguler. Pengujian ini dijalankan oleh perusahaan independen yang memiliki spesialisasi pada pengujian keamanan.

Pertanyaan Lebih Lanjut?

Untuk pertanyaan atau informasi lebih lanjut, hubungi kami di +1 803 015 203 9790 atau kirim email ke support@teamviewer.com.

Kontak

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