Información de seguridad de TeamViewer

Grupo objetivo

Este documento está destinado a administradores de redes profesionales. La información contenida en este documento es de naturaleza técnica y muy detallada. Basándose en esta información, los profesionales de TI obtendrán una imagen detallada acerca de los estándares de seguridad de TeamViewer permitiéndoles resolver cualquier duda antes de hacer uso de nuestro software. Puede distribuir este documento a sus clientes con el fin de resolver cualquier posible problema de seguridad.

Si considera que no forma parte del grupo objetivo, la información contenida en la sección "La compañía/el software" le ayudará a obtener una idea clara de cómo nos tomamos en serio la seguridad.

La compañía/el software

Sobre nosotros

TeamViewer GmbH fue fundada en 2005 y tiene su sede en la ciudad de Göppingen (cerca de Stuttgart), en el sur de Alemania, con filiales en Australia y los Estados Unidos. Desarrollamos y vendemos exclusivamente sistemas seguros para la colaboración basada en web. Nuestra licencia Freemium ha experimentado un rápido crecimiento en muy poco tiempo, con más de 200 millones de usuarios del software TeamViewer en más de 1.400 millones de dispositivos y en más de 200 países de todo el mundo. El software está disponible en más de 30 idiomas.

Nuestra forma de entender la seguridad

TeamViewer es utilizado por más de 30 millones de usuarios en un momento dado de un día cualquiera. Estos usuarios proveen soporte espontáneo a través de Internet accediendo a ordenadores desatendidos (es decir, soporte remoto para servidores) y para el hosting de reuniones en línea. Dependiendo de la configuración, TeamViewer puede ser utilizado para el control remoto de otro equipo, como si estuviera sentado directamente frente a él. Si el usuario que inicia sesión en un equipo remoto es un administrador de Windows, Mac o Linux, también se le concederán derechos de administrador en este equipo.

Es evidente que esta potente funcionalidad a través de un Internet potencialmente inseguro necesita ser minuciosamente protegida contra ataques. De hecho, el tema de la seguridad predomina en todos nuestros objetivos de desarrollo y es algo que vivimos y respiramos en todo lo que hacemos. Queremos garantizar que el acceso a su equipo sea seguro y, de este modo, proteger nuestros propios intereses: millones de usuarios en todo el mundo solo confían en una solución segura y solo una solución segura asegura el éxito de nuestro negocio a largo plazo.

Evaluación por expertos externos

Nuestro software, TeamViewer, ha sido galardonado con un sello de calidad de cinco estrellas (valor máximo) por la Asociación Federal de Expertos y Auditores en TI (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.). Los auditores independientes de BISG e.V. inspeccionan la calidad, seguridad y características de servicio de los productos de productores cualificados.

Referencias

Actualmente, TeamViewer es utilizado por más de 200 millones de usuarios. Las principales corporaciones internacionales de todo tipo de industrias (incluidos sectores tan sensibles como la banca, las finanzas, la sanidad y el gobierno) están utilizando TeamViewer satisfactoriamente.

Le invitamos a echar un vistazo a nuestras referencias que se pueden encontrar en Internet con el fin de obtener una primera impresión de la aceptación de nuestra solución. Se dará cuenta de que, probablemente, la mayoría de las otras compañías tenían requisitos de seguridad y disponibilidad similares antes de que finalmente, y después de un examen exhaustivo, se decidieran por TeamViewer. No obstante, en el resto del documento encontrará algunos detalles técnicos para que pueda formarse su propia opinión.

Sesiones TeamViewer

Creación de una sesión y tipos de conexiones

Cuando se establece una sesión, TeamViewer determina el tipo óptimo de conexión. Después de la conexión a través de nuestros servidores maestros, en el 70 % de los casos se establece una conexión directa a través de UDP o TCP (incluso en equipos protegidos por puertas de enlace predeterminadas, NAT y cortafuegos). El resto de las conexiones se realizan a través de nuestra red de enrutadores altamente redundante a través de TCP o tunelización https. No necesita abrir ningún puerto para poder trabajar con TeamViewer

Como se describe más adelante en el párrafo "Cifrado y autenticación", ni siquiera nosotros, como operadores de los servidores de enrutamiento, podemos leer el tráfico de datos cifrados.

Cifrado y autenticación

El tráfico de TeamViewer se protege mediante el intercambio de claves públicas y privadas RSA y el cifrado de sesión AES (256 bits). Esta tecnología se utiliza en una forma comparable a http/SSL y es considerada completamente segura por los estándares actuales. Como la clave privada nunca sale del equipo del cliente, este procedimiento garantiza que los equipos interconectados, incluidos los servidores de enrutamiento de TeamViewer, no pueden descifrar el flujo de datos.

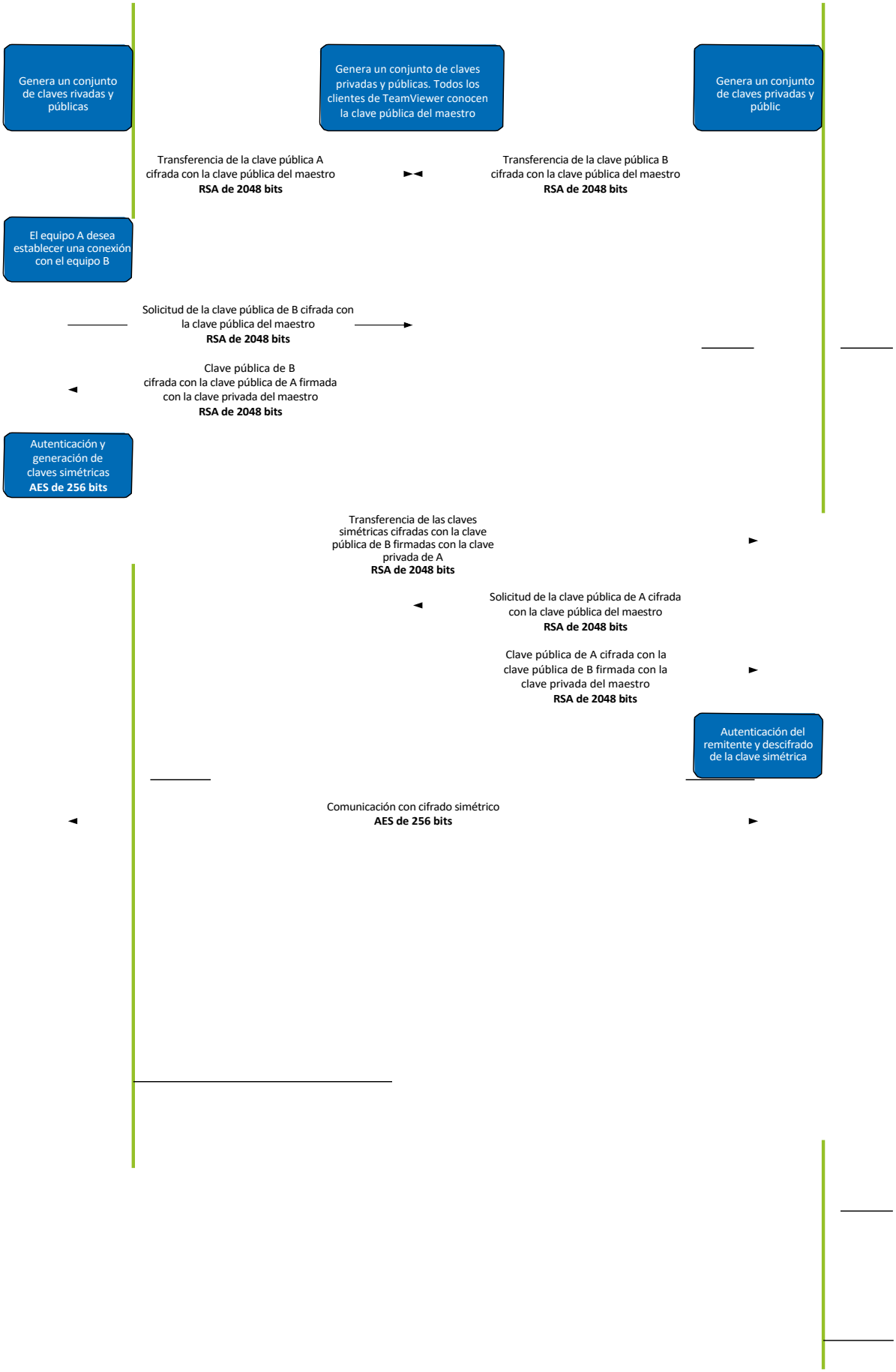
Cada cliente TeamViewer ya tiene implementada la clave pública del clúster maestro y, por lo tanto, puede cifrar los mensajes en el clúster maestro y comprobar los mensajes firmados por él. La PKI (infraestructura de clave pública) evita eficazmente los ataques de intermediarios (man-in-the-middle). A pesar del cifrado, la contraseña nunca se envía directamente, sino solo a través de un procedimiento de desafío-respuesta y solamente se guarda en el equipo local.

Durante el proceso de autenticación, la contraseña nunca se transfiere directamente, ya que se utiliza un protocolo de contraseña remota segura (SRP). En el equipo local únicamente se almacena el verificador

TeamViewer A

TeamViewer Master

TeamViewer B


Genera un conjunto de claves rivadas y públicas
Genera un conjunto de claves privadas y públicas. Todos los clientes de TeamViewer conocen la clave pública del maestro
Genera un conjunto de claves privadas y públic
Transferencia de la clave pública A cifrada con la clave pública del maestro
RSA de 2048 bits
Transferencia de la clave pública B cifrada con la clave pública del maestro
RSA de 2048 bits
El equipo A desea establecer una conexión con el equipo B
Solicitud de la clave pública de B cifrada con la clave pública del maestro
RSA de 2048 bits
Clave pública de B cifrada con la clave pública de A firmada con la clave privada del maestro
RSA de 2048 bits
Autenticación y generación de claves simétricas
AES de 256 bits
Transferencia de las claves simétricas cifradas con la clave pública de B firmadas con la clave privada de A
RSA de 2048 bits
Solicitud de la clave pública de A cifrada con la clave pública del maestro
RSA de 2048 bits
Clave pública de A cifrada con la clave pública de B firmada con la clave privada del maestro
RSA de 2048 bits
Autenticación del remitente y descifrado de la clave simétrica
Comunicación con cifrado simétrico
AES de 256 bits

Cifrado y autenticación de TeamViewer

Validación de los identificadores de TeamViewer

Los identificadores de TeamViewer se basan en diversas características de hardware y software y son generados automáticamente por TeamViewer. Los servidores de TeamViewer comprueban la validez de estos identificadores antes de cada conexión.

Protección contra ataques de fuerza bruta

Los clientes potenciales que realizan consultas acerca de la seguridad de TeamViewer suelen preguntar por el cifrado. Es comprensible que los mayores temores se centren en el riesgo de que un tercero pueda monitorear la conexión o utilizar los datos de acceso de TeamViewer. Sin embargo, la realidad es que los ataques más elementales suelen ser los más peligrosos.

En el contexto de la seguridad informática, un ataque de fuerza bruta es un método de prueba y error con el fin de adivinar la contraseña que protege un recurso. El crecimiento del poder de cálculo de las computadoras estándar ha reducido significativamente el tiempo necesario para adivinar contraseñas largas.

Como una defensa contra los ataques de fuerza bruta, TeamViewer ha incrementado exponencialmente el retraso entre los intentos de conexión. Por consiguiente, se necesitan hasta 17 horas para realizar 24 intentos. Esta latencia solo se restablece una vez introducida la contraseña correcta.

TeamViewer no solo cuenta con un mecanismo para proteger a sus clientes de ataques de un equipo específico, sino también de ataques procedentes de múltiples equipos, conocidos como ataques de botnet, que intentan acceder a un identificador de TeamViewer en particular.

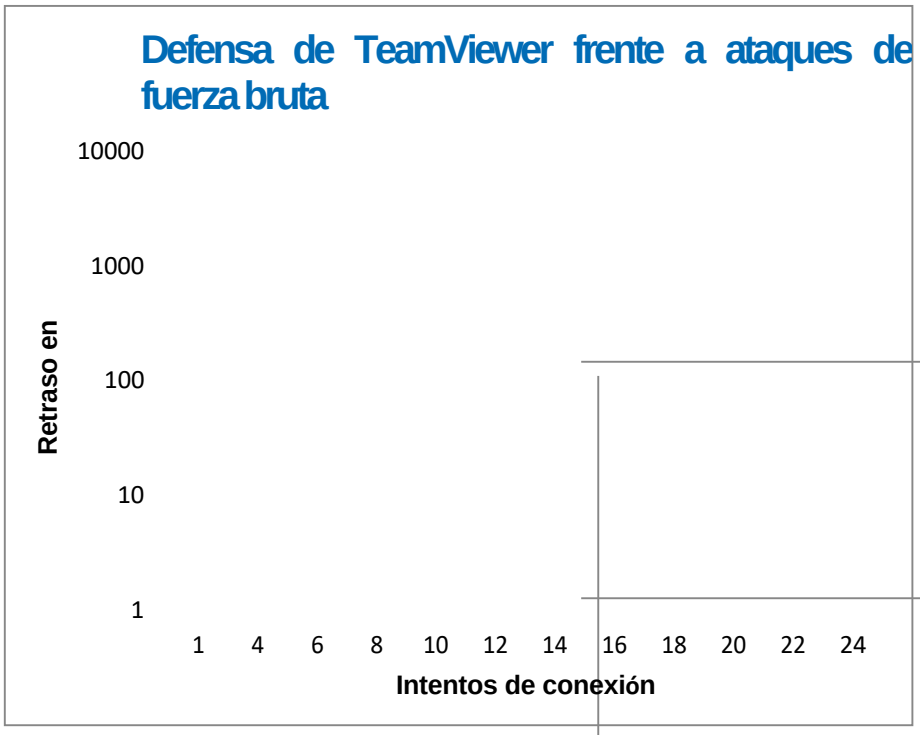


Gráfico: Tiempo transcurrido después de n intentos de conexión durante un ataque de fuerza bruta

Firma de código

Como una característica de seguridad adicional, todo nuestro software se firma a través de la firma de código de VeriSign. De este modo, el editor del software siempre es fácilmente identificable. Si el software se modifica con posterioridad, la firma digital se invalida automáticamente.

Centro de datos y red central

Con el fin de proporcionar la mejor seguridad y disponibilidad posible de los servicios de TeamViewer, todos los servidores de TeamViewer están localizados en centros de datos que cumplen con la norma ISO 27001 y hacen uso de conexiones de portador multirredundantes y fuentes de alimentación redundantes. Además, solo se utiliza hardware de marcas punteras. Adicionalmente, todos los servidores que almacenan datos sensibles están ubicados en Alemania o Austria.

La certificación ISO 27001 significa que el control de acceso personal, la videovigilancia, los detectores de movimiento, la monitorización 24x7, así como el personal de seguridad in situ garantizan que el acceso al centro de datos solo se concede a personas autorizadas y aseguran la mejor seguridad posible para el hardware y los datos. También se efectúa una minuciosa verificación de identificación en el punto de entrada único al centro de datos.

Cuenta TeamViewer

Las cuentas de TeamViewer se alojan en servidores TeamViewer dedicados. Para obtener información acerca del control de acceso, consulte la sección anterior "Centro de datos y red central". Para el cifrado de autorizaciones y contraseñas se utiliza el protocolo de contraseña remota segura (SRP), un protocolo aumentado de establecimiento autenticado de claves de contraseña (PAKE). Un infiltrador o intermediario (man in the middle) no es capaz de obtener la información suficiente para poder adivinar una contraseña mediante la fuerza bruta. Esto significa que es posible obtener una seguridad sólida incluso utilizando contraseñas débiles. Los datos sensibles de una cuenta TeamViewer, por ejemplo, la información de inicio de sesión del almacenamiento en la nube se almacena con cifrado AES/RSA de 2048 bits.

Consola de gestión

La consola de gestión de TeamViewer es una plataforma basada en web para la gestión de usuarios, la generación de informes de conexión y la gestión de equipos y contactos. Se aloja en centros de datos con certificación ISO 27001 y de conformidad con la HIPAA. Todas las transferencias de datos se efectúan a través de canales seguros utilizando cifrado TSL (Transport Security Layer), el estándar para las conexiones seguras a la red de Internet. Además, los datos sensibles se almacenan cifrados con AES/RSA de 2048 bits. Para el cifrado de autorizaciones y contraseñas se utiliza el protocolo de contraseña remota segura (SRP). SRP es un protocolo de autenticación bien establecido y robusto, basado en contraseña segura con intercambio de claves que utiliza un módulo de 2048 bits.

Configuración basada en políticas

Desde la consola de gestión de TeamViewer, los usuarios pueden definir, distribuir y aplicar políticas de configuración para las instalaciones de software de TeamViewer en dispositivos que les pertenezcan específicamente. Las políticas de configuración están firmadas digitalmente por la cuenta que las generó. Esto asegura que la única cuenta que tiene permiso para asignar una política a un dispositivo es la cuenta a la que pertenece el dispositivo.

Seguridad de aplicaciones en TeamViewer

Lista negra y lista blanca

Especialmente, si TeamViewer se utiliza para mantener equipos desatendidos (es decir, TeamViewer se instala como un servicio de Windows), podría ser de interés la función de seguridad adicional que permite restringir el acceso a estos equipos a un número específico de clientes.

Con la función de lista blanca es posible especificar explícitamente qué identificadores y/o cuentas de TeamViewer tienen acceso al equipo. Mediante la función de lista negra es posible bloquear ciertos identificadores y cuentas de TeamViewer. Una lista blanca central está disponible como parte de la "configuración basada en políticas" descrita anteriormente en la sección "Consola de gestión".

Cifrado de chat y vídeo

Los historiales de chat están asociados a su cuenta TeamViewer y, por lo tanto, se cifran y almacenan utilizando la misma seguridad de cifrado AES/RSA de 2048 bits descrita en la sección "Cuenta TeamViewer". Todos los mensajes de chat y el tráfico de vídeo se cifran de extremo a extremo utilizando el cifrado de sesión AES (256 bits).

Sin modo oculto

No existe ninguna función que le permita tener TeamViewer ejecutándose completamente en segundo plano. Incluso cuando la aplicación se está ejecutando como un servicio de Windows en segundo plano, TeamViewer siempre está visible por medio de un icono en la bandeja del sistema.

Una vez establecida la conexión, siempre hay un pequeño panel de control visible sobre la bandeja del sistema. De este modo, TeamViewer es deliberadamente inadecuado para la supervisión encubierta de equipos o empleados.

Protección de contraseñas

TeamViewer (TeamViewer QuickSupport) genera una contraseña de sesión (contraseña de un solo uso) para el soporte espontáneo del cliente. Si su cliente le facilita la contraseña, podrá conectarse a su equipo introduciendo su identificador y la contraseña facilitada. Si el cliente reinicia TeamViewer, se generará una contraseña de sesión nueva, de modo que solamente podrá conectarse a los equipos de su cliente si éste le invita a hacerlo.

Cuando TeamViewer se implementa para el soporte remoto desatendido (p. ej., de servidores), se establece una contraseña fija individual que protege el acceso al equipo.

Control de acceso entrante y saliente

Los modos de conexión de TeamViewer se pueden configurar individualmente. Por ejemplo, puede configurar su soporte remoto o de reunión de manera que no se permitan conexiones entrantes.

Limitar la funcionalidad a aquellas características realmente necesarias siempre significa limitar posibles puntos débiles para ataques potenciales.

Autenticación de dos factores

TeamViewer apoya el cumplimiento de las empresas con los requisitos normativos de HIPAA y PCI. La autenticación de dos factores añade una capa de seguridad adicional para proteger las cuentas de TeamViewer contra el acceso no autorizado.

Además del nombre de usuario y la contraseña, el usuario también debe introducir un código para poder autenticarse. Este código se genera por medio de un algoritmo generador de contraseñas de un solo uso y basado en tiempo (TOTP). Por consiguiente, el código solamente es válido durante un corto periodo de tiempo.

Gracias a la autenticación de dos factores y el acceso limitado mediante listas blancas, TeamViewer ayuda a cumplir con todos los criterios necesarios para la certificación HIPAA y PCI.

Pruebas de seguridad

Tanto la infraestructura de TeamViewer como el software TeamViewer son sometidos periódicamente a pruebas de penetración. Las pruebas son llevadas a cabo por empresas independientes especializadas en pruebas de seguridad.

¿Tiene más preguntas?

Si tiene más preguntas o desea recibir información adicional, no dude en ponerse en contacto con nosotros llamando al +34 931 842 346 o envíenos un correo electrónico a support@teamviewer.com.

Contacto

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