Informações de segurança do TeamViewer

Grupo em foco

Este documento destina-se aos administradores de redes profissionais. As informações nele contidas são de natureza técnica e bastante minuciosas. Com base nessas informações, os profissionais de TI podem ter uma noção mais detalhada da segurança do software antes de instalar o TeamViewer. Você pode distribuir este documento a seus clientes para solucionar possíveis questões de segurança.

Caso você não se considere como pertencente ao grupoem foco, os fatos da seção "A Empresa/ o Software" o ajudarão a ter uma ideia subjetiva sobre o assunto.

A Empresa /o Software

Sobre nós

Fundada em 2005, a TeamViewer GmbH está sediada na cidade alemã de Göppingen próximo a Stuttgart. Lidamos exclusivamente com o desenvolvimento e com a venda de sistemas de alta segurança para dar apoio via web. O rápido início e crescimento de nossa firma se deve às milhões de instalações do software TeamViewer, com usuários em mais de 200 países no mundo inteiro e dentro de um curto período de tempo. E atualmente, nosso software está disponível em mais de 30 idiomas.

O que entendemos por segurança

O TeamViewer é utilizado milhões de vezes no mundo inteiro, para oferecer suporte instantâneo pela internet ou para acessar computadores sem supervisão (por exemplo, como suporte remoto para servidores). Dependendo da configuração do TeamViewer, isso significa que o computador remoto pode ser controlado como se você estivesse sentado à sua frente. Se o usuário que estiver conectado em um computador remoto for um administrador de Windows, Mac ou Linux, também terá direitos de administrador nesse computador.

Obviamente que uma funcionalidade tão poderosa pela internet, um ambiente potencialmente inseguro, precisa estar protegida de várias formas contra os possíveis ataques. Na verdade, o tópico da segurança é para nós um dos mais importantes de todas as nossas outras metas de desenvolvimento: primeiro para tornar o acesso ao seu computador seguro e segundo também em nosso próprio interesse. Nossos clientes, milhões de usuários em todo o mundo, só poderiam confiar em uma solução segura, e apenas uma solução segura pode garantir nosso sucesso a longo prazo como empresa.

Gerenciamento da qualidade

Ao nosso entender, a administração da segurança é um processo impensável se não houver um gerenciamento de qualidade implementado. A TeamViewer GmbH é uma das poucas fornecedoras do mercado que pratica um gerenciamento de qualidade certificado, de acordo com a norma ISO 9001. Nosso gerenciamento de qualidade obedece aos padrões reconhecidos internacionalmente. Nosso sistema de GQ é controlado anualmente por auditorias externas.

Avaliação por peritos externos

Nosso software TeamViewer recebeu um selo de qualidade (valor máximo) da Associação Federal de Peritos e Revisores de TI (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.). Os revisores autônomos da BISG e.V. inspecionam os produtos de fabricantes qualificados quanto à sua qualidade, segurança e à qualidade dos serviços.

Inspeção de segurança

O TeamViewer foi submetido a uma verificação de segurança pelas empresas alemãs FIDUCIA IT AG e GAD eG (operadores de centros de processamento de dados para cerca de 1200 bancos) e aprovado para a utilização em estações de trabalho até em bancos.

Referências

Neste momento, o TeamViewer está sendo utilizado em mais de 200.000.000 computadores. As maiores corporações internacionais de todos os tipos de indústrias (inclusive de setores altamente complexos e frágeis, como bancos e outras instituições financeiras) estão utilizando o TeamViewer com sucesso.

Sugerimos que consulte nossas referências na internet para obter uma primeira impressão de como nossa solução está sendo aceita. Com certeza você concordará que, supostamente, a maioria das empresas possui requisitos de segurança e disponibilidade semelhantes pelos quais nossos produtos, através de uma análise extensiva e intensiva têm que passar, antes que se decida pela utilização do TeamViewer. Mesmo assim, para que você tenha sua própria impressão, verifique alguns detalhes técnicos nos parágrafos a seguir.

Criação e operação de uma sessão no TeamViewer

Criação de uma sessão e tipos de conexões.

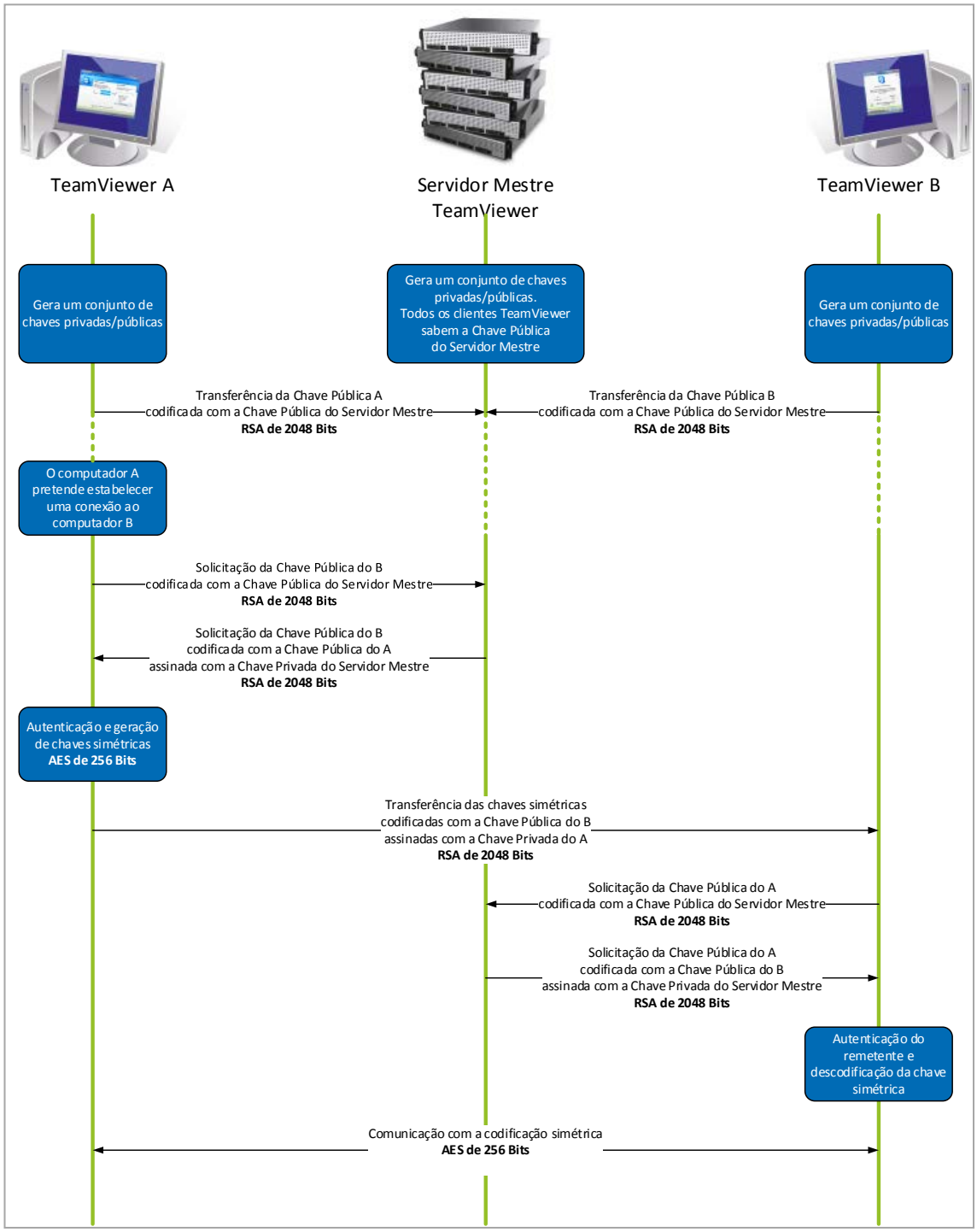
Ao criar uma sessão, o TeamViewer determina o tipo de conexão ideal. Após o handshake feito através de nosso servidores mestre, em 70% dos casos é estabelecida uma conexão direta via UDP ou TCP (mesmo passando por gateways padrão, NATs e firewalls). O restante das conexões é encaminhado através de nossa rede de routers altamente complexa via TCP ou http-tunnelling. Não é necessário abrir qualquer porta para trabalhar com o TeamViewer!

Como descrito mais adiante no parágrafo "Criptografia e autenticação", nem mesmo nós, operadores dos servidores de encaminhamento, podemos ler o tráfego de dados criptografados.

Criptografia e autenticação

O TeamViewer trabalha com uma criptografia completa, baseada no RSA public/private key exchange e AES (256 Bit) session encoding. Essa tecnologia é utilizada de uma forma comparável para https/SSL, podendo ser considerada totalmente segura, pelos padrões atuais. Como a chave privada nunca sai do computador cliente, esse procedimento garante que os computadores interconectados, incluindo os servidores de rota do TeamViewer, não possam decifrar os dados transmitidos.

Cada cliente do TeamViewer já terá implementado a chave pública do cluster mestre, e por isso poderá criptografar mensagens para o servidor mestre e verificar sua assinatura, respectivamente. A PKI (Public Key Infrastructure) previne efetivamente os ataques do tipo "Man-in-the-middle". Apesar da criptografia, a senha nunca é enviada diretamente, mas sim através de um procedimento de desafio-resposta, sendo gravada apenas no computador local.



Criptografia e autenticação no TeamViewer

Validação das IDs do TeamViewer

As IDs do TeamViewer são automaticamente geradas pelo próprio TeamViewer, com base nas características do hardware. Os servidores do TeamViewer verificam a validade da ID antes de cada conexão, por isso não é possível gerar e utilizar IDs falsas.

Proteção contra ataques de força bruta

Quando os clientes potencia is fazem perguntas sobre a segurança do TeamViewer, normalmente perguntam sobre a criptografia. Como se pode entender, o risco de que uma terceira pessoa obtenha acesso à conexão ou de que os dados de acesso ao TeamViewer estejam sendo captados ou interrompidos são os mais temidos. Na verdade, os ataques mais perigosos são frequentemente os mais primitivos.

No contexto de segurança do computador, os ataques de força bruta são geralmente tentativas de adivinhar uma senha que esteja protegendo um recurso, usando o método de tentativa e erro. Com o aumento do poder de cálculo dos computadores padrões, o tempo necessário para adivinhar até mesmo uma senha mais longa tem se reduzido cada vez mais.

Como defesa contra os ataques de força bruta, o TeamViewer aumenta exponencialmente a latência entre as tentativas de conexão. Para 24 tentativas, o tempo necessário é de 17 horas. A latência só é reiniciada depois que se introduz a senha corretamente.

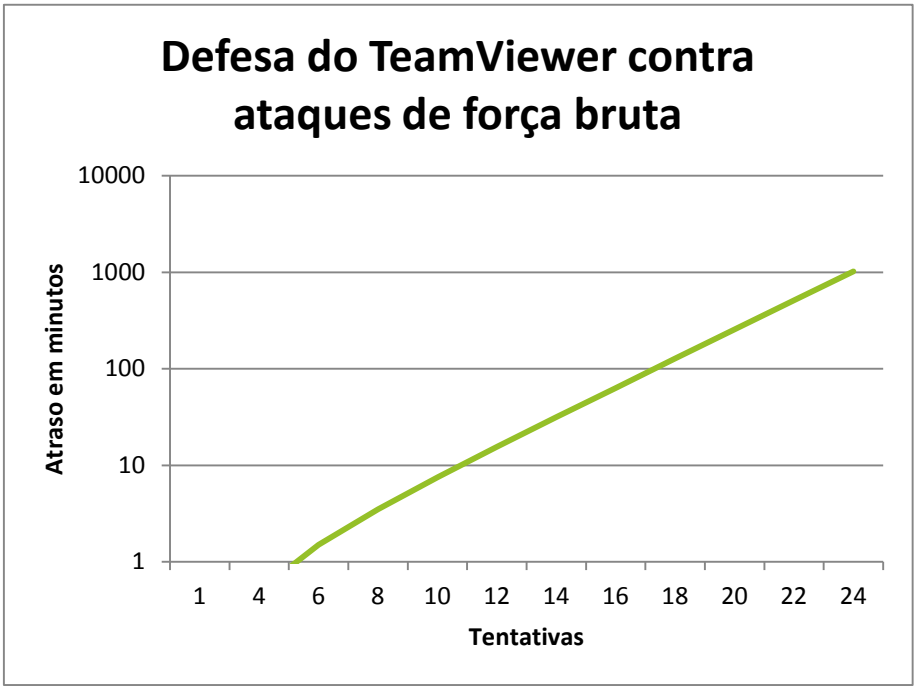


Gráfico: Tempo decorrido após n tentativas de conexão, durante um ataque de força bruta

Assinatura por códigos

Como recurso de segurança adicional, todos os nossos programas são assinado através de VeriSign Code Signing. Por esse motivo, é sempre possível identificar de forma confiável o publicador do software. Caso o software tenha sido modificado posteriormente, a assinatura digital torna-se automaticamente inválida. Até os módulos personalizáveis são assinado de maneira dinâmica enquanto está sendo gerado.

Centro de dados & backbone

Esses dois tópicos dizem respeito à disponibilidade, bem como à segurança. Os servidores centrais do TeamViewer estão localizados em um centro de dados ultra moderno com suporte de conexão multi-redundante e fonte de alimentação redundante. O hardware utilizado é exclusivamente com marca de nome (Cisco, Foundry, Juniper).

O acesso ao centro de dados só é possível após uma minuciosa verificação da identidade, feita através de um único gate de entrada. Um sistema CCTV, detecção de incursão, vigilância 24 horas por dia 7 dias por semana, e uma equipe de segurança local protege nossos servidores contra ataques internos.

Segurança das aplicações no TeamViewer

Lista negra e branca

Principalmente se o TeamViewer for utilizado para a manutenção de computadores sem supervisão (ou seja, se o TeamViewer estiver instalado como um serviço do Windows), isto pode ser útil, além de todos os outros mecanismos de segurança, para restringir o acesso a esses computadores para um determinado número de clientes.

Com a função de lista branca, você pode indicar explicitamente que IDs do TeamViewer podem acessar esse computador, e com a função de lista negra, você pode bloquear determinadas IDs do TeamViewer.

Sem modo Stealth

Não existe nenhuma função que lhe permite utilizar o TeamViewer totalmente invisível. Mesmo que a aplicação esteja sendo executada como serviço do Windows em segundo plano, o TeamViewer fica sempre visível através de um ícone no gerenciador de tarefas.

Depois de estabelecida uma conexão, existe sempre um pequeno painel de controle visível acima do gerenciador de tarefas, e portanto o TeamViewer não pode ser utilizado intencionalmente para monitorar secretamente os computadores ou funcionários.

Proteção por senha

Para efetuar o suporte instantâneo dos clientes, o TeamViewer (TeamViewer QuickSupport) gera uma senha para cada sessão a qual é, portanto, utilizada uma única vez. Se seu cliente lhe informar sua senha, você pode conectar-se ao respectivo computador, inserindo a ID e a senha. Após uma reinicialização no lado do cliente, será gerada uma nova senha de sessão, de forma que você só poderá acessar os computadores dos clientes caso você seja explicitamente convidado a fazê-lo.

Ao utilizar o TeamViewer para suporte remoto não supervisionado (por exemplo, em servidores), você define uma senha fixa individual, que lhe garante o acesso a esse computador.

Controle de acesso na entrada e na saída

Você pode configurar individualmente os modos de conexão do TeamViewer. Por exemplo, pode configurar seu computador de apresentação ou de suporte remoto de forma que não seja possível receber conexões.

Limitar a funcionalidade às funções realmente necessárias significa limitar os possíveis pontos vulneráveis a possíveis ataques.

Autentição de dois fatores

TeamViewer ajuda empresas com suas especificações de conformidade com a HIPAA e a PCI. A autenticação de dois fatores adiciona uma nível extra de segurança para proteger as contas TeamViewer de acesso não autorizado. Junto com o controle de acesso por meio da lista branca, o TeamViewer permite que você esteja pronto para HIPAA e PCI.

Com a autenticação de dois fatores, mais o nome do usuário e a senha, um código gerado em um dispositivo móvel é necessário para acessar uma conta TeamViewer. O código é gerado por meio do algoritmo da senha dinâmica baseada em tempo (TOTP).

Alguma pergunta?

Se tiver qualquer pergunta, teremos muito prazer em atender sua ligação para os números (BR) 0 800 892 2167 e (PT) +351 800 863 340 ou em responder a seus e-mails enviados para support@teamviewer.com.

Empresas

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

Diretoria: Holger Felgner
Registro: Ulm HRB 534075