Informação de Segurança TeamViewer

Grupo-Alvo

Esse documento é direcionado para administradores de rede profissional. A informação contida nesse documento é de natureza bastante técnica e muito detalhada. Com base nestas informações, os profissionais de TI receberão uma imagem detalhada dos padrões de segurança no TeamViewer e terão quaisquer preocupações resolvidas antes de implementar o nosso software. Sinta-se à vontade para distribuir este documento para seus clientes, a fim de aliviar possíveis preocupações de segurança.

Se você não se considera parte do grupo-alvo, os fatos da seção A Empresa / o Software ainda o ajudarão a ter uma visão clara de como levamos a segurança a sério.

A Empresa / o Software

Sobre nós

A TeamViewer GmbH foi fundada em 2005 e está localizada no sul da Alemanha, na cidade de Göppingen (perto de Stuttgart), com subsidiárias na Austrália e nos Estados Unidos. Nós desenvolvemos e vendemos exclusivamente sistemas seguros para colaboração baseada na web. Em um curto espaço de tempo, nosso licenciamento Freemium teve um rápido crescimento, com mais de 200 milhões de usuários do software TeamViewer em mais de 1,4 bilhões de dispositivos, em mais de 200 países ao redor do globo. O software está disponível em mais de 30 idiomas.

Nossa Compreensão de Segurança

TeamViewer é usado por mais de 30 milhões de usuários em qualquer ponto, em qualquer dia. Esses usuários estão fornecendo suporte espontâneo através da Internet, acessando computadores autônomos (ou seja, suporte remoto para servidores) e para hospedar reuniões online. Dependendo da configuração, o TeamViewer pode ser usado para controlar remotamente outro computador, como se você estivesse sentado diretamente na frente dele. Se o usuário conectado a um computador remoto for um administrador do Windows, do Mac ou do Linux, essa pessoa receberá direitos de administrador nesse computador também.

É claro que tal funcionalidade tão poderosa sobre a Internet potencialmente insegura deve ser protegida contra os ataques com grande minúcia. Na verdade, o tema da segurança domina todos os nossos objetivos de desenvolvimento e é algo que vivemos e respiramos em tudo o que fazemos. Queremos garantir que o acesso ao seu computador seja seguro e proteger os nossos próprios interesses: milhões de usuários em todo o mundo só confiam numa solução segura e apenas uma solução segura garante o nosso sucesso a longo prazo como um negócio.

Avaliação Externa de Peritos

O nosso software, TeamViewer, foi premiado com um selo de qualidade de cinco estrelas (valor máximo) pela Associação Federal de Peritos e Revisores de TI (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.). Os revisores independentes da BISG e.V. inspecionam os produtos de produtores qualificados pelas suas características de qualidade, segurança e serviço.

Referências

Atualmente, TeamViewer é utilizado por mais de 200 milhões de usuários. Corporações internacionais de todos os tipos de indústrias (incluindo setores altamente sensíveis como bancos, finanças, saúde e governo) estão usando o TeamViewer com êxito.

Convidamo-lo a dar uma olhada nas nossas referências encontradas em toda a Internet, a fim de obter uma primeira impressão da aceitação da nossa solução. Você descobrirá que, presumivelmente, a maioria das outras empresas tinham requisitos semelhantes de segurança e disponibilidade antes que eles - após um exame intensivo - finalmente decidissem pelo TeamViewer. Para formar sua própria impressão, por favor, encontre alguns detalhes técnicos no restante deste documento.

Sessões TeamViewer

Criando uma Sessão e Tipos de Conexões

Ao estabelecer uma sessão, TeamViewer determina o tipo ideal de conexão. Após o handshake (reconhecimento digital) através de nossos servidores mestres, uma conexão direta via UDP ou TCP é estabelecida em 70% de todos os casos (mesmo atrás de gateways padrão, NATs e firewalls). O resto das conexões é encaminhada através de nossa rede de roteadores altamente redundantes via TCP ou encapsulamento https. Você não precisa abrir nenhuma porta para trabalhar com o TeamViewer

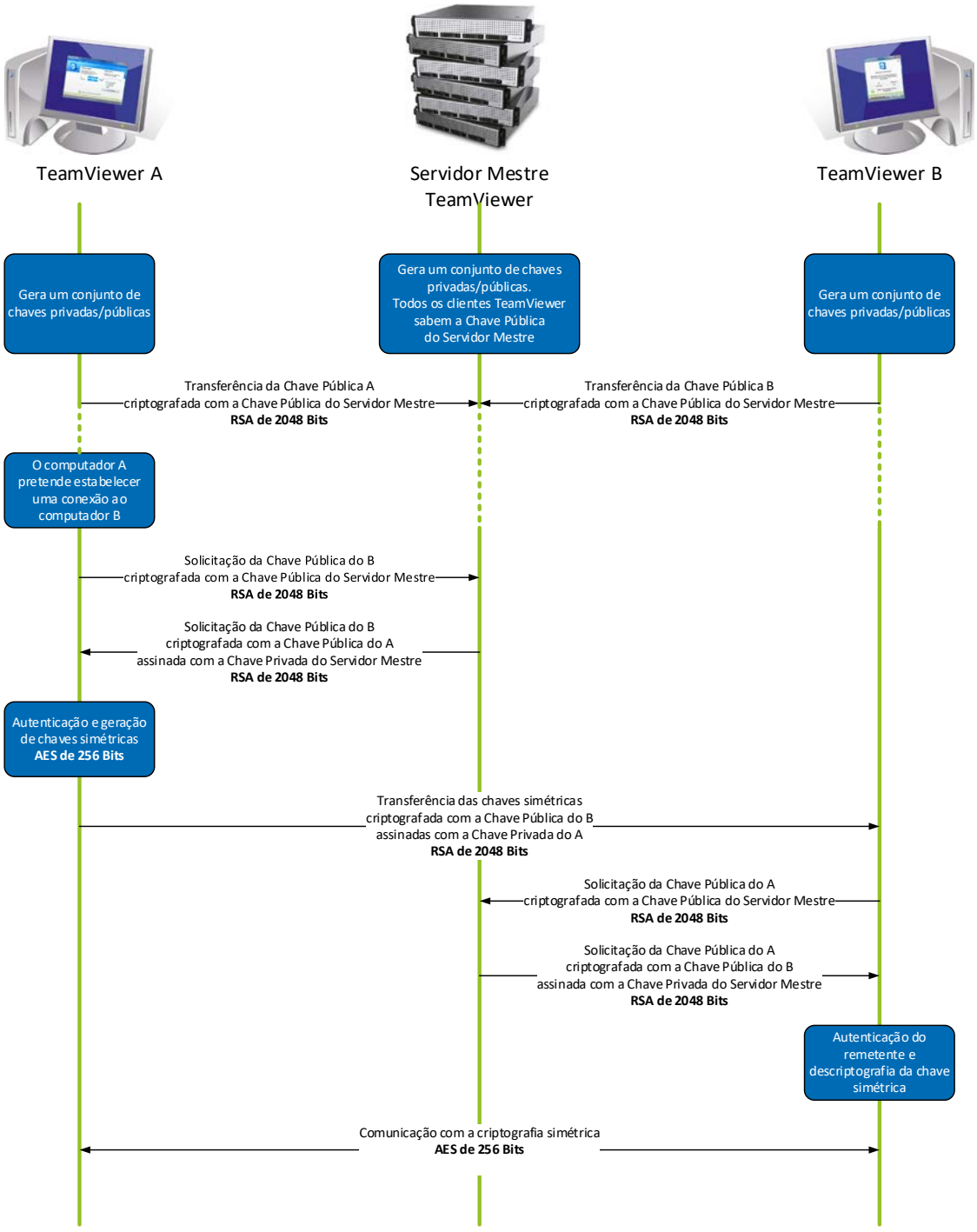
Como descrito mais adiante no parágrafo Criptografia e Autenticação, nem mesmo nós, como os operadores dos servidores de roteamento, podemos ler o tráfego de dados criptografados.

Criptografia e Autenticação

O TeamViewer Traffic é protegido usando a troca de chaves pública/privada RSA e criptografia de sessão AES (256 bit). Esta tecnologia é usada de forma comparável para http/SSL e é considerada completamente segura pelos padrões atuais. Como a chave privada nunca sai do computador cliente, esse procedimento garante que computadores interconectados - incluindo os servidores de roteamento TeamViewer - não possam decifrar o fluxo de dados.

Cada cliente TeamViewer já implementou a chave pública do cluster principal e, portanto, pode criptografar mensagens para o cluster principal e verificar as mensagens assinadas por ele. A infra-estrutura de chave pública (PKI) impede eficazmente os ataques de “man-in-the-middle”. Apesar da criptografia, a senha nunca é enviada diretamente, mas apenas através de um procedimento de resposta a desafio, e é salva somente no computador local.

Durante a autenticação, a senha nunca é transferida diretamente porque o protocolo Secure Remote Password (SRP) é usado. Somente um verificador de senha é armazenado no computador local.



Criptografia e autenticação TeamViewer

Validação de IDs da TeamViewer

Os IDs do TeamViewer são baseados em várias características de hardware e software e são gerados automaticamente pelo TeamViewer. Os servidores TeamViewer verificam a validade desses IDs antes de cada conexão.

Proteção de Força Bruta

Clientes potenciais que perguntam sobre a segurança do TeamViewer regularmente perguntam sobre criptografia. Compreensivelmente, o risco de que um terceiro possa monitorar a conexão ou que os dados de acesso do TeamViewer estejam sendo aproveitados é o que mais temem. No entanto, a realidade é que os ataques primitivos são muitas vezes os mais perigosos.

No contexto da segurança do computador, um ataque de força bruta é um método de tentativa e erro para adivinhar uma senha que está protegendo um recurso. Com o crescente poder de computação dos computadores padrão, o tempo necessário para adivinhar senhas longas tem sido cada vez mais reduzido.

Como uma defesa contra os ataques de força bruta, o TeamViewer aumenta exponencialmente o atraso entre tentativas de conexão. Assim, leva até 17 horas para 24 tentativas. A latência só é redefinida depois de introduzir a senha correta com sucesso.

O TeamViewer não só possui um mecanismo para proteger seus clientes de ataques de um computador específico, mas também de vários computadores, conhecidos como ataques de botnet, que estão tentando acessar um ID de TeamViewer em particular.

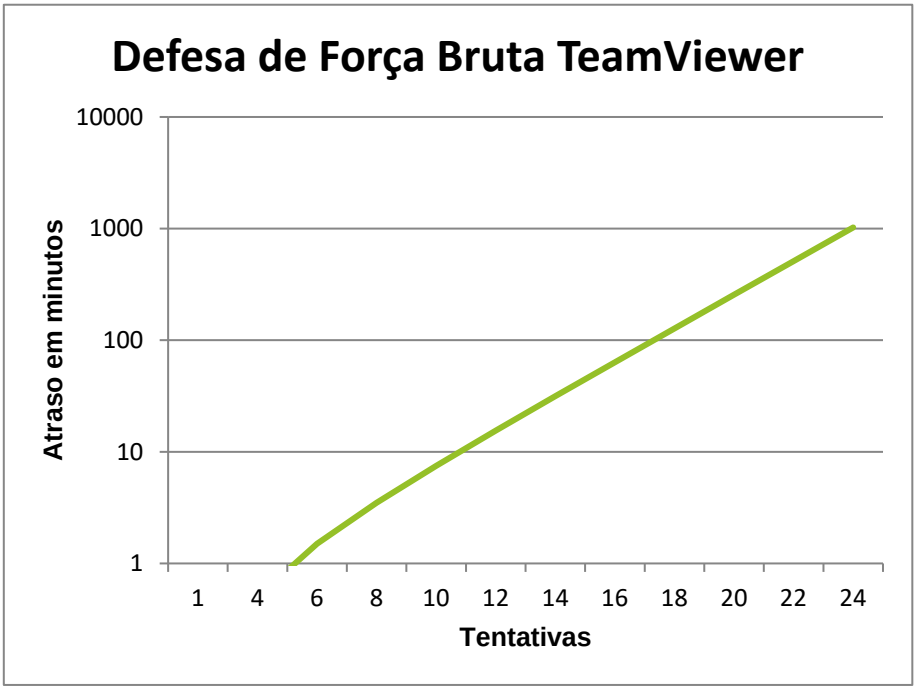


Gráfico: Tempo decorrido após n tentativas de conexão durante um ataque de força bruta

Assinatura de Código

Como um recurso de segurança adicional, todos os nossos softwares são assinados via VeriSign Code Signing. Desta forma, o editor do software é sempre prontamente identificável. Se o software tiver sido alterado posteriormente, a assinatura digital será automaticamente inválida.

Centros de dados & Backbone

Para fornecer a melhor segurança possível e disponibilidade dos serviços TeamViewer, todos os servidores TeamViewer estão localizados em centros de dados que estão em conformidade com a norma ISO 27001 e alavancam conexões portadoras multi-redundantes e fontes de alimentação redundantes. Além disso, somente é usado hardware de uma marca de ponta. Adicionalmente, todos os servidores de dados confidenciais estão localizados na Alemanha ou Áustria.

A certificação ISO 27001 significa que o controle de acesso pessoal, a vigilância de câmeras de vídeo, os detectores de movimento, o monitoramento 24 horas por dia e o pessoal de segurança no local asseguram que o acesso ao centro de dados só é concedido a pessoas autorizadas e garante a melhor segurança possível para hardware e dados. Há também uma verificação detalhada da identificação no único ponto-da-entrada ao centro de dados.

Conta TeamViewer

As contas TeamViewer são hospedadas em servidores TeamViewer dedicados. Para obter informações sobre controle de acesso, consulte a seção Centro de Dados & Backbone acima. Para autorização e criptografia de senhas, é utilizado o protocolo Secure Remote Password (SRP), um protocolo de chave com senha autenticada aumentada (PAKE). Um infiltrador ou um ataque “man-in-the-middle” não pode obter informações suficientes para ser capaz de adivinhar uma senha por força bruta. Isso significa que forte segurança pode ser obtida até com a utilização de senhas fracas. Dados sensíveis dentro da conta do TeamViewer, por exemplo, informações de login de armazenamento em nuvem, são armazenados em criptografia AES / RSA 2048 bits.

Management Console

O TeamViewer Management Console é uma plataforma baseada na Web para gerenciamento de usuários, relatórios de conexões e gerenciamento de Computadores & Contatos. Está hospedado em centros de dados certificados com ISO-27001, e conformidade HIPAA. Toda a transferência de dados é através de um canal seguro usando a criptografia TSL (Transport Security Layer), o padrão para conexões de rede seguras na Internet. Os dados sensíveis são ainda armazenados AES/RSA 2048 bits criptografados. Para autorização e criptografia de senha, o protocolo Secure Remote Password (SRP) é usado. O SRP é um método de autenticação e troca de chaves bem estabelecido, robusto e seguro baseado em senha usando módulo de 2048 bits.

Configurações baseadas em políticas

No TeamViewer Management Console, os usuários podem definir, distribuir e impor políticas de configuração para as instalações do software TeamViewer em dispositivos que pertençam especificamente a eles. As diretivas de configuração são assinadas digitalmente pela conta que as gerou. Isso garante que a única conta autorizada a atribuir uma diretiva a um dispositivo seja a conta à qual o d

Segurança de aplicativos no TeamViewer

Lista negra & branca

Particularmente, se o TeamViewer estiver sendo usado para manter computadores autônomos (ou seja, o TeamViewer é instalado como um serviço do Windows), a opção de segurança adicional para restringir o acesso a esses computadores a um número de clientes específicos pode ser de interesse.

Com a função lista branca, você pode indicar explicitamente quais IDs TeamViewer e/ou contas TeamViewer têm permissão para acessar um computador. Com a função de lista negra, você pode bloquear determinadas ID do TeamViewer e contas do TeamViewer. Uma lista branca central está disponível como parte das “configurações baseadas em políticas” descritas acima em “Management Console".

Criptografia de bate-papo e vídeo

Históricos de bate-papo estão associados à sua conta do TeamViewer e, portanto, são criptografados e armazenados usando a mesma segurança de criptografia AES/RSA de 2048 bits, conforme descrito no cabeçalho “Conta TeamViewer". Todas as mensagens de bate-papo e tráfego de vídeo são criptografados de ponta a ponta usando criptografia de sessão AES (256 bit).

Sem Modo Oculto

Não há nenhuma função que permite que você tenha TeamViewer executando completamente em segundo plano. Mesmo se o aplicativo estiver sendo executado como um serviço do Windows em segundo plano, o TeamViewer estará sempre visível por meio de um ícone na bandeja do sistema.

Após estabelecer uma conexão, há sempre um pequeno painel de controle visível acima da bandeja do sistema. Portanto, o TeamViewer é intencionalmente inadequado para monitorar em segredo computadores ou funcionários.

Proteção de Senha

Para suporte ao cliente espontâneo, TeamViewer (TeamViewer QuickSupport) gera uma senha de sessão (senha de uso único). Se o cliente lhe disser sua senha, você pode se conectar ao seu computador digitando seu ID e senha. Após uma reinicialização do TeamViewer pelo cliente, uma nova senha de sessão será gerada para que você só possa se conectar aos computadores do cliente se você for convidado a fazê-lo.

Ao implementar o TeamViewer para suporte remoto autônomo (por exemplo, de servidores), você define uma senha fixa individual, que protege o acesso ao computador.

Controle de Acesso de Entrada e Saída

Você pode configurar individualmente os modos de conexão do TeamViewer. Por exemplo, você pode configurar seu computador de suporte remoto ou reunião de forma que nenhuma conexão de entrada seja possível.

Limitar a funcionalidade a esses recursos realmente necessários sempre significa limitar possíveis pontos fracos para possíveis ataques.

Autenticação de Dois Fatores

O TeamViewer auxilia as empresas com seus requisitos de conformidade HIPAA e PCI. A autenticação de dois fatores adiciona uma camada de segurança adicional para proteger as contas do TeamViewer de acesso não autorizado. Além do nome do usuário e da senha, o usuário deve inserir um código para autenticar. Esse código é gerado através do algoritmo de senha de uso único baseado em tempo (TOTP). Portanto, o código é válido apenas por um curto período de tempo.

Através de autenticação de dois fatores e limitando o acesso por meio da listagem branca, o TeamViewer auxilia no cumprimento de todos os critérios necessários para a certificação HIPAA e PCI.

Teste de Segurança

Tanto a infraestrutura TeamViewer quanto o TeamViewer Software estão sujeitos a testes de penetração em uma base regular. Os testes são realizados por empresas independentes, especializadas em testes de segurança.

Outras perguntas?

Para outras perguntas ou informação, sinta-se à vontade para nos contatar (BR) 0 800 892 2167 e (PT) +351 800 863 340 ou enviar um e-mail para support@teamviewer.com.

Contato

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