Informations de sécurité TeamViewer

Groupe-cible

Ce document s'adresse aux administrateurs réseau professionnels. Les informations contenues dans ce document sont de nature relativement technique et très détaillées. Ces informations permettront aux professionnels de l'informatique d'avoir une vision détaillée des normes de sécurité chez TeamViewer et de résoudre les éventuels problèmes, avant le déploiement de notre logiciel. N'hésitez pas à distribuer ce document à vos clients afin de répondre à toute inquiétude liée à la sécurité.

Si vous considérez que vous ne faites pas partir du groupe-cible, les données de la section L'entreprise / Le logiciel vous permettront néanmoins de comprendre clairement à quel point nous prenons la sécurité au sérieux.

L'entreprise / Le logiciel

À propos de nous

TeamViewer GmbH a été fondé en 2005 et est implanté dans le sud de l'Allemagne, dans la ville de Göppingen (près de Stuttgart), avec des filiales en Australie et aux États-Unis. Nous développons et commercialisons de manière exclusive des systèmes sécurisés pour la collaboration basée sur le Web. En peu de temps, notre système de licence Freemium a généré une croissance rapide, avec plus de 200 millions d'utilisateurs du logiciel TeamViewer sur plus de 1,4 milliard d'appareils, dans plus de 200 pays à travers le monde. Le logiciel est disponible dans plus de 30 langues.

Notre vision de la sécurité

TeamViewer est utilisé par plus de 30 millions d'utilisateurs à n'importe quel moment de la journée. Ces utilisateurs fournissent une aide spontanée sur Internet, accèdent à des ordinateurs laissés sans surveillance (c.-à-d. assistance à distance pour serveurs) et organisent des réunions en ligne. Selon la configuration, TeamViewer peut être utilisé pour contrôler un autre ordinateur à distance, comme si vous étiez assis devant son écran. Si l'utilisateur connecté à un ordinateur distant est un administrateur Windows, Mac ou Linux, cette personne se verra également octroyer des droits d'administrateur sur cette ordinateur-là.

Naturellement, une fonctionnalité si puissante doit être protégée de manière rigoureuse contre les attaques sur l'Internet potentiellement dangereux. En réalité, le thème de la sécurité domine tous nos objectifs de développement et se retrouve dans tous nos faits et gestes. Nous voulons garantir un accès sécurisé à votre ordinateur et protéger nos propres intérêts : les millions d'utilisateurs à travers le monde font uniquement confiance à une solution sécurisée, et seule une solution sécurisé peut assurer notre réussite à long terme en tant qu'entreprise.

Évaluation d'experts externes

Notre logiciel, TeamViewer, s'est vu attribuer le label de qualité cinq étoiles (valeur maximale) par l'Association fédérale des experts et auditeurs informatiques (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.). Les auditeurs indépendants du BISG e.V. inspectent les produits des développeurs qualifiés quant à leurs caractéristiques de qualité, sécurité et service.

Références

Aujourd'hui, TeamViewer est utilisé par plus de 200 millions d'utilisateurs. Des corporations internationales de premier plan de tous types d'industries (dont des secteurs aussi sensibles que la banque, la finance, les soins de santé et les gouvernements) utilisent avec succès TeamViewer.

Nous vous invitons à étudier nos références partout sur Internet pour vous faire une première impression de l'acceptation de notre solution. Vous découvrirez que la plupart des autres entreprises avaient vraisemblablement des exigences de sécurité et de disponibilité similaires avant d'opter finalement, après un examen approfondi, pour TeamViewer. Toutefois, pour vous forger votre propre impression, vous trouverez quelques détails techniques dans la suite de ce document.

Sessions TeamViewer

Création d'une session et types de connexions

Lors de la création d'une session, TeamViewer détermine le type de connexion optimal. Après un passage par nos serveurs maîtres, une connexion directe via UDP ou TCP est établie dans 70 % des cas (même derrière des passerelles, NAT et pare-feux standard). Les autres connexions sont acheminées par le biais de notre réseau de routeurs hautement redondants, via TCP ou tunnellisation https. Il n'est pas nécessaire d'ouvrir des ports pour travailler avec TeamViewer.

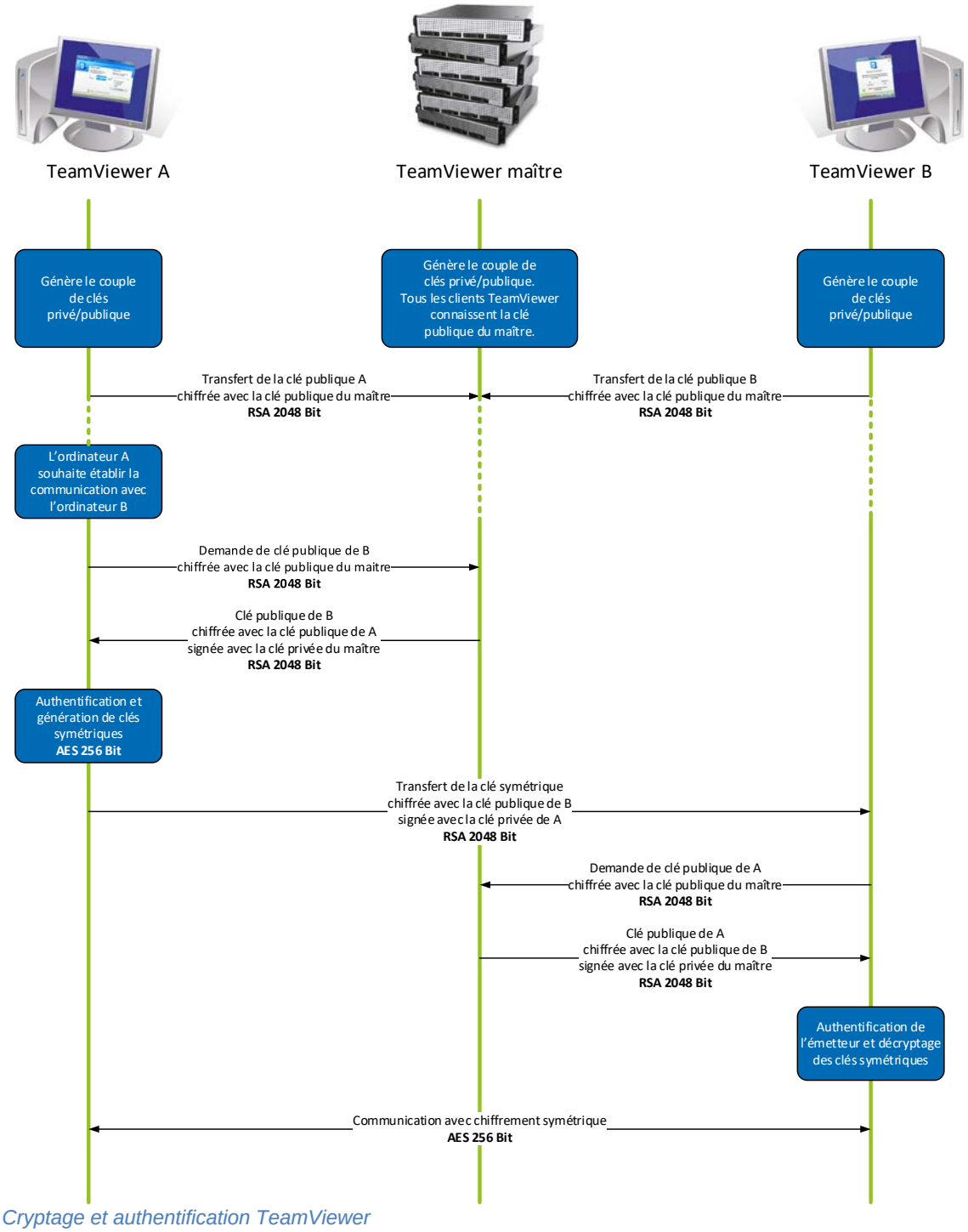
Comme décrit ultérieurement dans le paragraphe Cryptage et authentification, pas même nous, opérateurs des serveurs de routage, ne sommes en mesure de lire le trafic de données cryptées.

Cryptage et authentification

Le trafic TeamViewer est sécurisé à l'aide d'un échange de clé publique/privée RSA et un cryptage de session AES (256 bits). Cette technologie est utilisée sous une forme comparable pour http/SSL et est considérée comme totalement sûre par les normes actuelles. La clé privée ne quittant jamais l'ordinateur client, cette procédure garantit que tous les ordinateurs interconnectés, y compris les serveurs de routage TeamViewer, ne peuvent pas déchiffrer le flux de données.

Chaque client TeamViewer a déjà implémenté la clé publique du cluster maître et peut donc décrypter les messages envoyés au cluster maître et consulter les messages qu'il signe. La PKI (Public Key Infrastructure ou infrastructure de clé publique) prévient efficacement les attaques de l'homme du milieu. Malgré le cryptage, le mot de passe n'est jamais envoyé directement, mais uniquement par le biais d'une procédure défi-réponse, et est enregistré uniquement sur l'ordinateur local.

Lors de l'authentification, le mot de passe n'est jamais transféré directement du fait que le protocole Secure Remote Password (SRP) est utilisé. Seul un vérificateur de mot de passe est stocké sur l'ordinateur local.



Cryptage et authentification TeamViewer

Validation des ID TeamViewer

Les ID TeamViewer s'appuient sur diverses caractéristiques matérielles et logicielles et sont automatiquement générés par TeamViewer. Les serveurs TeamViewer contrôlent la validité de ces ID avant chaque connexion.

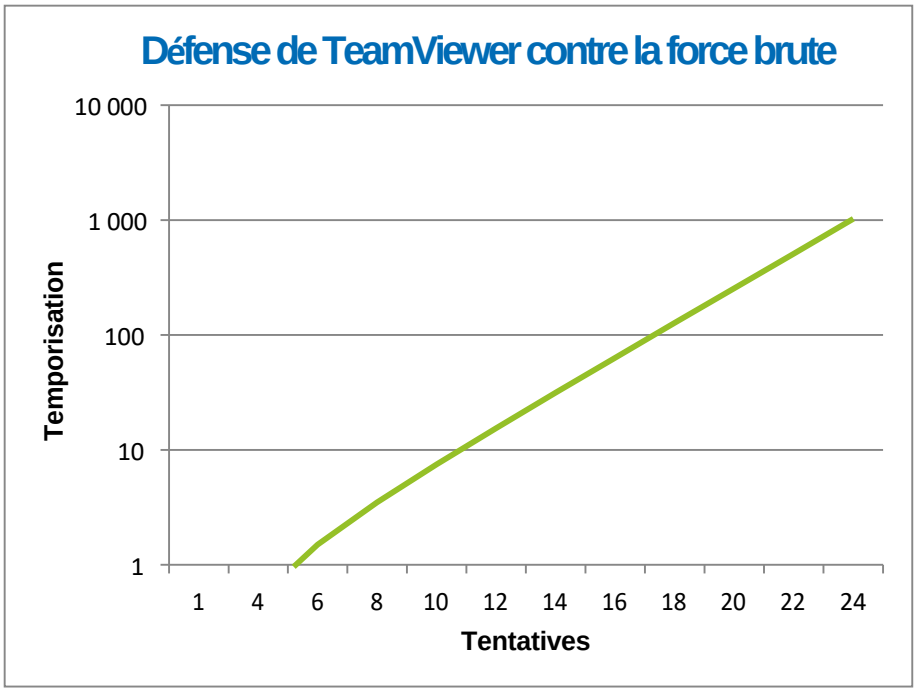
Protection contre la force brute

Les futurs clients qui s'inquiètent de la sécurité de TeamViewer posent souvent des questions sur le cryptage. Et ce à juste titre, car le risque qu'une tierce personne puisse contrôler la connexion ou que les données d'accès à TeamViewer soient exploitées est leur plus grande crainte. Pourtant, dans la réalité, ce sont les attaques plutôt primitives qui s'avèrent souvent les plus dangereuses.

Dans le contexte de la sécurité informatique, une attaque par force brute consiste à appliquer une méthode essai-erreur pour deviner un mot de passe qui protège une ressource. Avec la puissance de traitement grandissante des ordinateurs standard, le temps nécessaire pour deviner des mots de passe longs ne cesse de diminuer.

En guise de défense contre les attaques par force brute, TeamViewer augmente de manière exponentielle la temporisation entre les tentatives de connexion. Ainsi, il faut pas moins de 17 heures pour 24 tentatives. La latence n'est réinitialisée qu'après la saisie réussie du bon mot de passe.

TeamViewer intègre non seulement un mécanisme pour protéger ses clients des attaques émanant d'un ordinateur spécifique, mais également de plusieurs ordinateurs, appelées attaques de botnet, qui tentent d'accéder à un ID TeamViewer spécifique.



Graphique : Durée écoulée après n tentatives de connexion lors d'une attaque par force brute

Signature du code

En guise de fonctionnalité de sécurité supplémentaire, l'intégralité de notre logiciel est signée via la signature de code VeriSign. De cette façon, l'éditeur du logiciel est toujours aisément identifiable. Si le logiciel est modifié par la suite, la signature numérique est automatiquement invalidée.

Centres de données et dorsale

Afin de fournir la meilleure sécurité et disponibilité possibles des services TeamViewer, tous les serveurs TeamViewer sont installés dans des centres de données conformes à la norme ISO 27001 et fournissent des connexions de support multi-redondantes et des alimentations électriques redondantes. En outre, seul un matériel dernier cri de marque est utilisé. Parallèlement, tous les serveurs qui stockent les données sensibles sont situés en Allemagne ou en Autriche.

La certification ISO 27001 signifie que le contrôle d'accès personnel, la surveillance par caméra vidéo, les détecteurs de mouvement, la surveillance 24 h/24 et 7 j/7 et le personnel de sécurité sur place garantissent que l'accès au centre de données n'est octroyé qu'aux personnes autorisées et que la sécurité du matériel et des données est la plus élevée possible. Un contrôle d'identification détaillé est également effectué à l'unique point d'entrée du centre de données.

Compte TeamViewer

Les comptes TeamViewer sont hébergés sur des serveurs TeamViewer dédiés. Pour plus d'informations sur le contrôle d'accès, consultez la section Centre de données et dorsale ci-dessus. Pour l'authentification et le cryptage du mot de passe, le protocole Secure Remote Password (SRP), un protocole de concordance de clé authentifiée par mot de passe (PAKE) augmenté, est utilisé. Un infiltrateur ou homme du milieu ne peut obtenir suffisamment d'informations pour deviner un mot de passe par force brute. Cela signifie qu'une sécurité élevée peut être obtenue même avec des mots de passe faibles. Les données sensibles du compte TeamViewer, par exemple les informations de connexion au stockage sur le cloud, sont stockées cryptées AES/RSA 2 048 bits.

Management Console

La TeamViewer Management Console est une plateforme basée sur le Web destinée à la gestion des utilisateurs, au rapport de connexion et à la gestion des ordinateurs et contacts. Elle est hébergée dans des centres de données certifiés ISO-27001, conformes à HIPAA. L'intégralité du transfert de données s'effectue via un canal sécurisé qui utilise le cryptage TSL (Transport Security Layer), la norme pour les connexions réseau Internet sécurisées. Les données sensibles sont également stockées cryptées AES/RSA 2 048 bits. Pour l'autorisation et le cryptage du mot de passe, le protocole Secure Remote Password (SRP) est utilisé. SRP est une méthode d'authentification et d'échange de clé basée sur un mot de passe qui est bien établie, robuste et sécurisée via un module 2 048 bits.

Politiques de paramètres

Depuis la TeamViewer Management Console, les utilisateurs peuvent définir, distribuer et appliquer des politiques de paramètres pour les installations du logiciel TeamViewer sur des appareils qui leur appartiennent spécifiquement. Les politiques de paramètres sont signées numériquement par le compte qui les a générées. Cela garantit que seul le compte autorisé à attribuer une politique à un appareil est le compte auquel l'appareil appartient.

Sécurité des applications dans TeamViewer

Liste noire et liste blanche

L'option de sécurité supplémentaire visant à restreindre l'accès à ces ordinateurs à un certain nombre de clients spécifiques peut s'avérer particulièrement utile si TeamViewer est utilisé pour gérer des ordinateurs laissés sans surveillance (c.-à-d. TeamViewer est installé en tant que service Windows).

La fonction de liste blanche vous permet d'indiquer explicitement quels ID et/ou comptes TeamViewer sont autorisés à accéder à un ordinateur. À l'opposé, la fonction de liste noire vous permet de bloquer certains ID et comptes TeamViewer. Une liste blanche centrale est disponible dans le cadre des « politiques de paramètres » décrites ci-dessus dans la section « Management Console ».

Cryptage du chat et de la vidéo

Des historiques de chat sont associés à votre compte TeamViewer et sont donc cryptés et stockés à l'aide de la même sécurité de cryptage AES/RSA 2 048 bits que celle décrite sous le titre « Compte TeamViewer ». L'ensemble des messages chat et du trafic vidéo est crypté de bout-en-bout à l'aide du cryptage de session AES (256 bits).

Pas de mode furtif

Il n'existe aucune fonction vous permettant d'exécuter TeamViewer totalement en arrière-plan. Même si l'application fonctionne en tant que service Windows en arrière-plan, TeamViewer est toujours visible au moyen d'une icône affichée dans la barre système.

Une fois la connexion établie, un petit panneau de commande reste toujours visible au-dessus de la barre système. Par conséquent, TeamViewer ne permet pas, et ce volontairement , de contrôler des ordinateurs ou employés en secret.

Protection par mot de passe

Pour l'assistance client spontanée, TeamViewer (TeamViewer QuickSupport) génère un mot de passe de session (mot de passe unique). Si votre client vous communique son mot de passe, vous pouvez vous connecter à son ordinateur en saisissant son identifiant et son mot de passe. Après redémarrage de TeamViewer du côté du client, un nouveau mot de passe de session est généré, de sorte que vous pouvez vous connecter aux ordinateurs de votre client uniquement si vous y êtes invité.

Lors du déploiement de TeamViewer dans le cadre d'une assistance à distance sans surveillance (par ex. pour des serveurs), vous configurez un mot de passe fixe individuel qui sécurise l'accès à l'ordinateur.

Contrôle de l'accès entrant et sortant

Vous pouvez configurer individuellement les modes de connexion de TeamViewer. Par exemple, vous pouvez configurer votre assistance à distance ou ordinateur de réunion de manière à empêcher toutes les connexions entrantes.

Limiter la fonctionnalité aux seules caractéristiques réellement nécessaires permet de limiter les points faibles pour des attaques potentielles.

Authentification à deux facteurs

TeamViewer accompagne les entreprises dans leurs exigences de conformité HIPAA et PCI. L'authentification à deux facteurs ajoute un niveau de sécurité supplémentaire pour protéger les comptes TeamViewer contre tout accès non autorisé.

En plus du nom d'utilisateur et du mot de passe, l'utilisateur doit saisir un code pour s'authentifier. Ce code est généré à l'aide de l'algorithme de mot de passe unique temporel (TOTP). Par conséquent, le code est valide uniquement pour un court laps de temps.

De par l'authentification à deux facteurs et la restriction d'accès via les listes blanches, TeamViewer vous aide à satisfaire tous les critères nécessaires pour la certification HIPAA et PCI.

Essais de sécurité

L'infrastructure TeamViewer et le logiciel TeamViewer sont tous deux soumis régulièrement à des tests de pénétration. Ces tests sont réalisés par des sociétés indépendantes, spécialisées dans les essais de sécurité.

Vous avez des questions ?

Pour plus de questions ou d'informations, n'hésitez pas à nous contacter au +33 (0)9 75 18 01 38 ou à envoyer un e-mail à support@teamviewer.com.

Contact

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