Informations de sécurité TeamViewer

Groupe cible

Le présent document s'adresse aux administrateurs réseaux. Les informations figurant dans ce document sont de nature technique et très détaillées. Ce document permet aux professionnels de l'informatique de se faire une idée précise de la sécurité du logiciel avant d'utiliser TeamViewer. Vous pouvez aussi remettre ce document à vos clients afin d'éliminer d'éventuels doutes concernant la sécurité.

Si vous estimez ne pas faire partie du groupe cible, les données immatérielles du chapitre « L'entreprise / le logiciel » pourront tout de même vous aider à vous faire une idée personnelle du logiciel.

L'entreprise et le logiciel

A notre propos

La société TeamViewer GmbH est basée dans la ville de Göppingen située au sud de l'Allemagne (près de Stuttgart) et a été fondée en 2005. Notre activité se limite exclusivement au développement et à la commercialisation de systèmes sécurisés pour la collaboration et la communication sur Internet Un démarrage fulgurant et une croissance rapide ont mené, en un temps très court, à plusieurs millions d'installations du logiciel TeamViewer par des utilisateurs de plus de 200 pays différents. Le logiciel est actuellement disponible dans plus de 30 langues.

Notre notion de la sécurité

TeamViewer est largement utilisé dans le monde pour l'assistance spontanée via Internet et pour l'accès à des serveurs non surveillés (par ex. la maintenance à distance des serveurs). En fonction de la configuration de TeamViewer, cela signifie que l'ordinateur distant peut être commandé comme si l'on était assis devant cet ordinateur. Si l'utilisateur ayant ouvert une session sur l'ordinateur distant est un administrateur Windows, Mac ou Linux, il obtient des droits d'administrateur sur cet ordinateur.

Il est évident que des fonctionnalités si importantes utilisées via l'Internet, généralement peu sûr, exigent une protection contre les types d'attaques les plus diverses. C'est pour cela que chez nous le thème de la sécurité est prioritaire sur tous les autres objectifs de développement afin que l'accès à votre ordinateur soit sûr, et naturellement aussi dans notre propre intérêt : parce que des millions d'utilisateurs dans le monde ne feront confiance qu'à une solution sûre, et que seule une solution sûre peut assurer durablement le succès de notre entreprise.

La gestion de la qualité

D’après nous, la gestion de la qualité n’est pas possible sans système d'assurance qualité certifié. La société TeamViewer GmbH est l’un des rares fournisseurs du marché à disposer d’un système d’assurance qualité certifié selon la norme ISO 9001. Notre gestion de la qualité applique ainsi des normes internationalement reconnues. Chaque année, notre système d’assurance qualité fait l’objet d’audits externes.

Des expertises externes

L’Union Fédérale des Experts Informatiques (Bundesverband der IT-Sach-verständigen und Gutachter e.V.) a décerné à notre logiciel TeamViewer cinq étoiles au label de qualité (c’est la valeur maximale). Les experts indépendants du BISG e.V. contrôlent les caractéristiques de qualité, de sécurité et d’application des produits de fabricants qualifiés.

Inspection liée à la sécurité

TeamViewer a subi une inspection en matière de sécurité par les opérateurs allemands FIDUCIA IT AG et GAD eG (deux exploitants de centres de traitement des données pour environ 1200 banques allemandes) et a été approuvé pour l'utilisation des postes de travail dans les banques.

Nos références

TeamViewer est actuellement utilisé sur plus de 200 millions d’ordinateurs. D’importantes entreprises internationales de tous domaines (y compris des secteurs très sensibles telles que les banques et les institutions financières) utilisent TeamViewer avec succès.

Nous vous invitons à ce sujet à visiter notre page de références sur Internet, afin d'obtenir une première impression de l’acceptation de notre solution. Vous conviendrez certainement du fait que la plupart de ces entreprises clientes disposaient probablement d'exigences de sécurité et de disponibilité similaires, avant d’opter pour TeamViewer après un examen approfondi. Vous trouverez ci-dessous des détails techniques qui vous permettront de vous faire une opinion personnelle.

Etablissement et déroulement d'une séance TeamViewer

Etablissement de la connexion et types de connexion

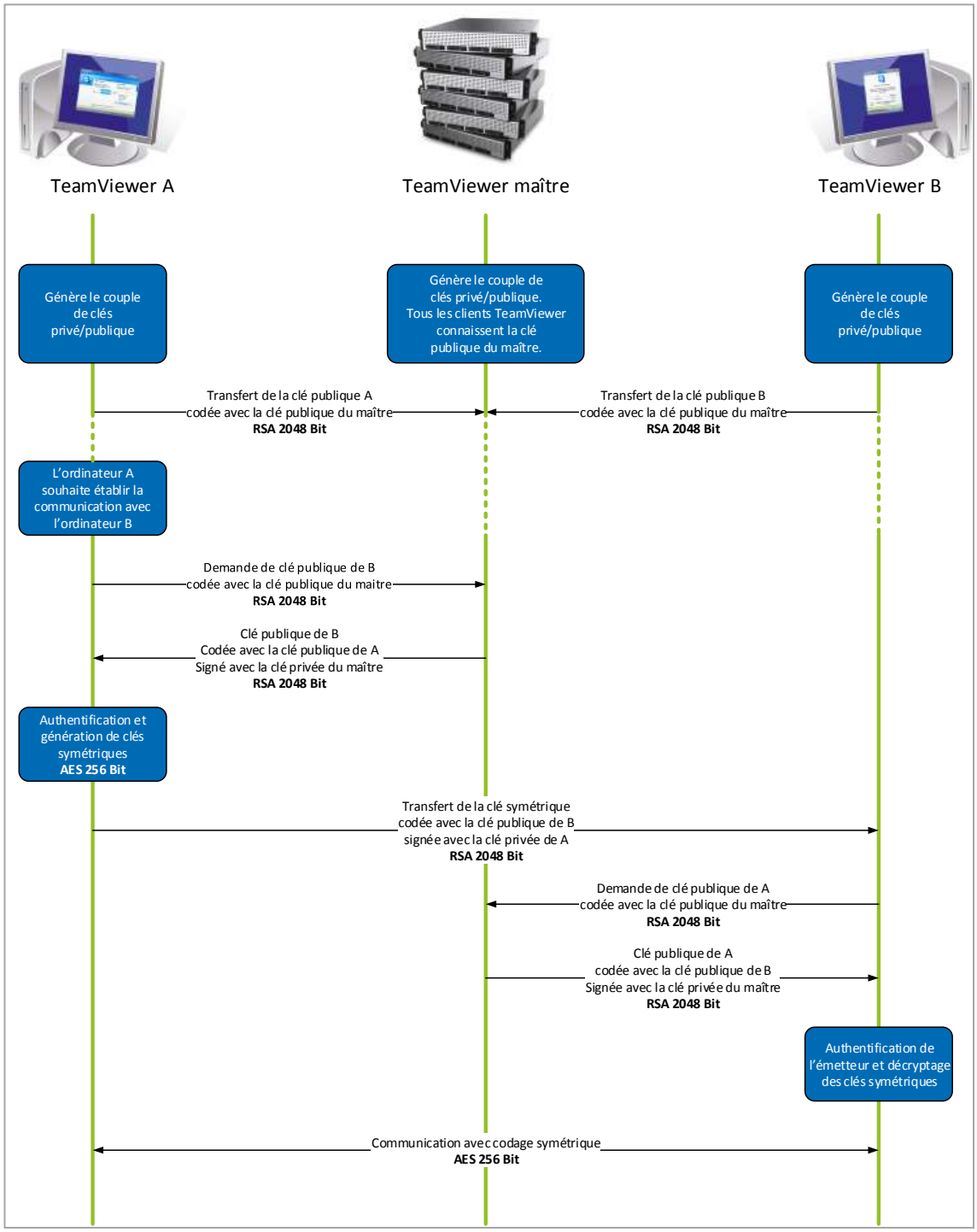
Lors de l'établissement d'une connexion, TeamViewer détermine le type de connexion optimal. Après authentification via nos serveurs, une connexion directe est établie dans 70 % des cas via UDP ou TCP (et ce même derrière les passerelles normalisées, les routeurs NAT et les pare-feux). Les autres connexions sont acheminées par le biais de notre réseau de routeurs hautement redondant via TCP ou tunnel HTTP. Vous n'avez donc pas besoin d'ouvrir des ports pour pouvoir travailler avec TeamViewer !

Comme décrit dans le chapitre « Codage et authentification » ci-après, même nous chez TeamViewer, en tant qu'exploitants des serveurs de routage, ne pouvons pas lire les données chiffrées échangées.

Codage et authentification

TeamViewer utilise une technique de chiffrement complète basée sur des échanges de clés publiques et privées RSA et un codage de session AES (256 bit). Cette technologie est basée sur les même standards que les technologies HTTPS ou SSL et est considérée comme parfaitement sécurisée selon les normes actuelles. Comme la clé privée ne quitte jamais l'ordinateur client, ce procédé permet d'assurer que les ordinateurs intermédiaires (y compris les serveurs TeamViewer) ne peuvent pas déchiffrer les données.

La clé publique des serveurs est déjà intégrée à chaque client TeamViewer et permet ainsi de chiffrer les messages pour ces serveur ou de vérifier la signature des serveurs. L'infrastructure à clé publique PKI empêche efficacement les attaques intermédiaires du type « man in the middle » (homme du milieu). Par ailleurs, malgré le codage, le mot de passe n'est jamais transmis directement, mais selon le procédé « challenge-response » (stimulation/réponse) et n'est mémorisé que sur les ordinateurs locaux.



Codage et authentification de TeamViewer

La validation des identifiants TeamViewer

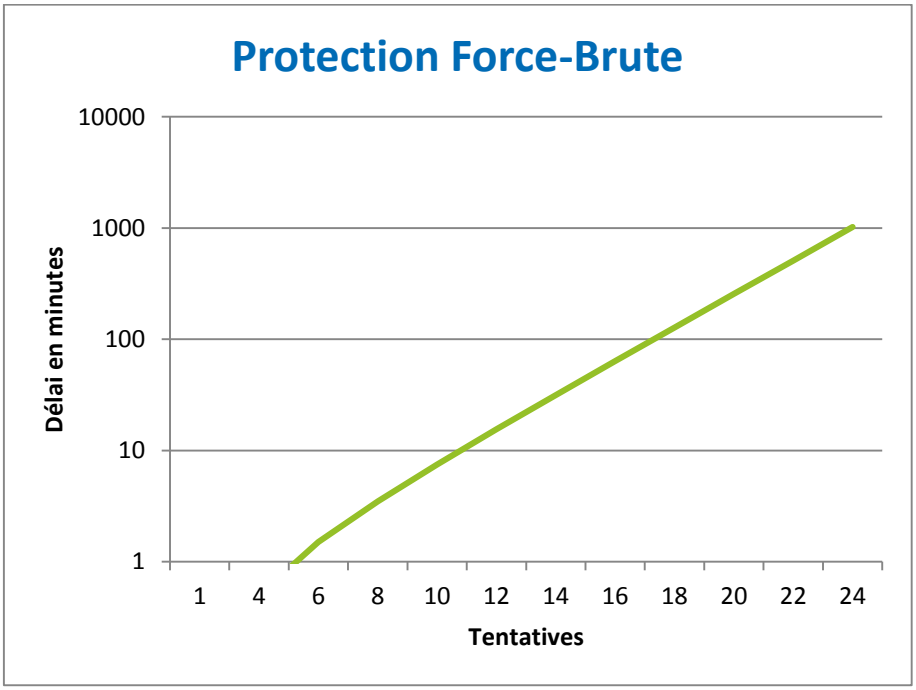
Les identifiants TeamViewer sont générés directement et automatiquement par TeamViewer à l'aide des caractéristiques matérielles de l'ordinateur. Les serveurs TeamViewer contrôlent la validité de cet identifiant à chaque connexion, de façon à rendre impossible la génération et l'utilisation d'identifiants falsifiés.

La protection contre les attaques par force brute

Quand des professionnels intéressés nous interrogent au sujet de la sécurité de TeamViewer, les questions portent régulièrement sur le codage. La crainte principale porte naturellement sur le risque que des tiers puissent visualiser une connexion ou intercepter les données d'accès de TeamViewer. Dans la pratique, ce sont cependant souvent des attaques très primitives qui s'avèrent les plus dangereuses.

Dans le contexte de la sécurité informatique, une attaque par force brute est souvent la tentative de deviner, par des essais répétés, un mot de passe qui protège l'accès à une ressource. Grâce à la puissance croissante des ordinateurs disponibles dans le commerce, le temps nécessaire aux essais de mots de passe même longs est de plus en plus court.

Pour dissuader les attaques par force brute, TeamViewer augmente de façon exponentielle le temps d'attente entre les tentatives de connexion. Ainsi, pour 24 tentatives, 17 heures sont nécessaires. Le temps d'attente entre les tentatives de connexion n'est réinitialisé qu'une fois le mot de passe entré avec succès.



Temps nécessaire pour le nombre n de tentatives lors d'une attaque par force brute.

La signature de code

En guise de fonction de sécurité supplémentaire, tous nos programmes sont signés à l'aide de la signature de code VeriSign Code Signing. De ce fait, l'éditeur du logiciel est toujours identifiable avec certitude. Si le logiciel est modifié ultérieurement, la signature numérique perd automatiquement sa validité.

Même les modules personnalisés avec votre logo et configurés individuellement sont pourvus d'une signature générée pendant leur création.

Centres de données et réseaux

Ces deux sujets concernent aussi bien la disponibilité que la sécurité. Les serveurs centraux TeamViewer se trouvent dans un centre de données ultramoderne avec des connexions réseaux multi-redondantes et une alimentation électrique elle aussi redondante. Nous n'utilisons que du matériel de marque reconnue (Cisco, Foundry, Juniper).

L'accès au centre de données est limité à un seul sas d'entrée et est soumis au contrôle et à l'identification des personnes. Des caméras de vidéosurveillance, des alertes d'infraction, une surveillance 24 heures sur 24 et 7 jours sur 7 ainsi qu'un personnel de sécurité sur site protègent nos serveurs contre les attaques de l'intérieur.

La sécurité d'application dans TeamViewer

Listes noire et blanche

Si vous installez TeamViewer sur des ordinateurs dont la maintenance doit être réalisée sans surveillance (si TeamViewer est installé en tant que service système Windows), il peut s'avérer intéressant de limiter l'accès à ces ordinateurs à certains clients, en plus des autres mécanismes de sécurité.

La fonction de liste blanche vous permet d'indiquer explicitement les ID TeamViewer autorisés à se connecter à un ordinateur, alors que la fonction de liste noire bloque certains ID TeamViewer.

Pas de mode discret

Il n'existe aucune fonction TeamViewer permettant d'exécuter le logiciel de façon totalement invisible en arrière-plan. Une icône dans la barre des tâches signale TeamViewer même lorsque l'application est exécutée en arrière-plan en tant que service système Windows.

Un petit tableau de contrôle s'affiche toujours après l'établissement d'une connexion, rendant TeamViewer délibérément impropre à la surveillance discrète des ordinateurs ou des collaborateurs.

La protection du mot de passe

Pour l’assistance client spontanée, TeamViewer (TeamViewer QuickSupport) génère un mot de passe de session (mot de passe à usage unique). Si votre client vous communique ce mot de passe, vous pouvez accéder à l’ordinateur de votre client en saisissant votre identifiant et le mot de passe. Lors du redémarrage de TeamViewer chez le client, un nouveau mot de passe de session est généré, de façon à ce que vous ne puissiez accéder aux ordinateurs de vos clients que si vous y êtes explicitement invité.

Lors de l’utilisation pour la maintenance à distance sans surveillance (par ex. pour des serveurs), vous attribuez un mot de passe individuel fixe qui protège l’accès à l’ordinateur.

Le contrôle d’accès entrant et sortant

Vous pouvez configurer individuellement les possibilités de connexion de TeamViewer. Vous pouvez, par exemple, configurer un ordinateur de maintenance à distance ou de présentation de sorte à empêcher toute connexion entrante.

Cette limitation de la fonctionnalité aux fonctions réellement nécessaires limite toujours aussi les points d’attaque possibles.

Authentification à deux facteurs

VTeamViewer assiste les sociétés pour répondre aux exigences de conformité HIPAA et PCI. L'authentification à deux facteurs ajoute un niveau de sécurité supplémentaire pour protéger les comptes TeamViewer contre un accès non autorisé. En combinaison avec le contrôle d'accès par liste blanche, TeamViewer vous permet d'être conforme aux normes HIPAA et PCI.

Avec l'authentification à deux facteurs, en plus du nom d'utilisateur et du mot de passe, un code généré sur un appareil mobile est nécessaire pour se connecter à un compte TeamViewer. Le code est généré via l'algorithme de mot de passe à usage unique et durée déterminée (TOTP). Le code TOTP est protégé par SRP et donc sûr contre les attaques de type intermédiaire. ous pouvez configurer individuellement les possibilités de connexion de TeamViewer.

D’autres questions ?

Si vous avez d’autres questions au sujet de la sécurité, nous nous ferons un plaisir d’y répondre par téléphone: +33 (0)9 75 18 01 38, ou par e-mail: support@teamviewer.com.

Contact

TeamViewer GmbH
Kuhnbergstr. 16
D-73037 Göppingen
Allemagne
service@teamviewer.com

Directeur: Holger Felgner
Registre du commerce: Ulm HRB 534075