Les BONNES PRATIQUES de sécurité avec votre serveur bureau distant TS2log

Les dégâts et préjudices financiers des cybers attaques sont malheureusement un constat récurrent et cet état de fait nous amène à vous communiquer les bonnes pratiques à mettre place dans votre environnement informatique Terminal Serveur TS2log.

En effet, outre les solutions antivirus tel EMSISOFT ou encore TS2log Security qui renforcent votre arsenal sécuritaire au niveau des postes de travail et des serveurs, il s'avère indispensable de mettre en œuvre une politique de sécurité efficace.

Dans un souci de conseil auprès de nos clients, veuillez trouver ci-dessous nos recommandations pour la sécurisation de votre serveur TS2log.

LES UTILISATEURS :

Assigner uniquement les utilisateurs qui doivent avoir un accès au serveur. Par défaut, tous les utilisateurs peuvent ouvrir une session à distance et accéder au Bureau.

Dans AdminTool > Applications > Assigner une application : sélectionner les utilisateurs ou les groupes sur la gauche et assigner à chacun la ou les applications auxquelles il aura accès.
Pour donner accès à la session Windows complète, donc au Bureau, il faudra sélectionner 'Microsoft Remote Desktop'.
Vérifier que le compte Administrateur dispose bien de l'application 'Microsoft Remote Desktop'.
Pour valider, fermer la fenêtre d'assignation par la croix en haut à droite.

Dans AdminTool > Sécurité > Options de sécurité avancées : cocher la case 'Autoriser uniquement les utilisateurs avec au moins 1 application assignée'.
Lire le commentaire affiché, puis cliquer sur 'OK'.
Pour valider, fermer la fenêtre d'assignation par la croix en haut à droite.

Désactiver le compte 'invité' ou changer son mot de passe.

Par défaut, le compte invité de Windows est activé. Ce compte ne dispose pas de mot de passe.

Si le serveur est accessible depuis l'extérieur, il sera donc très facile d'ouvrir une session, d'accéder aux ressources ou d'exécuter des applications.

Par exemple il sera aisé d'exécuter un fichier Excel dont la macro supprimera ou cryptera des données sur le serveur.

Utiliser une stratégie de mot de passe forte.

Le mécanisme de sécurité Windows ne bloquera pas les tentatives de connexion avec un mot de passe erroné.

Les robots pourront donc effectuer autant de tentatives qu'ils le désirent, jusqu'à ce qu'ils trouvent le mot de passe et accèdent au serveur.

- Un mot de passe faible comme 'Jacques' ou 'AZEQSDWXC' sera 'cassé' dans la minute.
- Un mot de passe comme 'Nicole1225' prendrait plusieurs semaines, si une partie du mot de passe n'est pas contenue dans le nom du profil Windows.
- Un mot de passe fort, par exemple '#45HoustonQHl75' ou 'Je mange des Chips à 11H !' ne sera pas 'cassé' avant plusieurs années.

Les applications de gestion de mot de passe sont un bon moyen de renforcer la sécurité, car on n'a pas à se souvenir de chaque mot de passe. Cette stratégie devrait être appliquée aux mots de passe de messagerie, aux comptes marchands sur Internet, …

LES ACCÈS :

Sécuriser les accès Web avec le certificat SSL.

TS2log Édition Mobile est livrée avec un module permettant de générer et d'utiliser une connexion cryptée et sécurisée entre le navigateur de l'utilisateur et le serveur.

Son déploiement est très simple, il suffit de disposer d'un nom de domaine et de rediriger ce dernier vers l'adresse ip publique du serveur (voir onglet 'Serveur', 'IP Lan / IP WAN').

Pour déployer le certificat SSL gratuit, ouvrir AdminTool > Sécurité > Générer un certificat SSL gratuit.

Sécuriser les accès RDP en n'exposant pas le port par défaut.

Sur tous les systèmes d'exploitation, le port Connexion Bureau à Distance par défaut est le port TCP 3389.

Il est donc recommandé de modifier la règle de redirection du routeur / Box ADSL et configurer un port d'écoute RDP différent.
Pour les connexions locales, au sein d'un réseau d'entreprise, ce port peut être utilisé.

Pour les connexions distantes, à l'extérieur du réseau, il faudra privilégier l'utilisation d'un port d'écoute public différent.

En effet, le port public 3389 sera le premier port testé par les robots à la recherche d'une faille de sécurité.

Vérifier les ressources locales partagées.

Plus de 80% des attaques proviennent de l'intérieur d'un réseau (dépôt de fichiers malveillants, pièces-jointes de mails non vérifiées, base antivirale obsolète). Nous préconisons de vérifier régulièrement l'état de l'antivirus sur le serveur, de vérifier les droits d'accès aux ressources partagées ainsi que la sauvegarde.

Sur l'ordinateur utilisateur, il faudra vérifier régulièrement l'état de l'antivirus, surtout si l'utilisateur partage ses ressources locales avec le serveur distant, comme la remontée des disques locaux ou des supports amovibles comme une clé usb.

Sur les ordinateurs clients, vous pouvez installer Cyberreason RansomFree. Il s'agit d'une solution gratuite et très efficace. https://ransomfree.cybereason.com

En cas de doute sur la sécurisation de vos serveurs, ou si vous avez une question d'ordre technique, n'hésitez pas à contacter notre support technique à :
support-ts2log@soft4europe.com
ou à consulter notre site internet :
https://soft4europe-france.com

En particulier les solutions de sécurisation des serveurs Bureaux Distants TS2log Security et les solutions Antivirus EMSISOFT

TS2log Security :
https://soft4europe-france.com/documentation-ts2log-security

EMSISOFT :
https://soft4europe-france.com/securite-antivirus-antimalware

LES MISES À JOUR

Mises à jour antivirales :

Il est extrêmement important de disposer d'une solution antivirale / anti-ransomware sur un serveur accessible depuis l'extérieur.
Cette solution de sécurité devra être à jour et active.
Certaines solutions antivirales désactivent le pare-feu Windows et peuvent potentiellement nuire à la sécurité si un ou plusieurs de leurs composants sont désactivés ou obsolètes.

Mises à jour Windows :

Les mises à jour Windows ne devraient pas être appliquées de manière automatique, mais planifiées. Par exemple deux fois par mois.
Certaines mises à jour appliquées de manières automatiques vont désactiver des services avant leur application.
Si le serveur n'est pas redémarré de manière automatique, ou parce que ce dernier est exploité par les utilisateurs, des failles de sécurité peuvent se produire jusqu'au prochain redémarrage.
Le serveur peut également avoir un comportement différent de son état normal.

Il sera également important d'appliquer uniquement les mises à jour importantes ou critiques préconisées par Windows Update.
L'application des mises à jour 'Preview' n'est pas recommandé sur les serveurs en production.

Après l'application des mises à jour Windows, il est fortement recommandé de redémarrer le serveur et de vérifier que l'accès à distance fonctionne correctement.

Mises à jour TS2log :

Nous vous invitons a vérifier régulièrement les mises à jour TS2LOG. Nous préconisons une vérification tous les trimestres a minima, pour disposer d'un produit toujours à jour, sécurisé et disposant des dernières fonctionnalités et correctifs.
Pour vérifier la mise à jour, ouvrir AdminTool > Licence > Vérifier la mise à jour.