CHAPITRE 3: PROTECTION CLIENT/SERVEUR

Introduction

Dans l'informatique moderne, de nombreuses applications fonctionnent selon un environnement client-serveur; cette dénomination signifie que des machines clientes (faisant partie du réseau) contactent un serveur - une machine généralement très puissante en termes de capacités d'entrées sorties - qui leur fournit des services. Nous allons voir comment cette technologie permet d'exploiter au mieux les réseaux, et permet un haut niveau de coopération entre différentes machines sans que l'utilisateur se préoccupe des détails de compatibilité.

Definition du Modèle Client/serveur

Le modèle client-serveur s'articule autour d'un réseau auquel sont connectés deux types d'ordinateurs le serveur et le client. Le client et le serveur communiquent via des protocoles. Les applications et les données sont réparties entre le client et le serveur de manière à réduire les coûts. Le client-serveur représente un dialogue entre deux processus informatiques par l'intermédiaire d'un échange de messages. Le processus client sous-traite au processus serveur des services à réaliser. Les processus sont généralement exécutés sur des machines, des OS et des réseaux hétérogènes.

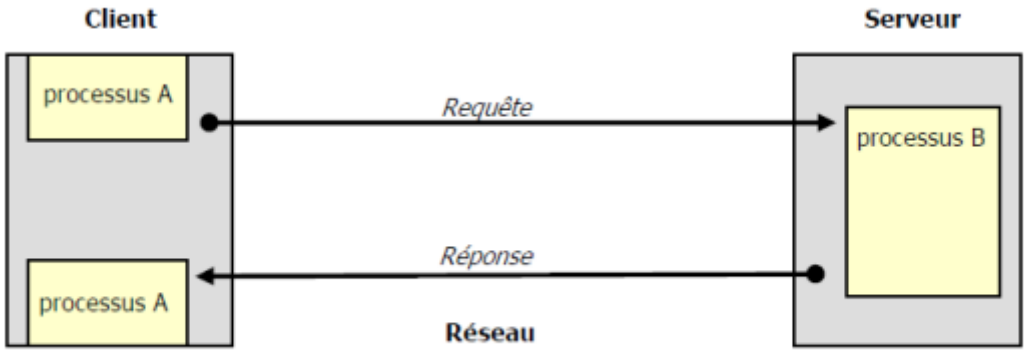


Figure : Le modèle Client/serveur

Caractéristiques des Systèmes Client Serveur

Les éléments qui caractérisent une architecture client-serveur sont :

Service : Le modèle client-serveur est une relation entre des processus qui tournent sur des machines séparées. Le serveur est un fournisseur de services. Le client est un consommateur de services.

Partage de ressources : Un serveur traite plusieurs clients et contrôle leurs accès aux ressources.

Transparence de Localisation : L'architecture client-serveur doit masquer au client la localisation du serveur (que le service soit sur la même machine ou accessible par le réseau). Transparence par rapport aux systèmes d'exploitation et aux plates-formes matérielles. Idéalement, le logiciel client serveur doit être indépendant de ces deux éléments.

Message : Les messages sont les moyens d'échanges entre client et serveur.

Encapsulation des Services : Un client demande un service. Le serveur décide de la façon de le rendre une mise à niveau du logiciel serveur doit être sans conséquence pour le client tant que l'interface message est identique.

Evolution : Une architecture client-serveur doit pouvoir évoluer horizontalement (évolution du nombre de clients) et verticalement (évolution du nombre et des caractéristiques des serveurs).

Sécurisation Client/serveur

I. Les mises à jour

Les appareils numériques et les logiciels que nous utilisons au quotidien sont exposés à des failles de sécurité. Ces failles peuvent être utilisées par des cybercriminels pour prendre le contrôle d'un ordinateur, d'un équipement mobile ou encore d'une montre connectée. Face à ces risques, les éditeurs et les fabricants proposent des mises à jour (*patch* en anglais) visant à corriger ces failles. Si l'opération de mise à jour est souvent ressentie comme une contrainte, il s'agit pourtant d'un acte essentiel pour se protéger.

Une **mise à jour** — parfois abrégée en **MAJ** ou **MàJ** —, parfois appelé **révision** ou **mise à niveau** est l'action qui consiste à déployer vers des équipements électroniques des utilisateurs les changements effectués (ou à effectuer) à un outil informatique, un service ou une prestation en téléchargeant, ou en chargeant, un nouveau logiciel, micro logiciel ou encore le contenu de quelconques données.

Lorsqu'elles touchent un logiciel ou un système d'exploitation, elles permettent généralement de passer à une version plus récente du logiciel ou du système d'exploitation. Plusieurs mises à jour peuvent donc se succéder.

Une mise à jour sert à améliorer le rendement, l'efficacité ou la prestation d'un service ou d'un produit, et parfois à corriger les anomalies d'un programme donné.

Elle vise le plus souvent à :

- améliorer les fonctionnalités ;
- optimiser le fonctionnement ou les performances ;
- procurer de nouvelles fonctionnalités ou applications ;
- corriger des dysfonctionnements ou bouges ;
- permettre au fournisseur de contrôler que le logiciel n'est pas illégalement copié ;

Différents types de mises à jour

• **Les mises à jour importantes ou critiques** corrigent des failles de sécurité qui peuvent être utilisées pour pirater votre équipement.
• **Les mises à jour de version** apportent en général de nouvelles fonctionnalités et corrigent également des failles de sécurité. Ce type de mise à jour peut être payant.

Afin de garantir la sécurité de votre Poste client, il est essentiel de bien gérer ses mises à jour. Voici certaines bonnes pratiques à adopter pour vos mises a jour.

1. **Pensez à mettre à jour sans tarder l'ensemble de vos appareils et logiciels**

Ordinateurs, téléphones, systèmes d'exploitation, logiciels de traitement de texte, objets connectés… nous utilisons un grand nombre d'appareils et de logiciels. Il suffit qu'un seul ne soit pas à jour et soit exposé à une faille de sécurité pour ouvrir une brèche dans votre environnement numérique. Afin d'empêcher les cybercriminels d'utiliser ces failles de sécurité pour vous pirater et vous dérober des informations personnelles sensibles, il est primordial de réaliser les mises à jour de vos équipements dès qu'elles sont disponibles.

2. **Téléchargez les mises à jour uniquement depuis les sites officiels**

Seuls les sites ou dispositifs officiels des éditeurs et fabricants vous garantissent au mieux que les mises à jours que vous allez installer ne sont pas infectées par un virus. À l'installation de vos mises à jour, soyez attentif aux éventuelles conditions d'utilisation ou cases pré-cochées qui pourraient valoir acceptation de l'installation d'un autre logiciel non désiré (logiciels publicitaires, par exemple).

3. **Identifiez l'ensemble des appareils et logiciels utilisés**

Il est conseillé d'identifier vos appareils, matériels et logiciels afin de les mettre à jour. Certains Fournisseurs d'Accès Internet (FAI) proposent une application d'inventaire qui permet de lister les appareils connectés à votre réseau informatique professionnel ou domestique. Si vous faites l'acquisition d'un nouvel appareil, remettez ses paramètres par défaut avant de l'utiliser en le réinitialisant et installez ensuite les différentes mises à jour proposées sur les sites du fabriquant ou des éditeurs des applications installées.

4. **Activez l'option de téléchargement et d'installation automatique des mises à jour**

Si le logiciel le permet, configurez-le pour que les mises à jour se téléchargent et s'installent automatiquement. Avec cette fonctionnalité, vous disposerez ainsi de la dernière version à jour de la solution de l'éditeur. Assurez-vous également que la mise à jour fonctionne par une vérification manuelle, au besoin.

5. **Définissez les règles de réalisation des mises à jour [PRO]**

Pour assurer votre cyber sécurité, la définition de certaines règles peut faciliter l'opération de mise à jour, notamment en entreprise. Il s'agit par exemple de spécifier la façon de réaliser l'inventaire des appareils et logiciels utilisés, de savoir où et comment rechercher les mises à jour, comment et qui procède à la mise à jour ou encore à quel moment réaliser cette opération.

6. **Planifiez les mises à jour lors de périodes d'inactivité**

Lorsqu'ils interrompent une activité personnelle ou professionnelle (visionnage d'une vidéo, rédaction d'un courriel…), les messages indiquant la disponibilité d'une mise à jour sont souvent ignorés car le processus de mise à jour peut être ressenti comme une contrainte. En effet, la mise à jour peut prendre du temps, allant de quelques secondes à plusieurs minutes ou heures, selon les cas. Aussi, profitez de périodes d'inactivité pour effectuer vos mises (déjeuner, réunion, de nuit…).

7. **Informez-vous sur la publication régulière des mises à jour de l'éditeur**

L'utilisation d'un appareil ou d'un logiciel pas à jour augmente les risques d'attaques informatiques. Si les mises à jour ne sont plus proposées, ils sont plus vulnérables. Aussi, avant

l'acquisition d'un nouveau matériel ou logiciel, vérifiez la publication régulière des mises à jour de l'éditeur ou du fabricant, ainsi que la date de fin de leur mise à disposition. Lorsqu'une solution arrive en fin de vie et que des mises à jour ne sont plus proposées, identifiez les délais et les ressources nécessaires pour migrer vers de nouveaux outils afin de rester protégé.

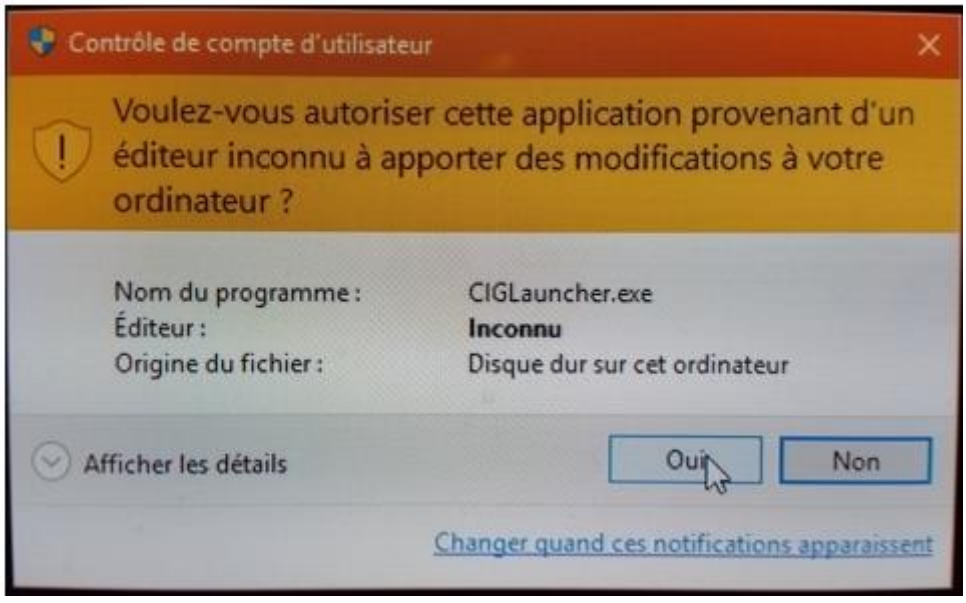
8. Protégez autrement les appareils qui ne peuvent pas être mis à jour

Dans certains cas, des appareils peuvent ne pas être mis à jour pour diverses raisons, comme leur ancienneté, la perte d'une garantie ou d'un agrément. Il est, par conséquent, nécessaire de protéger ce dispositif autrement, par exemple en ne le connectant pas à Internet, en le séparant du reste du réseau informatique ou encore, en désactivant les services vulnérables.

II. L'UAC : Le Contrôle de Comptes Utilisateurs

Si vous disposez d'un réseau d'ordinateurs à votre domicile ou sur votre lieu de travail, vous devez notamment contrôler quels utilisateurs ou applications peuvent modifier les éléments de ce système. Une façon d'empêcher les modifications non autorisées est de désigner une personne comme administrateur du réseau. Cependant, il ne suffit pas d'avoir une seule personne qui gère tout, et c'est là qu'intervient la fonction de contrôle d'accès des utilisateurs (UAC), en anglais **User Account Control.**

L'UAC est une fonctionnalité de sécurité de Windows 10 qui empêche toute modification non autorisée ou involontaire du système d'exploitation. Cette fonction faisait d'abord partie du système de sécurité de Windows Vista et a depuis été améliorée avec chaque nouvelle version de Windows. De telles modifications peuvent être provoquées par les utilisateurs, des virus, des logiciels malveillants ou des applications. Mais si l'administrateur n'approuve pas les modifications, elles ne seront pas exécutées. La saisie du mot de passe administrateur est donc obligatoire pour effectuer certaines manipulations.



Parmi les modifications qui nécessitent des privilèges administratifs, on peut citer :

- Exécuter le planificateur de tâches.
- Modifier les paramètres de l'UAC.
- Configuration de Windows Update.
- Ajout ou suppression de comptes d'utilisateurs.
- Modification des fichiers ou des paramètres du système dans les dossiers de Windows.
- Visualisation ou modification des fichiers ou dossiers d'autres utilisateurs.
- Lancer les applications en tant qu'administrateur.
- Installation ou désinstallation d'applications ou de pilotes.
- Modification des paramètres de date et d'heure, du pare-feu Windows ou du système.
- Configurer la sécurité de la famille ou le contrôle parental.
- Modification du type de compte d'un utilisateur.

Chaque fois que vous exécutez une application de bureau qui nécessite des autorisations d'administrateur, l'UAC s'affiche. Vous le verrez également lorsque vous voudrez modifier des paramètres importants du système qui nécessitent l'approbation de l'administrateur.

Tous les utilisateurs de votre réseau peuvent se connecter à leur ordinateur en utilisant un compte utilisateur standard, mais tous les processus qu'ils lancent seront exécutés en utilisant les droits d'accès accordés à un utilisateur standard.

Par exemple, toute application lancée à l'aide de l'Explorateur Windows s'exécutera avec des autorisations de niveau utilisateur standard. Cela comprend les applications incluses avec Windows 10 lui-même.

III. Mot de Passe

Un **mot de passe, ou *password***, est une séquence de caractères ou mot qu'un sujet donne à un système pour authentification, validation ou vérification. Un mot de passe fort permet davantage de sécurité.

Si votre mot de passe ressemble à « 123456 », « azerty », « password » ou encore « iloveyou » alors préparez-vous à le changer. Vos comptes sont loin d'être sécurisés.

Il est parfois très facile pour des personnes malveillantes de découvrir un mot de passe, et lorsque cela arrive, c'est une entrée directe sur vos données personnelles.

Pour éviter une telle situation, il est indispensable de renforcer votre mot de passe, et voici comment faire.

1. **Créer plusieurs mots de passe**

Nous sommes nombreux à n'utiliser qu'un seul et même mot de passe pour tous nos comptes dans un souci de mémorisation. Pourtant, c'est une pratique à éviter car si quelqu'un venait à découvrir votre mot de passe il aurait accès sans difficultés à toutes vos données. Pour éviter d'être piraté en cascade privilégiez un mot de passe unique pour chaque compte.

2. **Utiliser un générateur de mot de passe et un gestionnaire de Mots de passe**

Solution de facilité, le générateur de mot de passe saura vous procurer une succession de lettres et de chiffres aléatoires, difficile à retenir certes, mais aussi difficile à pirater.

Un gestionnaire de mot de passe se présente sous la forme d'une base de données dans laquelle vous pouvez enregistrer de façon sécurisée vos identifiants et mots de passe. Pour y accéder, vous devrez bien entendu saisir un mot de passe mais ce sera finalement le seul à retenir.

Bitwarden est un générateur et gestionnaire de mot de passe reconnu qui vous donne la possibilité de choisir la longueur de ce dernier. Vous pouvez même choisir d'inclure ou non des lettres, des chiffres et des symboles.

3. **Miser sur la longueur**

Si vous ne souhaitez pas utiliser de générateur de mot de passe mais que vous préférez le créer vous-même, misé sur la longueur. Cela signifie que vous devez insérer plus de 10 caractères, 12 et 14 étant de bonnes moyennes. Plus votre mot de passe sera long, plus il sera compliqué à deviner.

4. **Varier les caractères**

Au-delà du nombre de caractères, leur type est aussi important. Idéalement, votre mot de passe doit contenir 4 types de caractères différents : Des lettres majuscules, Des lettres minuscules, Des chiffres, Des caractères spéciaux. N'hésitez pas à bien les mélanger pour obtenir un effet aléatoire.

5. **Préférer l'aléatoire**

Votre mot de passe ne doit pas avoir de signification particulière telle qu'une date, un surnom, le nom de votre chien, une suite logique de chiffres et de lettres, etc. Optez pour un mot de passe aléatoire, qui ne veut rien dire.

6. **Changer de mot de passe régulièrement**

Pour plus de sécurité, il est recommandé de changer régulièrement son mot de passe, surtout en entreprise lorsqu'ils donnent accès à des données sensibles. Si une personne quitte votre société ou si vous arrêtez votre collaboration avec un prestataire ayant accès à certains de vos comptes, changez rapidement vos mots de passe.

IV. Protection du serveur d'Email

Un **serveur de messagerie électronique** est un logiciel serveur de courrier électronique. Il a pour vocation de transférer les messages électroniques d'un serveur à un autre. Un utilisateur n'est jamais en contact direct avec ce serveur mais utilise soit un client de messagerie installé sur son terminal (ordinateur ou smartphone), soit une messagerie web, qui se charge de

contacter le serveur pour envoyer ou recevoir les messages. On parle dans le premier cas de client lourd, dans le deuxième cas de client léger.

La plupart des serveurs de messagerie actuels disposent des fonctions d'envoi et de réception, mais elles sont indépendantes, et peuvent être dissociées physiquement.

Serveur de messagerie : Comment ça fonctionne ?

Le fonctionnement du courrier électronique repose sur des ordinateurs puissants, reliés au réseau Internet en permanence, qui assurent les échanges d'informations. Ces machines sont appelées des serveurs, en l'occurrence des serveurs mails. Les courriers sont acheminés d'un poste vers un autre en suivent des protocoles bien précis. Pour mieux comprendre ce cheminement, tentons l'analogie avec le courrier postal :

Cheminement du courrier postal :

- **Etape 1 :** Vous rédigez un message et le glissez dans une enveloppe
- **Etape 2 :** Vous postez votre courrier via votre bureau de poste
- **Etape 3 :** La Poste envoie le courrier au destinataire
- **Etape 4 :** Vous trouvez votre courrier, à votre adresse, dans votre boîte aux lettres

Cheminement du courrier électronique (mail) :

- **Etape 1 :** Vous rédigez un message sur votre ordinateur
- **Etape 2 :** Votre mail est envoyé grâce au protocole SMTP (La Poste joue le rôle du serveur SMTP)
- **Etape 3 :** Votre courrier électronique est envoyé au serveur POP ou IMAP du destinataire
- **Etape 4 :** Vous consultez votre mail, en vous connectant à votre boîte aux lettres électronique

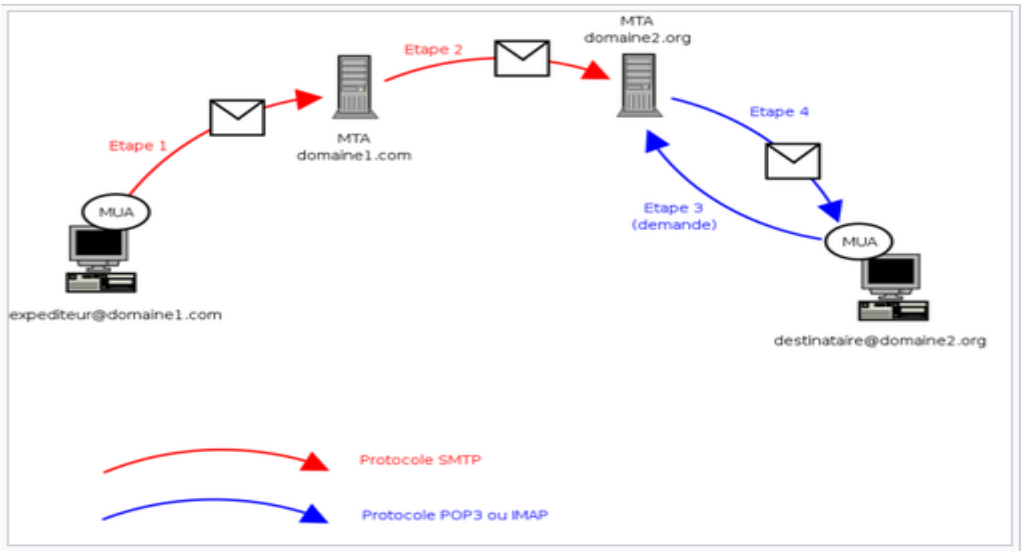


Figure : Fonctionnement du courrier électronique

COMMENT SÉCURISER SA MESSAGERIE ÉLECTRONIQUE PROFESSIONNELLE ?

Pour se prémunir contre ses attaques dont les conséquences peuvent s'avérer désastreuses. La première des choses à faire est de choisir un service de messagerie professionnelle qui vous permettra de :

- Filtrer vos mails selon des règles prédéfinies
- Instaurer des niveaux de sécurité selon les domaines
- Installer un anti-virus capable de détecter la présence de virus dans vos mails
- Gérer les différentes boîtes mails de l'entreprise via une seule et même plateforme
- Vous faire accompagner par un prestataire informatique

D'autres principes de base vous permettront de vous protéger. Parmi eux,

- Ne jamais ouvrir une pièce jointe envoyée par un expéditeur inconnu
- Sensibiliser les employés de l'entreprise aux menaces que représentent les mails
- Ne jamais cliquer sur des liens douteux

V. Protection du Serveur Web

Un serveur Web est un programme qui utilise le protocole HTTP pour fournir les fichiers qui constituent les pages Web que les utilisateurs ont demandées via des requêtes transmises par les clients HTPP de leurs ordinateurs. Des ordinateurs et des Appliance dédiés peuvent également jouer le rôle de serveurs Web.

Le processus est une application du modèle client/serveur. Tous les ordinateurs qui hébergent des sites Web doivent disposer de programmes serveurs Web. Les principaux serveurs Web sont Apache (le serveur Web le plus répandu), IIS (Internet Information Server) de Microsoft et Nginx (prononcé *engine X*) de NGINX. Il existe d'autres serveurs Web, notamment le serveur NetWare de Novell, Google Web Server (GWS) et la gamme des serveurs Domino d'IBM. Les serveurs Web font souvent partie d'un ensemble de programmes de gestion d'Internet et d'intranet chargés d'acheminer les e-mails, de télécharger les requêtes de fichiers FTP et de reconstituer et de publier des pages Web.

Pour choisir un serveur Web, il faut tenir compte de certaines de ses caractéristiques, à savoir : compatibilité avec le système d'exploitation et les autres serveurs, capacité à prendre en charge la programmation côté serveur, les mécanismes de sécurité et les outils particuliers fournis pour la publication, le moteur de recherche et la création de site.

Les attaques pirates visent particulièrement les sites des entreprises, y compris celles de taille réduite. Les principaux risques sont la défiguration, ou défaçage, où l'attaquant modifie le contenu du site, et le déni de service, où les utilisateurs ne peuvent plus accéder au site, celui-ci étant saturé de requêtes et donc plus capable d'accueillir de nouveaux visiteurs. Il est aussi possible de se servir d'un site web comme d'une porte d'entrée vers le système d'information, pour déposer des contenus illégaux, ou piéger les internautes. "Un site hacker provoque des conséquences importantes, même si ce n'est qu'un site vitrine, alerte Benoît Grunemwald, expert en cyber sécurité chez l'éditeur d'antivirus et de programmes de sécurité Eset. Les pirates

peuvent accéder aux logins et mots de passe, se servir du site piraté comme hébergement pour relayer des menaces, et par exemple mener des attaques de spear phishing, un phishing social, en donnant l'impression que les mails viennent d'un site sécurisé ". Pour s'en prémunir, il existe différents procédés, selon ses moyens techniques et financiers.

Mettre à jour

Bien qu'extrêmement simple, tout le monde n'y pense pas. Les mises à jour permettent aux logiciels de réparer les failles des versions précédentes qui permettent à des pirates de s'infiltrer. "Beaucoup de sites abritant à leur insu des produits illicites le sont parce que le CMS n'est pas à jour" Avec un CMS très populaire pas à jour, on peut être sûr que cela arrivera ".

Limiter et sécuriser les accès

Plus les personnes qui ont les accès d'administration ou d'édition d'un site sont nombreuses, plus le risque de piratage est grand. Il faut donc s'assurer que les mots de passe des administrateurs comme des utilisateurs sont suffisamment sécurisés. Il faut éviter les mots de passe trop génériques ou identiques aux identifiants qui ne changent jamais et ne pas utiliser de comptes utilisateurs partagés par plusieurs personnes.

Ajouter des couches de protection au serveur

Il est essentiel de contrôler les données qui transitent sur le site. C'est le rôle d'un pare-feu, qu'il est possible de paramétrer et ainsi définir ce qui soit être bloqué ou non. Il est aussi fondamental de mettre en place un protocole https. "C'est capital pour les sites marchands". Ce protocole de communication client–serveur (entre une machine qui envoie des requêtes et une autre qui y répond, comme par exemple un navigateur web qui envoie des requêtes aux serveurs d'un site internet) est une variante du protocole de communication standard http, sécurisée par l'usage de protocoles de sécurisation TLS qui chiffrent les données, contrairement au http.

Faire auditer le code et l'infrastructure

Il est quasiment impossible aux non experts de savoir si l'architecture d'un site est configurée correctement pour résister aux attaques. C'est pourquoi il est recommande de "faire auditer son code et son infrastructure par des professionnels, afin de voir les vulnérabilités, a minima lors du déploiement, et ensuite idéalement dès qu'il y a un changement important dans l'infrastructure".

Surveiller l'activité des serveurs

Cela reste le meilleur moyen de repérer une activité suspecte : connexions à des heures anormales, trop fréquentes au vu du nombre d'autorisations, trafic extrêmement élevé à des endroits inhabituels….

VI. Protection du Serveur FTP

Un **serveur FTP** (File Transfer Protocol) est un logiciel utilisé dans le transfert de fichiers entre deux ordinateurs. Il est, avec le client FTP, l'une des deux composantes d'un transfert de fichiers via le langage FTP.

De manière classique, un **serveur FTP** installé sur un ordinateur autorise le téléchargement, la lecture, la modification ou la suppression à distance, via Internet ou un réseau local, de fichiers par un utilisateur. L'investigateur de ces échanges de fichiers est appelé client FTP.

De nos jours, le **serveur FTP** est principalement utilisé par les webmasters qui gèrent des sites Internet pour la mise en ligne, la modification ou encore la sauvegarde de contenus. Certaines entreprises utilisent encore le protocole FTP pour échanger des fichiers volumineux avec des partenaires et/ou des collaborateurs

Les protocoles de FTP sécurisés actuels

Il existe deux principaux protocoles de FTP sécurisé :

SFTP (FTP via SSH) et **FTPS** (FTP via SSL)

SFTP et FTPS utilisent des algorithmes renforcés tels qu'AES et Triple DES pour chiffrer les données transférées, et offrent ainsi un haut niveau de protection. SFTP et FTPS possèdent de nombreuses fonctionnalités avec un large ensemble de commandes pour transférer et traiter des fichiers.

Suivant les besoins de votre société, chacune des deux options pourrait vous permettre de sécuriser vos transferts de fichiers. Cependant, il y a quelques différences notables concernant la façon dont les connexions sont authentifiées et gérées.

Avec SFTP, une connexion peut être authentifiée au moyen de deux techniques différentes :

1. Pour l'authentification de base, vous ou votre partenaire commercial aurez uniquement besoin d'un identifiant utilisateur et un mot de passe pour vous connecter au serveur SFTP.

Il est important de noter que les identifiants utilisateur et les mots de passe fournis à travers la connexion SFTP sont chiffrés (ce qui est un grand avantage par rapport au FTP standard).

2. Les clés SSH peuvent aussi être utilisées pour authentifier les connexions SFTP, en plus ou à la place des mots de passe.

Avec l'authentification basée sur les clés, vous devrez générer préalablement une clé privée et une clé publique SSH. Si vous voulez vous connecter au serveur SFTP d'un partenaire commercial, vous devrez alors lui envoyer votre clé publique SSH pour qu'il puisse la charger sur son serveur et l'associer à votre compte. Puis, une fois que vous serez connecté à son serveur SFTP, votre logiciel client transmettra votre clé publique au serveur pour l'authentification. Si les clés correspondent et que l'utilisateur et le mot de passe utilisé sont corrects, l'authentification réussira.

Avec FTPS, une connexion est authentifiée à l'aide d'un identifiant utilisateur, d'un mot de passe et d'un certificat :

Comme avec SFTP, les noms d'utilisateur et les mots de passe pour les connexions FTPS sont chiffrés.

Lorsque vous vous connectez au serveur FTPS d'un partenaire commercial, votre client FTPS vérifie d'abord que le certificat du serveur est digne de confiance. Le certificat est considéré comme digne de confiance si le certificat a été signé par une autorité de certification connue, telle que Verisign, ou si le certificat a été auto-signé par votre partenaire. Pour vérifier les certificats auto-signés, vous devez avoir une copie de leur certificat public dans votre fichier de clés dignes de confiance.

Votre partenaire peut aussi demander que vous fournissiez un certificat lorsque vous vous connectez à lui. Votre certificat peut être signé par une autorité de certification tierce ou bien votre partenaire peut vous permettre d'auto-signer votre certificat, à condition que vous lui envoyiez la partie publique de votre certificat pour qu'il la charge dans son fichier de clés dignes de confiance.

SFTP ou FTPS : Implémentation

Le protocole sécurisé SFTP est considéré plus facile à implémenter que le FTPS. SFTP a besoin d'un seul port (22 par défaut), impliquant ainsi une configuration simple pour un pare-feu. Ce port SFTP unique sera utilisé pour toutes les communications, c'est-à-dire l'authentification initiale, toutes les commandes émises et toutes les données transférées.

FTPS peut, malheureusement, être très difficile à installer à travers un pare-feu solidement protégé. FTPS utilise plusieurs ports. Le numéro de port initial (21 par défaut) est utilisé pour l'authentification et la transmission des commandes. Cependant, chaque fois qu'une demande de transfert de fichiers (par exemple *get* ou *put*) ou une demande de liste des répertoires est effectuée, un autre port doit être ouvert. Vous et vos partenaires commerciaux devrez donc ouvrir une série de ports dans vos pare-feu pour permettre les connexions FTPS, ce qui peut rendre votre réseau vulnérable et affaiblir vos défenses de cyber sécurité.

En résumé, SFTP et FTPS sont tous les deux des protocoles FTP sécurisés avec des options d'authentification renforcées. Cependant, dans la mesure où SFTP est beaucoup plus facile à installer à travers les pare-feu, nous pensons que SFTP ressort nettement vainqueur de la comparaison entre les deux protocoles.