Date : 09/2016 | Votre interlocuteur : Yann BELZ | Mail : contact@espace-technologie.com | # 01

Parc d'Activités Schweitzer
26 rue du Bois Fossé
85300 CHALLANS
Tél. 02 51 49 31 31

espace technologie

FICHE CONSEIL

Protection de votre serveur EXCHANGE

COMPÉTENCES - TRANSPARENCE - CONFIANCE

L'ESSENTIEL

Les risques sur internet ont évolué, les opérateurs internet ont pris des mesures afin de se protéger. Ces mesures necessitent que votre serveur Exchange fonctionne en autonomie et non plus par l'intermédiaire d'un serveur de mails.

En effet, auparavant les emails transitaient par un serveur de mails. Ce serveur avait plusieurs rôles :

- sécurité (blocage de virus et blocage de spams avant qu'ils n'arrivent sur votre serveur),
- continuité de services (en cas de panne de votre serveur vous aviez accès aux mails en « WEBMAIL ».
- C'est aussi lui qui subissait et vous protégeaient des attaques pirates.

CE QUI A CHANGE

CE QUE VOUS DEVEZ COMPRENDRE

Pour circuler un email doit être « certifié » par un protocole c'est ce que l'on appelle « SMTP » « Simple Mail Protocole »

Auparavant, (moins d'un an) le SMTP est habituellement délivré par le fournisseur d'accès internet (FAI).

Maintenant les fournisseurs d'accès ne veulent plus prendre la responsabilité d'assurer ce protocole pour les emails des entreprises (@nomdesociete.xxx)

Cette politique engendre des problèmes aléatoires d'envois et réceptions de mails pour les configurations historiques (cf. l'essentiel).

LA SOLUTION

Afin de résoudre ces problématiques et surtout ne pas engendrer d'autres soucis, nous avons défini un cahier des charges que nous vous conseillons de suivre :

Configurer votre serveur de mails en « MX », c'est-à-dire qu'il recevra directement les emails sans passer par un serveur de mails.

Cette configuration engendre des effets pervers qu'il faut résoudre :

- Ouverture des ports 25 et 443 de votre routeur ce qui potentiellement expose le serveur aux attaques.
    - Par conséquent il faut le protéger de ces attaques. Pour cela, vous devrez activer les fonctionnalités d'IDS/IPS de votre routeur (IDS : Intrusion Détection System ; IPS : Intrusion Protection System).
- Ensuite il conviendra de protéger vos utilisateurs de ces ports ouverts au monde : en effet, le monde entier peut contacter votre serveur Exchange, les spammeurs vont donc s'en donner à cœur joie ! Vous devrez donc installer une protection anti spam.
- Nous conseillons vivement un anti spam cloud qui contrôle en amont vos mails pour bloquer les spam et virus avant qu'ils n'arrivent sur votre serveur (MAX MAIL est la solution que nous préconisons)
- Cette solution permet aussi de contrôler les mails qui sortent ce qui garantit que vos emails sortants vont être acheminés :
- Votre IP publique ne doit pas être Blacklistée (vérifier sur www.espace-technologie.com rubrique espace privé, contrôle Blacklist Serveurs)
    - Exemple

- Vous devez vérifier périodiquement que votre nom de domaine n'est pas Blacklisté.

- Mise en place d'un enregistrement SPF :
    - Le protocole Simple Mail Transfer Protocol (SMTP) dont on a parlé précédemment est utilisé pour le transfert du courrier électronique sur Internet ne prévoit pas de mécanisme de vérification de l'expéditeur, c'est-à-dire qu'il est facile

d'envoyer un courrier avec une adresse d'expéditeur factice, voire usurpée. SPF vise à réduire les possibilités d'usurpation en publiant, dans le DNS, un enregistrement (de type TXT) indiquant quelles adresses IP sont autorisées ou interdites à envoyer du courrier pour le domaine considéré.

- Les utilisateurs distants (Smartphones, portables tablettes etc…)
  - Il vous faudra acheter un certificat auprès d'une autorité de certificat

Un certificat, c'est quoi ?

Un certificat, c'est un document numérique en 2 parties, voué à chiffrer les données entre un client et un serveur.

Lorsque vous vous connectez à votre banque, vous le faites par le protocole HTTPS (https://www.mabanque.fr). Le 'S' signifie 'Sécurisé', car la communication entre votre poste et le serveur de la banque est chiffrée.

Concrètement, lorsque vous vous connectez à votre banque, le serveur de la banque vous envoie sa clé publique. Vous chiffrez les informations avec cette clé publique, vous envoyez les données, et le serveur de la banque est le seul à pouvoir les déchiffrer.

SAUVEGARDE

Bien évidemment, il conviendra de sauvegarder votre serveur de messagerie.

- Attention la sauvegarde de messagerie est différente de la sauvegarde de fichiers.
    - En effet, les emails sont stockés dans une base de données
    - Si l'on sauvegarde avec un outil non adapté la base entière sera sauvegardée, par conséquent la restauration sera elle aussi la base complète.
    - Cependant, imaginez que vous souhaitiez récupérer un email, il vous faudra restaurer la base entière et les emails reçus (ainsi que ceux de vos collaborateurs) après seront supprimés et perdus
- Suivant les cas nous proposons des logiciels comme ARCSERV ou VEEAM qui savent restaurer une partie de la base de données des emails.

SOLUTION

Comme vous pouvez le constater ce qui était vrai hier ne l'est plus aujourd'hui.

Ceci est un peu compliqué mais nos équipes sont à votre disposition pour mettre en place une solution fiable adaptée à votre infrastructure informatique.

N'hésitez pas à nous consulter.

Vous souhaitez un conseil :

contact@espace-technologie.com

02 51 49 31 31