



Sécuriser les échanges avec ses partenaires

L'activité des entreprises repose souvent sur la rapidité et la qualité des échanges d'informations avec ses partenaires, clients, prospects et fournisseurs. Cette nécessité explique l'utilisation de plus en plus courantes de moyens d'échanges dématérialisés comme les mails, la mise en ligne de documents sur des sites internet ou la mise en place d'extranets.

Mais ces échanges s'accompagnent de risques multiples pour l'entreprise.

Les risques liés aux échanges avec ses partenaires :

- Les informations contenues dans un mail, qui équivaut en fait à une carte postale sans enveloppe, peuvent facilement être lues ou récupérées.
- L'identité de l'expéditeur d'un mail n'étant, en général, pas certifiée, une personne mal intentionnée peut détourner le mail, modifier son contenu et le réexpédier au destinataire.
- Il est possible aussi d'usurper l'identité d'une personne et d'envoyer tout simplement un mail avec son adresse volée.
- Des informations confidentielles hébergées sur un site internet peuvent être récupérées facilement car elles transitent en clair à travers internet.
- Outre les données confidentielles, ce sont aussi les codes d'accès des partenaires autorisés à se connecter au site, qu'un pirate peut facilement récupérer. Il peut ainsi se faire passer pour un utilisateur référencé, se connecter et consulter des informations dont il ne doit pas avoir l'accès.
- Enfin, l'utilisation d'un extranet peut ouvrir une brèche dans la sécurité informatique de l'entreprise et exposer son système d'information.

Comme les moyens techniques de sécurité vont dépendre des besoins et usages de l'entreprise, nous allons traiter 2 cas, qui nous semblent les plus courants.

Cas 1 : L'entreprise Ganymède veut envoyer par mail des informations confidentielles à son expert comptable.

Cas 2 : L'entreprise Archeo Construction, quant à elle, veut mettre à disposition sur un site internet des plans de fabrication, qui doivent être utilisés par ses sous-traitants.

Cas 1 : L'entreprise Ganymède



L'entreprise Ganymède veut envoyer par mail des informations confidentielles à son expert comptable.

Facilité de mise en œuvre : Facile
Facilité d'exploitation : Facile
Hauteur de l'investissement humain : moyenne

La solution technique adoptée par l'entreprise :

- Des certificats numériques sont utilisés, afin :
 - de signer numériquement le mail, qui permet d'authentifier l'identité de l'expéditeur ;
 - et de crypter les informations et documents confidentiels contenus dans les mails échangés entre l'entreprise Ganymède et l'expert comptable.
- Ces certificats sont installés dans les clients de messagerie utilisés par la comptable de l'entreprise Ganymède (Outlook express) et par l'expert comptable (Microsoft Office Outlook).

Les règles à suivre pour utiliser un certificat.

- Echanger tout d'abord les certificats entre la comptable de Ganymède et l'expert comptable, afin qu'ils puissent ensuite s'échanger des messages cryptés sur Internet. Ils peuvent par exemple s'envoyer mutuellement un mail signé numériquement. Chacun d'eux pourra ainsi ajouter le nom de l'expéditeur et son certificat à ses Contacts.
- Envoyer de préférence les documents sous format pdf, car c'est un format de fichier non modifiable. Cela évitera à un pirate d'intercepter, de modifier puis de renvoyer le fichier avec des données erronées.

Cas 2 : l'entreprise Archeo Construction

L'entreprise Archeo Construction, quant à elle, veut mettre à disposition sur un site internet des plans de fabrication, qui doivent être utilisés par ses sous-traitants.

Facilité de mise en œuvre : moyenne
Facilité d'exploitation : Facile
Hauteur de l'investissement humain : moyenne

La solution technique adoptée par l'entreprise :

- Le site Web est hébergé hors des locaux de l'entreprise, chez le fournisseur d'accès à Internet, afin de minimiser les risques d'intrusion sur le réseau informatique interne.
- Le protocole de communication réseau sécurisé SSL est implémenté sur le site, afin de créer un canal de communication crypté entre le serveur Web et le navigateur Internet des sous-traitants. La transmission des données est ainsi sécurisée.
- Des certificats numériques sont également utilisés par le sous-traitant, qui accède au site Internet et par le serveur web, qui héberge ce site. Ces 2 entités peuvent ainsi s'authentifier mutuellement avant d'échanger quoique ce soit.

Les règles que l'entreprise doit suivre pour sécuriser les accès.

- Bien vérifier que les pages restent inaccessibles aux utilisateurs non identifiés ou non autorisés.
- **Effectuer l'identification de l'utilisateur autorisé, en cryptant la transmission du login et du mot de passe. Ceci évitera l'usurpation d'identité de l'un des partenaires et l'accès illicite aux données confidentielles, qui sont mises en ligne sur le site web. Un cadenas fermé doit être indiqué en bas de la fenêtre du navigateur Web et l'adresse du site doit commencer par https.**