Sécurisation numérique PME en 12 points

Pour qu'elles soient pérennes, les entreprises doivent définir une politique de sécurité informatique absolue. Les douze points évoqués ci-dessous permettront de tendre vers cet objectif.


Les mots de passe :
Une politique de mots de masse (MDP) doit être judicieusement mise en place afin d'augmenter la sécurité informatique de l'entreprise. Un MDP doit comporter au moins 8 caractères alphanumériques comprenant des caractères spéciaux. Aidez-vous d'un coffre fort numérique du style Dashlane ou Keepass permettant de générer et d'enregistrer l'ensemble de vos MDP. Prenez soin de choisir un mot de passe différent pour chacun de vos comptes.

Le BYOD :
Bring Your Own Device (BYOD) signifie utiliser son matériel personnel à des fins professionnelles. Il convient de proscrire cette utilisation autant que possible. Sinon, il est absolument nécessaire d'imposer les mesures suivantes : chiffrement actif de l'appareil, applications validées, antivirus professionnel à jour, effectuer des sauvegardes régulières et en cas de perte ou de vol du dit-matériel, capacité de suppression à distance des données.

Les postes nomades :
Pour éviter le vol de données sur un ordinateur portable, nous conseillons de crypter les données sensibles à l'aide d'un utilitaire comme TrueCrypt permettant de créer un disque virtuel chiffré et ainsi de protéger vos informations. A noter également la préconisation par l'Agence Nationale de la Sécurité des Systèmes d'Information d'un conteneur nommé ''ZED'' permettant de protéger des fichiers au sein de conteneurs à des fins d'archivage et d'échange par courriel sur des réseaux publics ou par support physique (clé USB).

Le Cloud :
Le recours au Cloud de confiance n'est pas un effet de mode mais un enjeu déterminant pour externaliser les applications et les données de manière sécurisée. Choisir un hébergeur français, vérifier le cadre juridique, le temps de rétablissement en cas de rupture d'accès aux données et la sécurisation des échanges avec les plates-formes Cloud sont un minimum à respecter.

Les pièces jointes :
Parfois un clic sur une pièce jointe peut engendrer bien des dégâts sur les Systèmes Informatiques (SI) d'une entreprise. Vers et virus se propagent facilement par ce biais. La vérification des pièces jointes par un antivirus à jour est indispensable. Ne cliquez que sur les pièces jointes dont vous connaissez la provenance.

Les réseaux sociaux :
Les réseaux sociaux ont le vent en poupe. Il convient de sensibiliser les employés sur l'utilisation de ces réseaux. Limiter, contrôler et faire valider les informations liées à l'entreprise pouvant être diffusées sur les réseaux. Mettre en place une veille rigoureuse sur les dirigeants et l'entreprise afin de pouvoir être réactif en cas de dénigrements. Il faut inciter à l'utilisation de mots de passe complexes permettant ainsi d'empêcher une utilisation frauduleuse des différents comptes.

Le wifi :
A n'utiliser que s'il est utile au bon fonctionnement de l'entreprise. Il convient de l'éteindre à la fermeture de l'entreprise le soir. Modifiez le nom de ce réseau et le niveau de la clé de chiffrement qui doit être de type WPA2. Enfin, cette clé de connexion doit comporter un mot de passe long et complexe.

Le LTS :
Le Local Technique de Site (LTS) est un local comprenant les serveurs informatiques et les arrivées Internet. Cœur numérique de l'entreprise, sa protection doit être absolue et efficiente. Le respect de la règle des 3 ''I'' : anti-Intrusion, anti-Inondation, anti-Incendie garantie sa sauvegarde. Éviter de matérialiser l'emplacement de ce LTS pour plus de discrétion est également judicieux.

Les logiciels :
Les failles de sécurité sur les logiciels et sur les systèmes d'exploitation sont nombreuses et les pirates informatiques les utilisent avec habileté. Pour limiter les risques de piratage, il convient de mettre à jour régulièrement les logiciels acquis légalement.

La sectorisation des serveurs et les sauvegardes :
La mise en place des droits des utilisateurs sur les serveurs de l'entreprise doit être organisée et systématique. En effet, l'application du concept sur le droit et le besoin d'en connaître est une nécessité pour garantir la discrétion des informations sensibles.
Les sauvegardes des serveurs sont indispensables. Elles doivent être déposées dans un lieu sécurisé et distant du Local Technique de Site.

Le poste de travail :
La sécurité des postes de travail doit être assurée à chaque instant. Outre les mots de passe, il est nécessaire d'être vigilant sur la gestion des supports amovibles (disques durs, clés USB etc.) et de passer ces éléments à l'analyse d'un antivirus à jour. La navigation sur Internet, les téléchargements, les courriels sont autant de risques potentiels à prendre au sérieux. Attention au ''clic'' malheureux pouvant entraîner l'infection d'une machine.

La sensibilisation des personnels :
La première action à conduire au sein d'une entreprise est la sensibilisation des personnels à l'utilisation et la sécurisation des systèmes informatiques de la société. L'humain est et restera toujours le maillon faible de la sécurité informatique d'une entreprise. La réalisation d'une sensibilisation annuelle portant sur les failles informatiques mais aussi sur les failles humaines, physiques est un minimum vital.

8 Rue Logerot – BP 649 – 86023 POITIERS CEDEX – Tél : 05.49.00.56.00.