www.inforisque.info
Pays : France
Dynamisme : 8

Visualiser l'article

Sécurité informatique : 10 bonnes résolutions pour une année 2016 sereine !

Alors que 2015 s'est achevée sur un arrière goût de cyber-attaque (piratages des réseaux PSN de Sony et Xbox Live de Microsoft par le groupe Lizard Squad à Noël pour ne citer qu'eux), WOOXO, expert français de la sauvegarde et de l'exploitation sécurisées de données informatiques professionnelles, s'adresse aujourd'hui à toutes les TPE et PME pour leur proposer quelques bonnes pratiques en matière de sécurité informatique pour bien débuter cette nouvelle année !

1) S'initier aux fondements de la sécurité informatique
La sécurité informatique s'appréhende sous trois aspects élémentaires et complémentaires : la prévention, la détection et la réaction. Elle vise généralement cinq principaux objectifs.

L'intégrité : garantir que les données sont bien celles que l'on croit être.
La disponibilité : maintenir le bon fonctionnement du système d'information.
La confidentialité : rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction.
La non répudiation : garantir qu'une transaction ne peut être niée.
L'authentification : assurer que seules les personnes autorisées ont accès aux ressources.
2) Sécuriser l'accès physique aux locaux de la société
La première des règles de vigilance est bien sûr la bonne sécurisation des locaux, et plus particulièrement la protection des espaces dits sensibles comme les salles d'hébergement des serveurs informatiques. Il faut conditionner leurs accès à des habilitations, clés, digicodes, badges nominatifs, etc.

3) Sécuriser les transferts de fichiers
Chaque jour les collaborateurs échangent et transfèrent des dizaines de fichiers à des tiers. Il faut alors s'assurer de sécuriser ces échanges par des mots de passe temporaires et de conserver le détail et l'historique de ces transferts (date de l'envoi, fichier mis à disposition, expéditeur et destinataire).

4) Formaliser une politique de sécurité du système d'information
L'évaluation de l'impact sur la sécurité informatique est un préalable à tout projet lié au système d'information. Il faut recenser les règles relatives à la sécurité informatique dans un document écrit et accessible à tous les collaborateurs. Il évoluera au rythme des modifications apportées au système d'information. Ce document dresse l'inventaire des vulnérabilités de l'exploitation informatique de la société, des menaces potentielles, des outils de monitoring (surveillance) ou contrôles mis en place pour détecter les menaces éventuelles.

5) Sauvegarder les données informatiques
Savoir-faire, procédures, fichiers clients, comptabilité, emails, les données informatiques constituent le patrimoine informationnel. Il s'agit de la richesse de l'entreprise, peut-être même son principal avantage concurrentiel, d'où la nécessité de les mettre en sécurité !

Différents systèmes de sauvegarde existent (cloud privé avec sauvegarde sur le site de l'entreprise, cloud public en data-center, cloud hybride), il faut alors choisir le plus adapté aux profils et besoins de sa société.

6) Anticiper les risques informatiques
Pour pouvoir relancer son activité dans les meilleurs délais suite à un incident, il est important de rédiger une procédure d'urgence explicative du fonctionnement des serveurs. Les données sauvegardées doivent être stockées sur les disques durs de serveurs dédiés, eux-mêmes sauvegardés régulièrement. Il est impératif également de stocker les supports de sauvegarde dans des serveurs conçus pour résister aux catastrophes naturelles ou sinistres majeurs, ou de les stocker dans locaux distincts et fortement protégés. Si le parc informatique est renouvelé, les machines en fin de vie doivent être physiquement détruites ou débarrassées de leur disque dur. Les périphériques de stockages amovibles doivent aussi être formatés avant réparation, recyclage ou changement d'utilisateur.

7) Sécuriser les postes de travail sédentaires et nomades
Pour prévenir toute utilisation frauduleuse, les ordinateurs de chaque collaborateur de l'entreprise doivent être paramétrés afin qu'ils se verrouillent automatiquement en cas d'absence ou d'inactivité prolongée. Sur les postes contenant des données critiques, un système de contrôles des ports USB doit être installé en complément.

8) Mettre en place un processus de création et de suppression des comptes utilisateurs
Sur tous les postes de travail de l'entreprise, il faut créer des comptes utilisateurs nominatifs afin de pouvoir tracer les actions des usagers et ainsi les responsabiliser.

9) Protéger les réseaux : local et sans fil
Aujourd'hui de plus en plus de malwares peuvent potentiellement nuire au système d'information : virus, chevaux de troie, keyloggers, spywares et autres vers. Des dispositifs de sécurité existent pour aider à limiter la vulnérabilité face aux attaques extérieures : routeurs filtrants, pare-feux, etc. Il faut veiller tout particulièrement à la protection des messageries électroniques, réseaux sans fils et accès distants.

10) Effectuer régulièrement des tests de restauration des fichiers des serveurs et ordinateurs.
Tester régulièrement (au moins une fois par an) la capacité de restauration de ses données pour s'assurer d'une reprise d'activité rapide après un incident. Il faut s'assurer également de sauvegarder les images système des serveurs et PC. Seule la sauvegarde de l'environnement (Mac, Windows, Linux, etc.) permettra de remonter les applications, logiciels métier et datas.

Auteur : Wooxo.