FICHE PRATIQUE

Votre prestataire vous rappelle les bonnes pratiques pour sécuriser vos systèmes d'information

Alors que le numérique fait désormais partie intégrante de nos vies personnelles et professionnelles, le niveau de sécurité appliqué dans la plupart des entreprises est très largement lacunaire. Les nouvelles technologies, porteuses de nouveaux risques pesant lourdement sur les entreprises, imposent de prendre en compte la sécurité dans nos usages.

L'acquisition de réflexes simples et de bon sens permet de sécuriser votre usage de l'informatique. Soucieux de votre sécurité, votre prestataire vous conseille et vous informe sur les risques et les moyens de vous en prémunir en acquérant des réflexes simples.

Votre prestataire, dans le cadre de son obligation de conseil et d'information, vous invite à adopter les bonnes pratiques et à mettre en œuvre sans délai l'ensemble des recommandations ci-dessous.

Préservez vos données

Nul ne pouvant garantir zéro défaillance ou zéro intrusion, les sauvegardes sont indispensables et doivent être réalisées à des échéances calculées en fonction de la quantité de données qui peut être perdue par l'entreprise sans mettre son exploitation en danger. Les sauvegardes, quel que soit le support, ne doivent pas être conservées sur le même lieux que les données.

Attention, selon l'usage, la surveillance de la bonne exécution des sauvegardes est de votre ressort. N'hésitez pas à solliciter votre prestataire pour la mise en place d'un contrat de supervision si vous souhaitez externaliser cette fonction vitale.

Une sauvegarde fiable est une sauvegarde testée. Il est nécessaire de planifier des tests réguliers. En outre, Cloud ne signifie pas sauvegarde. Vos données dans le Cloud ne sont pas implicitement sauvegardées.

Faites les mises à jour

Les mises à jour de vos systèmes d'exploitation, logiciels et applications doivent être réalisées, idéalement automatiquement, sinon, téléchargez les correctifs de sécurité disponibles.

Un antivirus de dernière génération, piloté et centralisé est indispensable sur tous vos postes et vos serveurs de fichiers. En cas d'alerte, il faut prévenir votre prestataire. Ne négligez pas non plus les appareils mobiles, soyez aussi prudents avec les smartphones et tablettes qu'avec les ordinateurs.

Choisissez vos mots de passe avec soin

Vous devez mettre en place une politique de gestion des mots de passe stricte et réfléchie. Pour vous aider, rendez-vous sur le site www.cybermalveillance.gouv.fr/tous-nos-contenus/

Sécurisez votre accès internet

Votre accès internet doit être protégé par un vrai UTM (United Threat Management). Les services inclus dans les boxes des opérateurs n'offrent AUCUNE sécurité. Par ailleurs, les accès à distance mis à disposition de vos collaborateurs nomades doivent être sécurisés via un accès SSL.

Soyez prudent lors de l'utilisation de la messagerie

Les courriels et pièces jointes jouent souvent un rôle central dans la réalisation des attaques informatiques. Evitez de cliquer sur les pièces jointes, liens ou messages inconnus.

Sensibilisez vos collaborateurs

Faites de la sécurité un enjeu partagé par l'ensemble des collaborateurs en mettant en place une campagne régulière d'information et de sensibilisation.

Une charte d'utilisation des systèmes d'information qui précisera de manière explicite les droits et devoirs des collaborateurs est indispensable. A défaut, il sera illégal et de votre stricte responsabilité de mener des opérations sur vos systèmes informatiques telles que la récupération d'e-mail après le départ d'un salarié, l'enregistrement des logs en cas de plainte, procédures disciplinaires...

Votre prestataire est là pour vous assister dans toutes ces démarches, et a une obligation de conseil, matérialisée par cette fiche, mais le choix de faire ou de ne pas faire n'appartient qu'à vous !