ATTAQUES CYBER & PROFESSIONNELS DE SANTÉ

Découvrez nos 10 conseils pour vous protéger

1. METTRE RÉGULIÈREMENT À JOUR VOS SYSTÈMES D'INFORMATIONS

Cette première mesure vous sera d'une grande utilité. A l'aide de patchs de sécurité de plus en plus fréquents, la mise à jour de vos réseaux, vos pares-feux, vos antivirus et vos applications va vous permettre d'**améliorer significativement le niveau de sécurité** de vos systèmes contre les cyberattaques.

2. CONFIGURER AVEC PRÉCAUTION LES PARES-FEUX ET LES SYSTÈMES DE DÉTECTION D'INTRUSION

Les pares-feux peuvent bloquer les tentatives d'intrusion non autorisées ; les systèmes de détection d'intrusion et les outils de surveillance du réseau peuvent vous aider à **détecter les activités suspectes** sur votre réseau informatique.

3. LIMITER LES ACCÈS AUX DONNÉES SENSIBLES

Vos employés ne doivent avoir accès qu'aux informations dont ils ont besoin pour effectuer leur travail. Les accès doivent être **régulièrement examinés et révoqués si nécessaire**. En effet, les hackers profitent de ces accès, quand ils sont mal gérés, pour élever leurs niveaux de privilèges et lancer efficacement leurs cyberattaques.

4. UTILISER DES MOTS DE PASSE COMPLEXES ET L'AUTHENTIFICATION MULTI-FACTEURS

En mettant en place une **politique rigoureuse de gestion des mots de passe** et de contrôle des accès au réseau informatique, vous restreindrez le risque d'intrusion.
L'**authentification multi-facteurs** est également un excellent moyen de réduire le risque d'intrusion en cas de mots de passe ayant fuité, d'attaques par brute force de mots de passe, etc.

5. CONTRÔLER LES POINTS D'ACCÈS DISTANTS À VOS SYSTÈMES D'INFORMATION

Les nouveaux modes de travail comme le télétravail entraînent une multiplication des accès externes à vos systèmes d'informations. Dans la mesure du possible, nous vous recommandons de les éviter ou alors de les contrôler de manière très rigoureuse, en **mettant en place un VPN sécurisé couplé à une authentification MFA** (Authentification multi-facteurs) par exemple.

6. METTRE EN PLACE UN PLAN DE SAUVEGARDE DES DONNÉES

En cas de défaillance du système d'information (SI), la possibilité de restaurer des données **préserve l'activité de votre structure**. Cette capacité de restauration des données professionnelles (sur les serveurs comme sur les postes de travail) est la **protection la plus efficace** contre les logiciels malveillants de type ransomware.

Votre cabinet pourra, en effet, poursuivre son activité en récupérant les données stockées et mises à jour régulièrement. Il faudra alors que ces sauvegardes soient **stockées à l'extérieur de votre entreprise** pour ne pas être cryptées en cas d'attaque au même titre que les autres fichiers de votre SI.

7. EVITER LES SITES NON-SÛRS ET LES LOGICIELS DOUTEUX

Les cybercriminels ont souvent recours à de **faux emails**. Ils dissimulent leur identité en prenant le nom de banques ou d'organismes de confiance.

Souvent, ils vous demandent ensuite de **suivre un lien en cliquant dessus**. De plus en plus d'infections proviennent de publications partagées sur les réseaux sociaux

Soyez particulièrement vigilants si **un mail ou un lien vous semble suspect** et envoyez régulièrement des communications à vos collaborateurs à ce sujet.

8. ÉDUQUER VOS CONFRERES SUR LES PRATIQUES DE SÉCURITÉ INFORMATIQUE

Vos salariés ou collaborateurs doivent être informés des **bonnes pratiques en matière de sécurité informatique** et être bien familiarisés aux risques de sécurité. Il est fondamental de les **sensibiliser**, de les aider à identifier les menaces cyber et même former les membres de l'entreprise face aux mesures à prendre contre les cyberattaques.
Par exemple, les employés doivent être encouragés à **changer régulièrement leurs mots de passe** et à avoir des mots de passe complexes.

9. ÊTRE EN CONFORMITÉ AVEC LA RÉGLEMENTATION

Si vous traitez des données personnelles, il est obligatoire que vous soyez en conformité avec le Règlement général de protection des données (RGPD). Vous devez également **nommer un délégué à la protection des données** (DPO) pour gérer cette question.
Ce référent est le lien de votre entreprise avec la Commission nationale informatique et libertés et est le garant de la conformité de votre entreprise au RGPD.

10. FAIRE APPEL À UN EXPERT EN SÉCURITÉ INFORMATIQUE

Les experts en sécurité informatique peuvent vous aider à **identifier les vulnérabilités et à mettre en place des mesures de sécurité** appropriées pour protéger l'entreprise contre les cyberattaques.
Le risque zéro n'existant pas, les conséquences financières d'une faille peuvent peser lourdement sur vos comptes.