Les 5 règles essentielles pour se protéger de la Cybercriminalité que les PME doivent absolument respecter | Denis JACOPINI

La protection des données numériques est rarement une priorité pour les dirigeants de PME alors même que les petites structures sont de plus en plus affectées par les problèmes de sécurité informatique et de cybercriminalité. Comment protéger votre entreprise ?

Des PME de plus en plus touchées par la cybercriminalité

Les PME n'ont pas toujours conscience d'être devenues les cibles de prédilection des pirates informatiques, et pourtant celles-ci concentrent désormais **près de 80 % des attaques** en France ! Un chiffre en constante augmentation qui démontre un changement de stratégie de la part des *«hackers»* et *«crackers»* qui ciblent les petites structures du fait de leur sécurité souvent défaillante.

Cette montée de la cybercriminalité concerne surtout le **vol de données numériques** (les fichiers clients, les coordonnées bancaires ou les contrats) qui sont ensuite revendues au plus offrant sur le marché noir. On note également des cas d'**espionnages économiques**, d'**escroqueries financières** ou de **sabotages des sites de commerce en ligne**.

Cibler une PME peut aussi être un moyen de s'attaquer à un plus gros poisson, dans le cadre d'une attaque de long terme. Puisqu'en infiltrant le réseau de cette petite structure, il devient plus facile de pénétrer par la suite dans celui d'un grand groupe dont elle est le sous-traitant.

Une problématique sérieuse d'autant que les entreprises victimes de cyberattaques font face à de sévères répercussions en termes de **pertes économiques** et d'**impact sur l'image de marque**. Ce risque peut néanmoins être réduit en appliquant quelques bonnes pratiques.

Les règles essentielles pour bien protéger votre entreprise

1.

Sensibiliser les employés de l'entreprise

Il est recommandé d'organiser une campagne de sensibilisation pour informer les employés sur le danger bien réel de la cybercriminalité en insistant sur la nécessité de :

• choisir des mots de passe d'au moins 12 ou 14 caractères mélangeant chiffres et lettres,
• effectuer des sauvegardes fréquentes sur des supports externes ou une plateforme cloud,
• adopter un usage prudent des messageries électroniques et des systèmes de paiement.

2.

Sécuriser l'ensemble des accès Internet

L'entreprise doit protéger tous les accès Internet (y compris les accès Wi-Fi) qui sont les principaux points d'entrée des pirates. De plus en plus de sociétés choisissent d'ailleurs d'installer un réseau privé virtuel (VPN) comprenant un seul et unique point d'échange sécurisé avec Internet.

3.

Uniformiser les logiciels et les maintenir à jour

Pour faire face aux nouvelles techniques d'attaques, il faut régulièrement mettre à jour les logiciels installés sur votre parc, dont les dernières versions doivent toujours être téléchargées sur les sites officiels des éditeurs. Une démarche qui peut être simplifiée en uniformisant le parc informatique avec un système d'exploitation et un logiciel de protection unique pour l'ensemble des appareils.

4.

Redoubler de vigilance avec les appareils mobiles

Il convient de faire preuve d'une vigilance particulière avec tous les appareils mobiles (smartphones et tablettes tactiles) qui sont généralement beaucoup moins sécurisés que les ordinateurs fixes, car chaque machine constitue une porte d'entrée potentielle pour les attaques informatiques.

5.

Adopter une politique de sécurité informatique

L'entreprise doit enfin mettre en place une politique de sécurité informatique précisant clairement les responsabilités de chacun et les procédures prévues en cas d'attaque, afin que les équipes ne soient pas prises au dépourvu et puissent reprendre l'activité le plus rapidement possible… [Lire la suite]

Réagissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :
Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

Quel est notre métier ?
Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**
  - EXPERTISES PRIVÉES
  - EXPERTISES DE VOTES ÉLECTRONIQUES
  - EXPERTISES JUDICIAIRES
  - RECHERCHE DE PREUVES
  - RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)

DÉSIGNATION
N° DPO-15945

Numéro de formateur
93 84 03041 84
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Datadock
Organisme validé
et référencé

Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041

84).
« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.
Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

Le Net Expert
INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Source : *Cybercriminalité & PME : 5 règles pour se protéger | Microsoft pour les PME*