6 bonnes pratiques pour se protéger du piratage informatique

6 bonnes pratiques pour se protéger du piratage informatique

Par manque de temps ou de ressources, les PME négligent le risque de piratage informatique. Quelques règles de bon sens suffisent pourtant à écarter en partie les menaces.

Perdre ses données suite à une attaque informatique peut avoir de lourdes conséquences pour une start-up ou une PME. L'entreprise peut même ne jamais s'en relever. Piratage de site Internet, clé USB piégée, vol de mot de passe, programme espion caché dans des pièces jointes… Les cyber menaces sont de plus en plus fréquentes. Quelles sont les règles simples pour s'en protéger ? Le point avec Stéphane Dahan, président de Securiview, entreprise spécialisée dans le management de la sécurité informatique.

#1 : Identifier les données les plus sensibles

« *Faites preuve d'une saine paranoïa*, affirme Stéphane Dahan. *C'est-à-dire sachez définir précisément quelles sont les informations à protéger dans l'entreprise* ». Inutile donc de mettre des barrières partout sans discernement. Quelle que soit leur forme (mail, papier, fichier), posez vous donc la question : quelles sont les données les plus sensibles et quelle est la probabilité qu'on me les vole ? « *Ensuite, il faut les localiser. Messagerie, Dropbox, téléphone, autant de pistes de fuite possible pour des informations qui ont de la valeur.* »

#2 : Mettre à jour les systèmes et sauvegarder

« *Ne pas oubliez de mettre à jour régulièrement ses antivirus et ses systèmes d'information. On voit trop souvent des entreprises négliger cet aspect* », soutient Stéphane Dahan. N'oubliez pas non plus de **sauvegarder périodiquement vos dossiers stratégiques**. « *Idéalement, ils doivent être stockés à plusieurs endroits. Si un serveur brûle, que vous soyez capable de les retrouver ailleurs* ».

#3 : Assurer la confidentialité des données clés

A l'intérieur de l'entreprise, assurez-vous que seuls les salariés ayant besoin des informations sensibles puissent y accéder. Par exemple, que les mots de passe ou clés de chiffrement ne soient **attribués qu'aux personnes qui ont besoin de les connaître**.

#4 : Définir et faire appliquer la politique de mot de passe

Attention dans le choix des mots de passe ! C'est trop souvent le talon d'Achille des systèmes d'information. « *Eviter de choisir les plus bateau comme abc123 ou 12345, une mauvaise habitude plus courante qu'on ne le dit* », insiste Stéphane Dahan. Idéalement, fixez des règles de choix et de dimensionnement des mots de passe et **renouveler ces derniers régulièrement**.

#5 : Protéger les terminaux mobiles

Les postes mobiles sont des points d'accès potentiels pour des pirates informatiques. Selon l'ANSSI (Agence nationale de la sécurité des systèmes d'information), ils doivent bénéficier au moins des mêmes mesures de sécurité que les postes fixes. Même si cela représente une contrainte supplémentaire, les conditions d'utilisation des terminaux nomades imposent même le renforcement de certaines fonctions de sécurité.

#6 : Sensibiliser l'équipe au risque de piratage

Périodiquement, rappelez à votre équipe quelques règles élémentaires : ne pas divulguer des mots de passe à un tiers, ne pas contourner les dispositifs de sécurité internes, éviter d'ouvrir la pièce jointe d'un message venant d'une adresse inconnue, etc. La sensibilisation doit également porter sur **l'utilisation des réseaux sociaux**. « *Les comptes Facebook ou Linkedin des collaborateurs sont des mines d'informations pour les pirates*, explique Stéphane Dahan. *Ils s'en servent pour adresser des messages très personnalisés qui vont leur permettre d'entrer dans le système d'information de l'entreprise.* »…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : 6 bonnes pratiques pour se protéger du piratage informatique, Marketing et Vente – Les Echos Business