

Vol de données : cinq conseils pour se protéger contre les intrusions | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer



Vol de données :
cinq conseils
pour se protéger
contre les
intrusions

Ransomware, chevaux de Troie et logiciels malveillants : les entreprises ne sont guère à l'abri des attaques de pirates qui représentent un grand risque pour leur sécurité. Mais contrairement aux idées préconçues, les menaces ne proviennent pas uniquement de l'extérieur. Les employés de l'entreprise peuvent ainsi mettre à profit les nombreuses possibilités qu'ils ont d'accéder aux systèmes de l'entreprise pour une utilisation frauduleuse des données, et cela sans beaucoup d'effort. Les organisations sont d'ailleurs rarement aussi bien protégées des attaques venant de l'interne que de celles extérieures.

Les cinq recommandations suivantes peuvent aider les entreprises à se protéger efficacement contre le vol de données par des employés.

1. Octroyer des droits d'accès différents

Pour protéger les données sensibles, il est nécessaire de donner aux employés travaillant dans différents départements des droits d'accès appropriés. Ainsi, le niveau de sécurité est déterminé par le besoin de connaissances d'un projet : un employé n'a accès à certains documents et dossiers que si ceux-ci sont nécessaires pour effectuer une tâche qui tombe sous sa responsabilité. Ces divers cloisonnements mis en place au sein de l'entreprise sous la forme de « murailles de Chine » empêchent l'échange d'informations non nécessaire entre les différents départements, permettant de limiter la perte de données.

2. Utiliser une double authentification forte

Afin de limiter tout risque, l'étape supplémentaire recommandée est une authentification à deux facteurs. Pour accéder au système, l'utilisateur doit, par exemple, non seulement entrer son mot de passe, mais aussi recevoir un SMS contenant un mot de passe unique, valable pour une seule session. Ainsi, il n'est pas possible d'accéder à l'information et aux données sensibles, même si le mot de passe a été volé.

3. Durcir la protection des informations

Les fonctionnalités en terme de sécurité doivent inclure la protection des données. Le fournisseur ne devrait en aucun cas avoir accès aux fichiers et documents, par exemple. En outre, les droits des administrateurs doivent être limités aux informations pertinentes à leurs activités.

4. Mettre en œuvre une gestion des droits d'information

Les technologies de gestion des droits d'information des documents sensibles peuvent contrôler et protéger contre le téléchargement non autorisé. Celles-ci assurent un contrôle efficace des documents même si les utilisateurs sont autorisés à accéder à l'information. Le filigrane empêche, en outre, une capture d'écran des informations. Il n'y a aucun risque de perte de données dans cet environnement protégé et elles ne tombent pas entre de mauvaises mains.

5. Enregistrer toute modification

Pour éviter le vol de données par un employé de l'entreprise et de s'en rendre compte après coup, il est conseillé d'enregistrer tous les changements effectués afin que ceux-ci soient répertoriés dans un historique. Cela permet un flux d'informations toujours clair et transparent.

Sofia Rufin, Vice Présidente Régionale de Brainloop, commente la menace croissante que représentent les employés de l'entreprise dans le cadre de vols de données : « Nous avons observé au cours des dernières années, une augmentation du nombre des pertes de données dues à des failles en interne, les entreprises faisant encore trop souvent confiance à des standards de sécurité défectueux. L'impact peut pourtant s'avérer désastreux sur l'image de l'entreprise, et les conséquences financières et légales peuvent menacer son développement économique... [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...)



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** ;



[Contactez-nous](#)



Source : *Vol de données : cinq conseils pour se protéger contre les intrusions – Global Security Mag Online*