5 conseils de base en Cybersécurité

	5 conseils de base en Cybersécurité

La cybersécurité est désormais sur la liste des priorités des dirigeants européens. En effet, d'après une récente étude menée par l'assureur britannique Lloyd, 54% d'entre eux seraient directement concernés par la question. Une problématique qui inclut la sécurité des informations, notamment en raison du rôle joué par les données, véritable carburant de l'entreprise, mais aussi à cause des lois et règlements qui régissent le traitement des données personnelles et enjoignent les entreprises à prendre de sérieuses dispositions.

Les attaques sont pour beaucoup organisées de l'extérieur, cependant il ne faut jamais exclure l'idée qu'elles puissent venir également de l'intérieur. Quel que soit le cas de figure, des mesures simples à mettre en place et à adopter permettent de compliquer la tâche de ceux qui chercheraient à s'emparer des informations critiques et vitales au fonctionnement de l'entreprise :

1. Identifier et classer les informations confidentielles
Tous les documents ne sont pas protégés. La création d'un simple système de classification avec des catégories permettant de discerner quel document est amené à être ouvert, partagé ou classé pour confidentialité, donne une vision précise de comment traiter chaque document et quels groupes de personnes y ont accès.

2. Définir les responsabilités
Tous les employés n'ont pas besoin d'accéder à toutes les informations sur le serveur de l'entreprise. Cela peut également concerner le service informatique qui peut intervenir dans de nombreux cas sans limitation. Plus le nombre de personnes admissibles est restreint, plus il est facile d'exclure les abus. Des fonctionnalités comme un historique et une gestion des droits d'information sont utiles pour restreindre, par exemple, l'impression ou l'enregistrement d'un document localement.

3. Protéger l'information au moyen des technologies
Outre les dispositions à prendre auprès des employés, les mesures techniques pour la sécurité de l'information sont aussi indispensables. De nombreuses conditions doivent cependant être remplies pour assurer une sécurité optimale comme un chiffrement de bout en bout, une gestion des accès et des droits et un contrôle par piste d'audit, associés à une facilité d'utilisation. Il existe des solutions Cloud qui répondent à ces exigences sécuritaires tout en proposant une implémentation simple. Chaque société nécessitant une telle solution doit tout d'abord s'assurer que son fournisseur n'ait jamais accès à ses données sensibles. L'emplacement du centre de données sera également important, le choix devant être déterminé en fonction des lois de protection des données valides. Les solutions Brainloop telles que Brainloop Secure Dataroom tiennent compte de ces exigences et permettent le stockage de données dans le pays d'origine des données, ainsi que dans son propre centre de données.

4. Introduire des politiques internes et former les employés
Même les meilleurs moyens de défense mis en place contre la cybercriminalité ne fonctionnent que s'ils sont connus et acceptés de tous. Cela suppose que la solution doit être facile d'utilisation et que l'entreprise investisse dans la formation de ses employés. Les règles établies pour traiter les données sensibles doivent être communiquées clairement, intégrées dans la culture de l'entreprise et être appliquées par tous.

5. Surveiller la conformité
L'entreprise doit veiller à ce que toutes les exigences soient effectivement respectées. Dans le cas d'une fuite de données, elle doit pouvoir garder une trace des données et pouvoir vérifier qui a eu accès.
Original de l'article mis en page : Cybersécurité en entreprises : cinq conseils pour ne plus passer à côté

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la 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 DIRTEF 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 : Cybersécurité en entreprises : cinq conseils pour ne plus passer à côté