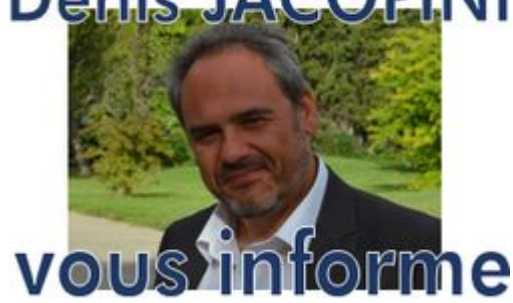
Les entreprises françaises toujours trop exposées aux risques de cyber-attaque

	Les entreprises françaises toujours trop exposées aux risques de cyber-attaque

A l'exception des grands groupes, la majorité des entreprises françaises sous-estiment les risques de cyber-attaque ; moins de 4 sur 10 d'entre elles décideurs considèrent comme « important », ou « très important », le risque que leur société subisse une cyber-attaque ces prochaines années… et ce, alors que 52% des entreprises ont déjà été piratées. C'est ce que montre une enquête réalisée par le cabinet Denjean & Associés en partenariat avec Gan Assurances

Les décideurs d'entreprise se font de fausses idées sur la cyber-fraude. Plus de trois sur quatre sous-estiment la vitesse de propagation de ce fléau dans l'Hexagone, pensant que le nombre des cyber-fraudes recensées en France n'a augmenté « que » de 10% ou de 25% en 2015, alors qu'il a crû de 50% ! (Source : Anssi, Agence nationale de sécurité des systèmes d'information). Questionnés sur les cibles visées en priorité par les pirates, 50% des décideurs citent les multinationales ; et pour 23% des répondants, les organismes publics constituent le premier choix des hackers. Seulement 28% des personnes interrogées connaissent la bonne réponse : les PME concentrent dans notre pays près de 80% des cyber-attaques (source : Syntec).

Globalement, 70% des entreprises s'estiment bien protégées contre la cyber-fraude. Une statistique qui recouvre des disparités : 100% des grands groupes affichent leur confiance dans leurs process de cybersécurité, tandis que 58% des TPE et environ 75% des PME et des ETI se jugent bien protégées.

Quelles bonnes pratiques ?

Les entreprises ayant adopté une politique de cybersécurité ont mis en place, en moyenne, trois bonnes pratiques. Les plus répandues sont le changement régulier par l'entreprise des codes d'accès à son réseau (mesure existant dans 56% des structures), et l'instauration en son sein d'une procédure d'authentification de tous les ordinateurs et commutateurs (53% des entreprises). La formation interne aux enjeux et aux précautions de base en matière de cybersécurité, et la création de différents degrés d'accès au réseau pour les collaborateurs selon leur niveau hiérarchique (respectivement pratiquées par 45% et 44% des sociétés) se disputent la troisième place sur le podium.
Deux entreprises sur trois comptent adopter en 2017 de nouvelles mesures pour lutter contre le piratage informatique qui se décomposent comme l'indique l'infographie ci-dessous.

98% des entreprises françaises sont disposées à investir chaque année pour se protéger efficacement contre la cyber-fraude, et 60% sont même prêtes à y consacrer un budget supérieur ou égal à 1% de leur chiffre d'affaires. Parmi les différentes catégories d'entreprises, les PME et les ETI se montrent les plus enclines à réaliser un effort financier conséquent : les trois-quarts d'entre elles acceptent de dépenser chaque année pour leur cybersécurité entre 1% et 2% de leur chiffre d'affaires.
Si l'on exclut les dirigeants de très petites structures, peu ou pas du tout concernés par ces sujets, les décideurs apparaissent bien conscients des nouveaux risques encourus par les entreprises, et décidés à les combattre. En effet, 66% des décisionnaires indiquent qu'ils se préoccuperont au cours des trois années à venir de lutter contre les « ransomwares » ; 70% disent qu'ils s'attacheront à sécuriser les données mises sur le cloud ; et 70% déclarent qu'ils veilleront à prévenir les risques liés aux objets connectés…

Original de l'article mis en page : Les entreprises françaises sous-estiment les risques de cyber-attaque

---

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 DIRECCTE 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