Sécurité des données : les entreprises récoltent une mauvaise note

Les entreprises récoltent une mauvaise note en matière de sécurité de données

Une étude internationale a interrogé 450 décideurs informatiques et révèle que de nombreuses sociétés se heurtent aux exigences de gouvernance et de sécurité des échanges de données.

« Les entreprises doivent respecter des exigences réglementaires toujours plus strictes en termes de conformité et de sécurité des données… »

23% des entreprises ont récemment échoué à un audit de sécurité, tandis que 17 % doutent de leur capacité à réussir un audit de conformité des échanges de données. C'est ce que révèle l'étude publiée par Axway, éditeur de logiciels spécialisé dans la gouvernance des flux de données ainsi que par le cabinet d'analyse Ovum. « Un audit de sécurité contrôle les systèmes et analyse leur perméabilité, précise Jean-Claude Bellando, directeur solution marketing pour Axway. Le but est de savoir si les données de l'entreprise sont exposées ou pas. »

Car pour se développer, les échanges entre partenaires nécessitent l'établissement d'une relation de confiance. Mais à l'heure de l'économie numérique, la confiance est relative à la sécurité, l'intégrité et la confidentialité des données échangées. Une relation d'autant plus difficile à établir que les partenaires n'ont pas forcément conscience du parcours et des étapes suivis par ces données. « Les partenaires décident alors d'un niveau d'exigence à atteindre, sur la base des règles et des bonnes pratiques de sécurité disponibles, ajoute Jean-Claude Bellando. Une règle communément admise consiste par exemple à proscrire les échanges via le protocole FTP. »
Coût de l'exposition. Pour préparer l'application de ces règles et bonnes pratiques mais aussi pour vérifier leur bonne application, les entreprises ont recours à des audits de sécurité. Ainsi récemment, Google, le géant de l'Internet, anticipant les craintes de ses clients entreprises, a décidé de publier unilatéralement les résultats d'audit de sécurité réalisés par deux cabinets indépendants. Ce type d'audit est de plus en plus souvent réalisé à la demande des clients de l'entreprise. Si celle-ci n'est pas en mesure de démontrer le respect des règles de sécurité, considérées comme nécessaires au bon déroulement de la relation commerciale, ses clients pourraient arrêter de travailler avec elle. L'enquête ajoute ainsi que le coût total moyen d'une atteinte à l'intégrité des données s'élève à 2,4 millions d'euros. « Les répercussions des cyberattaques sont sérieuses sur le plan économique et pour l'image de l'entreprise », explique Jean-Claude Bellando.

Pour répondre à ces problématiques, Axway préconise une gestion groupée de l'intégration informatique et de la gouvernance d'entreprise. Or, dans la majorité des entreprises (71%), la stratégie d'intégration n'est pas alignée avec les structures et les politiques de gouvernance, de confidentialité et de sécurité des données. « Les entreprises doivent respecter des exigences réglementaires toujours plus strictes en termes de conformité et de sécurité des données, indique Dean Hidalgo, vice-président exécutif en charge du marketing d'Axway. En s'appuyant sur des technologies éprouvées de gestion de transfert de fichier (MFT) et de gestion d'interfaces de type API (Application Programming Interface), sur site ou dans le cloud, et en développant une stratégie d'intégration plus globale et unifiée, les organisations sont en mesure de gouverner leurs flux de données à travers l'ensemble de leur écosystème, en interne comme en externe. »
Par Caroline Albenois

Premier type de risque : Les attaques venant de l'extérieur.
Solution : Demandez un test de pénétration (PENTEST) de votre système informatique à Denis JACOPINI

Second type de risque : Les actes malveillants, illicites ou défaillances internes à votre entreprise.
Solution : Demandez un audit de sécurité infomatique à Denis JACOPINI

Troisième type de risque : Votre système de traitement de données informatiques n'est pas réglementaire selon la loi Informatique et Libertés et des déclaration ou complémentats de déclaration à la CNIL doivent être effectuées.
Solution : Demandez un audit de mise en conformité CNIL à Denis JACOPINI

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://www.info.expoprotection.com/site/FR/L_actu_des_risques_malveillance__feu/Zoom_article,I1602,Zoom-ce92e8de85306f8f94bb572e6ec6d325.htm