

# Comment protéger au mieux les données clients des cyberattaques ?



Les derniers piratages des données bancaires de plus de 1,3 millions de clients Orange, les 83 millions de données de clients volées à la banque américaine JP Morgan Chase ou les menaces d'hackers de divulguer l'identité de 36 millions d'utilisateurs du site de rencontres canadien Ashley Madison... Tous ces épisodes démontrent que les cyber-attaques menacent aujourd'hui fortement la liberté individuelle et les données personnelles.

Elles viennent également rappeler qu'aucune entreprise, même bien protégée, n'est aujourd'hui en mesure de garantir à 100% la sécurité des données qu'elle manipule. Face à ce constat, les entreprises doivent changer la façon dont elles peuvent rapidement détecter et répondre en utilisant de nouvelles solutions plus précises, plus actionnables pour les équipes de sécurité.

C'est un véritable enjeu pour les entreprises d'assurer à leurs clients la protection la plus fiable possible.

Voici 4 conseils aux entreprises pour protéger au mieux les données sensibles de leurs clients et les actions à mettre en place lors d'une attaque :

- Toute organisation chargée de la gestion des données personnelles très sensibles de leurs clients doit prendre ses responsabilités très au sérieux et protéger ainsi les données contre les accès non autorisés indésirables. Cela impliquerait de multiples niveaux de contrôles de sécurité au niveau de l'IT, peut-être en commençant par le cryptage des données personnelles alors qu'elles sont actives et en cours d'utilisation. Cette approche peut être efficace à la protection des données hautement sensibles, même si le réseau dans lequel elles résident est compromis. Cela peut paraître coûteux à mettre en œuvre mais c'est une méthode de protection efficace.
- Il est capital d'avoir des processus et procédures internes qui garantissent l'accès physique aux centres de stockage de données sécurisées y compris de CLOUD. Les comptes d'utilisateurs inutilisés devraient être supprimés rapidement et les restrictions d'accès gérés de façon stricte pour s'assurer que tous les employés n'aient pas accès aux données de n'importe quel autre utilisateur.
- Nous pouvons également parler d'une nouvelle génération, solide dans son approche, permettant d'atténuer les menaces (en constante évolution) d'attaques malveillantes des réseaux d'entreprise provenant de l'extérieur. Les organisations "pirates" peuvent percevoir cela comme une énorme opportunité financière à voler les données personnelles détenues par quelque organisme que ce soit. Le fait d'avoir des défenses périmétriques fortes mises en place comme un pare-feu, des anti-virus sur toutes les stations de travail, d'une solution de filtrage d'e-mail, ou encore d'une solution IPS / IDS et un SIEM offrant la possibilité de surveiller les événements de toutes ces technologies en un seul endroit, ne restent malheureusement pas les plus fiables et beaucoup de sociétés ayant mis en place ces solutions ont quand même été attaquées, des brèches ont été exploitées car toutes ces solutions ne permettent pas d'arrêter tous les logiciels malveillants persistants qui vont compromettre un réseau en offrant la possibilité de se déplacer librement afin de trouver des données ciblées à voler.
- Là où les entreprises doivent se focaliser (en plus d'autres options internes déjà mentionnées), c'est de déployer une solution de détection des menaces plus intégrée qui peut extraire des informations à partir de plusieurs points dans le réseau, d'analyser ce qui se passe en temps réel (sur les stations de travail et sur le réseau) et défendre activement les réseaux d'entreprise avec la possibilité d'automatiser les réponses défensives générées en temps réel et 24 heures sur 24. Il y a encore à ce jour une réticence au niveau des comités exécutifs des entreprises de reconnaître la nécessité d'avoir un budget propre à la « Cyber Sécurité » mais qui permettrait de continuer à investir sur les dernières générations de solutions qui sont adaptées aux nouvelles menaces. Jusqu'à ce que cela change ; les cyber attaques vont continuer, les hackers utilisant des outils automatisés de pointe. Et nous continuerons de découvrir de nouvelles attaques de grandes ampleurs, quasiment tous les jours !



Réagissez à cet article

Source

<http://www.infodsi.com/articles/157575/proteger-mieux-donnees-clients-cyberattaques-bernard-girbal-vice-president-emea-chez-hexis-cyber-solutions.html>