Protection des données des entreprises v.s. combat anti-terroriste

	Protection des données des entreprises v.s. combat anti-terroriste

Critiqué par certaines forces antiterroristes, le chiffrement des messages en entreprise, aussi appelé cryptographie, reste une solution contre l'espionnage industriel.

Critiqué par certaines forces antiterroristes, le chiffrement des messages en entreprise, aussi appelé cryptographie, reste une solution contre l'espionnage industriel.

Cet été, une directrice au sein d'un grand groupe industriel s'est fait voler son ordinateur portable professionnel. Heureusement, un système de chiffrement protégeait l'accès aux informations confidentielles qui s'y trouvaient. Bilan : cet épisode n'a pas eu d'autres conséquences que l'achat d'un nouvel outil de travail pour la collaboratrice, pour 300 euros, loin du coût d'une fuite de documents sensibles que ce fleuron français a frôlé.

Le chiffrement, aussi appelé « cryptage » (un anglicisme), consiste à encoder un document ou le contenu d'un smartphone ou d'un ordinateur pour le rendre inintelligible. La lecture de ce document n'est possible que pour celui qui connaît la clef du code (souvent un mot de passe, plus rarement une empreinte digitale). Les experts considèrent que seul un ordinateur quantique pourrait tester aléatoirement toutes les combinaisons possibles d'une clef solide et reconstituer un message…

Un outil défensif

Dans un contexte de cyberinsécurité grandissante, où l'espionnage industriel n'est plus à prouver suite aux révélations d'Edward Snowden, les services secrets français (la DGSI) et l'Agence nationale de la sécurité des systèmes d'information (Anssi) encouragent les entreprises à chiffrer leurs données les plus sensibles. « C'est un outil défensif, essentiel à la protection des données numériques d'une immense majorité d'utilisateurs honnêtes ; il ne me semble pas raisonnable de l'interdire au motif que quelques individus pourraient s'en servir pour préparer des crimes ou des attentats, aussi odieux soient-ils », défend Guillaume Poupard, le directeur général de l'agence placée sous l'autorité du Premier ministre.
Cette structure est chargée de coordonner et d'aider les entreprises françaises et l'Etat à se protéger des cyberattaques. Mais son propos est quelque peu brouillé par certaines voix haut placées et un concert de discours sécuritaires. Un ancien directeur de la CIA, le procureur de la République de Paris (François Molins), le ministre de l'Intérieur (Bernard Cazeneuve) et même le chef du gouvernement britannique (David Cameron) se sont tour à tour exprimés pour demander un affaiblissement des algorithmes de chiffrement des messageries. Ce qui permettrait aux enquêteurs de police habilités de lire la correspondance protégée de certains suspects, notamment pour lutter contre le terrorisme . En octobre, le Premier ministre Manuel Valls se déclarait favorable pour les entreprises à « toutes les ressources qu'offre la cryptologie légale », une formule polémique puisque jusqu'à présent aucun mode de chiffrement, même les plus forts, n'est illégal pour elles.

« Jusqu'à une période récente, le chiffrement était considéré comme un luxe par les entreprises, mais avec la migration des messageries dans le cloud, notamment via Microsoft, les besoins dans ce domaine ont augmenté », constate Alain Bouillé, le président du Cesin, une association de responsable de la sécurité des systèmes d'information. La majorité des grandes entreprises françaises proposent des solutions de chiffrement à leurs collaborateurs. Mais peu d'entre eux les utilisent vraiment, car ces systèmes sont peu pratiques au quotidien . « Certaines briques de logiciels peuvent compléter le client-mail standard mais le chiffrement n'est pas toujours parfait avec ces modules plus simples », remarque Christophe Kiciak, le directeur audit et sécurité de Provadys, une entreprise de cybersécurité. « Apple pour les iPhones et Google pour certains smartphones Android ont des solutions qui cryptent de bout en bout certains services de messagerie, sans même que l'utilisateur s'en aperçoivent, mais elles sont menacées par les gouvernements », souligne également Gérôme Billois, consultant chez Solucom.

La seule solution de protection

Les experts sont unanimes : « Le chiffrement est la seule solution pour se protéger du vol de données suite à une attaque informatique. » Quand un smartphone est perdu, le chiffrement empêche aussi que la personne qui le retrouve en profite pour s'approprier des informations sensibles. Tout reste illisible. « Le chiffrement protège aussi de l'employé qui se trompe de destinataire pour un e-mail », note Stéphane Calé, le président de la commission « Cyber » du Club des directeurs de sécurité des entreprises.
En interne, les responsables de la protection de l'information des sociétés tentent de sensibiliser sur ces questions. « 15 à 20 % des collaborateurs sont concernés, ils travaillent dans le management, dans les bureaux d'études et les services financiers », compte Bernard Ourghanlian, le directeur technique et sécurité de Microsoft France. « Le chiffrement doit surtout protéger les données stratégiques comme les projets de rachat ou de développement à l'international », précise Christophe Kiciak. Un système de classification de données selon leur sensibilité, à la manière de la grille « secret défense » des militaires, est recommandé pour les entreprises. De tels barèmes permettent d'adapter les exigences envers chaque collaborateur, par rapport à son exposition au risque. Des formations spécifiques existent pour les assistants de direction. Le problème reste au niveau des dirigeants, souvent peu indulgents quand la sécurité vient perturber l'usage de leur smartphone dernier cri.

Réagissez à cet article

Source : http://business.lesechos.fr/directions-numeriques/technologie/cybersecurite/021549442285-quand-la-protection-des-donnees-des-entreprises-percute-le-combat-anti-terroriste-205384.php
Par FL Debes