



Certains pays d'Asie et du Moyen-Orient souhaitent surveiller les échanges numériques de leurs concitoyens.

SÉCURITÉ

Les grandes entreprises se méfient du BlackBerry

Les services de renseignement étrangers sont nombreux à vouloir accéder aux flux chiffrés des BlackBerry. Les grandes entreprises s'interrogent sur le risque que représentent ces terminaux.

Wall Street a peur. Début août, les représentants de grandes banques américaines, dont Goldman Sachs et JP-Morgan Chase, se sont entretenus avec des dirigeants de Research In Motion (RIM) à propos de la sécurité des smartphones BlackBerry, qui équipent nombre de financiers outre-Atlantique, et dont les données circulent de manière chiffrée au travers du réseau privé du constructeur canadien.

En effet, depuis quelques semaines, RIM est soumis à une forte pression de la part de pays d'Asie et du Moyen-Orient, qui souhaitent accéder à son infrastructure pour surveiller les échanges numériques de leurs concitoyens. Des discussions ont même commencé avec l'Inde et l'Arabie saoudite. RIM va-t-il donner un accès permanent aux flux chiffrés ? Dans ce cas, les cadres des grandes entreprises bancaires ou industrielles devront-ils craindre que leurs messages soient interceptés par des services de renseignement étrangers, lors de leurs déplacements dans ces régions du monde ? A l'heure actuelle, les informations sont assez floues, voire contradictoires. L'Arabie saoudite explique disposer



d'ajouter : « le fait que des gouvernements se plaignent de ne pouvoir décrypter les messages échangés par Blackberry, et demandent l'installation d'un serveur sur leur territoire, souligne que le niveau de sécurité est bien celui annoncé par le constructeur, et qu'il existe des entrées cachées sur les serveurs de routage, contrairement à ce que ce dernier a toujours annoncé. » C'est également l'avis d'un chercheur français en cryptographie qui souhaite, lui aussi, rester anonyme. « On ne peut avoir aucune garantie dans un système comme Blackberry, où la cryptographie est gérée de manière relativement

RIM soutient qu'on ne peut accéder aux communications chiffrées de son terminal Blackberry

opaque. J'ai la conviction – validée par l'expérience sur des systèmes similaires – que ceux-ci sont piégés, ou du moins qu'ils peuvent le devenir dynamiquement quand on le souhaite, par exemple sur une durée de vingt-quatre heures. C'est probablement une des raisons pour lesquelles le gouvernement français interdit l'utilisation de terminaux Blackberry dans la sphère étatique », ajoute-t-il.

« de codes » pour accéder aux données de Blackberry Messenger, l'application de messagerie instantanée. Et l'Inde testerait « des solutions techniques » pour lire les courriels chiffrés. Le constructeur, lui, n'arrête pas de souligner le niveau de sécurité et l'intégrité du système Blackberry. « RIM ne possède pas de " clé maître ", et il n'existe pas de porte dérobée par laquelle RIM, ou un tiers, accéderait aux informations chiffrées des entreprises », lit-on dans l'un de ses communiqués. Pour autant, le constructeur refuse de s'exprimer sur la teneur des discussions en cours.

Les gouvernants français interdits de Blackberry

Le sujet reste, à n'en pas douter, très sensible, et les langues ne se délient pas spontanément. Selon le responsable de la sécurité des systèmes d'information (RSSI) d'une grande banque française, qui souhaite garder l'anonymat, il faut rester très vigilant : « Blackberry communique depuis le début sur la sécurité de sa solution. Des questions se sont toujours posées sur la réelle confidentialité des échanges, notamment vis-à-vis du système d'écoute Echelon. » Et

Quoi qu'il en soit, les grandes entreprises françaises ont intérêt à se pencher sur la question si elles souhaitent protéger leurs communications des attaques d'espionnage industriel. Le premier organisme à contacter est l'Agence nationale de la sécurité des systèmes d'information (Anssi), qui élabore des outils méthodologiques, propose une liste de produits de sécurité agréés, et donne des conseils pratiques aux voyageurs quant à l'utilisation de leurs téléphones mobiles.

Les entreprises peuvent aussi se rapprocher des équipes de la Direction centrale du renseignement intérieur (DCRI), qui les aideront à définir leur politique de sécurité en cas de situation sensible. Il serait d'ailleurs souhaitable que le gouvernement français fournisse systématiquement des indications aux acteurs économiques sur le niveau de confiance à avoir, en fonction des régions du monde. « Sans une ligne claire donnée par l'Etat, chaque RSSI bâtira sa liste noire au doigt mouillé, avec le risque d'oubli ou de surprotection, toujours gênante pour le business », estime le RSSI d'une grande banque française. ■ GILBERT KALLENBORN

2 QUESTIONS À...



Cédric Manca,
responsable sécurité de
la direction industrielle
chez Thales Services

Quelle confiance accorder aux terminaux Blackberry ?

C'est avant tout un problème d'usage. Sachant que rien n'est sécurisé sur un portable, et dans la mesure où les serveurs de messagerie sont gérés par un tiers, les Blackberry ne doivent pas être utilisés pour échanger des informations confidentielles. Dans ce cas, il faut s'orienter vers d'autres solutions.

Quels produits choisir alors ?

Les moyens de chiffrement évalués et agréés par l'Anssi aident à respecter un niveau de sécurité de type confidentiel-Industrie, voire même secret-défense. Certes, ces solutions ont un coût. Chez Thales, nous n'utilisons pas de Blackberry et maîtrisons le chiffrement des flux d'échanges de bout en bout.

L'AVIS DE L'EXPERT



Nicolas Arpagian,
Centre d'étude et de
prospective stratégique
(CEPS)

Dès 2005, la Direction centrale de la sécurité des systèmes d'information française

(désormais rebaptisée Anssi) avait pointé le risque que représentait le Blackberry pour la confidentialité des échanges électroniques. Car la société RIM accède aux données transférées sur ses serveurs. Certains Etats lui reprochent la performance de son cryptage, qui empêcherait leurs services de sécurité d'intercepter les communications transitant par ses appareils. La défense des intérêts économiques et la lutte antiterroriste sont des priorités nationales dans de nombreux pays : les utilisateurs de ces téléphones intelligents doivent donc s'attendre à ce que leurs connexions soient surveillées.