Analyse des risques associés à l'utilisation des équipements informatiques portables

Pratiques recommandées en matière de sécurité de l'information

Mars 2014

Québec

Table des matières

Introduction

Le préjudice causé par le vol ou la perte d'un ordinateur portable va bien au-delà de la valeur du matériel. La perte des informations hébergées sur un disque dur peut entraîner toutes sortes de graves désagréments : divulgation d'informations personnelles et confidentielles, atteinte à l'image de marque de l'organisme public, non-respect des clauses contractuelles et risques de poursuites judiciaires.

Constats

Les médias ne cessent de relater des cas de perte ou de vol d'ordinateurs portables pouvant contenir des données sensibles, non protégées par un système de chiffrement, citons à titre d'exemple, les cas suivants :

- En avril 2013, la perte accidentelle d'un appareil portable appartenant à l'Organisme canadien de réglementation du commerce des valeurs mobilières contenant des renseignements personnels sur 52 000 clients et dépourvu de système de cryptage devrait leur coûter 5,2 M$.
- À la suite d'un vol d'un ordinateur portable contenant des informations personnelles non chiffrées de milliers de collaborateurs et de sous-traitants, la NASA a rendu obligatoire le chiffrement des disques durs des ordinateurs portables de ses employés. Elle a également décidé qu'aucun ordinateur ne pourra quitter ses installations sans un tel chiffrement, qu'il contienne ou non des données sensibles. Par ailleurs, elle interdit le stockage de toute information sensible sur des téléphones intelligents ou autres terminaux mobiles.
- À la suite du vol ou de la perte de nombreux ordinateurs portables au CNRS (France), ce dernier a procédé à une analyse des risques, laquelle a montré que la plupart des ordinateurs portables sont susceptibles de contenir des informations sensibles, ne serait-ce que les codes permettant de se connecter au réseau ou d'accéder aux applications. L'orientation choisie étant le chiffrement de tous les ordinateurs portables, en accord avec la demande du ministère de la Recherche. Le dispositif de chiffrement retenu repose sur une mise en œuvre à deux niveaux : une protection de base par chiffrement applicable à tous les ordinateurs portables et une protection des données très sensibles par l'ajout d'une deuxième couche de chiffrement.

Tendances

Afin d'éviter de telles déconvenues, un certain nombre d'organisations gouvernementales ont adopté des mesures de sécurité en ayant recours aux techniques de chiffrement d'équipements informatiques portables. Celles-ci sont établies en fonction des risques et de leurs impacts et visent à assurer la disponibilité, l'intégrité et la confidentialité de l'information qu'ils contiennent. À titre d'exemple, les tendances suivantes sont observées :

- Au Royaume-Uni, la commission relative aux informations (Information Commissioner Office) a indiqué que les pertes de données non protégées par chiffrement allaient entraîner l'adoption de nouvelles mesures réglementaires.
- Au gouvernement fédéral canadien, une recommandation sur la configuration de base des postes de travail itinérants, émise par le dirigeant principal de l'information, intègre l'usage du chiffrement de l'information stockée sur les équipements informatiques portables.
- Au gouvernement du Québec, plusieurs organismes publics, à l'instar de l'Agence du Revenu du Québec, de la commission de la santé et de la sécurité du travail ou du ministère de la Justice, privilégient le recours au chiffrement des données emmagasinées sur les ordinateurs portables.

Cadre juridique des technologies de l'information du gouvernement du Québec

La Loi concernant le cadre juridique des technologies de l'information énonce, à l'article 25, que *« La personne responsable de l'accès à un document technologique qui porte un renseignement confidentiel doit prendre les mesures de sécurité propres à en assurer la confidentialité, notamment par un contrôle d'accès effectué au moyen d'un procédé de visibilité réduite ou d'un procédé qui empêche une personne non autorisée de prendre connaissance du renseignement ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder. »*

Recommandation

Considérant le contexte ci-dessus et face à la métamorphose continuelle et rapide des cybermenaces, à leur virulence et à la gravité des conséquences imputables aux cyberattaques, la protection proactive des données demeure un impératif incontournable au gouvernement du Québec.

À cet égard, le dirigeant principal de l'information recommande fortement aux organismes publics de s'assurer de l'application de mesures visant à garantir la sécurité de l'information stockée sur les équipements informatiques portables, notamment par le recours aux techniques de chiffrement. Cette mesure universellement reconnue et utilisée pour la protection de l'information est le moyen de prévention à privilégier compte tenu de son efficacité avérée face aux risques de perte ou de vol d'équipements informatiques portables.