SÃ©curitÃ© des donnÃ©es : Une prioritÃ© au chiffrement en PME et administrations
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 18/12/2013 13:00:00

L'annÃ©e 2013 aura Ã©tÃ© particuliÃ¨rement riche en rÃ©vÃ©lations dans le domaine du cyber espionnage.
Qu'il s'agisse des diffÃ©rentes ramifications de l'affaire PRISM sur l'importance de l'espionnage effectuÃ© par la NSA ou d'autres agences gouvernementales, des soupÃ§ons d'espionnage industriel de la Chine au travers des Ã©quipements de Huawei, ou plus rÃ©cemment, du tÃ©moignage d'un hacker dÃ©montrant qu'il Ã©tait relativement simple de pouvoir accÃ©der aux emails des parlementaires europÃ©ens, les exemples ne manquent pas pour dÃ©montrer que les entreprises et les administrations doivent protÃ©ger leurs donnÃ©es et celles de leurs clients/utilisateurs.

CotÃ© franÃ§ais le rÃ©cent vote en faveur la Loi de Programmation Militaire (LPM) va faciliter l'accÃ¨s aux donnÃ©es tÃ©lÃ©phoniques ou informatiques aux services de renseignement intÃ©rieur, Ã la police et Ã la gendarmerie, sans avoir recours Ã l'intervention d'un juge.

Par consÃ©quent, les hÃ©bergeurs basÃ©s sur le territoire franÃ§ais auront pour obligation de rÃ©pondre aux demandes de mise Ã disposition de donnÃ©es. Ces derniers se verront donc dans lâincapacitÃ© de garantir la confidentialitÃ© des donnÃ©es critiques dâune entreprise qui sâappuierait sur un datacenter externe ou une solution Cloud.

Une mesure qui risque Ã©galement de porter prÃ©judice aux deux Clouds souverains franÃ§ais lancÃ©s cette annÃ©e qui ne pourront plus garantir le mÃªme niveau de sÃ©curitÃ© et de confidentialitÃ©.

Certains, ont depuis longtemps, dÃ©cidÃ© de protÃ©ger leurs donnÃ©es et leurs Ã©changes en s'appuyant sur le chiffrement.

Et l'efficacitÃ© de l'utilisation des techniques de cryptage pour rendre des donnÃ©es illisibles n'est plus Ã dÃ©montrer.

Ce n'est pas pour rien que la NSA a Ã©tÃ© impliquÃ©e dans la qualification ou la crÃ©ation de certains standards de sÃ©curitÃ© conjointement avec le NIST (Institut National des Standards et Technologies), quâ□□elle se soit appuyÃ©e sur la justice amÃ©ricaine pour rÃ©cupÃ©rer les clÃ©s de chiffrement du service Lavabit ou quâ□□elle ait souhaitÃ© rÃ©cupÃ©rer les clÃ©s SSL de quelques-uns des principaux gÃ©ants du net amÃ©ricains.

Lâ□□utilisation du chiffrement reste un gage de sÃ©curitÃ© majeur. D'ailleurs, nombreuses sont les entreprises qui suite Ã toutes ces rÃ©vÃ©lations ont dÃ©cidÃ© d'opter pour le chiffrement de certains de leurs services.

Des sociÃ©tÃ©s telles que Yahoo, Google, Microsoft, Twitter, etc. ont procÃ©dÃ© Ã des annonces pour attirer l'attention du public sur la mise en place du chiffrement ou leur intention de le faire dans un avenir proche.

La France n'est pas en reste sur le sujet. On a ainsi assistÃ© Ã un rappel Ã l'ordre effectuÃ© par les services du Premier Ministre Jean-Marc Ayrault auprÃ¨s de l'ensemble des ministÃ¨res pour leur souligner la faiblesse du niveau de sÃ©curitÃ© des smartphones et tablettes grand public et de leurs lacunes en matiÃ¨re de prÃ©servation de la confidentialitÃ© des diffÃ©rents Ã©changes susceptibles donc d'Ãªtre interceptÃ©s.

On a ainsi vu revenir sur le devant de la scÃ¨ne le tÃ©lÃ©phone sÃ©curisÃ© Teorem de Thales et assistÃ© au rÃ©cent lancement du Hoox m2 de Bull qui permet d'aller sur Internet, d'envoyer des e-mails et des SMS et de tÃ©lÃ©phoner de maniÃ¨re chiffrÃ©e.

A juste titre, le chiffrement connait un regain d'intÃ©rÃªt qui, si on en croit les prÃ©dictions du Gartner, devrait se poursuivre en 2014 et au delÃ . Le Gartner a ainsi rÃ©cemment soulignÃ© que le marchÃ© de la sÃ©curitÃ© dans le Cloud allait atteindre prÃ¨s de 2,1 milliards de dollars en cette fin dâ□□annÃ©e (+3,1 milliards en lâ□□espace de deux ans), anticipÃ© une croissance forte pour lâ□□annÃ©e prochaine et souligne que le chiffrement devient de plus en plus populaire.

Au niveau europÃ©en, lâ□□ENISA (agence europÃ©enne chargÃ©e de la sÃ©curitÃ© des rÃ©seaux et de lâ□□information) vient ainsi de publier un guide de recommandations Ã suivre pour la mise en Å□uvre du chiffrement au sein des entreprises, ce qui devrait inciter bon nombre d'entre elles Ã franchir le pas.

Au niveau mondial, le groupe de travail HTTPbis de l'IETF (Internet Engineering Task Force) qui a pour mission d'Ã©laborer la spÃ©cification HTTP 2.0 â□□ qui sera utilisÃ©e dans le cadre de la navigation sur Internet dans le futur â□□ a formulÃ© trois propositions pour contrer l'espionnage des diffÃ©rents programmes de surveillance des organisations gouvernementales. Chacune de ces propositions suggÃ¨rent l'utilisation du chiffrement.

Lorsque lâ□□on fait le bilan des Ã©volutions rÃ©glementaires et des diffÃ©rentes affaires dâ□□espionnage qui ont Ã©tÃ© rÃ©vÃ©lÃ©es au cours de lâ□□annÃ©e 2013, ces recommandations et ces Ã©volutions sont tout Ã fait justifiÃ©es. Partant de ce constat, on peut sâ□□attendre Ã 4 Ã©volutions Ã venir dans le domaine du chiffrement :

- Une gÃ©nÃ©ralisation de lâ□□utilisation du chiffrement de la part des entreprises et des particuliers.

- Le regain de sÃ©lection de solutions franÃ§aises ou europÃ©ennes bÃ©nÃ©ficiant de certifications, gages de sÃ©rieux face aux soupÃ§ons dâ□□espionnage pesant sur les USA ou la Chine.

- La mise en Å□uvre par les entreprises de stratÃ©gie de gouvernance de leurs donnÃ©es et des accÃ¨s Ã ces derniÃ¨res. Les entreprises vont se prÃ©munir des accÃ¨s technique aux donnÃ©es, se protÃ©ger contre les tiers internes ou externes Ã lâ□□entreprise qui ont des droits dâ□□administration mais qui ne doivent pas lire le contenu (cloisonnement et chiffrement pour empÃªcher la lecture des donnÃ©es mais en laissant possible leur administration).

- Une rÃ©vision, Ã plus ou moins long terme, des standards de chiffrements qui sont utilisÃ©s aujourdâ□□hui afin que les limitations de chiffrement soient notamment revues Ã la hausse.

Pour conclure, on ne peut que se fÃ©liciter du regain dâ□□intÃ©rÃªt pour le chiffrement celui-ci ayant largement fait ses preuves en matiÃ¨re de sÃ©curitÃ©. Quels que soient les systÃ¨mes de stockage des donnÃ©es (sur sites, dans le Cloud ou hybride), les modes dâ□□accÃ¨s (dans lâ□□entreprise, en situation de mobilitÃ©, etc.) ou les techniques de partage utilisÃ©es, le chiffrement reste incontournable.

Il convient toutefois de le mettre en Å□uvre correctement et en utilisant des solutions fiables et certifiÃ©es. Sur cet aspect le point de dÃ©part idÃ©al sera de consulter les recommandations de lâ□□ANSSI et plus rÃ©cemment celles publiÃ©es par lâ□□ENISA.

Propos de Xavier Dreux, Responsable marketing chez Primâ□□X