Gérôme Billois, Solucom : « PRISM est une opportunité pour les RSSI »

Pour **Neelie Kroes**, la commissaire européenne chargée du numérique, le programme d'écoutes PRISM, mené par la NSA américaine et révélé par **Edward Snowden**, aura des conséquences « à plusieurs milliards d'euros » pour les fournisseurs américains de services Cloud. Une perspective que semble confirmer une étude de la Cloud Security Alliance, une association qui a sondé 500 de ses membres sur le sujet. 10 % des entreprises non américaines y indiquent avoir déjà annulé un projet avec un fournisseur de Cloud américain en raison des révélations sur les écoutes généralisées pratiquées par l'agence de renseignement de Fort Meade (Maryland).

Pour mesurer les conséquences de l'affaire PRISM en France, nous avons interrogé **Gérôme Billois**, senior manager en gestion des risques et sécurité chez Solucom, un cabinet de conseil intervenant surtout auprès des grandes entreprises.

***Silicon.fr* : Suite à l'affaire PRISM, avez-vous ressenti un changement d'attitude dans les entreprises françaises ?**

Gérôme Billois : Ce n'est pas un raz-de-marée mais nous avons eu ces dernières semaines une dizaine de contacts sur ce sujet. En fait, les équipes sécurité sont plutôt soulagées de voir sortir des informations concrètes auprès du grand public sur ces sujets. Car cela fait très longtemps que les spécialistes de sécurité parlent de ce risque, l'intègrent dans leurs analyses. Le sujet des écoutes généralisées était déjà sur la table il y a une dizaine d'années, avec le programme Echelon. De même, l'existence d'un « PRISM à la française », révélée au grand public par un article du *Monde*, était connue des spécialistes au moins depuis 2010, la DGSE s'étant exprimée sur le sujet lors d'une conférence réunissant des experts. Pour les RSSI (Responsables de la sécurité des systèmes d'information), le bruit médiatique autour de PRISM constitue l'occasion d'appuyer leurs discours auprès des directions générales ou métiers, et de surpondérer un élément qu'ils intégraient déjà à leurs analyses de risques mais que leurs interlocuteurs avaient tendance à minimiser. Par ailleurs, l'origine de la fuite qui a permis la divulgation de PRISM permet aux RSSI de replacer sous les projecteurs la question des administrateurs systèmes issus de sous-traitants et accédant à des informations confidentielles.

En parallèle, auprès des directions générales ou métiers, l'affaire PRISM a rendu concrètes les capacités d'écoute de certains États. Dans certains cas, cela a soulevé des inquiétudes sur certains périmètres sensibles. Même si aucune preuve formelle n'a été produite, des soupçons d'espionnage industriel sont toujours présents dans certaines entreprises.

Cette inquiétude s'est-elle traduite par des abandons de projet ou des velléités de transfert de contrats vers des prestataires non américains ?

Je n'ai pas eu connaissance de projet arrêté ou ayant changé de dimension suite à PRISM. Par contre, l'attention accordée aux solutions de sécurité a été renforcée, des organisations envisageant le déploiement de solutions de chiffrement et la conservation des clefs en interne pour certains de leurs projets.

L'argument classique des fournisseurs de Cloud américains – la localisation des datacenters en Europe – vous paraît-il suffisant ?

Non, en raison de la portée d'un texte de loi comme le Patriot Act. Au point que des débats juridiques existent sur le fait de savoir si l'existence d'une filiale aux Etats-Unis dans un groupe non américain ne suffit pas aux autorités US pour demander un accès aux données. Jusqu'à PRISM, les fournisseurs de Cloud étaient plutôt dans le déni de ces pratiques d'écoutes généralisées. Depuis, leur discours a changé : ils tendent à banaliser ces pratiques, expliquant que tous les pays y ont recours.

Existe-t-il des moyens de se protéger de ces écoutes ?

Avant de considérer les solutions techniques envisageables, il faut se pencher sur les volets méthodologique et juridique. Et commencer par se demander si les données d'une organisation ont besoin d'être protégées des menaces d'écoutes étatiques. Si elles sont analysées par une puissance étrangère, y aura-t-il un impact financier pour l'entreprise ? PRISM a généré un phénomène d'emballement ; des interlocuteurs s'inquiétant de la confidentialité d'informations sans réelle valeur pour un concurrent ! Les directions des entreprises doivent donc avant tout apprendre à relativiser, à définir précisément les périmètres à risque. Ensuite, on peut envisager de mettre en place des obstacles juridiques, en demandant par exemple aux fournisseurs une clause systématisant les recours en cas de requête judiciaire. Objectif : ralentir le processus, car dans les affaires d'espionnage économique, le timing est essentiel.

Enfin, il existe des parades techniques. Le chiffrement apparaît comme une solution efficace pour le stockage de données. Mais il est inopérant dès que le service Cloud comporte une logique de traitement de l'information, comme c'est le cas pour les applications SaaS par exemple. Aucune solution technique n'est prête à ce jour pour s'assurer que le fournisseur n'ait pas accès à l'information véhiculée sur ces services. Même si les recherches sur ce qu'on appelle le chiffrement homomorphique – qui doit fournir une réponse à ce besoin – avancent avec la sortie récente des premières initiatives.

Lire également : Jean-Noël de Galzain (Pdg de Wallix) : « PRISM sert de révélateur aux problèmes de sécurité des comptes à privilèges »