Cobol, le usual suspect des attaques contre le gouvernement US

Deux universitaires viennent de rendre un rapport sur les failles de sécurité du gouvernement américain. 38 pages pour dresser un bilan des problématiques de sécurité des infrastructures de l'administration américaine. Et le rapport est riche d'enseignements.

En premier lieu, Min-Seok Pang, professeur adjoint en gestion des systèmes d'information à l'Université Temple (Pennsylvanie), et Huseyin Tanriverdi, professeur agrégé au Département de l'information, des risques et des opérations de l'Université du Texas à Austin, ont constaté une explosion des incidents de sécurité en près de 10 ans. Sur la période allant de 2006 à 2014, le nombre d'incidents de sécurité a cru de 1 121 % passant de 5 503 à 67 108. Le champion toute catégorie étant le vol de données de l'Office of Personnal Management (OPM) en avril 2014 où 22 millions de comptes ont été compromis.

La « security by anitiquity » n'existe pas

Sur ce dernier cas, une enquête a montré la responsabilité « *d'un mainframe vieux de 30 ans utilisant le Cobol pour la base de données du personnel. Une technologie techniquement obsolète qui rend impossible le chiffrement des données* », peut-on lire dans l'introduction du rapport. Un moyen de tordre le coup aux discours de certains spécialistes qui estiment que des technologies anciennes comme le Cobol ou Fortran sont à l'abri des problèmes de sécurité, car méconnues des cybercriminels.

Cette hypothèse se résume sous le vocable « *security by antiquity* ». Le problème est que ces systèmes sont de plus en plus connectés au sein d'architecture plus complexe et reçoivent de moins en moins de mises à jour de sécurité. Ils ne sont donc plus adaptés aux exigences de sécurité actuelles (chiffrement, authentification forte, etc.). De même, il y a de moins en moins de compétence sur ces vieux langages. Aux Etats-Unis, 3400 personnes sont chargées leur maintenance, a-t-on appris lors de l'enquête sur OPM.

Rénover, cloudifier et disperser

Mieux dans leurs analyses, les deux chercheurs montrent que la prééminence de l'IT historique et la volonté d'investir dans sa maintenance concourent à la fragilité des systèmes face aux attaques. « *Technologiquement, nous avons trouvé que la forte proportion de systèmes IT historiques au sein de l'administration fédérale américaine est une cause majeure des incidents de sécurité* », livre le rapport dans ses conclusions.

Au terme de leur démonstration, les deux experts constatent que les investissements dans des nouveaux systèmes IT sont une bonne chose en matière de sécurité. Ainsi, ils démontrent que « *en investissant 1% de budget en plus dans une IT plus moderne, le risque d'incidents de sécurité baisse de 5%* ». Autre porte de sortie préconisée par les scientifiques, le recours au Cloud, « *les agences fédérales qui externalisent leur système historique dans le Cloud sont moins touchées par les problèmes de sécurité* ». Le

gouvernement américain et notamment les premiers DSI fédéraux ont mis en place une politique de Cloud aux seins des administrations. Le dernier en date Tony Scott, un ancien de VMware qui a piloté au sein de Microsoft le déploiement d'Azure et d'Office 365.

Enfin, les universitaires émettent une autre préconisation, la dispersion géographique. « *Les agences qui sont fonctionnellement ou géographiquement dispersées ont une fréquence des incidents de sécurité moindre que les systèmes centralisés.* »

A lire aussi :

Dépense IT : le gouvernement US vote pour le Cloud… et la France ?

HTTPS sera déployé sur tous les sites du gouvernement US

Photo credit: Stuck in Customs via Visual Hunt / CC BY-NC-SA