

LE TEMPS

Dossier spécial Jeudi 30 décembre 2010

L'échec des forteresses numériques

Par François Pilet

Banques et gouvernements protègent leurs données sensibles dans des sites toujours plus sécurisés. Un domaine où les sociétés suisses règnent en maîtresses. Ces systèmes ne les ont pourtant pas protégées du pire

La firme chargée de protéger la diplomatie suisse d'une fuite à la WikiLeaks s'appelle Crypto AG. Début 2010, la société zougnoise a mis en service le nouveau centre informatique ultra-sécurisé du Département fédéral des affaires étrangères (DFAE) dans un lieu tenu secret, quelque part sous les Alpes. Blottis dans les galeries d'une ancienne forteresse militaire, des dizaines de serveurs sont bercés par le ronron des installations frigorifiques. Caméras de surveillance, détecteurs de mouvement, groupes électrogènes et filtres à air, dortoirs et réserves de vivres pour les techniciens; «tout y est prévu pour assurer un fonctionnement ininterrompu même en cas de crise», assure Crypto AG. La société, fondée en 1952, fournit ses services à une centaine de gouvernements à travers le monde.

Ce genre de blockhaus numérique n'est pas l'apanage des Etats. A Genève, à un jet de pierre de l'aéroport, existe un centre de données dernier cri et hautement sécurisé, en mains privées. Opéré par la société Safe Host, il est équipé d'un centre de contrôle automatisé, de capteurs de mouvement à infrarouge et ultrason, d'un système anti-incendie à l'azote, de générateurs d'appoint diesel et de contrôles d'accès biométriques. Des gardes patrouillent nuit et jour. C'est dans ce bâtiment anonyme de Plan-les-Ouates que dorment les copies des données les plus sensibles de plusieurs banques privées genevoises.

Les entreprises et les gouvernements ont dépensé des sommes considérables ces dix dernières années pour centraliser et protéger leurs informations secrètes. Ces investissements ont permis l'essor de nombreuses sociétés spécialisées, notamment en Suisse (voir encadré). Mais le recours au tout crypté n'a pas protégé ces organisations de fuites d'une gravité sans précédent depuis deux ans.

Malgré l'usage d'un système de communication ultramoderne et flambant neuf, des diplomates suisses sont parvenus à éventer les plans d'une opération de sauvetage de nos otages en Libye. Pire, et malgré des précautions encore plus drastiques, les banques suisses ont subi des fuites d'une telle ampleur ces deux dernières années qu'elles ont conduit à l'abandon de facto du secret bancaire.

«On estime dans la branche que 80% des fuites proviennent de l'intérieur des organisations, explique Jerry Krattiger, cofondateur de la société Solvis spécialisée dans l'installation de logiciels de cryptages dans les entreprises. Or si les systèmes informatiques sont bien protégés contre les intrusions extérieures, ils le sont bien moins contre les fuites internes, qu'il s'agisse d'actes de malveillance ou de maladresses.»

Début 2010, l'antédiluvien «cryptofax» en usage dans les 200 ambassades suisses a été remplacé par un système de cryptage moderne, le TC-007, utilisé par les 450 fonctionnaires fédéraux en poste à l'étranger. Ceux-ci transmettent chaque jour près de 5000 messages et documents confidentiels à la centrale de Berne, qui sont ensuite sauvegardés dans la forteresse alpine protégée par Crypto AG.

Cette démonstration du savoir-faire helvétique en matière de technologie de cryptage n'a pas empêché la diplomatie suisse de passer à deux doigts de la catastrophe en 2009, comme l'a révélé le récent rapport parlementaire sur la crise libyenne. Malgré l'envoi du diplomate Jacques Pitteloup, chargé d'installer le système de codage TC-007 à l'ambassade de Tripoli, les diplomates suisses sur

place ont multiplié les gaffes. Un fax faisant état des plans d'exfiltration des otages a par exemple été envoyé à diverses administrations à Berne, bien au-delà du cercle des personnes autorisées. Un téléphone portable et un ordinateur ont été perdus en route entre l'ambassade et l'aéroport. L'opération de sauvetage des deux otages par des commandos d'élite de l'armée aurait pu être gravement compromise, si elle n'avait pas été abandonnée. «D'une certaine façon, trop de sécurité tue la sécurité, observe Serge Vaudenay, professeur de cryptographie à l'EPFL. L'erreur est d'oublier que les êtres humains ne se comportent pas comme des ordinateurs.»

Les mésaventures des fonctionnaires suisses en Libye paraissent anecdotiques au regard du scandale qui secoue le Département d'Etat américain, après la divulgation de centaines de câbles diplomatiques par WikiLeaks cet automne. Les deux affaires révèlent pourtant un même phénomène: plus les systèmes de cryptage deviennent complexes et centralisés, plus ils représentent un danger pour l'organisation qui les déploie. «Il est nécessaire d'avoir recours à des techniciens pour utiliser ces mécanismes, ce qui introduit une faiblesse supplémentaire dans le système, poursuit Serge Vaudenay: des informaticiens peuvent avoir accès aux clefs et récupérer les données.»

Avec le risque de fuite qui s'ensuit. C'est ce qui s'est passé une première fois en 2008 au sein de la banque LGT du Liechtenstein, après qu'un employé a dérobé et vendu aux autorités allemandes une liste de milliers de clients. Le siège genevois de HSBC a connu le même scénario catastrophe, en 2008, avec le vol par un informaticien, Hervé Falciani, de la quasi-totalité de ses données. Idem dans l'affaire WikiLeaks, lorsqu'une recrue de 22 ans en poste en Irak, Bradley Manning, s'est trouvée en position de télécharger 251 287 câbles diplomatiques depuis son poste de travail sur le réseau SiproNet, un réseau sécurisé rassemblant des informations classées «confidentielles» et «secrètes». «Il existe une tension permanente entre les exigences de productivité et de sécurité, entre la volonté de concentrer les informations pour les rendre plus accessibles aux collaborateurs et celle de limiter leurs accès», decode Jerry Krattiger.

L'idée d'un système informatique unifié entre le Département d'Etat et le Pentagone avait été lancée peu après les attentats du 11 septembre 2001 par Paul Wolfowitz, le secrétaire adjoint à la Défense nommé par Georges W. Bush. Vilipendé pour n'avoir rien vu venir de l'attaque qui se tramait, le néo-conservateur s'était fait le porte-drapeau du concept «net-centric» qui devait assurer à tous les «combattants», de l'analyste de Washington aux commandos en Irak, un même accès aux données collectées par les administrations américaines et alliées. Avec pour résultat qu'en 2009, près de trois millions de personnes avaient accès à SiproNet. D'après une enquête du Washington Post, 850 000 fonctionnaires et collaborateurs des services d'intelligence américains seraient autorisés à consulter des informations «top secret», c'est-à-dire susceptibles de causer un danger «exceptionnellement grave» à la sécurité nationale.

«La faiblesse de ces systèmes provient d'une déficience au niveau des ressources humaines plus que d'un défaut technique, se défend Serge Vaudenay. L'informatique permet de rationaliser la gestion des informations. En même temps, elle les concentre dans les mêmes endroits ce qui rend leur exposition plus critique. Je ne pense pas qu'il y ait plus de fuites qu'avant mais leur impact est beaucoup plus considérable, poursuit l'informaticien. La sécurité des infrastructures n'a pas diminué mais les menaces ont augmenté. Gouvernements et grandes entreprises n'évoluent plus dans un monde de gentlemen.»

Un point que confirme Jerry Krattiger: «Nous vivons depuis deux ans dans un contexte de crise qui a exacerbé les tensions, qu'elles soient sociales ou idéologiques, entre les organisations et les individus. En agissant par vengeance ou parce qu'elle se sent flouée, on découvre aujourd'hui qu'une personne seule peut causer des dégâts considérables.»