Piratage massif au FBI : comment les services de renseignement peuvent-ils s'adapter au monde de Wikileaks et des hackers ?

Les services de renseignement doivent depuis plusieurs années faire face aux attaques de hackers, des Anonymous, aux publications de Wikileaks ou encore aux révélations de lanceurs d'alerte comme Edward Snowden. Un nouveau défi.

Avec Jérôme de Labriffe

Atlantico : L'ère du numérique a-t-il rendu les services de renseignements plus vulnérables qu'auparavant ?

Jérôme de Labriffe : Concernant le piratage des contacts associés des employés du FBI et des collaborateurs du DHS, il semble que ce piratage ait été effectué en « attaquant » le système informatique du Département de la Justice et non pas le FBI lui-même.

Cette attaque a exploité des méthodes tout à fait classique d'ingénierie sociale mettant en exergue le défi qu'elle constitue pour toutes organisation, comme nous avons eu l'occasion de le souligner en France, avec la « fraude au président ». Seule la mise en place de procédure de sécurité à respecter rigoureusement, et la formation des personnels peuvent permettre de réduire le risque lié à ce type d'attaque.

L'ère du numérique et toutes ses conséquences ont effectivement créé des modifications profondes pour toutes les organisations, privées et publiques qui se sont adaptées à cette « facilitation » des modes de communication (email, messagerie instantanée, réseaux sociaux), pour accéder à l'ensemble des informations disponibles sur internet (web, web 2.0, bases de données, etc.), pour faciliter les transactions, (e-commerce, dématérialisation de certains échanges administratifs)

Les acteurs du renseignement qui sont organisés par tradition et par culture autour de la culture du secret et du cloisonnement ont dû s'adapter à cette « transformation digital » qui s'organise autour du partage et de la diffusion en masse de l'information, ce qui a augmenté le nombre et le type de risques.

Pour remplir ses missions, mais aussi pour se développer en tant qu'organisation, un service de renseignement a désormais la nécessité d'organiser sa communication pour faire comprendre ses challenges, et obtenir les moyens financiers ou réglementaires nécessaires. De plus, les personnels de ses services sont eux-mêmes confrontés, dans leur vie privée, à un monde beaucoup plus ouvert, à travers les réseaux sociaux.

Ces challenges sont évidemment mieux maîtrisés que dans les autres organisations, dans un environnement habitué à la culture du secret et de la sécurité. Néanmoins, entre ouverture et secret, les services de renseignement sont aujourd'hui confrontés à une savante gestion de l'équilibre.

Les hackers comme les Anonymous et les « lanceurs d'alerte » comme Edward Snowden ont-ils un impact sur les activités des services de renseignement ?

Il est clairement démontré aujourd'hui que les révélations liées à Snowden ont impacté fortement les services de renseignement, ne serait-ce qu'au niveau de leur communication et de leur perception par les opinions publiques. Il semble également évident que les conséquences de ces révélations ont été à l'origine de modification significatives des méthodes de travail des services qui ont dû revoir et adapter leurs procédures internes aux challenges proposés par l'économie numérique.

La galaxie internet qui décuple la circulation de l'information crée de nouveaux repères et donc un nouveau type de transparence qui conjugue "l'indélébilité" et le "mixage" de multiples sources d''information. Ce cocktail peut sembler plus transparent en terme de "quantité" mais plus "flou" en terme de qualité.

Comment adaptent-ils leurs modes d'action à ce nouvel environnement numérique et à ces nouvelles menaces ? Va-t-on revenir aux bonnes vieilles méthodes : l'encre sympathique, les boîtes aux lettres mortes etc. ?

Le numérique propose de nouvelles règles, il est donc normal de s'y adapter. C'est par ailleurs un contexte en permanente évolution, il est donc important d'avoir cette capacité de réactivité et d'anticipation. Ce sont les deux clés pour appréhender les enjeux du digital.

Quant à revenir à des méthodes plus que traditionnelles, cela pourrait être tentant à court terme dans certains cas pour résoudre un problème précis. Mais le numérique est une "never ending story" que l'on arrête pas et qui ne fait pas marche arrière.

Où en est la France dans sa réflexion stratégique de cyberdéfense ? Elle semble avoir été moins victimes d'attaques et fuites que les Etats-Unis…

Comparer la France et les Etats Unis est toujours un exercice difficile, les ordres de valeur étant tellement différents que cette comparaison est souvent un non-sens. En matière de cyber-sécurité ou cyberdéfense c'est le même principe. La question est plutôt de savoir quel est le potentiel d'efficacité et de réaction de la France sur ces sujets.

Si l'on regarde la prise de conscience politique et collective de ces menaces depuis quelques années, qui s'appuient sur des relais opérationnels organisés et déterminés comme l'ANSSI par exemple, pour déployer les politiques annoncées et assurer la prévention du risque cyber, nous avons là les deux piliers vitaux d'une stratégie cyber.