Dîner du savoir : une sécurité qui n'est pas sans risques pour les DSI

L'Agora des DSI et celle des directeurs de la sécurité se sont données rendez-vous pour plancher et échanger sur la cyberconfiance et le risque numérique. Pour parler de ces sujets, Alain Bauer, professeur de criminologie au Conservatoire National des Arts et Métiers (CNAM) et Guillaume Poupard, directeur général de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). Dès le début, le criminologue pose le débat en expliquant que la nature du risque a changé. Selon lui, « *dans 99% des cas, le risque était le fait de la stupidité d'un seul individu. Le reste était résiduel* ».

En 1973, un piratage depuis une prison a changé la donne. Un informaticien y a détourné plusieurs millions de dollars en glanant les centimes additionnels lors de transaction, rappelle Alain Bauer. Un signal faible, « *puis pendant 40 ans plus rien. Sauf que les systèmes sont devenus de plus en plus interconnectés et que le niveau de sécurité a baissé. La conséquence s'est traduite par les piratages de Target, du vol de plusieurs millions de coordonnées bancaires en Corée du Sud ou des attaques sur des ATM à New York* ». Une succession d'évènements de sécurité qui a eu pour conséquence de provoquer « *une cyberconfusion* », assure l'enseignant.

Le coût du risque IT impossible à évaluer

Cette confusion et cette multiplicité des menaces rend bien difficile l'évaluation du coût du risque. « *Aujourd'hui, on ne peut pas évaluer ce coût* », admet Guillaume Poupard et d'ajouter : « *Certaines attaques sont silencieuses avec un objectif pour les pirates de rester dans l'entreprise. La majorité vise à voler des données.* » Alain Bauer est plus brutal en mettant en exergue une différence culturelle entre « *l'esprit français qui est de dire cela ne va pas nous arriver, tandis que le monde anglo-saxon s'interroge sur combien cela va nous coûter* ».

Et de dire *in fine* que malgré les avertissements, il arrive que les sociétés soient piratées et « *qu'une bonne fessée est parfois une œuvre de pédagogie utile* ». Une théorie par l'exemple que ne dément pas Guillaume Poupard. « *Snowden nous a beaucoup aidé pour cela. Il a fait prendre conscience qu'il fallait normaliser le risque IT, c'est-à-dire le prendre en compte comme un autre risque. Cela signifie notamment qu'il faut développer un système d'assurance et de réassurance autour de ce risque.* »

Détection et souveraineté

Mais une fois posé le diagnostic et les questions du coût, quelles solutions choisir pour se protéger des risques numériques ? Guillaume Poupard écarte d'emblée l'hypothèse d'une protection à la française. « *Un cyber bouclier, c'est complètement idiot.* » « *Le problème ne se pose pas sur la protection, la doctrine est simple la sécurité doit être prise en compte dans chaque projet numérique* », insiste le dirigeant. Un point d'achoppement avec Alain Bauer, qui évoque le problème de souveraineté en matière de sécurité. Il rappelle que « *la France ne dispose pas de serveur racine pour Internet, cela pose un problème de dépendance* ». Guillaume Poupard préfère parler d'une souveraineté numérique européenne et

du développement d'une industrie européenne en matière de sécurité.

Le sujet par contre plus nouveau pour les entreprises, c'est la détection des menaces, « *c'est cher et il faut trouver les technologies de confiance* », avoue le directeur de l'ANSSI qui œuvre avec ses équipes pour la qualification de solutions. Une détection qui a parfois ses limites et qui tourne « *au fétichisme technologique. Nous sommes dans le fantasme de l'inspecteur Google qui ne peut rien contre l'imam YouTube* », répond doctement Alain Bauer. Cela signifie que le monde de la sécurité a besoin d'analystes et non de machines. Jamais avare de bons mots, il résume le problème : « *Quand on passe de 2 oreilles et 1 cerveau à 4 oreilles et un cerveau, ce n'est pas une amélioration.* »

Sensibilisation et cercle du secret élargi

Reste la question de la sensibilisation, un élément important pour l'ANSSI. « *A une époque, la plus grande faille, c'était le VIP qui demandait un accès au SI avec sa tablette ou son smartphone* », précise Guillaume Poupard devant un auditoire acquis. Pour répondre à cette problématique, « *il faut adapter la sensibilisation au public. On parle différemment de la sécurité et des risques à un directeur général, un directeur juridique ou un directeur financier. Il y a avant tout un problème de langage* ».

Nonobstant, il faut que le « *cercle du secret* » autour de la sécurité IT s'élargisse. « *Au début les seuls à savoir étaient les RSSI, puis ils ont intégré les DSI et eux-mêmes ont commencé à investir le Comex où on se pose maintenant la question quel est l'état de la sécurité des réseaux* », constate Guillaume Poupard. C'est une avancée à poursuivre, conclut le dirigeant.

A lire aussi :

Sécurité : DSI et direction juridique unies, mais dialogue à approfondir ?

Gala DSI : « Sur le numérique, tout le monde a besoin des DSI »