Cybersécurité : les grandes entreprises trouvent un modus vivendi avec l'Anssi

Les quelque 200 opérateurs d'importance vitale (OIV), des organisations jugées essentielles au fonctionnement de la nation, n'ont plus que quelques mois pour se préparer. Lors du FIC (Forum International de la Cybersécurité), **Guillaume Poupard**, le directeur général de l'Anssi, a annoncé la sortie imminente des arrêtés sectoriels d'application de la Loi de programmation militaire (LPM), votée fin 2013. La fin d'une longue marche pour l'Agence nationale de la sécurité des systèmes d'information, pour qui il s'agit là d'un chantier majeur.

« *18 arrêtés correspondant à autant de secteurs d'activité vont être publiés, car nous avons voulu coller à la réalité de ces entreprises* », explique Guillaume Poupard. Y figureront les règles découlant de la LPM et portant sur la **notification des incidents de sécurité** par les OIV ou encore sur la façon dont ils seront contrôlés. L'entrée en application de la législation est prévue pour le 1er juillet, avec des délais de mise en œuvre allant de 3 à 18 mois en fonction de cas. Une échéance assez brève au regard du timing des investissements informatiques, mais qui s'explique par le fait que ces arrêtés ont été négociés depuis des mois avec les OIV eux-mêmes. Ces derniers connaissent donc déjà les grandes lignes des modalités d'applications.

« Quelques millions d'euros »

« *Dès le départ, nous avons annoncé que la LPM était un prétexte pour établir un dialogue avec les opérateurs d'importance vitale. On a voulu prendre le temps pour parvenir à des règles co-écrites avec eux et tenant compte de leurs contraintes, notamment financières* », ajoute le directeur de l'Anssi. Qui précise quand même que pour un OIV 'standard', le coût de mise en œuvre de la réglementation se chiffrera à plusieurs millions d'euros, auxquels s'ajouteront quelques autres millions pour le fonctionnement chaque année (il faudra notamment payer les prestataires d'audit).

Les RSSI croisés dans les couloirs du FIC nuancent toutefois le propos. Jean-Luc Molinier, le directeur de la sécurité d'Orange, explique ainsi que si les recommandations de l'Anssi obligent à repenser dans certains cas les architectures réseaux maison – « *ce qui est coûteux en terme de design, de câblage ou de reprogrammation* » -, l'écart entre ce qui est déployé chez l'opérateur et ce que préconisera l'arrêté pour le secteur des télécoms n'est pas si important. A la SNCF, Joël Noirot, le RSSI groupe, assure avoir **anticipé les nouvelles contraintes** sur ses budgets 2014 et 2015. « *Le marché en parle depuis si longtemps que la publication des arrêtés ne va pas tout changer* », résume Christophe Moret, le vice-président cybersecurity d'Atos, qui accueille toutefois positivement la fin du processus, notant que ce dernier a pu avoir un « *effet inhibiteur* » sur les investissements des entreprises.

Certifiés ou qualifiés Anssi ?

Au cours de cette co-construction, les OIV sont parvenus à rendre relativement flexible un texte qui, au départ, pouvait apparaître comme contraignant. « *On laissera les opérateurs définir le périmètre des*

systèmes d'information à caractère vital », précise ainsi Julien Barnu, le chef de cabinet de l'Anssi. Autrement dit, ce sont les OIV eux-mêmes qui **choisiront les systèmes sur lesquels la loi va s'appliquer**. Un périmètre touchant à tout ce qui peut mettre en péril le potentiel militaire ou économique de la nation. Autrement dit, les systèmes dont la compromission entrainerait un 'simple' préjudice commercial ne sont pas concernés, remarque ainsi Joël Noirot.

Si les arrêtés sont attendus dans les prochaines semaines, quelques zones de flous persistent. Première nappe de brouillard : quels seront les incidents de sécurité notifiés à l'Anssi ? « *On ne peut évidemment pas recevoir une alerte à chaque scan de ports, sinon ce serait une formidable attaque par déni de service sur l'Anssi*, s'amuse Guillaume Poupard. *Nous sommes en train de calibrer les incidents qui seront remontés et ceux qui ne le seront pas* ».

Mais l'incertitude numéro un concerne le niveau de labellisation Anssi des produits de sécurité que recommandera l'agence sur les systèmes considérés d'importance vitale. Se contentera-t-on d'une certification par un laboratoire indépendant, un niveau assez facilement accessible ? Ou ira-t-on vers une qualification, un processus beaucoup lourd impliquant la fourniture du code source par l'industriel ? « *Nous poussons pour aller vers une qualification* », assure Guillaume Poupard. Une solution qui pourrait gêner aux entournures un certain nombre d'industriels, surtout américains : « *certains ne peuvent pas répondre à nos critères* », reconnaît d'ailleurs le directeur de l'agence. Chez FireEye, on assure toutefois que l'accès au code source du produit ne constitue pas un point de blocage. Même si l'éditeur américain reconnaît n'en être qu'aux prémisses du processus. Chez Trend Micro, Renaud Bidou, le directeur technique Europe du Sud, explique « *envisager d'aller jusqu'à la qualification. Mais on étudie encore sur quel produit on va réaliser cet investissement, car notre catalogue en comprend de nombreux.* »

Simple recommandation… pour l'instant

De toute façon, qu'ils soient qualifiés ou certifiés, les produits référencés par l'Anssi seront simplement recommandés aux OIV, comme nous l'a confirmé Guillaume Poupard. Pas imposés. « *C'est une démarche pragmatique*, plaide le directeur général de l'Anssi. *Dans certains domaines, il faut avoir conscience qu'il n'y a pas encore d'offre qualifiée ou que le processus de qualification lui-même n'existe pas. Par contre, quand ce sera réaliste, nous irons vers une obligation ; les arrêtés ont vocation à être renégociés dans deux ou trois ans. Par exemple, dans un domaine sensible comme la détection d'intrusion, nous finirons certainement par imposer la qualification des produits aux OIV.* »

En attendant, les RSSI restent circonspects et attendent d'évaluer les produits recommandés par l'agence. Chez Orange, Jean-Luc Molinier explique ainsi qu'en matière de sondes, son groupe va soupeser les solutions que l'Anssi propose et **vérifier que ces produits sont bien supérieurs à ceux déployés** actuellement avant de prendre toute décision de remplacement. A la SNCF, Joël Noirot note : « *sur les outils sophistiqués, l'offre française reste limitée. En matière de cybersécurité, il demeure difficile de se passer de la technologie américaine.* »

Une vision que conteste évidemment Airbus Defence and Space Cybersecurity qui, via sa division Stormshield, propose des firewalls, des solutions de protection des terminaux et des données. « *Nous espérons une harmonisation européenne des certifications qui favoriserait le développement des industriels du continent* », plaide Matthieu Bonenfant, directeur marketing produits de Stormshield.

Une voie qui permettrait de limiter les investissements dans les processus de certification des divers pays de l'Union tout en favorisant la lisibilité de l'offre pour les donneurs d'ordre. La future directive NIS, une LPM 'light' en cours de discussion à Bruxelles, aurait pu être ce texte fédérateur, sauf que son application sera laissée à l'appréciation de chaque état. Parallèlement, bien qu'officiellement proches, l'Anssi française et son homologue allemand (le BSI) ne sont pas parvenus à s'aligner sur les critères de certification des produits de sécurité.

A lire aussi :

Assises de la sécurité 2015 : L'Anssi couve les OIV

Audits de sécurité : le gouvernement des Etats-Unis rase gratis