

Assises de la sécurité 2016 : l'urgentiste Poupard prescrit ses remèdes

La 16^{ème} édition des Assises de la sécurité, qui se déroulent actuellement à Monaco, s'est ouverte par l'intervention de Guillaume Poupard, une intervention attendue après une année bien remplie pour l'Anssi. D'emblée, le directeur général de cette agence assure que son rôle est celui « *de médecin urgentiste pour soigner des blessés graves et même très graves, victimes d'attaques souvent puissantes* ». Pour autant, un certain spleen s'installe en évoquant l'obligation de protéger « *des motards qui roulent sans casque et à 200 km/h sur autoroute* ».

Souveraineté sans protectionnisme

Des sorties de route involontaires que l'Anssi souhaite éviter en misant sur une triple démarche : souveraine, européenne et ouverte. La première concerne donc la souveraineté et, pour Guillaume Poupard, il ne s'agit pas « *d'un gros mot, il doit exister une sécurité numérique en France* ». Et les premiers concernés sont les OIV, les opérateurs d'importance vitale (au nombre de 250) qui ont placé sur la sellette par la loi de programmation militaire (LPM) et plus exactement son article 22. Plusieurs arrêtés sectoriels sont sortis cet été, ce qui fait dire au dirigeant de l'Anssi : « *nous avons fini avec la phase de build et nous passons maintenant à la phase de run* ». Autrement dit, il s'agit maintenant de faire tourner le dispositif – assez complexe – qui encadre la sécurité de ces quelque 250 organisations publiques ou privées.

Et, dans cette phase, l'agence n'entend pas être seule. « *Certaines règles fixées ont besoin de produits et de services de sécurité* », dit Guillaume Poupard. D'où l'idée de lancer un système de qualification de plusieurs offres de produits ou de services. Par exemple sur les PASSI concernant l'audit : « *j'ai été surpris de voir arriver pas moins d'une vingtaine de demandes de qualification, aujourd'hui 14 sont en cours* », avoue Guillaume Poupard. D'autres offres sont en phase expérimentale, c'est le cas de la détection d'incident (PDIS), avec 8 acteurs dans la boucle, et de la réponse sur incident (PRIS), où 6 candidats se sont déjà déclarés. Plusieurs offreurs français figurent parmi ces candidats à la qualification. Pour autant, « *souveraineté ne signifie pas protectionnisme* », insiste Guillaume Poupard. « *Il faut une ouverture aux industriels et éditeurs non européens. Ils ne sont pas des parias* », assure-t-il. Avant de compléter son propos : « *nous sommes pour une coopération internationale intelligente et non naïve* ».

Un pragmatisme que l'on retrouve dans la labellisation des offres Cloud : « *les Cloud des GAFAM (soit les GAFA plus Microsoft, NDLR) sont les bienvenus, mais ils doivent respecter les règles* ». Comprendre se plier au référentiel basé sur la certification ISO 27001 qui devrait être finalisé à la fin de l'année, mais aussi une domiciliation en Europe ou en France. Les dernières annonces d'Amazon et Microsoft, qui ont tous deux annoncé l'ouverture de datacenters en France pour leur Cloud AWS et Azure, vont dans ce sens.

Directive NIS : au-delà des OIV

Le second axe de travail s'appuie sur l'Europe. A plusieurs niveaux. Sur le plan réglementaire, la [directive NIS](#) a été adoptée et doit maintenant être transposée avant 2018 dans le droit des Etats membres. Elle intègre notamment la notion d'opérateur essentiel, « *un concept plus large que celui des OIV* », indique Guillaume Poupard. Et de citer des exemples de cette extension à de nouveaux acteurs : « *les assurances ou les supermarchés et plus particulièrement leurs chaînes logistiques* ». L'Anssi va donc s'atteler à lister les différents opérateurs qui rentreront dans ce cadre, et « *la liste ne sera pas figée* ».

Autre point important au niveau européen : l'initiative de la Commission européenne de promouvoir une cybersécurité européenne à travers un partenariat public-privé. « *Un fonds de 450 millions d'euros sur 3 ans est dédié pour la R&D en matière de cybersécurité. Il y a des opportunités et nous allons défendre nos orientations, SOC, objets connectés, Scada* ». Enfin, le dirigeant de l'Anssi reste vigilant sur les négociations d'accords transatlantiques : « *nous devons y défendre nos valeurs* », martèle-t-il.

Une immunité pour les remontées de failles

La dernière démarche de l'Anssi vise l'ouverture à la société civile. Avec un focus sur les personnes qui déclarent des bugs ou des failles à l'Agence. « *Le problème était de trouver un statut pour ceux qui nous remontent de l'information. Il y a eu beaucoup de discussions avec les ministères et finalement un compromis a été trouvé* », juge Guillaume Poupard. Ce consensus se nomme article 20 septies de la loi sur le numérique récemment adoptée, mais non encore publiée. Ce texte modifie l'article 323-1 du code de procédure pénale en indiquant que « *toute personne qui a tenté de commettre ou a commis le délit prévu au présent article est exempté de peine si elle a immédiatement averti l'autorité administrative ou judiciaire ou le responsable du système de traitement automatisé de données en cause d'un risque d'atteinte aux données ou au fonctionnement du système* ».

Si le cadre est maintenant clair, Guillaume Poupard reste dans l'expectative « *sur le volume que ces signalements va représenter. Aujourd'hui, nous en avons quelques-unes par mois* ». Par contre, l'agence se prépare en annonçant [un guichet unique](#) pour ces signalements. Elle garantira aussi l'anonymat des personnes soumettant leurs découvertes. Guillaume Poupard souhaite aussi éditer un guide pour expliquer les limites de l'exercice : « *il faut que les gens soient prudents, car ce procédé est basé sur la bonne foi, mais in fine, en cas de problème, c'est un juge qui décidera* ».

A lire aussi :

[OIV : la détection des attaques passe sous le contrôle de l'Etat](#)

[Avec SecNumedu, l'Anssi labellise des formations supérieures en sécurité](#)