CYBERSÉCURITÉ

LA CYBERSÉCURITÉ AU CŒUR DE TOUS LES ENJEUX

Aujourd'hui, les questions de cybersécurité sont une combinaison de souveraineté nationale, d'accompagnement du tissu économique et industriel français et de coopérations nationales et internationales. Le point avec Guillaume Poupard (92), directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Guillaume Poupard (92)

BIO EXPRESS

Guillaume Poupard (92) est ingénieur de l'armement en option recherche. Il est titulaire d'une thèse de doctorat en cryptographie. Il est également diplômé de l'enseignement supérieur en psychologie. Il débute sa carrière comme expert puis chef du laboratoire de cryptographie de la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI). Cette direction est transformée en 2009 pour devenir l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Il rejoint en 2006 le ministère de la Défense, toujours dans le domaine de la cryptographie gouvernementale puis de la cyberdéfense. En novembre 2010, il devient responsable du pôle « sécurité des systèmes d'information » au sein de la direction technique de la Direction Générale de l'Armement (DGA), responsable de l'expertise et de la politique technique dans le domaine de la cybersécurité. En mars 2014, il est nommé directeur général de l'Agence nationale de la sécurité des systèmes d'information.

Que pouvez-vous nous dire sur l'ANSSI et sur son périmètre d'action ?

L'ANSSI a vu le jour en 2009 et est rattachée au Secrétaire général de la défense et de la sécurité nationale. C'est une autorité nationale qui opère et intervient dans le domaine de la sécurité des réseaux informatiques les plus sensibles au niveau des administrations et, depuis 2013, contribue à celle des opérateurs d'importance vitale (OIV).

Contrairement à certains de nos alliés, nous n'intervenons que sur un plan défensif. Dans d'autres pays, cet aspect est souvent rattaché aux services de renseignement technique, mais en France, le choix a été fait de séparer les activités offensives et la protection des réseaux. Notre autre originalité est notre statut interministériel : nous ne sommes rattachés à aucun ministère, ce qui nous donne une forme de neutralité et surtout une capacité à travailler plus aisément avec l'ensemble des acteurs nationaux.

Dans ce cadre, notre mission est triple :

- **Prévenir les menaces** en anticipant les modes d'attaques et en impliquant les ministères et les administrations, mais aussi le secteur privé et ainsi créer un écosystème compétent et de confiance ;
- **Défendre les systèmes** grâce à la détection des attaques puis apporter un support aux victimes dans la compréhension et la remédiation des crises informatiques ;
- **Informer et sensibiliser** nos différents publics aux bonnes pratiques informatiques.

Lors de notre création en 2009, nous avions une centaine de personnes aujourd'hui nous sommes 500. Cette forte croissance traduit une volonté réelle des plus hautes autorités de la Nation de faire face aux nouvelles menaces associées au cyberespace. Elle reflète également une prise de conscience de la nécessité de faire face à ces enjeux qui évoluent très rapidement dans le monde, et en France en particulier. D'ailleurs, la France fait partie du premier cercle de pays qui prennent très au sérieux le risque cyber.

Quel bilan tirez-vous de l'année 2016 ? Quels seront vos principaux enjeux en 2017 ?

Le bilan de l'année 2016 est contrasté. Nous observons une croissance du nombre d'attaques qui sont de plus en plus graves. Les attaquants sont plus nombreux,

mieux organisés, voire plus spécialisés. Mais en parallèle, nous sommes en veille permanente ce qui nous permet de détecter beaucoup plus d'attaques. Aujourd'hui, les attaques majeures ont pour but de voler des informations, le plus souvent d'ordre économique, technique ou stratégique. Les attaquants sont obsédés par la nécessité de rester discrets pour exploiter le plus longtemps possible le réseau pénétré. Les cas les plus critiques sont observés au niveau des grandes entreprises. D'autres attaques visent à déstabiliser, à saboter, voire à détruire une victime. Nous nous rappelons tous du cas de TV5 Monde où l'attaquant a tout simplement voulu détruire sa victime sans pour autant chercher à gagner de l'argent ou à voler des informations. Cet aspect est un phénomène nouveau.

Les messages de prévention associés au développement de la réglementation ont, toutefois, permis une véritable prise de conscience. Les dirigeants d'entreprises et des administrations sont plus sensibles aux risques cyber. Ils ont effet compris que la cybersécurité n'est pas un sujet purement technique et qu'ils doivent y porter une plus grande attention. La cybersécurité est un vrai sujet de gouvernance. Cela se traduit par une volonté de construire une protection efficace et de rapprocher les enjeux cybers des préoccupations des COMEX.

Pouvez-vous nous rappeler en quoi consiste la Loi de Programmation Militaire ? Quels sont les changements qui vont en découler ?

La France a été le premier pays à faire de la question de la cybersécurité une obligation pour ses acteurs les plus critiques. La Loi de la Programmation Militaire, votée en 2013, impose ainsi aux opérateurs d'importance vitale un cadre législatif clair. Environ 230 opérateurs, dont la sécurité est un jeu pour la sécurité nationale, sont concernés. Ils opèrent dans des domaines aussi différents que la finance, le transport, l'énergie, l'industrie, etc.

Nous leur imposons des règles de sécurité à appliquer sur les systèmes d'information les plus sensibles. Nous leur demandons également de nous notifier de manière confidentielle les incidents et les attaques informatiques. Ces mesures sont définies par un arrêté propre à chaque secteur d'activité et publié au Journal officiel. Cela nous permet d'identifier les victimes, de voir s'il y a d'autres victimes potentielles et de les aider à faire face à cette menace. Le Premier ministre, à travers l'ANSSI, a aussi la possibilité de donner des consignes exceptionnelles en cas de crises majeures pour enrayer le risque de contagion et limiter les impacts. Cette démarche permet d'inscrire la cybersécurité comme une priorité au sein des différents opérateurs.

Nos voisins, comme l'Allemagne, se sont lancés dans une démarche similaire. En Europe, la directive NIS sur la sécurité des réseaux, impose également aux opérateurs et aux secteurs critiques l'obligation de se plier à des règles de sécurité. Cette prise en main en amont de ce risque nous permet de réduire les conséquences néfastes des attaques éventuelles.

Mais, au-delà de l'aspect très contraignant et autoritaire de cette démarche, nous collaborons étroitement avec les opérateurs afin de pouvoir mettre en place des directives et des règles qu'ils pourront ensuite appliquer efficacement. Afin d'accompagner ces réglementations, l'ANSSI travaille également en lien avec la filière industrielle de la cybersécurité. Nous mettons ainsi au service des OIV des produits et des services qualifiés pour assurer la protection de leurs systèmes. En France, cela nous a permis de contribuer à structurer un écosystème industriel de haute qualité et de confiance. C'est un challenge important pour la France, mais aussi pour l'Europe.

Au niveau européen, quels sont les projets qui vous mobilisent ? Quelles sont vos perspectives ?

VIE DES ENTREPRISES

ANSSI EN CHIFFRES CLÉS (2016)

- 500 agents
- 65% d'agents de moins de 40 ans
- 40 publications de recherche
- 202 réunions internationales en relation avec 30 pays
- 4000 signalements reçus
- 350 rencontres bilatérales entre l'agence et les entreprises françaises de la cybersécurité
- 266 bénéficiaires de formation au sein de l'ANSSI

L'Europe est une priorité. Au niveau national, nous avons beaucoup évolué et avons pu identifier les limites à notre action. Il est temps pour nous de se tourner vers l'Europe. Plusieurs projets ont été lancés comme, par exemple, la directive NIS qui est une transposition de ce que nous avons fait au niveau français en matière de sécurité des systèmes d'information les plus sensibles. Elle va nous permettre notamment d'échanger plus efficacement avec l'ensemble de nos homologues européens sur ce sujet.

Aujourd'hui, nous avons en effet une Europe à deux vitesses : des pays comme la France, le Royaume-Uni et l'Allemagne qui ont pris les choses en main, et d'autres pays qui n'ont pas su s'organiser ou n'ont pas les moyens de le faire. La directive NIS impose à tous les états membres de se mobiliser et de travailler ensemble sur la base du volontariat pour échanger des informations en cas d'attaques.

Il y a également une démarche européenne visant la R&D avec un partenariat public privé (PPP). Nous soutenons cette initiative. L'ANSSI est membre de l'association qui participe à ce PPP et j'en suis moi-même un des vice-présidents.

Nous assistons à l'émergence d'une véritable volonté d'autonomie stratégique européenne et d'une certaine indépendance dans nos choix et réalisations sans pour autant tourner le dos à nos alliés non-Européens. Mais il est important que nous puissions avoir notre propre capacité de développement et de réflexion. Le PPP va nous donner les moyens de structurer pertinemment tout cela.

Et il y a enfin un axe franco-allemand fort qui continue à se renforcer grâce au partage d'idées et de perspectives sur ces questions. Ainsi, à titre d'exemple, nous allons bientôt lancer une démarche en commun au niveau du « *cloud computing* ». Il s'agit d'une certification visant à identifier les prestataires sérieux qui répondent aux standards sécuritaires. L'objectif est ensuite d'étendre cette logique au niveau européen.

Qu'en est-il de l'axe stratégique de la sécurité numérique ?

En octobre 2015, le Premier ministre a présenté une stratégie nationale structurée autour de 5 axes :

- La souveraineté nationale dont nous avons déjà parlé ;
- Le développement d'une cyber industrie en France et en Europe ;
- La capacité d'aider des victimes qui n'ont pas forcément un lien direct avec la sécurité nationale : les industries, les PME, les citoyens
- La formation et la sensibilisation de tout un chacun avec des messages appropriés, mais également la capacité de former des experts à travers des formations labellisées.
- Le développement de la coopération internationale bilatérales et multilatérales incluant une action de « *capacity building* ».

Ce dernier point se traduit par une capacité à apporter de l'aide aux pays qui sont moins en avance sur ces sujets sur tous les continents. Le but n'est pas de traiter leurs problèmes à leur place, cela n'aurait pas de sens, mais de les accompagner afin qu'ils puissent développer leurs propres moyens. Cette démarche vise à éviter l'apparition de zones de non-droit dans le cyberespace ce qui est une menace directe pour la France. Il y a un intérêt commun à faire monter ces pays en compétence.

Et pour conclure ?

Aujourd'hui, la cybersécurité est un sujet qui n'est plus exclusivement destiné aux experts. Les dirigeants et responsables au sein des entreprises (directeur général, directeur financier ou juridique, responsables « métier », etc.) doivent développer un intérêt et une véritable vigilance quant aux enjeux de sécurité liés au cyber. Ceci peut s'avérer primordial pour la survie même de l'entreprise ! ■