SÉCURITÉ INFORMATIQUE

ANSSI : SE SÉCURISER FACE À LA MENACE DES ATTAQUES INFORMATIQUES

Guillaume Poupard (92)

Chargée de la cybersécurité, l'ANSSI dépend du Secrétaire Général de la Défense et de la Sécurité Nationale qui assiste le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationales. Guillaume Poupard (92), DG de l'ANSSI, nous propose un tour d'horizon des missions majeures mises en œuvre au sein de cette agence française créée en 2009 (anciennement DCSSI).

BIO EXPRESS

Guillaume Poupard (92) est docteur en cryptographie et 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 sera 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 sécurité des systèmes d'information.

A quels dangers les entreprises sont-elles exposées via le WEB ?

Les entreprises sont sujettes à trois types de menace.
La première a pour objectif de porter atteinte à l'image via la défiguration d'un site Internet par exemple.
La deuxième menace concerne l'espionnage. L'interconnexion des réseaux informatiques, l'usage de plus en plus développé du numérique favorisent les possibilités d'exploitation de vulnérabilités par des attaquants. Ainsi, aujourd'hui, l'ensemble des professionnels détenteurs d'un savoir-faire technique ou d'éléments commerciaux sont soumis à un tel risque. Les groupes d'attaquants sont de plus en plus organisés, spécialisés et discrets.
La troisième menace, potentiellement plus grave encore, est le sabotage. Elle vise à pénétrer des systèmes informatiques afin de les faire dysfonctionner pour, *in fine*, les arrêter, voire les détruire ! Les cibles de choix pour les attaquants sont notamment les sites industriels, les systèmes de commande contrôle, les systèmes de production devenus numériques en très peu de temps et qui sont en général peu ou mal sécurisés.
L'environnement actuel ne permet pas toujours d'identifier clairement le véritable objectif des attaquants : Est-ce du renseignement en préparation ? L'amorce d'un sabotage ? Des tests pour préparer l'avenir ?

LA LOI EST AINSI UN LEVIER INCONTOURNABLE POUR IMPOSER DES CONTRÔLES ET DES RÈGLES DE SÉCURITÉ DE MANIÈRE À ALLER PLUS VITE FACE À DES ATTAQUANTS, QUI EUX, NE NOUS ATTENDENT PAS.

Quelle est la vocation de l'ANSSI face à un tel contexte ?

La mission de l'ANSSI est de prévenir la menace et de défendre les systèmes d'information les plus sensibles s'ils sont victimes d'une cyberattaque.
Dotés d'une capacité d'expertise forte, nos spécialistes couvrent des domaines très pointus. Ils apportent des réponses précises sur des questions technologiques liées aux systèmes d'information et proposent différentes techniques d'attaque. Ces métiers font ainsi face aux problématiques suivantes : Quelle méthode adopter pour comprendre le mode opératoire de l'attaquant ?

SÉCURITÉ INFORMATIQUE

L'ANSSI PORTE LE MESSAGE QUE LA SÉCURITÉ PASSE AVANT TOUT PAR UNE PRISE DE CONSCIENCE DES RISQUES ET L'APPLICATION DES BONNES PRATIQUES.

Comment l'empêcher de nuire ? Comment faire en sorte qu'il ne revienne pas ?
Nous comptons également parmi nous des métiers liés à la réglementation. La sécurité ne peut pas en faire l'impasse et doit au contraire l'utiliser avec discernement afin de gagner du temps.
Certains acteurs et notamment les opérateurs d'importance vitale sont ainsi soumis à des règles bien définies. Celles-ci s'adressent à tous les opérateurs publics ou privés exploitant des établissements ou utilisant des installations, dont l'indisponibilité aurait un impact sur la sécurité de la Nation. Ils travaillent dans les secteurs stratégiques comme l'énergie, les transports, la finance, etc. La loi est ainsi un levier incontournable pour imposer des contrôles et des règles de sécurité de manière à aller plus vite face à des attaquants, qui eux, ne nous attendent pas. Par ailleurs, nous avons la responsabilité d'assurer des relations internationales avec nos alliés. Sans qu'il n'y ait de paradoxe à cela, la cybersécurité relève à la fois des questions de souveraineté nationale mais également de coopération à l'international. Nous sommes en général confrontés à des menaces communes et il est important de coopérer efficacement mais sans naïveté.
Ensuite, des qualités de communication nous sont nécessaires car malgré la technicité du sujet, l'humain demeure un facteur essentiel. Il faut être capable de porter le bon message au bon moment aux bonnes personnes, que ce soient aux citoyens, aux administrations, aux PDG de grandes sociétés, bref à toutes les victimes potentielles.

Comment cela est-il organisé ?

Rattachée au Premier ministre, l'ANSSI travaille en étroite collaboration avec les ministères afin d'assurer la sécurité et la Défense des systèmes d'information de l'Etat. Plusieurs ministères ont également un rôle à jouer en matière de cybersécurité. Le ministère de la defense, par exemple, se focalise sur la protection de ses nombreux systèmes d'information et systèmes d'armes, déployés lors des opérations extérieures. Le ministère de l'Intérieur est quant à lui en charge des questions liées à la cybercriminalité, à la protection des citoyens et aux méthodes d'enquête. Le ministère de l'Économie s'intéresse également à la cybersécurité car elle représente à la fois une des grandes menaces qui pèse sur l'économie et une opportunité pour développer un nouveau champ économique. L'ANSSI pilote et coordonne donc un sujet transverse dans le cadre duquel chacun a un rôle à jouer.

La France a-t-elle une forte expertise en matière de cybersécurité par rapport à d'autres pays comme les Etas-Unis par exemple ?

La comparaison à l'international est importante. L'ambition très claire de la France est de faire partie du premier cercle des pays capables de protéger leurs systèmes d'information, leur économie et cela de manière souveraine, c'est-à-dire autonome. Cela s'exprime par l'expertise de l'ANSSI et le déploiement d'un écosystème privé capable de proposer des produits et des services de sécurité.
La France est un des rares pays à pouvoir assurer sa cybersécurité. Nous faisons partie de ceux qui ont encore la volonté et la capacité d'assurer leur propre défense dans le domaine informatique.

Le nombre d'attaques de plus en plus sophistiquées se multiplie. Quelle est votre stratégie face à ce constat ?

Notre stratégie consiste à identifier et à protéger les systèmes les plus critiques, ceux liés à l'Etat et à certains systèmes privés particulièrement sensibles. Nous nous efforçons d'avoir toujours un coup d'avance sur les attaquants. Pour toutes les autres victimes potentielles, l'ANSSI porte le message que la sécurité passe avant tout par une prise de conscience des risques et l'application des bonnes pratiques.
Les risques ne cessent de se renouveler et il faut en permanence s'adapter. Typiquement, le fait d'utiliser son téléphone personnel dans le cadre professionnel ou l'externalisation de plus en plus fréquente de l'informatique entraînent évidemment de nouvelles questions en termes de sécurité. Notre mission est d'accompagner l'ensemble de ces nouveaux usages et d'apporter des solutions de sécurité. ■

EN BREF

L'ANSSI protège et défend les entreprises, les administrations et les particuliers des risques liés aux attaques informatiques.