La France tente de rattraper son retard en matière de cyberdéfense

Publié le 07 février 2014, à 10h10

Actus Reuters, L'Usine Digitale Défense, Cybersécurité

La France tente de rattraper son retard en matière de cyberdéfense

La France présente ce 7 février les grands axes de son pacte de cyberdéfense, doté d'un milliard d'euros et censé lui permettre de rattraper son retard à l'heure où les attaques informatiques contre les armées occidentales augmentent.

A LIRE SUR LE MÊME SUJET

Ce Prism à la française caché dans la loi de programmation militaire

Au FIC, Le Drian soigne sa cyberdéfense

Le Livre blanc sur les grandes orientations sécuritaires du gouvernement pour les prochaines années avait donné le ton en avril 2013, en marquant pour la première fois la volonté de l'Etat de se doter de capacités offensives et non plus seulement défensives en matière de cyberdéfense. Dix mois plus tard, les cinquante mesures contenues dans le pacte 2014-2016 qui sera présenté ce 7 février par Jean-Yves Le Drian à Cesson-Sevigné (Ille-et-Vilaine) traduisent cette volonté. Pour leur grande majorité, elles visent à durcir le niveau de sécurité des systèmes d'information et les moyens de défense du ministère, qui a fait l'objet de quelque 800 attaques informatiques en 2013, et de ses partenaires stratégiques.

"Aujourd'hui ces attaques on les contient, elles n'ont pas d'effet particulièrement destructeur parce qu'on est organisé pour les maîtriser", assure-t-on au ministère. "L'objectif du pacte, c'est que dans le temps, face à des attaques de plus en plus sophistiquées, on reste à la pointe et on ait des équipements de plus en plus performants."

Au total, un milliard d'euros va être consacré à la cyberdéfense, dont plus de 400 millions d'euros porteront sur l'industrie via des équipements de lutte contre les cyberattaques : téléphones sécurisés, équipements de type pare-feux, chiffreurs, renforcement de l'emploi de la cryptographie des échanges, détection et surveillance des réseaux.

DES JURISTES SPÉCIALISÉS RECRUTÉS

En France, le nombre d'attaques traitées par le Centre d'analyse de lutte informatique défensive, le Calid, est passé de 196 en 2011 à 420 en 2012. A l'heure actuelle, très peu de plaintes déposées par le ministère auprès de la gendarmerie après des attaques dites "de bas niveau", comme des défigurations de sites ou la mise en ligne de faux comptes sur les réseaux sociaux, aboutissent. "*L'identification de la source, on y arrive, mais être capable d'apporter une preuve au sens juridique du terme, c'est extrêmement difficile parce que quelqu'un qui fait bien les choses, il va rebondir sur des serveurs qui sont un peu partout dans le monde*", dit Guillaume Poupard, responsable du pôle de sécurité des systèmes d'information à la Direction générale de l'armement (DGA). Des juristes spécialisés vont donc être recrutés et l'ensemble des juristes du ministère seront quant à eux formés.

Dans les affaires plus sensibles, qui menacent directement une capacité militaire, la direction de la protection et de la sécurité de la défense (DPSD) est alertée pour déterminer s'il s'agit d'une tentative de compromission menée par des services. "*Pour nous, une affaire grave c'est une affaire où un bateau se retrouve à la mer sans protection, où un avion de combat ne peut plus décoller, où le coeur stratégique se retrouve compromis, ça c'est extrêmement grave et il n'y a pas ça dans les 800 attaques*" recensées en 2013, souligne Guillaume Poupard. "*Tout l'enjeu, c'est de faire en sorte que ce coeur stratégique ne soit pas touché par les attaques, y compris en tenant compte d'attaquants de très haut niveau*."

PRIORITÉ À LA FORMATION

Pour y parvenir, le ministère mise entre autres sur la sensibilisation et la formation de son personnel aux règles de base à respecter sur internet. "*Le premier rempart, c'est le comportement du personnel du ministère de la Défense*", souligne le contre-amiral Arnaud Coustillière, officier général en charge de la cyberdéfense à l'état-major. "*On peut mettre tous les systèmes que l'on veut, si les gens n'ont pas les bons réflexes, cela ne sert à rien.*" Des formations vont être menées suivant le profil du personnel, du simple utilisateur au spécialiste technique et à l'ingénieur en passant par le chef militaire.

Un pôle d'excellence dédié à la formation, l'entraînement ainsi que la recherche et développement en cyberdéfense va être créé autour de Rennes dans une région qui accueille actuellement l'école des transmissions, le centre de la Direction générale de l'armement (DGA) ou encore l'école de Saint-Cyr. Dans le même temps, la recherche va être encouragée et le nombre de thèses soutenues par le ministère et approfondissant l'expertise va être multiplié par deux entre 2014 et 2019. Les effectifs du Calid vont être multipliés par six, passant de 20 à 120, indique-t-on au ministère. Les échanges vont s'intensifier avec l'ANSSI (agence nationale de sécurité des systèmes d'information) qui dépend de Matignon pour protéger les opérateurs stratégiques.

Contrairement aux Américains, aux Allemands ou aux Britanniques, "*la France a pris conscience des risques il y a très peu de temps*", estime Jean-François Beuze, président de la société de conseil informatique Sifaris et spécialiste des questions de cybersécurité. "*L'important aujourd'hui c'est de protéger des entreprises vitales à l'activité de l'état, les opérateurs, les administrations, les banques, c'est de véhiculer les bonnes pratiques*", ajoute-t-il. Les ministres de la Défense de l'Otan ont approuvé pour la première fois en juin dernier la création d'une force d'action rapide permettant de protéger les réseaux

Avec Reuters (Marine Pennetier, Yves Clarisse)

Partagez l'info :

DANS LA MÊME RUBRIQUE

Un rapport dénonce l'illégalité d'un programme de […]
24/01/2014

Les grands acteurs du net condamnent l'adoption de la loi de […]
11/12/2013

Ce Prism à la française caché dans la loi de programmation […]
27/11/2013

Affaire PRISM : les CNIL européennes lancent une vaste […]
19/08/2013

PUBLICITÉ

RÉAGISSEZ À CET ARTICLE

Pseudo (obligatoire) **Email** (obligatoire) - ne sera pas visible

Votre commentaire (obligatoire) - 100 caractères minimum

COMMENTER