Hacker éthique : la législation française enfin claire ?

En complétant le code de la défense, la loi du 7 octobre 2016 pour une République numérique entérine la protection des hackers éthiques. En tout cas ceux qui signalent une faille informatique découverte par leurs soins à l'Agence nationale pour la sécurité des systèmes d'information (Anssi). La législation confirme ainsi le rôle central de cette dernière dans le signalement des vulnérabilités.

« *Ce texte va surtout permettre une officialisation* », explique à *Silicon.fr* François Coupez, avocat associé du cabinet Atipic. « *L'Anssi apparaît bien comme le second point de contact officiel, en plus du responsable du système d'information objet des vulnérabilités* ». Ce point de contact « *est utile pour les cas où les 'hackers éthiques' supposeraient qu'ils ne peuvent joindre directement l'entité dont le SI est vulnérable, quelle qu'en soit la raison : responsable supposé peu réceptif, responsable déjà contacté en vain, etc.* ».

Protéger le hacker dit « éthique »

Pour distinguer le hacker éthique du pirate (l'article 323-1 du code pénal sanctionne le piratage frauduleux d'au moins deux ans d'emprisonnement et de 60 000 euros d'amende), l'article 47 de la loi numérique complète le code de la défense par un article L2321-4 ainsi rédigé :

« *Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données.*

L'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée.

L'autorité peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace mentionnés au premier alinéa du présent article aux fins d'avertir l'hébergeur, l'opérateur ou le responsable du système d'information. »

Sécuriser les agents de l'Anssi

Rappelons que l'article 40 du code pénal cité dans cet article L2321-4 indique : « *Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs.* »

Or, dans la loi portée par Axelle Lemaire, cette obligation prévue à l'article 40 ne s'applique pas aux *white hats*. Ce qui arrivait déjà, en fait, avant la promulgation du texte. « *D'après ce qu'a pu indiquer à certaines occasions l'Anssi elle-même, la pratique interne était déjà de ne pas appliquer l'article 40 dans les hypothèses similaires à celles visées par cet article L2321-4 du code de la défense nouvellement créé. Et ce afin de faciliter les remontées d'informations. Ce que la loi République numérique légitime dorénavant via cet*

article, et c'est une très bonne chose pour la sécurité juridique des agents de l'Anssi », ajoute François Coupez.

Anssi plateforme

La loi apporte donc une sécurité juridique aux agents et permet aux hackers éthiques d'éviter la sanction pénale… À la condition que la faille découverte dans un système soit signalée dans la foulée à l'Anssi, sans que l'information ait été rendue publique préalablement par le hacker.

Malgré toutes ces précautions, un dépôt de plainte contre le hacker intrus par le responsable du SI en question est toujours possible. Cependant, *« l'intervention de l'Anssi pourra être de nature à tempérer les ardeurs de l'entreprise [ndlr: ciblée par l'intrusion] lors d'une éventuelle plainte, et aboutir, là aussi, à une meilleure protection des white hats »*, expliquait déjà l'avocat dans une tribune, en mai dernier.

Il explique aujourd'hui que l'Anssi s'organise pour *« centraliser en un point de contact unique les remontées d'informations »*. *« L'avenir et l'Anssi nous diront si le volume de signalement des vulnérabilités remontées par ce canal a un impact réel sur l'accroissement de la sécurité des SI »* des organisations.

Lire aussi :

Y-a-t-il une place pour les white hats dans la République numérique ? (tribune)

Lanceurs d'alerte : des conséquences floues pour les DSI

Administrateur système : n'est pas lanceur d'alerte qui veut ! (tribune)