Hacking des élections : les partis politiques français sont-ils prêts ?

Dans une conférence de presse, l'Anssi (Agence nationale de la sécurité des systèmes d'information) a confirmé avoir organisé une réunion fin octobre avec les partis politiques français, afin de les sensibiliser aux risques pouvant entourer le processus électoral qui doit déboucher sur l'élection du prochain président de la République, en mai prochain. Comme l'expliquaient nos confrères de *l'Express* fin octobre, les présidents de 13 formations politiques de la représentation nationale et des 11 groupes parlementaires de l'Assemblée et du Sénat ont été conviés à un séminaire dédié, qui s'est tenu le 26 octobre dernier.

« *Une telle initiative pouvait paraître inhabituelle de la part de l'Anssi. Mais, au vu de ce qui défrayait la chronique aux Etats-Unis, après les attaques sur les organisations en charge de la primaire outre-Atlantique, cela nous semblait nécessaire, même si cela ne relevait pas de notre stricte compétence* », explique Louis Gautier, le secrétaire général de la défense et de la sécurité nationale, à l'origine de cette invitation à laquelle ont répondu l'ensemble des partis (Front National excepté).

« *Hors de notre zone de confort* »

L'initiative du Secrétariat général de la défense et de la sécurité nationale, dont dépend l'Anssi, s'explique, selon Louis Gautier, par le caractère relativement nouveau des événements se produisant aux Etats-Unis. « *Nous nous étions polarisés sur la fraude électorale, alors qu'on parle cette fois plutôt d'ingérences extérieures venant perturber les élections* », dit-il. Aux Etats-Unis en effet, les attaques se sont concentrées non pas sur les machines à voter, mais plutôt sur les organisations chargées d'organiser la primaire et sur les pratiques d'une candidate en particulier, Hillary Clinton.

« *En France, nous travaillons depuis longtemps avec le ministère des Affaires étrangères sur la question du vote électronique des Français de l'étranger (les seuls pour l'heure à utiliser ce mode d'expression, NDLR),* commente Guillaume Poupard, le directeur de l'Anssi. *Mais, là, nous sommes hors de notre zone de confort, avec des risques plus complexes. C'est un des messages que nous avons voulu faire passer aux partis politiques.* »

L'Ukraine déjà

La caractère inédit des attaques dont a été victime le camp démocrate reste à relativiser. Si c'est effectivement la première fois qu'un président américain est élu en partie avec l'aide de coups de pouce cyber d'une puissance étrangère – Obama désignant clairement Vladimir Poutine comme étant à l'origine des cyberattaques -, ce n'est pas la première fois que des hackers sont employés pour perturber une élection. En 2014, en Ukraine, un hacking sophistiqué avait mis les systèmes de la commission électorale du pays à genoux, à quelques jours d'un vote crucial. Selon un enquêteur ukrainien, s'exprimant sur NBC News, les traces laissées par ce piratage renvoient à APT 28 ou Fancy Bear, un groupe de hackers réputé lié au renseignement militaire russe (GRU) et qui est aussi intervenu aux Etats-Unis dans les piratages contre le camp Clinton.

Un article de *Bloomberg* rappelle aussi les interventions multiples d'un groupe de hackers sud-américains, des mercenaires pilotés par un certain Andres Sepulveda, dans nombre d'élections sur le continent. Dont récemment une opération en faveur du président mexicain Enrique Peña Nieto, élu en 2012. Au menu des équipes de Sepulveda : hacking de smartphones, clonage de sites Web, piratage des équipes adverses, publication de hoax sur les réseaux sociaux…

PS : une authentification qui fait hurler la Cnil

Si l'Anssi a donc fait passer aux partis français un certain nombre de messages, et distillé des conseils en matière de solutions à déployer, elle n'assure ni suivi, ni contrôle des éventuelles actions engagées. « *L'Etat n'est pas fondé à agir par la contrainte dans ce domaine* », relève Louis Gautier. Pas question donc pour l"Anssi d'aller voir ce qui est réellement déployé. Si Guillaume Poupard précise qu'il n'a pas eu l'impression d'avoir affaire, au cours de ce séminaire, à des gens « *naïfs* » sur la cybersécurité, il reconnaît toutefois que la tâche des informaticiens en charge de la sécurité au sein des partis n'est pas forcément aisée, par exemple en raison de la présence de VIP en interne peu enclins à se plier à des contraintes qui leur apparaîtraient superflues.

Plus globalement, c'est le niveau de préparation des partis à des menaces sophistiquées – comme celles de APT 28 ou de son cousin, APT 29, lui aussi réputé proche de Moscou – qui pose question. En octobre – ironiquement environ à la même date que le séminaire de l'Anssi -, le Parti Socialiste recevait un avertissement public de la Cnil en raison d'une grave faille de sécurité affectant l'application d'adhésion en ligne. En l'occurrence, des liens personnalisés envoyés aux aspirants socialistes donnaient accès à l'ensemble des données confidentielles stockées par le site Web dédié à l'adhésion.

Lors d'un contrôle rue de Solférino, la Cnil a vertement critiqué la méthode d'authentification utilisée, reposant sur l'intégration du secret d'authentification de l'utilisateur dans l'URL et sur l'emploi de l'algorithme obsolète MD5 (sans salage qui plus est). Des pratiques qui, à tout le moins, ne dénotent pas d'un sens aigu de la cybersécurité, ni d'une application empressée des bonnes pratiques les plus récentes en la matière. Pour rappel, les premières alertes sur la faiblesse de MD5 remontent au milieu des années 90 (Lionel Jospin était premier secrétaire). L'intérêt du salage, ajoutant un aléa afin de retarder les attaques par force brute, en complément d'un hachage est lui reconnu par les spécialistes depuis les années 70 (François Mitterrand dirigeait la rue de Solférino).

A lire aussi :

L'élection de Trump brouillée par le piratage

Piratage de campagne par la Russie : Trump n'y croit pas, Obama enquête

Sécurité : la CNIL vote un carton jaune au Parti Socialiste

Crédit photo : GlebStock / Shutterstock