Le Magazine de Décembre 2011

Guerre économique : les défis de la cybersécurité

Christophe-Alexandre Paillard

Le développement d'internet a ouvert la voie à un nouveau type d'attaque que l'on peut qualifier de guerre. Les menaces sont rée pour les entreprises stratégiques et les systèmes informatiques nationaux.

Au printemps 2007, les Etats du monde entier ont pris la mesure de la en puissance des risques du cybermonde. Cette année là, l'Estonie a attaque sans précédent. Elle faisait suite au transfert d'un monument à gloire de l'Armée rouge qui a déclenché la colère de la minorité russop d'Estonie. Des hackers russes ont pris pour cibles des journaux, des b et des institutions gouvernementales, les forçant à fermer leurs sites p éviter le vol de données et un blocage complet de leurs serveurs.

Cet évènement a conduit l'OTAN à créer une agence de cybersécurité 2008 basée à Tallinn. Des programmes ambitieux de définition de poli de cybersécurité ont été menés dans de nombreux Etats. La France s exemple dotée d'une stratégie pour se défendre et se protéger dans le cyberespace. Elle a créé l'ANSSI (agence nationale de la sécurité des systèmes d'information) le 8 juillet 2009.

Autre exemple, en juin 2010, un virus particulièrement sophistiqué dénommé Win32 Stuxnet s'est attaqué en Iran à de systèmes d'automatismes équipés d'automates programmables en provenance de la société allemande Siemens. Ce portait en lui deux codes malveillants. L'un a permis de détruire le système de commande des centrifugeuses présente le centre d'enrichissement de Natanz. L'autre a ciblé les turbines à vapeur fabriquées par l'industriel russe Power Mac la centrale nucléaire de Busher, à partir des technologies de Siemens. Les centrifugeuses iraniennes ont été graveme endommagées et le cycle d'enrichissement d'uranium engagé par l'Iran a probablement été retardé de trois ans.

Les menaces ne faiblissent pas. A l'automne 2010, Bercy a été victime d'attaques. Le 29 septembre 2011, Areva a rec avoir été victime d'attaques durant deux ans sur l'ensemble de ses installations informatiques. Le développement d'int donc ouvert la voie à un nouveau type d'attaque que l'on peut qualifier de guerre, forçant tous les pays à revoir leurs s de sécurité. Toutefois, les pirates ne lancent jamais une attaque directe depuis leurs propres ordinateurs : ils piratent l ordinateurs d'autrui afin d'en prendre le contrôle au moment choisi, ces ordinateurs étant des zombies. Le temps entre piratage d'un ordinateur et le moment où celui-ci est utilisé pour lancer une attaque rend toute possibilité de remonter l'ordinateur de l'attaquant particulièrement difficile.

La compromission d'un ordinateur peut se faire de différentes manières : en ouvrant une pièce jointe d'un email, qu'il s d'un programme, mais plus sournoisement également s'il s'agit d'un pdf infecté, ou encore d'un contenu multimédia (v photo, mp3), via une clé USB, depuis un site internet infecté, etc. Car les logiciels d'un ordinateur ne sont jamais exem failles de sécurité, connues ou non encore divulguées, à partir desquelles un malware pourra en prendre le contrôle.

Parmi les modes de cyberattaques, on peut distinguer celles utilisant les bombes logiques : le malware ayant infecté le ordinateurs qui vont participer à l'attaque est programmé de façon à déclencher celle-ci à une date prédéfinie à l'avanc évoluées sont les attaques lancées à partir de botnet, un ensemble d'ordinateurs compromis auxquels les pirates sont capables de transmettre des commandes depuis internet. L'attaque dite de déni de service distribué peut faire appel à centaines de milliers d'ordinateurs manipulés, avec pour résultat que le site web attaqué sera injoignable car inondé p de demandes.

Patrick Pailloux, directeur de l'ANSSI, rappelait en octobre 2010 qu'un nombre très important d'attaques à des fins d'espionnage étaient détectées par l'administration et les entreprises. Il évoquait la nécessité d'appliquer des « règles d'hygiène informatique élémentaire » avec comme exemples « la limitation des droits d'accès, l'analyse des mouveme suspects sur les systèmes d'information, la sanctuarisation des éléments les plus critiques comme les dispositifs de ge des droits d'accès, l'application régulière des correctifs de sécurité ». On ne saurait mieux dire.

Christophe-Alexandre **Paillard**, directeur des affaires juridiques, des affaires internationales et de l'expertise technolo la Commission Nationale de l'informatique et des libertés (CNIL), directeur de recherche à l'Institut Choiseul, est l'aute « Les nouvelles guerres économiques » (Editions Ophrys. Novembre 2011) qui traite notamment des liens entre les problématiques économiques et les questions de sécurité. www.ophrys.fr

Réagir à cet article

Vos commentaires