La cyberguerre est devenue une menace réelle

- Informatique - Sécurité Informatique -

Date de mise en ligne : mardi 10 août 2010

Spyworld Actu

Alors que l'Allemagne vient de révéler qu'elle était visée par des cyberattaques de grande ampleur, de nombreux pays s'organisent pour développer des capacités défensives et offensives

Le ministre allemand de l'intérieur, Thomas de Maizière, a fait état, lundi 9 août, d'une « augmentation dramatique des attaques » contre les réseaux allemands de téléphonie et Internet, en particulier ceux du gouvernement.

« Ministères, ambassades et administration sont victimes d'une offensive de grande envergure de piratage de leurs réseaux de communication », a-t-il déclaré au quotidien Handelsblatt. Il a demandé aux ministres et hauts responsables de l'administration de bannir l'usage des téléphones mobiles iPhone et BlackBerry pour protéger le pays d'une menace jugée « sérieuse ».

On le sait aujourd'hui, des pays et des entreprises sont l'objet d'attaques visant à empêcher, gêner ou détourner le fonctionnement de leurs systèmes d'information et de communication. Explications.

Qu'est-ce que la cyberguerre ?

Le concept de cyberguerre s'est imposé au printemps 2007, dans le sillage d'attaques informatiques ciblant les serveurs du ministère de la défense américain et l'Estonie. Cette cyberguerre - la première à avoir été identifiée - n'a fait aucun mort et les structures physiques du pays sont restées intactes.

Certains spécialistes décrivent ainsi les cyberattaques comme des « armes de nuisance massive », par opposition aux armes de destruction massive et à la guerre nucléaire. « Qu'une bande de hackers mette à plat votre système informatique, c'est affreux, mais ça n'équivaudra jamais à une arme qui rase New York », affirme l'expert Roger Molander.

Que recouvrent exactement les cyberattaques ?

Les experts en sécurité reconnaissent trois strates constitutives du cyberespace : la strate physique (infrastructures, câbles, routeurs et commutateurs) ; la strate sémantique, qui désigne les données brutes véhiculées par le cyberespace et exploitées par les humains ou les machines ; la strate syntaxique, qui met en liaison les deux autres en formatant les informations et en leur conférant des standards et des protocoles (tel le TCP/IP sur lequel repose Internet). Ces informations peuvent aller du simple courriel jusqu'aux images de reconnaissance transmises par un drone aérien à sa station de contrôle en Irak.

L'expert Jean-Loup Samaan (1) distingue les attaques contre la strate sémantique, qui consistent à voler, modifier ou supprimer des informations ; les attaques contre les strates syntaxiques, qui entendent endommager la diffusion des données via des virus ou autres outils de brouillage ; enfin, les attaques contre la strate physique, qui ciblent des infrastructures réelles et impliquent donc un déploiement physique de l'ennemi.

Créer des outils tels que virus, chevaux de Troie et interdiction d'accès s'avère aujourd'hui plus simple et moins coûteux que de se munir d'artillerie ou d'obusiers. Ces intrusions informatiques peuvent causer une réelle nuisance.

Quels sont les cibles potentielles ?

Au coeur des infrastructures vitales ou stratégiques (industries nucléaire et chimique, systèmes financier, alimentaire, énergétique et sanitaire, trafic routier, réseaux de transport, gouvernement, police, armée), les systèmes de contrôle et de communication (Scada) constituent des cibles potentielles, car elles sont indispensables au bon fonctionnement de la vie quotidienne et donc de l'économie.

Au Brésil, en novembre 2009, le cyberpiratage d'une centrale hydroélectrique a privé pendant trois jours, une dizaine de villes et leurs 60 millions d'habitants de transports en commun, de feux de circulation, de télécommunications et d'ascenseurs. Dépôts de carburants, banques, centres commerciaux et sites industriels par milliers furent paralysés ou ralentis. Parce qu'elles sont liées à l'interface informatique et qu'elles fonctionnent sur un mode civil, la vulnérabilité des infrastructures critiques semble importante face à une cyberattaque.

Jusqu'où pourraient aller des agresseurs ?

Le cyberespace abrite une grande variété de menaces et d'agresseurs potentiels ou réels. Les motivations, les tactiques et les objectifs diffèrent selon qu'il s'agit d'organisations non étatiques (criminelles, terroristes), d'États en conflit, de hackers isolés ou de collectif « hacktiviste ».

Pour une organisation non étatique malveillante, souligne Charles Bwele, consultant en technologies de l'information (2), « une cyberattaque contre une infrastructure vitale constituerait un instrument de terreur ou de représailles. Pour des États en conflit, une telle action s'inscrirait plus probablement dans une action militaire globale. Pour un hacker isolé ou pour un collectif "hacktiviste", ce serait une forme délirante d'exploit technique. »

La dimension logistique et technologique, ainsi que le coût de la préparation rendent cependant difficile une cyberattaque de grande envergure par des terroristes, par ailleurs dépendants, eux aussi, du cyberespace.

Comment les États se protègent-ils ?

La sécurité des systèmes d'information et de communication fait aujourd'hui intégralement partie de la stratégie de défense des gouvernements. Pour les militaires, le cyberespace devient le cinquième « domaine » de la guerre, après la terre, la mer, l'air et l'espace. Aux États-Unis, Barack Obama en a fait une priorité nationale et a nommé, en janvier, un coordonnateur pour la cybersécurité à la Maison-Blanche.

Au mois de mai, le Pentagone a créé Cybercom, un nouveau commandement militaire chargé de défendre les réseaux informatiques militaires américains et de développer des capacités offensives, sous l'autorité du général Keith Alexander, par ailleurs directeur de la National Security Agency (NSA). La Grande-Bretagne dispose d'un « centre d'opérations » spécialisé au sein de son quartier général interarmées.

Quant à la Chine, elle ne fait pas mystère de ses ambitions dans le domaine de la guerre de l'information, l'objectif figurant dans le livre blanc sur la politique de défense publié en 2006. L'Armée populaire chinoise (APL) dispose d'une structure dédiée au sein de son état-major. Quelque 20 000 « hackers patriotiques » font partie d'une nébuleuse de deux millions d'agents, permanents ou occasionnels, des services de renseignement chinois. À la recherche d'une économie de moyens, l'APL met en pratique une doctrine de « dissuasion asymétrique » en développant une capacité de nuisance à travers quelques techniques de pointe.

De nombreux autres pays s'organisent pour la cyberguerre, en particulier la Russie, Israël, la Corée du Nord et l'Iran.

Par ailleurs, en l'absence de frontières étatiques dans le cyberespace, une coordination des efforts au niveau international s'est développée au sein de l'Otan et de l'UE.

(1) « Mythes et réalités des cyberguerres », revue Politique étrangère, Hiver 2008.

(2) Revue Défense nationale, juin 2010.

Post-scriptum :

http://www.la-croix.com/La-cybergue...