CERCLE DES PARTENAIRES

IHEDN

FONDATION EADS

# CHAIRE CASTEX

# de

# CYBERSTRATÉGIE

# Cyberdéfense : une complexité exponentielle

Malgré leur retard technologique et leur coût élevé, les moyens de défense des systèmes d'information peuvent créer des conditions rendant difficiles les cyberattaques, qui deviennent de plus en plus subtiles.

Laurent Bloch, directeur du système d'information de l'université Paris-Dauphine, a fait le point sur les menaces, vulnérabilités et contremesures, au cours d'une conférence organisée le 19 avril 2012 à Paris par la chaire Castex de cyberstratégie. Le professeur François Géré est également intervenu.

**Les attaques**, souvent d'origines inconnues ou indirectes, ciblent autant les entreprises privées que les Etats (*voir revue téléchargeable juin 2011 p.9-16*). Elles font perdre des sommes considérables, notamment aux banques (fraudes à la carte bleue) et à l'industrie pharmaceutique (pillage de recherches non encore rendues publiques). Le ministère américain de l'énergie, responsable d'une partie du programme nucléaire militaire, reçoit dix millions d'attaques par jour, dont 95 % proviennent… des Etats-Unis ! Depuis dix ans, les efforts de recherche et le développement sur les attaques des systèmes d'information sont plus importants que sur leur sécurisation. La productivité de telles entreprises à but lucratif est élevée, surtout en Ukraine, Russie et Chine où les salaires des ingénieurs sont bas. La frontière entre la cybercriminalité et l'agression à des fins militaires devient poreuse, en raison de la similitude des méthodes. L'agresseur, pragmatique, cherche la faille pour s'introduire dans un système protégé ou le mettre hors service. Il observe le réseau et cherche à dérober les données qui y circulent. Au départ, l'attaque est aléatoire (virus ou spam), mais si elle réussit, elle devient systématique. Des robots scannent automatiquement des sites internet.

**Les vulnérabilités** face aux menaces terroristes, nucléaires, radiologiques, chimiques, biologiques et informatiques, sont étudiées par tous les ministères de l'Intérieur ou agences de sécurité étatiques depuis les attentats terroristes du 11 septembre aux Etats-Unis. Celles du cyberespace sont infinies et augmentent de manière sensible. Les moyens informatiques sont d'acquisition aisée, car réalisés à bas coûts et sans préoccupation de sécurité. Les téléphones portables, objets à

protéger en raison de toutes les données personnelles et des accès divers qu'ils renferment, se perdent ou s'oublient facilement. Quant aux ordinateurs, les attaquants attendent les mises à jour des fabricants et les comparent avec les appareils des nombreux utilisateurs qui ne les ont pas encore effectuées. Ainsi, l'interposition d'un intrus, susceptible de modifier le contenu d'un ordinateur, sera très difficile à détecter. Un « espion dactylographique » (« keylogger ») introduit dans un ordinateur peut retrouver les mots de passe et leurs modifications successives et donc connaître toutes les données personnelles de l'utilisateur. « *Les ripostes législatives sont inappropriées* », estime Laurent Bloch. En effet, pour réduire les vulnérabilités informatiques des lois ont été récemment débattues ou votées aux Etats-Unis et en France pour protéger l'industrie du divertissement, mais elles seront difficiles à faire appliquer par les autorités judiciaires et faciles à contourner. En conséquence, elles risquent d'avoir des effets négatifs sur internet. Si le DNS (système américain de gestion des adresses des ordinateurs connectés à un réseau) est soumis à la censure, des DNS alternatifs apparaîtront, compromettant l'ubiquité et l'universalité d'internet. La Chine a déjà créé un système qui lui permet d'échapper au DNS.

**La protection** à 100 % n'existe pas, mais elle peut s'améliorer sur l'accès au système et par les deux types de chiffrement (cryptographie) du canal de communication au réseau. Celui dit « symétrique » consiste en une « clé » secrète, partagée entre deux personnes qui doivent se rencontrer Celui dit « asymétrique » repose sur deux clés : l'une, publique pour le chiffrement, l'autre, privée et secrète, pour le déchiffrement. La signature électronique nécessite l'emploi d'un algorithme (suite d'opérations pour résoudre un problème) dit de « condensation ». Ce dernier détermine les « empreintes » ou « condensats » qui authentifient un message envoyé après un chiffrement asymétrique. Sur internet, la garantie de confidentialité des échanges privés, commerciaux en ligne, administratifs et médicaux, repose sur la confiance accordée aux fabricants de clés et à l'autorité de certification qui les publie dans un annuaire. Les algorithmes de chiffrement vivent environ une quinzaine d'années, avant d'être surclassés par des versions beaucoup plus complexes et font régulièrement l'objet d'attaques pour les « casser », notamment de la part d'experts chinois. Aujourd'hui, la protection des serveurs et des réseaux, devenue insuffisante, doit se compléter par celle des contenus, notamment des « Smartphones », mobiles divers et autres matériels privés volés. Le DVD d'un film, protégé par un DRM (dispositif de gestion des droits numériques), contient le logiciel de déchiffrement

et … la clé secrète de chiffrement ! Un « expert » qui l'a acheté peut donc prendre tout son temps pour analyser son programme et tenter de le casser. Un système d'armes contient un dispositif analogue, mais cette fois, l'acquéreur, généralement étatique, essaiera de découvrir ses secrets en vue de les copier. Par contre, le système « Skype » de téléphonie par internet, utilisé par 663 millions de personnes dans le monde, est particulièrement bien protégé. Sur un plan plus vaste, le ministère américain de la Sécurité intérieure a mis sur pied le programme « Einstein », qui réagit instantanément à toute activité suspecte sur le réseau d'une agence ou d'une administration fédérale. A terme, il compte l'appliquer aux systèmes de gestion des infrastructures stratégiques, comme l'eau, l'électricité et les télécommunications. En outre, selon Laurent Bloch, l'agence américaine de sécurité nationale NSA, responsable de la collecte et de l'analyse de toute forme de communications, « *a certainement déjà réussi à casser les systèmes cryptés, mais ça, on ne le saura jamais !* »

**Loïc Salmon**

*Le Cercle des partenaires de l'IHEDN (Institut des hautes études de défense nationale) et la Fondation d'entreprise EADS se sont associés en novembre 2011 pour créer la « chaire Castex de cyberstratégie », du nom de l'amiral Castex, fondateur en 1936 du Collège des hautes études de défense nationale qui deviendra l'IHEDN en 1948. La chaire concentre ses recherches sur l'étude et le suivi des menaces, le coût des cyberattaques, les enjeux politiques et stratégiques, les réponses juridiques et réglementaires aux conflits. Son titulaire est le professeur François Géré, directeur de recherches à l'université Paris III. Fondée en 2004, la Fondation d'entreprise EADS a notamment soutenu plus de 110 projets de recherches scientifiques et économiques et créé huit chaires de recherche et d'enseignement.*