La sécurité est liée à la culture du risque

La sécurisation de l'information ne peut se résumer à des prouesses technologiques ou à des considérations budgétaires.

BEN MUSSO
Chief Security Officer, REYL & Cie

Enoncée voilà maintenant 50 ans, la loi de Moore prédisait que le nombre de transistors des microprocesseurs sur une puce de silicium allait doubler environ tous les deux ans permettant ainsi la fabrication d'ordinateurs moins coûteux et plus puissants. Il semblerait que cette règle, proposée par Gordon Moore, un des fondateurs d'Intel, peut tout aussi bien s'appliquer à la cybercriminalité dont la rentabilité est supérieure à celle du trafic de drogue. Selon Edward Amoroso, RSSI de l'opérateur américain AT&T, le montant généré par la cybercriminalité serait de 1000 milliards de dollars, ce chiffre pourrait être sans doute encore plus élevé si toutes les sociétés dans le monde communiquaient sur les pertes financières liées à la cybercriminalité[1].

Le prestige de certaines cibles ne donne que plus d'ampleur au phénomène. Home Depot, Icann, Sony Pictures, ATM, eBay, Le Financial Times ou encore JP Morgan Chase: les pirates informatiques n'hésitent pas à s'en prendre aux enseignes les plus célèbres. Le phénomène a atteint une telle importance qu'un rapport de l'OCDE, en 2011, classait la cybercriminalité parmi l'une des cinq plus grandes menaces planant sur l'économie mondiale.

Les banques, et le secteur financier dans son ensemble, sont forcément parmi les entités les plus exposées. Selon le cabinet PricewaterhouseCoopers, le quart des cyberattaques connues menées en 2013 à travers le monde auraient été dirigées contre elles. Autrefois, le butin des «casses du siècle», version «brick and mortar», s'élevait tout au mieux à quelques dizaines de millions de francs, de dollars ou d'euros. A Genève, l'UBS avait été ainsi délestée, en 1990, de 31 millions de francs en l'espace d'un week-end. Un montant cependant dérisoire en comparaison avec les sommes considérables en jeu aujourd'hui. Ainsi, l'an passé un groupe de pirates informatiques a réussi à détourner plusieurs centaines de millions de dollars après s'être infiltré, sur deux années, dans une centaine de banques. Les souris et les claviers d'ordinateurs occasionnent maintenant beaucoup plus de dégâts que les burins des marteaux-piqueurs ou les mèches des perceuses.

A l'ère du numérique, la multiplication des voies d'accès et des protocoles de communication obligent les entreprises financières à déployer d'énormes moyens pour préserver la confidentialité et l'intégrité de leurs données, ainsi que pour garantir la disponibilité de leurs systèmes d'information. Malheureusement, si la cybercriminalité est en plein essor, les budgets alloués à la sécurité de l'information ne suivent pas la même courbe de croissance. Malgré les enjeux, la direction opérationnelle de nombreux établissements considère les outils de lutte contre ce fléau comme des gadgets onéreux. Elle ne mesure pas encore les dangers encourus en raison de cette attitude.

On se croirait presque revenu à la fin des années 80, lorsque l'informatique de bureau a connu de profonds bouleversements avec l'arrivée des réseaux locaux, des progiciels de gestion puis des applications client/serveur. A l'époque, beaucoup d'entreprises n'avaient pas évalué à sa juste mesure les conséquences de ce tournant décisif, tardant à moderniser leurs systèmes d'information. Il en va de même aujourd'hui pour la sécurité de l'information, qu'il est préférable de ne pas catégoriser comme une mode passagère. Plutôt qu'une pièce «ajoutée», il s'agit d'une pièce essentielle qui doit trouver naturellement sa place à la charnière du dispositif des Technologies de l'Information et de la Communication (TIC).

ELLE NE DOIT PAS ÊTRE VUE COMME UN CENTRE DE COÛTS MAIS COMME UN MAILLON FORT DU PROCESSUS DE CRÉATION DE VALEUR.

Dans l'échelle des priorités, il est grand temps de la faire remonter au plus haut, exercice particulièrement délicat. Face aux menaces résultant de l'imagination débordante des pirates informatiques et aux ressources dont ils disposent (temps et main-d'œuvre illimités, outils logiciels peu coûteux), il est toujours plus compliqué de se protéger. Certes, que ce soient les pare-feu, les contrôles d'accès ou les systèmes de détection d'intrusions, les solutions ne manquent pas, mais aussi sophistiquées soient-elles, elles ne suffisent pas. En effet, il est devenu tout aussi important, sinon plus, de se protéger des risques provenant de l'intérieur même de l'entreprise. Les comportements inadéquats des employés, volontaires ou non, sont souvent à l'origine des incidents. Il suffit par exemple de l'ouverture inconsidérée d'un email infecté pour créer une brèche dans le système de sécurité de l'entreprise. Mais dans ce cas, il existe des solutions techniques efficaces telles que les systèmes de filtrage des emails (email gateway, email filtering).

L'existence d'une culture du risque, liée à la sécurité de l'information, est la base d'un système pour se défendre face à la cybercriminalité. Cette culture du risque, c'est-à-dire l'appropriation, par l'entreprise, des enjeux de la sécurité de l'information, doit être communiquée et inculquée à tous les acteurs concernés, membres de la direction opérationnelle et collaborateurs.

La sécurité de l'information ne peut se résumer à des prouesses technologiques ou à des considérations budgétaires. Les responsables de la sécurité ou de l'IT doivent pouvoir s'appuyer sur des décideurs qui se sentent concernés. Celle-ci ne doit pas être vue comme un centre de coûts, mais comme un maillon fort du processus de création de valeur. La sécurité réclame l'adhésion de tous. Après tout, sa finalité n'est autre que la protection de l'entreprise, de ses clients, de son patrimoine, de ses collaborateurs et de leur sphère privée et, enfin, de ses actionnaires. ■

(1) http://www.silicon.fr/la-cybercriminalite-rapporte-plus-que-la-drogue-55193.html

---

SOLANGE GHERNAOUTI
Professeure, directrice du Swiss Cybersecurity Advisory & Research Group, HEC – Unil (www.scarg.org)

CYBERSÉCURITÉ

La guerre psychologique passe aussi par là

Il y a trois sortes d'organisations: celles qui ont déjà été piratées, celles qui le sont mais qui ne le savent pas et celles qui vont l'être. Il y a celles qui pensent que cela n'arrive qu'aux autres, celles qui mettent des mois à identifier l'intrusion dans leurs systèmes et celles qui sont immédiatement confrontées à la réalité des cyberattaques. C'est le cas notamment lors de la prise en otage des ressources informatiques et d'un chantage menaçant de rendre public des données sensibles volées.

Menace la plus probable à laquelle nous sommes tous exposés. Le mois dernier, la Fédération de laboratoires d'analyse médical français (Labio.fr) a fait l'objet d'un piratage portant sur 40.000 identifiants (nom, prénom, login, mot de passe) et sur plusieurs milliers de bilans médicaux. L'entreprise a porté plainte, refusant de payer une rançon de 20.000 euros au groupe de cybercrimels rassemblés sous le nom évocateur de Rex Mundi (Roi du monde). Des données de santé de nombreux patients se sont retrouvées sur le Net, au grand désarroi de leurs propriétaires…

Dans un autre registre, la défiguration de sites web signée par l'Etat Islamique, dont font systématiquement l'objet les sites traitant de cybersécurité comme ceux appartenant à des institutions gouvernementales et privées de par le monde, est une menace omniprésente et une attaque directement identifiable. Bien que la motivation des terroristes ne soit pas liée, comme lors de la prise en otage des ressources informatiques, à un désir d'enrichissement, ces deux types d'attaques possèdent quelques points en commun, à savoir: l'intrusion illicite dans des systèmes informatiques et la possibilité qu'ils aient en plus été infectés par des logiciels malveillants (espiongiciel, cheval de Troie, virus, bombe logique, menaces persistantes…); L'exploitation de vulnérabilités; Le coût des cyberattaques porté par les victimes; La difficulté à assurer les cyber risques; La perte de confiance et une certaine déstabilisation économique et émotionnelle.

Il ne faut pas sous-estimer l'importance de l'impact psychologique des cyberattaques sur l'ensemble des acteurs, qu'ils soient monsieur et madame Toulemonde, dirigeants politique ou économique ou acteur institutionnel.

Les groupes terroristes l'ont bien compris et le cyberespace n'est pas uniquement réservé à la guerre économique ou à la surveillance de masse. Il est désormais également le moyen et la cible de la guerre psychologique, de la guerre d'influence. La guerre de l'information, par l'information, est devenue notre réalité. Un acronyme existe pour la désigner: CNI, *Computer Network Influence*. Des rumeurs peuvent faire varier le cours des actions, des pages Facebook de personnes décédées peuvent être alimentées comme si elles étaient toujours vivantes…

Tout internaute peut devenir un vecteur et une cible de cybermenace. Les Anonymous sont légion et peuvent se mobiliser via le Web, comme les terroristes d'ailleurs, pour s'attaquer à des symboles par des cyberattaques en déni de services.

«L'ennemi» nous connaît, nous nous sommes exposés volontairement sur le Web, les données dont il a besoin sont disponibles en libre accès sur le Net ou peuvent être achetées, voire piratées à des organisations qui ont su se les approprier, le plus souvent, à notre insu. Nous avons peut-être eu l'occasion de donner notre consentement à la collecte de nos données en contrepartie d'un service, toutefois, notre consentement a rarement été éclairé, méconnaissant sa porté et sa durée ou l'usage final des données exploitées. Le choix est souvent contraint, car la seule alternative au refus des conditions générales est de se passer du service, ce qui est parfois impossible.

Avec Internet nous avons ouvert la boite de Pandore. Désormais, il est plus important de se demander si nous sommes suffisamment robustes et résilient, que de s'interroger sur le fait que nous allons être éventuellement piratés. Oui nous sommes vulnérables, oui des cyberattaques ciblent nos systèmes.

Au delà de la recherche de responsabilité, et de savoir qui doit payer la sécurité, sommes-nous en mesure de faire face aux changements de paradigme que nous imposent les technologies de l'information, l'économie du numérique et la réalité des cyber risques? Sommes-nous capables de transformer la menace Cyber en opportunité? Sommes-nous suffisamment innovants, proactifs et réactifs pour penser la cybersécurité dont nous avons tous besoin? ■