S'adapter à la CYBER

Keren Elazari

Chaque appareil connecté est une cible potentielle pour les cybercriminels. Les gouvernements ne pourront sécuriser le cyberespace que si les particuliers sécurisent leurs propres équipements.

En termes de cybersécurité, aiment à dire les spécialistes, il existe deux types d'organisations : celles qui ont été touchées et celles qui ne le savent pas encore. Les récents titres de la presse tendent à leur donner raison. Des cybercriminels ont volé les informations des cartes de crédit et les données personnelles de milliers de clients de sociétés telles que les entreprises américaines Target et Home Depot (grande distribution) ou JPMorgan Chase (société de portefeuille). Les chercheurs en sécurité informatique ont découvert des failles fondamentales dans les constituants d'Internet, telle la vulnérabilité Heartbleed dans la bibliothèque de logiciels de cryptographie OpenSSL. Une destruction massive de données a obligé Sony Pictures Entertainment à revenir au papier et au crayon. Des criminels ont accédé aux données de plus de 80 millions de clients de l'entreprise américaine d'assurance maladie Anthem. Et il ne s'agit que des incidents les plus connus.

Dans les années à venir, les cyberattaques vont probablement s'intensifier. Le problème nous concerne tous. Nous sommes tous, d'une façon ou d'une autre, connectés au cyberespace – *via* les téléphones, les ordinateurs portables, les réseaux d'entreprise –, et donc exposés. Le piratage des réseaux, serveurs, ordinateurs personnels et comptes en ligne est devenu une ressource essentielle tant des cybercriminels que des services d'espionnage des États. Votre réseau local d'entreprise, votre PC de jeu deviennent autant d'outils supplémentaires dans l'arsenal des criminels – ou des cyberespions financés par le contribuable. Les ordinateurs compromis servent de tremplin pour l'attaque suivante ou deviennent les maillons d'un «botnet», un réseau malveillant de machines zombies contrôlées et louées à l'heure pour lancer des attaques par déni de service (qui rendent un service indisponible) ou distribuer des spams.

En réponse à de telles menaces, le réflexe des gouvernements consiste à militariser le cyberespace, à essayer de contrôler le monde numérique en s'appuyant sur des agences secrètes et des administrations centralisées. Mais cette approche ne fonctionnera jamais. Elle risque même d'empirer les choses. La cybersécurité est comme un problème de santé publique : seules, les agences de santé

GUERRE

gouvernementales n'ont pas les moyens d'arrêter la propagation des maladies. Elles ne peuvent remplir leur rôle que si les citoyens remplissent le leur.

Un cyberespace multiforme

Une difficulté pour protéger le cyberespace est que celui-ci n'est pas une entité unique. Le cyberespace est un vaste ensemble de systèmes interconnectés en perpétuelles mutation et croissance. Pour en prendre la mesure, il faut remonter un demi-siècle plus tôt, aux travaux de Norbert Wiener, professeur de mathématiques à l'Institut de technologie du Massachusetts. En 1948, Wiener a emprunté un terme du grec ancien pour décrire une nouvelle discipline qu'il développait : la cybernétique, ou l'étude du « contrôle et de la communication chez l'animal et la machine ». En grec ancien, *κυβερνήτης* désignait le timonier ou le pilote qui dirigeait et contrôlait les navires en Méditerranée. Par analogie, le cyberespace est l'ensemble des technologies électroniques et numériques interconnectées qui permettent le contrôle et la communication de tous les systèmes sur lesquels repose la vie moderne. Le cyberespace est constitué d'un large éventail de technologies de commande à distance et de communication, allant des pompes à insuline pilotées par radiofréquences aux satellites de géolocalisation GPS.

Le cyberespace n'est pas une eau internationale. Il ne s'agit pas d'un ensemble de territoires que des gouvernements ou des armées pourraient contrôler. La plupart des technologies et réseaux qui constituent le cyberespace sont détenus et entretenus par des multinationales à but lucratif.

Le nombre et la diversité des technologies incluses dans cet espace croissent rapidement. Le fournisseur de matériel réseau Cisco Systems prédit que d'ici 2020, 50 milliards d'appareils seront connectés à Internet, dont, pour une grande part, des dispositifs et systèmes liés à l'industrie, l'armée et l'aérospatiale. Chaque nouveau dispositif qui se connecte au cyberespace est une cible potentielle et les attaquants décèlent vite les maillons les plus faibles des réseaux. Les pirates qui se sont introduits fin 2013 dans les terminaux de points de

L'ESSENTIEL

- **Les cyberattaques se multiplieront dans les années à venir. Tout utilisateur des technologies modernes est une cible potentielle.**
- **Les nouvelles attaques visent certes les données, mais aussi les objets connectés et les infrastructures matérielles.**
- **Seuls, les gouvernements et l'industrie technologique ne peuvent sécuriser le cyberespace.**
- **Avec l'aide des pirates informatiques et des particuliers, il faut construire un système « immunitaire » distribué.**

L'AUTEURE

Keren ELAZARI, spécialiste israélienne de la sécurité, est consultante en cybersécurité et chercheuse associée du groupe de travail Science, sécurité et technologie de l'université de Tel Aviv.

SUR LE WEB

La conférence TED de Keren Elazari, *Who are the hackers ?*, 2014 : www.ted.com/playlists/10/who_are_the_hackers

vente du distributeur américain Target et ont volé les données de millions de cartes bancaires, par exemple, ont pénétré dans le réseau du détaillant en s'attaquant d'abord à une cible facile : Fazio Mechanical Services, l'entreprise de maintenance frigorifique qui gère les systèmes de chauffage et de réfrigération de Target. Ceux qui, en 2011, ont accédé aux réseaux de l'entreprise américaine de défense Lockheed Martin s'en sont d'abord pris à la compagnie de sécurité RSA, qui fournissait à Lockheed Martin ses jetons d'authentification. RSA elle-même a été compromise parce qu'un employé de sa société mère, EMC, avait ouvert un fichier Excel attaché en pièce jointe à un courriel.

Les « objets » de l'Internet des objets – smartphones, tablettes, animaux marqués d'une puce… –, tous ces éléments auxquels Internet s'étend aujourd'hui, ne sont pas simplement des fenêtres *via* lesquelles les attaquants peuvent s'infiltrer. Ils constituent eux-mêmes des cibles potentielles de sabotage. Dès 2008, des chercheurs en sécurité ont prouvé qu'il était possible de pirater à distance des stimulateurs cardiaques. Depuis, des hackers ont montré qu'ils étaient capables de prendre le contrôle de pompes à insuline au moyen de signaux radio et de déclencher l'injection d'insuline dans le système sanguin des patients.

Les infrastructures physiques sont aussi menacées. Le virus informatique Stuxnet l'a montré en 2010 en causant la destruction des centrifugeuses d'enrichissement de l'uranium au sein d'une installation clandestine à Natanz, en Iran. Fruit supposé d'une collaboration coûteuse entre les États-Unis et Israël, Stuxnet a révélé qu'un code numérique suffit à perturber et détruire des systèmes physiques analogiques. Depuis, d'autres attaques l'ont confirmé. En décembre 2014, l'Office fédéral allemand de la sécurité des technologies de l'information a rapporté que des pirates avaient perturbé certains systèmes d'une aciérie, empêchant le haut-fourneau de s'arrêter et infligeant d'importants dégâts au système. Trois mois plus tôt, des pirates chinois avaient attaqué les sites web de l'Agence américaine d'observation océanique et atmosphérique (NOAA) qui traitent des données satellitaires servant entre autres à l'aviation et à la réaction aux catastrophes.

La cybersécurité ne concerne pas seulement la sécurisation des ordinateurs, des réseaux ou des serveurs web

En d'autres termes, la cybersécurité ne concerne pas seulement la sécurisation des ordinateurs, des réseaux ou des serveurs web. Il ne s'agit pas juste de sécuriser des « secrets » (comme si nous en avions encore beaucoup pour Google et Facebook !). La bataille du cyberespace concerne la protection des objets, des infrastructures et des processus. Le danger encouru est la subversion et le sabotage des technologies que nous utilisons tous les jours : nos automobiles, distributeurs bancaires et appareils médicaux ; nos réseaux électriques, satellites de communication et réseaux téléphoniques. La cybersécurité vise à protéger notre mode de vie.

Des vulnérabilités entretenues

Sécuriser le cyberespace confronte les gouvernements à des conflits profonds. De nombreuses agences fédérales, dont le Département de la sécurité intérieure des États-Unis, ont un réel intérêt à protéger les sociétés nationales et les citoyens des cyberattaques. Mais d'autres entités gouvernementales ont intérêt que le réseau mondial reste criblé de vulnérabilités. Des groupes clandestins tels que la NSA, l'Agence de sécurité américaine, investissent des millions pour trouver et maîtriser des failles techniques qui permettraient à un attaquant de prendre le contrôle d'un système.

La vulnérabilité de sécurité des uns est l'arme secrète des autres. Prenons le bug Heartbleed. Si vous avez utilisé Internet au cours des cinq dernières années, votre information a probablement été cryptée et décryptée par des ordinateurs équipés du logiciel OpenSSL. SSL est la technologie derrière les icônes en forme de cadenas qui signalent les sites web sécurisés. La vulnérabilité Heartbleed était le résultat d'une erreur élémentaire de développement logiciel dans Heartbeat, une des extensions d'OpenSSL, d'où le nom *(voir l'encadré page 55)*. Exploitée, la faille donnait aux indiscrets un accès facile aux clés de chiffrement, noms d'utilisateurs et mots de passe, rendant illusoire toute sécurité offerte par le chiffrement SSL. OpenSSL a été vulnérable pendant deux ans avant que deux équipes distinctes de chercheurs

© 360b / Shutterstock.com

© Jstone / Shutterstock.com

en sécurité (l'une dirigée par Neel Mehta, expert en sécurité chez Google, et l'autre de Codenomicon, dont le siège est en Finlande) ne découvrent le bug. Quelques jours plus tard, le magazine *Bloomberg Businessweek* citait des sources anonymes affirmant que la NSA utilisait cette faille depuis des années pour le cyberespionnage.

Nombre d'États puissants ont affecté leurs meilleurs techniciens et des millions d'euros à la découverte et à l'exploitation de vulnérabilités telles que Heartbleed. Les gouvernements achètent aussi des bugs sur le marché libre, contribuant à soutenir l'industrie des failles de sécurité. Un nombre croissant d'entreprises, telles que Vupen Security, à Montpellier, et Exodus Intelligence, à Austin, se spécialisent dans la découverte et la commercialisation de ces précieux bugs. Certains gouvernements dépensent même plus pour la recherche et le développement de capacités offensives que pour la défense contre les cyberattaques. Le Pentagone emploie nombre de chercheurs en vulnérabilités, et le budget de la NSA pour la cyberrecherche offensive est plus du double de celui consacré à la défense.

Cela ne signifie pas que les gouvernements ont des intentions malfaisantes ou qu'ils sont des ennemis de la cybersécurité. Les agences telles que la NSA recueillent des renseignements afin d'empêcher des actes abominables et il est logique qu'elles utilisent tout outil à leur disposition pour y parvenir. Toutefois, une étape importante de la sécurisation du cyberespace consistera à soupeser avec honnêteté les coûts et avantages de l'entretien des vulnérabilités par les agences gouvernementales. Une autre clé de la réussite sera de tirer le plein parti du pouvoir des gouvernements, qui peuvent par exemple obliger des entreprises et autres organismes à partager leurs informations sur les cyberattaques.

Les banques, en particulier, auraient tout intérêt à le faire, car les attaques sur les institutions financières suivent d'ordinaire un schéma prévisible : quand les criminels trouvent un angle d'attaque qui fonctionne avec une banque, ils l'essaient sur une autre, puis une autre… Toutefois, les banques évitent de divulguer des informations sur les attaques subies, car cela soulève des questions sur leur propre sécurité. Elles évitent aussi de communiquer avec leurs concurrentes ; dans certains cas même, les lois antitrust l'interdisent. Les gouvernements, en revanche, peuvent faciliter le partage d'informations entre banques. Ce partage est déjà mis en place aux États-Unis sous la forme du Centre de partage et d'analyse d'informations pour les services financiers (FS-ISAC), qui sert aussi les organismes financiers mondiaux. Et en février, Barack Obama a signé un décret présidentiel qui enjoint d'autres entreprises à partager leurs renseignements entre elles et avec le gouvernement.

DEUX CYBERATTAQUES qui ont marqué les esprits : le 24 novembre 2014, Sony Pictures Entertainment, filiale américaine du groupe japonais Sony, est piratée. De nombreuses données sont détruites, d'autres sont divulguées, notamment des films en postproduction. Quelques mois plus tôt, durant l'été 2014, des pirates ont volé les données personnelles de milliers de clients de la société américaine de portefeuille JP Morgan Chase.

Les pirates à la rescousse

Tant que les hommes écriront des programmes, des vulnérabilités existeront. Sous la pression concurrentielle, les entreprises du secteur des technologies introduisent leurs produits sur le marché plus vite que jamais. Ces entreprises seraient bien avisées d'exploiter l'énorme ressource humaine que constitue la communauté mondiale des hackers. Au cours de l'année passée, catalysées par des événements tels que les révélations d'Edward Snowden sur la NSA, l'industrie technologique et la communauté des hackers ont commencé à accepter l'idée de travailler ensemble. À présent, des centaines d'entreprises voient l'intérêt d'embaucher des hackers en les attirant au moyen de programmes qui récompensent la découverte de bugs ou de vulnérabilités