La sécurité numérique façonne l'avenir de notre société

ENJEUX/ Nicolas Arpagian est directeur scientifique du cycle Sécurité numérique à l'Institut national des hautes études de la sécurité et de la justice (INHESJ), établissement public placé auprès du Premier ministre français. Il explique les enjeux de la cybersécurité.

Nous confions à notre ordinateur et à notre smartphone les séquences les plus intimes de notre activité quotidienne : correspondances personnelles et sentimentales, transactions bancaires, déclarations fiscales et bientôt notre dossier médical. Les entreprises et les administrations pratiquent ce même mouvement de numérisation en généralisant l'informatisation de leurs procédures et de leurs transactions. Les équipements des industriels et des sociétés de services sont plus que jamais pilotés par des systèmes d'information. Qui ont souvent comme particularité de n'avoir jamais été conçus pour prendre en compte prioritairement la sécurité. Leur performance technique et leur prix sont en général les critères prioritaires. Un seul mot d'ordre : business first !

Savoir-faire crapuleux sur la Toile

Les organisations criminelles ont à leur tour adopté ce virage technologique. En déployant sur la Toile l'intégralité de leur savoir-faire crapuleux : vol d'informations, usurpations d'identité, extorsion, détournement de fonds, escroquerie… Chaque activité illicite connaît son volet numérique puisque l'informatique favorise leur essor et revêt toutes les « qualités » aux yeux des pirates. Elle permet à une personne isolée d'attaquer un collectif, d'accéder à des outils de piratage dont le maniement est aisé et le coût unitaire limité à quelques dizaines d'euros. La cyberattaque peut s'effectuer à l'échelle internationale et impliquer suffisamment d'ordinateurs répartis sur le globe pour rendre l'identification de l'assaillant extrêmement difficile, voire impossible. Enfin, l'intensité relativement modeste de la coopération judiciaire internationale limite les risques de poursuite et de sanction. Il est frappant de constater que les logiciels de piratage de téléphone mobile avec à la clé la captation des données de géolocalisation, la liste des appels, le détail des sms et de la navigation sur Internet sont facilement accessibles avec un moteur de recherche grand public.

« L'arme numérique est employée pour salir la réputation d'un tiers ou passer au crible sa vie privée. Cela ne relève plus de la science-fiction ou du roman d'espionnage. »

Cyberarsenal

L'offre des cyberpirates ne fait que répondre à la demande… La consumérisation des outils d'intrusion informatique témoigne de la demande croissante émanant de personnes ou d'entités, notamment des entreprises, qui n'entretiennent aucun lien avec le crime organisé. Mais qui voient dans ce cyberarsenal un moyen bon marché et potentiellement efficace de parvenir à leurs fins pour régler un contentieux, prendre de l'avance ou rattraper un compétiteur. Cela va du vol de données économiques à des campagnes de dénigrement sur des réseaux sociaux pour déstabiliser tel concurrent jugé gênant. Des conflits intrafamiliaux ou de voisinage sont également l'occasion d'espionner son futur ex-conjoint ou un proche que l'on souhaite humilier. L'arme numérique est alors employée pour salir la réputation d'un tiers ou passer au crible sa vie privée. Cela ne relève plus de la science-fiction ou du roman d'espionnage. Il convient donc d'éduquer chacun au risque numérique. Pour que nous ayons toujours conscience de ce que nous mettons en jeu : qu'il s'agisse des risques de fraude liés à la fréquentation de certains sites Internet ou du pillage de nos données personnelles par les multinationales du Net

© Photo Victor Tonelli/ OECD

EXPERT/Nicolas Arpagian est notamment l'auteur de *La Cybersécurité*, 2015, Presses Universitaires de France (Collection Que Sais-Je ?).

(Google, Amazon, Facebook, Apple, Microsoft...). La société numérique qui se construit chaque jour est porteuse d'un immense potentiel de croissance et de services innovants. Mais il serait irresponsable de ne pas prendre en compte son impact en matière de sécurité de nos existences. Plus les citoyens-consommateurs seront éclairés quant au fonctionnement de cet environnement qui mêle les technologies à notre quotidien, plus ils en feront un usage responsable. Et moins ils seront des objets technologiques, sans capacité à exprimer leur libre-arbitre.

_PAR NICOLAS ARPAGIAN
(WWW.ARPAGIAN.EU)

EN BREF/

Le piratage, à la portée de tous ?

Le piratage serait-il un jeu d'enfants ? Il est en tout cas expliqué méthodiquement à tous sur... Internet. Il suffit d'écrire sur un moteur de recherche : *« Comment »*...puis, taper les trois lettres suivantes : *« p », «i »* et *« r »*... Vous verrez que le premier lien que l'on vous propose est : *« Comment pirater un compte Facebook. » « Ce sont des tutoriels simplifiés qui vont vous permettre, sans avoir de grandes connaissances, de pirater votre voisin de bureau ou votre ex-petit ami »*, explique Nicolas Arpagian. Bien évidemment, aucune obligation de mettre à exécution ces conseils...

Sociétés ultra-connectées

Le monde comptait en 2015 environ 3,07 milliards d'internautes. Et ils devraient être 3,6 milliards en 2018. Ce qui représente 48,2 % de la population mondiale (Données de l'institut eMarketer).

Géographie des cyberattaques

Les cinq premiers pays dont seraient originaires les cyberattaques seraient : les Etats-Unis (20 %), la Chine (9,1 %), l'Italie (6 %), Taïwan (6 %) et le Brésil (5,7 %). Mais attention : l'origine géographique ne peut pas toujours être établie avec certitude. Et le fait de localiser les ordinateurs d'où sont parties les attaques, ne signifie pas que ceux-ci aient été utilisés avec l'accord de leur propriétaire légitimes ou l'assentiment des autorités de l'Etat en question. (Estimation annuelle publiée par la société de cybersécurité Symantec.)