Résister aux cyberattaques, est-ce vraiment possible ?

Comment protéger nos entreprises des cyberattaques ? Lors de la Maddy Keynote qui a eu lieu les 30 et 31 janvier derniers au Centquatre, trois acteurs majeurs en cybersécurité ont débattu autour de cette problématique.

Temps de lecture : minute

8 février 2020

Au cinéma comme dans les séries télé, l'image du hacker en sweat à capuche noir qui pirate en trois clics le Pentagone a encore la peau dure. Loin de la fiction, les risques de cyberattaques sont néanmoins réels. Depuis les révélations d'Edward Snowden en juin 2013, le grand public sait pertinemment que - sans précautions au préalable - chacune de ses data peut tomber entre les mains de n'importe qui, n'importe où et n'importe quand. Les entreprises, elles aussi, l'ont bien compris et se mobilisent pour protéger aux mieux leurs données, une denrée qui vaut aujourd'hui de l'or. D'autant que les risques de conflits technologiques n'ont jamais été aussi grands dans l'histoire de l'humanité. Le 31 janvier dernier, à l'occasion de la Maddy Keynote, trois experts en cybersécurité ont partagé leur vision sur les enjeux futurs de la sécurité informatique.

Leçon n°1 : Redorer l'image des hackers

Encore trop souvent, le hacker souffre des idées reçues. Il est davantage perçu comme un individu aux motivations crapuleuses. Dans les faits, c'est pourtant loin d'être le cas, tient à souligner Nicolas Arpagian, directeur de la stratégie et des affaires publiques chez Orange Cyberdefense. " *Au contraire, c'est quelqu'un qui cherche à comprendre*

une technologie et qui va essayer de la personnaliser, considère-t-il. Le hacker est doté d'une certaine tournure d'esprit et d'une vraie qualité intellectuelle. " Concrètement, s'il doit tester la sécurité d'un programme informatique, le hacker va tout faire pour trouver une faille. Il s'agira de la réparer, une fois celle-ci détectée. Et pour cause : l'objectif derrière un hacking est surtout de renforcer la sécurité informatique d'une infrastructure. Pour Gaël Musquet, lui-même hacker dit " éthique " (ou " white hat "), la meilleure définition du hacking provient de l'Israélienne Keren Elazari. La chercheuse estime que le hacker est tout simplement " le système immunitaire d'Internet " puisque tout devient interconnecté. Même son de cloche chez Jacques de La Rivière, CEO et cofondateur de Gatewatcher (plateforme de détection d'intrusions et de menaces avancées). " *Au même titre que les explorateurs il y a plusieurs siècles, le hacker a un objectif : celui de sécuriser les territoires. Forcément, cet esprit curieux et positif a été rejoint par des gens moins attentionnés qui y ont trouvé une économie criminelle lucrative, d'où la distinction entre hackers éthiques et malveillants* ", fait observer l'entrepreneur.

Leçon n°2 : Soigner son hygiène numérique

Mais doit-on vraiment craindre les attaques étrangères ? Sur ce point, les trois experts en cybersécurité sont unanimes : le danger est partout. " *La notion de menace étrangère n'a au fond pas vraiment de sens, juge Nicolas Arpagian d'Orange Cyberdefense. La menace est parfois bien plus proche que ce que l'on pense. Pour hacker, on a parfois recours à des relais, des sous-traitants, des forces technologiques extérieures donc à partir de quand peut-on qualifier que la menace est étrangère ? Cela se discute.* " Quand il assume son titre de hacker, Gaël Musquet confie rencontrer à chaque fois les mêmes sollicitations : " *Peux-tu pirater le compte Facebook de mon ex ?* " Face à ce constat, le spécialiste recommande de soigner son hygiène numérique. "*Il y a des principes de base à respecter qui font partie du bon sens. Finalement, on doit*

appliquer les mêmes mécanismes que dans la vie quotidienne. Quand vous urinez, vous fermez la porte pour veiller à votre intimité; avec le numérique, il faut fonctionner de la même manière", soutient le hacker français, célèbre pour s'impliquer dans l'anticipation, la prévision et la prévention des catastrophes naturelles.

Leçon n°3 : Anticiper les risques

Les entreprises ont-elles compris que la menace est réelle ? Oui, s'accordent à dire les trois spécialistes interrogés lors de la Maddy Keynote. " *Seulement, la sécurité informatique est un luxe que peuvent s'offrir les grandes entreprises, cela reste encore cher pour beaucoup d'entre elles* ", affirme Jacques de La Rivière. Mais le fondateur de Gatewatcher le rappelle : les risques existent et les barrières sont souvent plus vite levées sur le virtuel qu'ailleurs. " *Les hackers ou les criminels ne se rendent pas compte à quel moment ils franchissent la ligne rouge. Or la simple tentative d'entrer est condamnable.* " Alors, comment se prémunir ? " *Hygiène, prévention, analyse des risques* ", résume Jacques de la Rivière. Quant à Nicolas Arpagian, il préconise la capacité de détection. " *Il ne faut pas sous-estimer les risques, prévient-il. Dès lors qu'une économie s'ouvre - c'est le cas avec l'émergence des objets connectés - et qu'on démultiplie de facto les interactions avec les tiers, il s'agit de se doter d'une capacité de détection.* " Dans le cas du télétravail en plein essor, le directeur d'Orange Cyberdefense affirme que le déploiement d'outils est une bonne manière d'assurer ses arrières. " *On peut, par exemple, utiliser un VPN (un tunnel informatique entre la box du salarié à la maison et l'entreprise, NDLR) qui va permettre à un employé de se connecter au réseau sécurisé de la société comme s'il était physiquement dans les locaux.* " De son côté, Gaël Musquet souhaite la mise en place de politiques de prévention. " I*l faut être capable d'anticiper et d'imager les risques pour ensuite faire de la pédagogie dans les entreprises comme à la maison, avec nos proches, conseille-t-il. Le*

guide de la sécurité des données personnelles de la CNIL peut être une bonne base. " Mieux vaut prévenir que guérir.

Maddyness, partenaire média d'Orange

Article écrit par Maddyness, avec Orange