6.3. Digitalisation et cybersécurité, les deux faces d'une même médaille

Toutes les vingt minutes, une centaine d'entreprises seraient confrontées à des attaques informatiques donnant lieu à des demandes de rançon. Tel est le revers de la médaille d'une digitalisation de l'économie toujours plus poussée Cela a aussi pour effet de soutenir la croissance des dépenses en matière de sécurité informatique et, par ricochet, les sociétés actives dans ce secteur. Une tendance de fond qui offre aux investisseurs une thématique d'investissement de long terme pour le moins prometteuse...

La digitalisation de l'économie progresse à grands pas, et ce dans quasi tous les secteurs d'activité. Il ne se passe pas un jour sans que la technologie nous rende service, que ce soit via, par exemple, Uber si l'on a besoin d'un moyen de transport, eBay ou Amazon si l'on souhaite acheter un bien, ou une application bancaire si l'on souhaite effectuer une transaction financière.

En 2018, le cadeau de Noël qui s'est le plus retrouvé sous le sapin n'est autre qu'Alexa, l'assistant domestique digital commercialisé par Amazon. Allumer la télévision, baisser les volets, éteindre la lumière, augmenter le chauffage, commander une pizza, ... tous les désirs des personnes hyper connectées peuvent désormais être assouvis par cette petite enceinte autonome qui vient compléter l'offre déjà fournie par les téléphones mobiles, tablettes et autres objets connectés.

Mais pour nous obéir au doigt et à la voix, ces interfaces doivent pouvoir nous localiser, nous entendre et nous contacter en permanence. Cela signifie que pour chaque interaction nous partageons, consciemment ou non, un nombre considérable de données avec les fournisseurs de services qui se trouvent derrière chaque application. Et c'est précisément là que le bât blesse ! Pour garantir la sécurité de ces échanges de données, les entreprises doivent consacrer toujours plus de temps et d'argent, les hackers ayant souvent une longueur d'avance. Les vols de données (adresses e-mail, mots de passe, numéros de compte, de carte d'identité, etc.) sont, en effet, devenus monnaie courante ces dernières années. Si nombre d'entre eux se révèlent mineurs et ne sont, pour la plupart, tout bonnement pas détectés, les cyber-attaques à grande échelle, sont, en revanche, beaucoup plus problématiques car elles peuvent mettre en péril le fonctionnement de toute une organisation.

FACE À LA MULTIPLICATION DES ATTAQUES INFORMATIQUES...

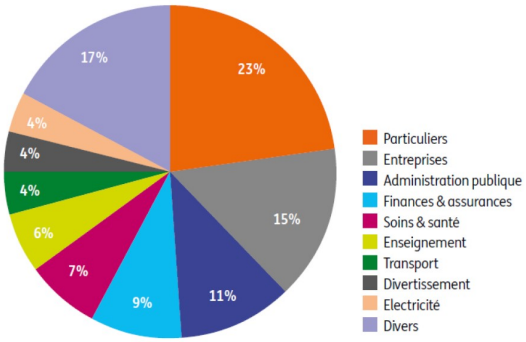
Aucun secteur n'échappe à la menace d'une attaque de sa plateforme informatique et d'un vol de données. Les sociétés technologiques, les institutions financières et le commerce en ligne sont évidemment les plus concernés, mais les soins de santé ou les hôtels peuvent également être «hackés». Parmi les attaques les plus médiatisées, on peut notamment revenir sur le cas emblématique de Yahoo! en 2016. L'attaque a provoqué une onde de choc planétaire en confirmant avoir connu en 2013 une faille monumentale dans sa sécurité informatique. À cette occasion, ce sont pas moins de trois milliards d'utilisateurs qui ont appris que leurs données personnelles avaient été dérobées. Entre 2014 et 2018, ce sont les informations de 383 millions de clients de Marriott, en ce compris des numéros de cartes bancaires et de passeports, qui ont été puisées dans la base de données de la chaîne d'hôtel. En 2015, les données de 80 millions d'affiliés d'Anthem, un des plus grands acteurs dans l'assurance maladie aux États-Unis, se sont retrouvées sur la place publique. Même mésaventure pour Office of Personnel Management dont la vétusté du système informatique a permis le vol de données, en ce compris des empreintes digitales, relatives à 22,5 millions d'employés du gouvernement fédéral des États-Unis.

Mais, avec l'essor des objets connectés, ce ne sont plus seulement les données personnelles qui peuvent être hackées mais aussi les voitures, les systèmes de sécurité et de surveillance, la domotique, les drones... En pénétrant sur un réseau wifi mal sécurisé, une personne mal intentionnée peut désormais prendre le contrôle d'un véhicule ou pénétrer dans une habitation. Qu'on le veuille ou non, les ménages, les administrations publiques et les entreprises, surtout financières, constituent les principales cibles des cyber-attaques !

Il ne faut, certes, pas sombrer dans la paranoïa. L'accès aux informations personnelles des utilisateurs n'engendre pas toujours des activités malveillantes.

Par exemple, lorsque les organisations ont recours au cryptage des informations les plus sensibles, comme les mots de passe reprises dans leurs bases de données. Les consommateurs peuvent prendre la précaution de sécuriser leurs applications et objets connectés en renouvelant régulièrement leurs mots de passe (idéalement un mot de passe par services et à condition de proscrire des solutions trop faciles comme «123456» ou «qwerty»).

(1) Principales cibles des attaques informatiques (mars 2018)



Il n'en reste pas moins que lorsque des numéros de sécurité sociale, de cartes de crédit, de passeports ou d'autres informations sensibles sont dérobées, les clients courent un risque élevé d'usurpation d'identité et de préjudices financiers. Lorsque l'on sait que, selon IHS markit, ce ne sont pas moins de 100 milliards d'objets connectés qui devraient s'être écoulés d'ici 2025, on mesure mieux les enjeux en termes de sécurité qui en découlent.

En outre, le vol de données a également un impact sur les organisations piratées elles-mêmes. Elles peuvent être condamnées à des dédommagements envers leurs clients et subir d'importants dommages en termes d'image de marque. Outre le risque financier et de réputation, les entreprises doivent aussi tenir compte du risque associé au Règlement général sur la protection des données (RGPD), dans la mesure où une entreprise - reconnue coupable de ne pas avoir fait ce qu'il fallait pour protéger ses données - peut encourir une amande pouvant s'élever jusqu'à 4% de ses revenus.

LES DÉPENSES DE CYBERSÉCURITÉ EXPLOSENT...

La moitié des entreprises britanniques auraient, selon leur gouvernement, été confrontées en 2017 à une cyber-attaque. Conscientes de cette menace potentielle qui ne fait que s'intensifier et se sophistiquer il n'est, dès lors, pas étonnant de constater que les grandes sociétés et les états en ont fait l'une de leur principale préoccupation. Il est loin le temps où un simple anti-virus pouvait protéger nos ordinateurs. On mesure mieux l'étendue du problème lorsque l'on apprend par Cybersecurity Ventures que toutes les vingt minutes, cent entreprises seraient confrontées à des demandes de rançon à la suite d'attaques informatiques. Mai 2017 reste, à cet égard, une date clef puisqu'elle est, à ce jour, la plus grande cyber attaque de l'histoire d'internet. Des hackers profitaient d'une faille dans le système de sécurité des versions antérieures à Windows 10. Ils sont parvenus à infecter plus de 300.000 ordinateurs dans le monde entier - dont ceux de l'administration des soins de santé britannique - avec un logiciel malveillant (« WannaCry 2.0») ayant pour but de crypter toutes les données jusqu'à ce qu'une rançon soit payée.

On l'aura compris, l'ardoise peut s'avérer salée pour les entreprises insuffisamment outillées pour faire face à ce genre de danger. Maersk, la plus grande compagnie maritime, aurait ainsi dû débourser quelques 300 millions de dollars. Faute de disposer en interne des outils et connaissances suffisantes, les entreprises n'ont donc pas d'autres alternatives que de se tourner vers les fournisseurs de services et de logiciels de sécurité informatique. Le cryptage des données, la protection des transactions financières et la sécurité des boites mails ne sont que quelques-uns des nombreux paramètres à sécuriser. Ce qui laisse présager une évolution potentiellement exponentielle des dépenses en la matière, que ce soit pour la protection des ordinateurs, des appareils mobiles ou des objets connectés. Pour la période 2017-2021, Cybersecurity Ventures évoque le chiffre de 1.000 milliards de dollars.

Morgan Stanley va même plus loin en estimant que les revenus de la cybersécurité pourraient, d'ici 2020, se révéler plus de quatre fois supérieurs à ceux de la totalité du secteur de la technologie. Pour être franc, les prévisions en la matière se révèlent trop disparates pour s'y fier.

Cela s'explique peut-être par le fait que les entreprises sont tentées de sous-estimer leurs besoins en cybersécurité pour ne pas donner l'impression qu'elles sont en retard. Du coup, la seule chose que l'on peut affirmer sans risque de se tromper, c'est que la croissance des ventes reste de mise. Comme le confirme Accenture, le coût de la cybercriminalité pour les entreprises est en hausse de près de 62,5 % (en moyenne) depuis 2013.

Signe de l'importance accordée par la Maison Blanche à cette problématique, les dépenses allouées dans le budget fédéral par le président Donald Trump à la recherche en cybersécurité s'élèvent à près de 15 milliards de dollars, contre 14,4 milliards en 2018 et 13,1 milliards en 2017. Et le secteur bancaire n'est pas en reste puisque des institutions comme JPMorgan ou Bank of America y ont consacré respectivement 500 et 400 millions de dollars en 2016.

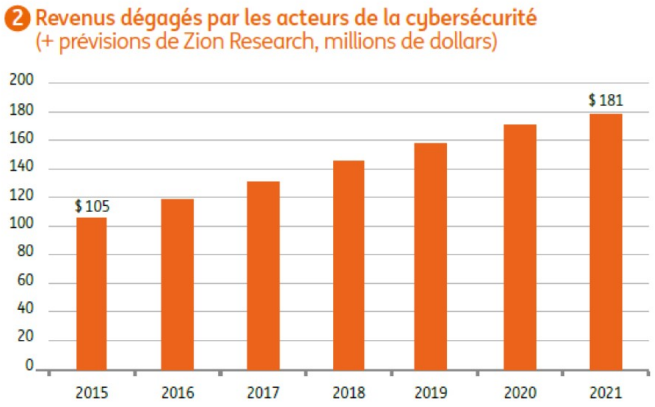
… ET LE SECTEUR SURPERFORME

On peut donc légitimement s'attendre à ce que la cybersécurité continue à afficher une tendance positive. D'autant que, si l'on en croit Zion Research, les revenus annuels générés par le secteur devraient progresser d'un peu plus de 100 milliards de dollars en 2015 à plus de 180 milliards de dollars en 2021.

Outre le nombre croissant d'attaques informatiques, le secteur de la cybersécurité devrait aussi être soutenu par un accroissement du nombre de partenariats entre les groupes actifs dans le secteur et les firmes de capital à risque. Ces dernières ont investi dans le secteur près de 14 milliards de dollars depuis 2013 !

Concrètement, les principales sources de croissance du marché de la cybersécurité devraient provenir des sous-secteurs liés à la sécurité des appareils mobiles (Mobile) et des objets connectés (IoT - Internet of Things en anglais), mais aussi à la détection et la prévention des virus informatiques. Même si ce dernier segment d'activité se révèle minuscule-il pèse 1,5 milliard de dollars, contre 35 milliards pour le segment dédié à la sécurité des ordinateurs (IT Security) -, son taux de croissance annuel moyen attendu est d'environ 28 %, soit plus de 20 % au-dessus des prévisions relatives à l'IT Security, contre 17% pour l'IoT et 13% pour le Mobile.

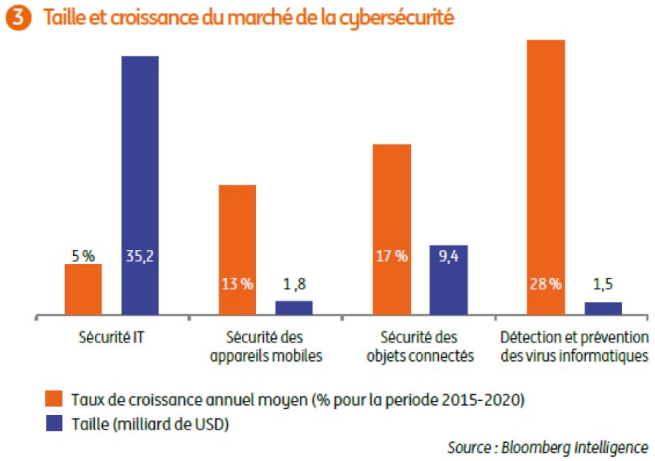
Preuve que cette conjonction de facteurs favorables soutient le secteur de la cyber sécurité, ce dernier a fait état en 2018 d'une belle résistance par rapport à la morosité observée sur la plupart des actifs à risque. Alors que les actions mondiales se sont dépréciées de 7% (indice MSCI World All Countries), l'indice de référence du marché de la cybersécurité (indice ISE Cyber Security UCITS) s'est renforcé de 15 % (en euros) : deux fois les gains enregistrés par le secteur mondial de la technologie (indice MSCI World IT Services). Et depuis le début de l'année, sa prestation (44%) se révèle près de sept fois plus élevée que celle des actions mondiales (6%).

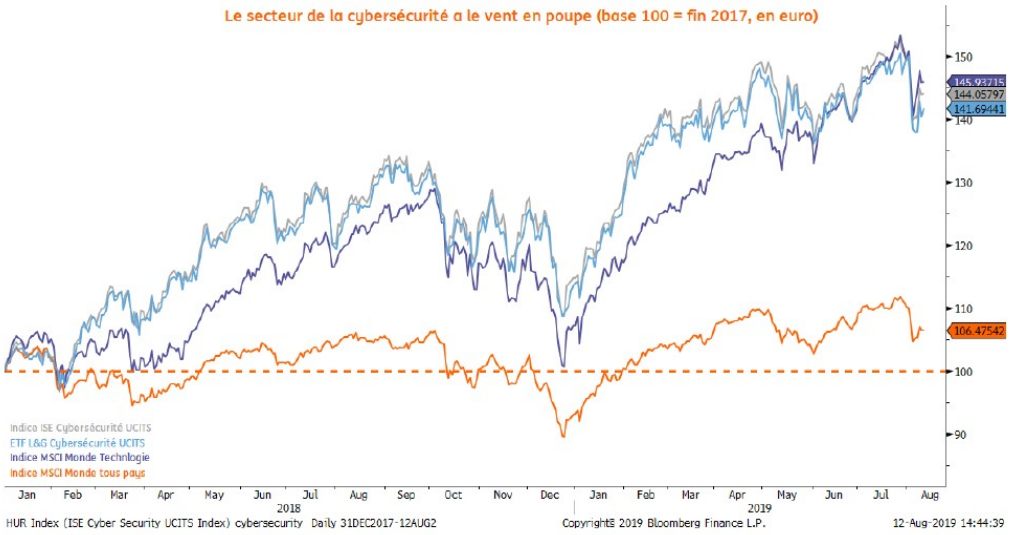


Pour l'investisseur convaincu par la croissance rapide des revenus dégagés par les sociétés de cybersécurité, cet indice offre une porte d'accès intéressant. Il se focalise, en particulier, sur les développeurs de logiciels dédiés à la protection informatique.

Ceci étant, il convient de constater que, par nature, ce secteur s'avère plus volatil puisqu'il se compose de sociétés de petites et moyennes tailles. Sur le long terme, la volatilité s'élève à 16, contre 14 pour les principales sociétés technologiques reprises dans l'indice Nasdaq et 8 pour les actions mondiales.

Pour réduire cette volatilité intrinsèque, l'indice ISE Cyber Security UCITS n'incorpore pas d'entreprises affichant une capitalisation boursière inférieure à 100 millions de dollars et dont la moyenne des transactions boursières journalières se révèle inférieure à 1 million de dollars (en rythme trimestriel).





En contrepartie de cette volatilité naturellement plus élevée, l'indice ISE Cyber Security UCITS peut se targuer, depuis début 2017, d'une croissance des ventes 2x plus élevée que dans le cas des grandes valeurs technologiques américaines. Cela s'explique par le fait que l'indice met l'accent sur les sociétés de cybersécurité investissant une grande partie de leurs revenus dans la recherche et développement (R&D). Les membres de l'indice ISE Cyber Security UCITS investissent 18,2% de leurs ventes dans la R&D, contre 16,3% pour les grandes pointures de l'indice Nasdaq.

Enfin, comme la cybercriminalité affecte les particuliers, les états et les entreprises, sans tenir compte des frontières, il convient d'aborder cette thématique d'investissement de manière globale en privilégiant les entreprises de cybersécurité dont les ventes se font à l'international. Une dimension que l'indice ISE Cyber Security UCITS tente également de prendre en compte puisque les entreprises qui le constituent réalisent plus de 38 % de leurs ventes à l'étranger.

ING PRIVATE BANKING

AIHE-REVUE Nr. 224 – AOÛT-SEPTEMBRE 2019