Cybersécurité

Ce document se veut une synthèse de l'intervention de M. Gilles CASTERAN, directeur exécutif au sein d'*Accenture Security*, traitant de la thématique de la cybersécurité, dans le cadre du module *Performance du Processus d'Informatisation*, encadré par M. Jean-Guy SAYOUS.

L'émergence des cyber-systèmes marque une **quatrième révolution industrielle**, après celles amenées par la mécanisation, l'électrification, et l'électronique. A l'image des précédentes, cette nouvelle révolution, dont la **matière première serait la donnée**, induit de **profondes modifications des pratiques**, demande de **nouvelles compétences**, mais est également accompagnée d'un certain nombre de **menaces** et de **risques**. Le monde s'en trouve également transformé, avec la domination de **deux superpuissances** que sont les **États-Unis** et la **Chine**, dominant le marché par le biais de géants du web : les **GAFAM** (*Google*, *Apple*, *Facebook*, *Amazon* et *Microsoft*) pour la première, et les **BATX** (*Baidu*, *Alibaba*, *Tencent* et *Xiaomi*) pour la seconde.

Espionnage, vol de données sensibles, déstabilisation, dégradation, les **motifs des cyberattaques** et piratages sont **de plus en plus nombreux** et leurs cibles le sont tout autant. Ainsi, un simple groupe de personnes est désormais en capacité de **déstabiliser des entreprises, des États**. Ces attaques peuvent être menées de différentes manières, allant la saturation du réseau informatique par déni de service (DDoS), aux logiciels malveillants (*ransomware*, *spyware*, etc.), en passant par l'hameçonnage (*phishing*). Ces dernières années, on assiste à un **bouleversement des pratiques des cybercriminels**, puisque les **cyberattaques deviennent de plus en plus indirectes**. En effet, à l'image d'Airbus, visé par la cyberattaque menée sur Altran, les attaques sont de plus en plus ciblées sur des sous-traitants, clients, afin de nuire indirectement à l'entreprise.
Les **menaces**, de plus en plus **nombreuses**, **sophistiquées**, **ciblées**, et **dévastatrices**, du fait de leurs conséquences financières élevées, **doivent donc être adressées par les entreprises**, c'est tout l'enjeu derrière la **cybersécurité**.

La cybersécurité est l'ensemble des **moyens techniques et non techniques** permettant d'assurer la **disponibilité**, **l'intégrité** et la **confidentialité des informations utilisées**, **transmises** et **stockées**.
Les grandes activités de la cybersécurité comprennent **l'identification**, la **protection**, la **détection**, la **réponse** et le **rétablissement** des attaques. Elle adresse une véritable **problématique de gestion de risques au sein de l'entreprise**.
Un risque peut être défini comme étant **l'éventualité qu'une menace parvienne à exploiter une vulnérabilité sur un actif métier en contournant les mesures de protection**. Il est donc fonction de trois paramètres, que sont la **vulnérabilité**, la **menace** et **l'impact**.
Il peut être traité de différentes manières : **accepté**, **annulé**, **transféré** ou **réduit**. Ainsi, pour les fournisseurs d'accès au Cloud, l'un des grands enjeux futurs, la réversibilité, correspond ici au transfert.
Les risques induits par les cyberattaques sont distingués à **différentes échelles** : **l'individu**, **l'entreprise**, et **l'état**, et **doivent être identifiés, cartographiés, et classifiés**.

Loin de faiblir, le **risque cyber devient de plus en plus prégnant**. La **transformation numérique** et ses corollaires (dépendance accrue aux outils, interconnectivité des systèmes d'information, généralisation du stockage dans le Cloud, émergence de l'IoT, etc.) ont généré un **ensemble de nouveaux risques** contre lesquels les entreprises ne sont pas suffisamment armées. Ainsi, le **cyber-incident** arrive en **deuxième position des risques les plus redoutés** par les organisations, devant les catastrophes naturelles, et juste **derrière l'interruption d'activité, avec laquelle il est interdépendant**. En effet, les incidents informatiques ont souvent pour conséquence une interruption ou un ralentissement de l'activité, du fait de l'interconnexion entre l'entreprise et son Système d'Information.

D'après une étude menée par *Accenture*, **les violations de sécurité ont augmentées de 11% sur 2 ans**, et de **67% sur 5 ans**. Toutefois, la même étude montre également une **amélioration de la défense** mise en place par les entreprises, puisqu'**en 2018**, **87% des attaques ont été déjouées**, contre 70% en 2017.
En ce sens, **un des axes de maturité face aux cyberattaques concerne leur détection**. En effet, si l'on pourrait penser que **la capacité de détection des entreprises s'améliore considérablement**, avec **23% de celles-ci détectant plus de 76% des attaques**, il ne faut pas oublier qu'à l'inverse, **24% des entreprises en détectent moins de la moitié**. Pour pallier à cela, les entreprises doivent s'inspirer des leaders, qui mettent en place des solutions telles que le **déploiement de la sécurité à l'échelle**, la **formation**, permettant ainsi d'introduire au sein de l'entreprise une certaine **culture de la sécurité**, ou encore la **collaboration**, apportant une réelle valeur ajoutée.

Les organisations doivent désormais partir du principe qu'elles **seront victimes d'une attaque**, puisqu'on estime que **80% d'entre-elles ont subi une cyberattaque en 2019**.
Une approche complémentaire à la cybersécurité, devrait donc être de **planifier une stratégie de cyber-résilience** afin de limiter l'impact d'une attaque. La cyber-résilience est la **capacité** que possède l'entreprise de **continuer son activité opérationnelle lorsqu'elle subit, ou a subi une attaque**.
Elle vise à gérer la sécurité en adoptant une **approche globale** impliquant à la fois les **individus**, les **processus** et la **technologie**. Elle impose une **méthodologie** à la fois **solide** et **évolutive** de **gestion**, **d'analyse** et **d'optimisation des risques.**

Les cinq sujets essentiels, qui doivent être adressés dans la cybersécurité de nouvelle génération sont donc la **confiance numérique**, **l'éthique**, qui permet de l'accentuer, la **souveraineté**, la **solidarité**, et la **cyber-résilience**.