Cybersécurité et entreprises : sont-elles en sécurité face au tsunami du numérique ?

Nous sommes dans un monde qui entre pleinement et rapidement dans la transformation numérique. Cette transformation n'est ni linéaire, ni arithmétique, mais géométrique et exponentielle. Cela signifie que si les entreprises et l'Etat continuent à avoir une vision linéaire dans leurs modes d'actions, dans leurs process politiques, administratifs et financiers, ils risqueront d'être collés au sol à côté de cette transformation numérique qui est en train de reformater toutes les organisations et l'accroissement des menaces cyber sur tous secteurs. Face à ce tsunami du numérique quelles réponses devons-nous apporter ? Cette problématique a fait l'objet de sérieuses discussions, de retours d'expériences utiles lors de la conférence « cybersécurité et entreprises : il y a urgence »[1] organisée le 30 septembre par le ministère de l'économie et des finances de Bercy, dans le cadre du mois européen de la cybersécurité.

Le cyber, un outil au service de l'usurpation d'identité

Le baromètre de cybersécurité réalisé en 2018 sur un échantillon de 300 entreprises de toute taille, par le Groupe Euler Hermès montre des chiffres alarmants : 70% des entreprises ont subi au moins une tentative de fraudes en 2018, 20% des entreprise ont subi plus de 10 tentatives de fraudes et 25% des entreprises ont subi une cyberattaque et donc un préjudice financier. Les risques de fraudes par usurpation d'identité sont très fréquents : le faux fournisseur (47% des tentatives), le faux président, le faux client. Selon Valentin LANNE, responsable de cybersécurité chez Euler Hermès, l'utilisation de l'outil cyber offre de nouvelles opportunités d'usurpation d'identité. Les attaquants pénètrent le système informatique de la victime, accèdent et

1 « Cybersécurité et Entreprises : il y a urgence ! » : https://www.economie.gouv.fr/files/files/2019/Cyberoctobre19%20programme%20conf%C3%A9rence.pdf

modifient les factures et les RIB pour ensuite lancer le mode d'usurpation d'identité. Le préjudice financier est énorme pour les entreprises. En effet, 20% des entreprises ont enregistré un préjudice financier de plus de 50 000 euros, 13% d'entre elles ont subi un préjudice de plus 100 000 euros et 5% pour un préjudice estimé à plus de 500 000 euros.

La 5G : quel impact à l'ère du cyber ?

Les enjeux autour de la 5G sont stratégiques car elle va permettre d'augmenter de manière considérable le nombre d'objets connectés, des systèmes connectés. Lors de la conférence cybersécurité à Bercy, Marc Watin-Augouard, Général des Armées et fondateur du Forum International de Cybersécurité (FIC), estime qu'en 2020 il y aura 80 milliards de systèmes connectés et près de 1000 milliards en 2030. Cela signifie qu'il y a effet d'annonce de changement des rapports entre les hommes et les machines. Autrement dit, nous allons rentrer dans un monde de relations non plus humains-machines mais de machines-machines. Pour Marc Watin-Augouard « *on va être entouré de machines, d'objets bavardes, qui vont parler sans nous, sur nous malgré nous, contre nous parce que ces systèmes connectés vont avoir un impact dans toutes les organisations dans les espaces intelligents. Dans les entreprises vont rentrer des personnes dont les vêtements sont connectés, des voitures connectées, des lunettes et des montres connectées, bref le tout connecté* ». Face à ce tsunami numérique comment va s'opérer la cyber résilience ?

Quelle place occupent les institutions publiques économiques dans cette course à la sécurité numérique ?

Aujourd'hui la cybersécurité concerne autant les services publics, que les entreprises et les personnes privées. L'agent public doit prendre conscience que les informations qu'il manipule au quotidien dans son service peuvent représenter un intérêt pour une puissance étrangère, des hacktivistes ou plus généralement des tiers malveillants. C'est pourquoi il y a une réelle prise de conscience des enjeux de la sécurité des systèmes d'information. En effet, une série d'outils a vu le jour notamment la loi de programmation militaire[2], la vérification par l'ANSSI (agence nationale de la sécurité des systèmes d'informations) de certains composants, la sécurité des OIV (opérateurs d'importance vitale), la revue stratégique de cyberdéfense. L'augmentation des effectifs de l'ANSSI passant de 60 personnes en 2009 à 600 personnes en 2019 révèle également l'importance des enjeux cyber dans la mise en œuvre de la politique de sécurité et de défense nationale.

2 Loi de programmation militaire 2019-2025 : textes officiels : voir le site du ministère des Armées

Replacer l'humain au cœur de la threat intelligence

Aujourd'hui, pour avoir un dispositif de bien protéger, il faut que les petits groupes deviennent des grands. En effet, au sein d'une entreprise tout le monde est concerné, ce n'est pas l'affaire du DSI et du RSSI. Ces fonctions sont stratégiques et doivent monter au plus haut niveau de la direction de l'entreprise. En d'autres termes, la conscience doit ruisseler de haut en bas et inversement, du bas vers le haut parce que sinon il y aura toujours le maillon faible. Il faut que tous les collaborateurs s'approprient d'une culture de cybersécurité quel que soit leur poste.

Mais le problème fondamental des entreprises aujourd'hui c'est l'investissement dans la sécurité numérique car elles attendent toujours un retour sur investissement. Or les attaques peuvent viser une entité en passant par une petite PME fournisseur de l'entité en question. Donc l'attaque de l'une est un moyen d'atteindre la grosse cible. C'est pourquoi il est important de construire une résilience collective car l'entreprise seule ou l'Etat seul ne peut rien faire. La gendarmerie nationale a mobilisé plus de 5000 enquêteurs répartis dans toute la France pour aider les victimes de cyberattaques. Parallèlement, le gouvernement a mis en place cybermalveillance.gouv.fr pour les aider à trouver des solutions. C'est une plateforme de mise en relation entre la victime et les prestataires pour résoudre les problèmes de cyberattaques.

Des solutions pour assurer une sécurité numérique gage de sécurité économique ?

Dans une démarche d'intelligence économique la protection des informations stratégiques est fondamentale pour la pérennité de l'activité économique de toute organisation. Au sein des administrations économiques de Bercy la mise en place en 2016 d'une politique générale de sécurité des systèmes d'informations dont le pilotage est assuré par le HFDS (haut fonctionnaire de défense et de sécurité) des ministères économiques et financiers (MEF), montre l'importance des enjeux de cybersécurité dans plus les hautes sphères de l'Etat. Selon Christian Dufour, chef par intérim du service HFDS, leur rôle est d'assurer la sécurité des données sensibles et stratégiques des ministères concernés, la gestion de crise, la sensibilisation de l'ensemble des collaborateurs de Bercy et d'autres ministères et de protéger les OIV en collaboration étroite avec l'ANSSI.

Aujourd'hui le diagnostic numérique est important pour vérifier l'état des mises à jour des outils de travail. Jean Philippe Papillon, responsable de cybersécurité des MEF, le diagnostic de la santé numérique de l'entreprise est fondamental pour anticiper les cyberattaques. Le HFDS a ainsi mis en place un outil

autodiagnostic cyber entièrement gratuit, permettant de vérifier :

- La mise à jour de son navigateur;
- La solidité de son domaine de messagerie contre la contrefaçon de courriel;
- La sécurité de ses mots de passes

Il comporte également un questionnaire pour évaluer la pertinence de son système de sauvegarde. Cet outil autodiagnostic est disponible sur ce lien :https://ssi.economie.gouv.fr/.

La DFCG (Association Nationale des Directeurs Financiers et de Contrôle de Gestion) regroupant 3000 PME et ETI a réalisé une étude sur l'auto-diagnostic en 2018 sur 300 entreprises adhérentes.
Selon Bruno de Laigue, président de la DFCG, très peu d'entreprises prennent conscience d'une cyber malveillance. En effet, les statistiques montrent que 82% des entreprises ont un domaine de messagerie non protégé, plus de 50% ont un mot de passe facilement détruisable et 67% des répondants n'ont pas une politique de sauvegarde des données fiable. L'une des premières pistes de solutions est l'humain. Car il faut nécessairement avoir les bons réflexes. Par exemple sur les mails reçus la vigilance est importante pour ne pas cliquer sur un lien ou une pièce jointe suspecte dont l'expéditeur est inconnu. La première des règles est d'être vigilant et de ne pas hésiter à signaler toute action ou réaction « anormale » de l'équipement utilisé. Les projets de transformation digitale doivent impérativement s'accompagner de sécurité numérique. Il faut donc s'adapter aux mutations technologiques, à l'évolution des modes d'attaques, développer une culture cyber au sein de l'entreprise afin de minimiser les risques de malveillance.

Boubacar DIALLO
Apprenti Intelligence économique & Data
b.diallo@ccifrance.fr
CCI FRANCE