CYBERSECURITE ET PME, DU CHEMIN A PARCOURIR

Be secure,

Be curious

Auteur : Bernard LABATUT, Membre fondateur EFCSE
Université Toulouse – Capitole - FRANCE

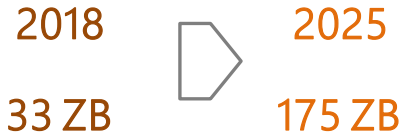
« La cybersécurité s'impose aujourd'hui comme condition essentielle pour façonner notre espace informationnel. Corollaire de cette affirmation, on ne peut imaginer de maîtriser l'espace numérique si le danger y est constant ».

Or, à l'heure actuelle, le niveau de danger ne cesse de croître – tant pour les individus que pour les entreprises et les Etats, tous confrontés aux vols de données, aux ramsomwares et aux menaces pour leur intégrité, qu'elle soit physique, économique ou territoriale.

S'agissant de l'entreprise, le numérique l'irrigue à tous les étages, dans toutes ses activités et dans toutes ses relations. Cela ne va pas aller en diminuant.

Ce que l'on appelle l'augmentation de la surface de risque est une réalité observable depuis longtemps, elle va connaître un véritable tsunami dans les années à venir. Les volumes de données générées vont en effet croitre de façon spectaculaire.

IDC, le premier fournisseur mondial de renseignements, de conseils et d'évènements sur le marché des nouvelles technologies de l'information et des télécommunications pronostique que les volumes de données générées par an en 2025 seront de 175 zettabytes[1] contre 33 pour 2018, soit une augmentation de plus de 60% chaque année.



L'impact du numérique est profond et durable

C'est pourquoi en matière de sécurité, le numérique, qui véhicule toute la valeur de l'entreprise, sa connaissance, ses projets et ses secrets, devient naturellement un élément critique à protéger et à surveiller activement.

C'est une révolution même s'il faut préciser que cette rupture technologique majeure, comme historiquement beaucoup d'autres innovations de ruptures, ne remet pas en cause les fondamentaux du cadre d'analyse stratégique de la sécurité globale.

> CONTRAIREMENT AU CREDO SELON LEQUEL LA MONDIALISATION SERAIT SYNONYME DE PAIX, EN MATIERE DE LUTTE ECONOMIQUE LA COMPETITION N'A FAIT QUE S'INTENSIFIER.

Les pratiques d'espionnage économique exacerbées par la concurrence accrue entre acteurs toujours plus nombreux ne vont pas se tarir. On voit même se profiler le spectre d'une guerre froide économique entre les Etats-Unis et la Chine comme en attestent les récentes décisions de la Maison Blanche concernant la coopération des grandes entreprises américaines du numérique avec Huaweï. La question n'est pas nouvelle.

[1] Zettabyte = 1000 puissance 7 bytes (21 zéros)

Au début des années 50 le général Carter Clarke qui dirigeait la NSA, l'agence de renseignement américaine, déclarait au sujet des alliés des Etats-Unis :

> « ILS SONT NOS AMIS AUJOURD'HUI ET SERONT NOS ENNEMIS DEMAIN. ALORS, APPRENONS-EN AUTANT QUE NOUS LE POUVONS A LEUR SUJET TANT QU'ILS SONT NOS AMIS, CAR CE NE SERA PLUS POSSIBLE LORSQU'ILS SERONT NOS ENNEMIS ».

La situation est d'autant plus complexe aujourd'hui car nous vivons dans une ère de « coopétition », où les entreprises sont régulièrement amenées à collaborer avec des concurrents potentiels, à utiliser leurs services, à avoir recours aux mêmes fournisseurs en ligne ou à se disputer les mêmes collaborateurs.

Cette « schizophrénie » des intérêts économiques va aller en augmentant, notamment si l'on considère les mutations profondes qu'implique la transformation numérique des entreprises. Celles qui ne prennent pas en compte cette vision se placent dans une position difficilement tenable pour l'avenir.

L'expérience de terrain nous montre que si les grandes entreprises mondialisées intègrent de plus en plus cette vision, les contraintes de la compétition économique pour les PME ne leur permettent pas bien souvent de se projeter dans des visions de long terme ni des planifications que ne permettent pas leurs ressources limitées en interne.

Pourtant, il n'est plus question de transformation numérique pour rester la tête au-dessus de l'eau au milieu de cet océan d'évolutions et de renouveaux qu'est le numérique. Il est désormais nécessaire et indispensable d'opérer une transformation numérique pour garantir la perdurance de son organisation pour les tendances à venir.

Dans bien des entreprises, la cybersécurité demeure une question qui se pose à un public très limité ou spécialisé, consulté en bout de chaîne, voire pas du tout dans certaines PME encore aujourd'hui. Certains parlent d'une vision de la « cybersécurité comme arrière-pensée ». Cette vision est condamnée.

> LA CYBERSECURITE EST AUJOURD'HUI, POUR LES ORGANISATIONS PUBLIQUES COMME PRIVEES, UNE QUESTION DE SURVIE

La cybersécurité doit être conçue « by design », une démarche qui est encore très loin d'être intégrée, notamment par les PME.

L'importance de la question impose une quadruple évolution dans la façon de traiter la question de cybersécurité :

1 - La question de la cybersécurité doit se poser tôt.

Dès la réflexion stratégique, la conception d'un service etc., et non en fin de parcours, d'autant plus que ce risque est difficilement transférable à l'assurance comme l'illustrent les démêlés de Maersk avec son assureur pour se faire rembourser les dégâts provoqués en 2017 par NotPetya[2].

2 - Elle doit se poser de façon prioritaire.

Longtemps parent pauvre, la cybersécurité voit aujourd'hui le budget qui lui est alloué augmenter dans nombre d'entreprises.

Mais au-delà du seul prisme budgétaire, elle doit aujourd'hui être considérée comme partie intégrante de la stratégie d'entreprise.

3 - Elle doit se poser largement.

Au niveau du top management, voire même des conseils d'administration : elle n'est pas le pré carré du CIO, du CTO ou du CISO.

En outre, la formation permanente des salariés joue un rôle prépondérant pour prévenir les attaques.

4 - Elle exige la coordination des efforts et la mise en œuvre de standards communs.

Les entreprises doivent accepter de ne pas avancer en ordre dispersé. La communauté des experts partage l'idée selon laquelle un niveau de protection élémentaire de tous les acteurs contribuera à éradiquer la vaste majorité des attaques. Si l'analogie a ses défauts, il est en revanche certain que la collaboration des acteurs jouera un rôle essentiel. Des domaines d'actions prioritaires sont identifiés : formation des collaborateurs, sécurité des chaînes d'approvisionnement, mise en place de principes internationaux de cybersécurité.

Pour toutes ces raisons,

> LA FORMATION DANS LE DOMAINE DE LA CYBERSECURITE EST DEVENUE UN ENJEU PRIMORDIAL POUR LES INDIVIDUS, LES ENTREPRISES ET LES ETATS.

Toutes les entreprises sont concernées, EFCSE souligne cependant l'importance d'un accompagnement plus spécifique des PME, qui constituent un élément essentiel du tissu économique européen.

EFCSE a un de ses Working Groups dédié éducation & formation.

Contact via efcse.eu

[2] NotPetya : 'attaque mondiale de ransomware