8 entreprises sur 10 font face à des brèches de cyber-sécurité en raison d'une mise en œuvre tardive de leur stratégie de protection

9 entreprises sur 10 ont une stratégie de cyber-sécurité, mais seulement une sur deux l'a entièrement implémentée. Résultat : 83 % des entreprises font face à des brèches de cyber-sécurité issues du décalage entre la stratégie de protection définie et sa mise en œuvre. Les hackers prospèrent dans un marché déréglementé et décentralisé, tandis que pour assurer leur défense, les entreprises se voient restreintes par le pouvoir exécutif et la bureaucratie. Les entreprises peinent à entretenir la motivation de leurs équipes informatiques dans les conditions où les cybercriminels ont toutes les chances de leur côté. Tels sont les principaux résultats de l'étude " *Tilting the Playing Field: How Misaligned Incentives Work Against Cybersecurity* " réalisée par Intel Security et le think-tank CSIS (Center for Strategic and International Studies).

Le rapport met en évidence les principales faiblesses dans l'approche des entreprises à la cyber-sécurité et leur propose d'adopter certaines pratiques des hackers afin d'éviter 3 incohérences majeures.

1. Les structures d'entreprise rigides versus la liberté d'action des cybercriminels
Le rapport d'Intel Security décortique les raisons qui ont permis aux hackers de prendre une longueur d'avance sur les spécialistes de la cyber-sécurité, dont l'agilité. Alors que le marché du cyber crime est fortement dynamique, les entreprises doivent souvent agir sous contrainte de la hiérarchie et des processus établis qui les mettent davantage en position réactive de défense face aux hackers.

« *Le marché du cyber-crime ne connaît pas la crise. Notamment grâce à sa propre structure, qui récompense rapidement les innovations et promeut les outils les plus performants* », commente Fabien Rech, Directeur Général d'Intel Security France. « *Afin de faire face aux hackers, les cyber-professionnels ont besoin d'être aussi agiles que les cybercriminels mais également de maintenir les motivations au sein de toute leur équipe informatique.* »

2. Un décalage entre la stratégie de cyber-sécurité définie et sa mise en place
Comme le démontre le rapport, il ne suffit pas simplement d'avoir établi une stratégie de cyber-sécurité pour être protégé, les surprises arrivent souvent lors de sa mise en œuvre.

Alors que plus de 90 % des entreprises affirment avoir une stratégie de cyber-sécurité, plus de la moitié avouent ne pas l'avoir totalement mise en place. 83 % admettent même avoir déjà constaté des brèches de sécurité malgré leur stratégie de protection, révélant ainsi une rupture entre la stratégie et l'implémentation.

« *C'est facile d'élaborer une stratégie, mais l'étape la plus complexe est surtout sa mise en place* », explique Denise Zheng, directrice adjointe chez CSIS. « *La manière dont les gouvernements et les entreprises adressent les possibles dissonances dans leur approche de la cyber sécurité va déterminer l'efficacité de toute leur stratégie de cyber défense. La question n'est plus de savoir ce qui devrait être fait, mais plutôt pourquoi tout n'est pas fait et surtout comment mieux le faire.* »

3. Un manque d'alignement entre l'équipe dirigeante et les personnes en charge de l'implémentation des mesures de sécurité

Les motivations des cyber professionnels ne sont pas aussi fortes que celles des cybercriminels, ce qui met en porte à faux l'ensemble de la stratégie de cyber-sécurité de l'entreprise. Par ailleurs, les dirigeants manquent souvent d'objectivité quand il s'agit d'évaluer l'efficacité des mesures incitatives envers leur équipe IT. Par exemple, 42 % des membres des équipes informatiques jugent qu'il n'existe aucune forme d'encouragement dans leur entreprise, tandis que 82 % des cadres exécutifs et 92 % des dirigeants sont persuadés de l'inverse.

A la lecture du rapport, il apparait donc que les entreprises du secteur public ont le plus de mal à implémenter une stratégie de cyber sécurité dans son intégralité (38 %). En parallèle, ce secteur constate un financement inadapté d'une grande partie de ses institutions (58 %) ainsi qu'une pénurie de compétences (63 %). Ces proportions sont moins marquées dans le secteur privé (respectivement 33 % et 43 %). Malgré le manque d'encouragement en interne, 65 % des professionnels reconnaissent être personnellement motivés pour renforcer la cyber sécurité de leur entreprise.

Les employés sont mieux placés que leur hiérarchie pour constater des insuffisances de financement et de pénurie d'effectif, à la source d'obstacles à la mise en place de stratégie de cyber sécurité réussie.
95 % des entreprises ont déjà expérimenté les conséquences de brèches de sécurité, incluant des perturbations/interruptions de leur opération, la perte d'adresse IP, des attaques directes à l'image de la marque, etc. Or, seules 32 % ont constaté une perte de revenu ou de bénéfice liée à ces brèches, ce qui peut fausser le sentiment de sécurité.

Les bonnes pratiques issues du cyber crime à adopter en entreprise :
- Opter pour une approche de Security-as-a-Service pour contrer le Cybercrime-as-a-Service ;
- S'appuyer sur une communication publique pour adresser les vulnérabilités de ses produits et services ;
- Garantir une plus grande transparence grâce au partage des informations sur les menaces ;
- Faciliter le recrutement de jeunes talents dans le domaine de la cyber sécurité ;
- Aligner les mesures incitatives à la cyber sécurité au sein de toute l'entreprise.

Pour les auteurs du rapport, de nombreuses entreprises reconnaissent la gravité du problème et sont prêtes à investir dans une stratégie de cyber sécurité. Aujourd'hui, les outils ne suffisent plus pour combattre les hackers ; il faudra déterminer également la bonne répartition entre les indicateurs de performance et les incentives dans chaque entreprise. Il est crucial que les secteurs public et privé dépassent leur vision de la cyber-sécurité comme étant une source de dépense, et qu'ils réinventent leurs approches pour reprendre une longueur d'avance sur les cybercriminels.

Méthodologie

Intel a fait appel à Vanson Bourne, spécialiste indépendant de recherche sur le marché de la technologie, afin d'entreprendre la recherche sur lequel ce rapport est basé. Intel a sondé plus de 800 personnes, provenant de compagnies de 500 à 5,000 employés de cinq secteurs majeurs, dont la finance, la santé et le secteur public. Le sondage a ciblé, aussi bien, des interlocuteurs avec des responsabilités dans la cyber sécurité que des agents avec des compétences techniques et des responsabilités dans la mise en oeuvre de la stratégie. Les pays représentés par leurs interlocuteurs sont l'Australie, le Brésil, la France, l'Allemagne, le Japon, le Mexique, Singapour, le Royaume-Uni et les Etats-Unis.

Source	http://www.infodsi.com/articles/167700/8-entreprises-10-font-face-breches-cyber-securite-raison-mise-oeuvre-tardive-strategie-protection.html