LA CYBERSECURITE

Aujourd'hui, aucune entreprise, quelle que soit sa taille, n'est à l'abri d'une cyberattaque. Ce risque cyber est souvent perçu comme un problème technique réservé aux informaticiens. C'est une erreur. Pour Guillaume Jeunot, expert en cybersécurité, « la cybersécurité est une question de gestion des risques et de protection des actifs stratégiques de l'entreprise ».

La cybersécurité reste fréquemment reléguée au second plan, par manque de temps, de compétences ou de perception du risque. « Tant qu'il ne leur est rien arrivé, beaucoup d'entreprises minimisent le risque cyber au regard des autres risques », explique Guillaume Jeunot. Mais lorsqu'un incident survient, les conséquences financières et opérationnelles peuvent être désastreuses. Alors comment se prémunir efficacement de ces menaces pour ne pas en supporter les coûts ?

Chaque année, des milliers d'entreprises françaises sont victimes de cyberattaques. Il est constaté une intensification et une diversification des attaques, touchant des structures de toute taille.

Les menaces généralement reconnues :

Les rançongiciels (ou ransomware) : prise d'otage des fichiers contre lesquels une rançon est exigée,

L'hameçonnage (ou phishing) : le réseau peut être compromis par un simple clic sur un lien frauduleux,

L'exploitation des failles de sécurité : par exemple, un simple oubli de mise à jour d'un logiciel peut devenir une porte d'entrée pour les hackers.

Cependant, pour Guillaume Jeunot, « la principale menace reste le manque de préparation des entreprises, tant sur le plan structurel que sur celui de la prise de conscience de leurs collaborateurs ».

La Cybersécurité, une nécessité pas forcément coûteuse

On croit souvent que la cybersécurité est un investissement trop lourd. Guillaume Jeunot invite les entreprises à changer de perspective : « Vous êtes-vous déjà posé la question du coût d'une paralysie totale de votre entreprise pendant plusieurs jours ? ».

Toute dépend de l'analyse du risque et du niveau d'acception que l'on veut mettre. Aux entreprises qu'il conseille, il explique que la sécurité est un risque à intégrer dans une démarche comme élément de valeur pour l'entreprise. Ainsi, « la sécurité n'est plus perçue comme un centre de coûts, mais plutôt comme une opportunité d'améliorer la performance », en se posant la question de la provenance de ce qui valorise l'entreprise. Une entreprise bien sécurisée gagne en efficacité et en crédibilité.

Contrairement aux idées reçues, la cybersécurité ne repose pas uniquement sur des solutions techniques coûteuses. Il s'agit avant tout de mettre en place des pratiques simples mais efficaces.

Il nous rappelle les fondamentaux à appliquer, pour lui, sans attendre :

Sensibiliser les équipes de manières transverse. « 90% des attaques commencent par une erreur humaine », avance Guillaume Jeunot.

Adopter une "hygiène informatique" minimale : des mots de passe robustes, des sauvegardes régulières et des mises à jour fréquentes

Contrôler les accès aux données sensibles : limiter les droits d'accès aux seuls employés concernés peut réduire considérablement les risques

Anticiper la réponse en cas d'attaque : « Avoir un plan de gestion de crise est indispensable. Il faut savoir que faire le jour où ça arrive ».

Guillaume Jeunot insiste sur un point essentiel : le premier niveau de sécurité ne relève pas de la cybersécurité, mais de la sécurité des systèmes d'information. « Avant de parler de cyberattaques, il faut déjà s'assurer que les bases sont en place. Trop souvent, ce n'est même pas le cas », précise-t-il.

Par ailleurs, avec l'essor des technologies comme l'IA, le durcissement de la réglementation sur le Cyber Résilience Act (CRA) imposant de nouvelles obligations aux entreprises ou encore l'arrivée des ordinateurs quantiques, les tendances à surveiller sont multiples. Guillaume Jeunot conseille : « Autant anticiper dès maintenant, les modèles de sécurité gagnant en obsolescence très rapidement ».

Cyberattaque, des coûts et des conséquences en cascade

Il apparait, lors d'échanges entre responsables de la sécurité des systèmes d'information (RSSI), que l'actualité est malheureusement riche en exemples d'entreprises ou de structures ayant subi des pertes significatives à la suite de cyberattaques. Toutefois, Guillaume Jeunot note que « ces incidents reçoivent moins d'attention de la part des médias ».

Pour Guillaume Jeunot, les conséquences sont bien réelles et les entreprises sous-estiment encore trop souvent l'impact économique d'une cyberattaque. « Ce n'est pas qu'une question de données volées, c'est du chiffre d'affaires perdu, une image ternie et parfois même des sanctions légales », précise-t-il.

Les entreprises doivent faire face à des coûts directs et indirects parfois sous-estimés. Il rappelle que « la reprise après une attaque est généralement plus longue et donc coûteuse que ce que les dirigeants imaginent ».

Les principaux coûts d'une cyberattaque :

Coût de remédiation : restauration des systèmes, expertise technique, renforcement des mesures de sécurité

Coûts juridiques et réglementaires : en cas de non-conformité (RGPD, NIS2, Cyber Resilience Act) des amendes peuvent s'appliquer

Coût de réputation : perte de confiance des clients et des partenaires peut impacter durablement l'activité

Coût liés aux rançons et fraudes : rien ne garantit la récupération des données après le paiement d'une rançon par exemple.

« Une attaque réussie peut faire basculer une entreprise en quelques semaines », souligne Guillaume Jeunot. Les commerçants et les PME sont particulièrement vulnérables, car ils disposent de moyens limités pour faire face aux conséquences financières d'une cyberattaque. Et cela peut aller jusqu'à la défaillance de l'entreprise. Le risque augmente d'environ 50% dans les 6 mois qui suivent l'annonce de l'incident d'une cyberattaque.

Sortir des confusions sémantiques pour mieux appréhender le risque

Guillaume Jeunot remarque que l'on parle de cybersécurité "à toutes les sauces". Il précise : « il y a une différence entre la sécurité des systèmes d'information et la cybersécurité. Et encore une autre entre sûreté et sécurité ». Un mélange qui n'aide pas à clarifier les concepts et peut nuire à la performance et à la mise en place de mesures efficaces.

Pour mieux comprendre, il nous invite à la réflexion :

Une coupure internet, est-ce un acte malveillant ou un problème technique ? Ce n'est pas la même chose en termes de réponse

Une faille logicielle non corrigée, est-ce une erreur ou une négligence ? Si un pirate l'exploite, la distinction devient cruciale.

Pour lui, « tant qu'on n'aura pas structuré ces notions, comme on l'a fait pour la sécurité physique, on continuera à perdre du temps et de l'argent ». Guillaume Jeunot rappelle une règle simple : « Le risque naît de l'exposition et plus une entreprise est connectée, plus elle est vulnérable ». La clé, c'est donc d'identifier ses points faibles et d'adopter une approche pragmatique. Il ne s'agit pas d'atteindre une sécurité absolue, mais de réduire le risque à un niveau acceptable. Et de conclure : « Une entreprise bien sécurisée, c'est une entreprise plus résiliente, plus compétitive et plus crédible aux yeux de ses clients ».

Face à la montée des cyber-menaces, il est urgent pour les entreprises de prendre conscience des risques et d'agir en conséquence. Il ne s'agit pas d'un luxe réservé aux grandes entreprises, mais d'une nécessité pour toutes les structures. La cybersécurité n'est pas qu'une question de technologie, c'est avant tout une question de bonnes pratiques, de vigilance humaine et de stratégie.