LA CYBERSÉCURITÉ est aussi une question de résilience

Bien plus qu'un sujet d'actualité, la cybersécurité a vocation à rester au cœur des préoccupations des entreprises françaises. Face à ce danger, KPMG conseille et accompagne ses clients afin de mieux anticiper et limiter les conséquences des cyberattaques. *Le point avec Vincent Maret, associé et responsable des activités cybersécurité et protection des données personnelles au sein du département Connected Tech de KPMG France.*

Vincent Maret

Comment se positionne KPMG vis-à-vis de la cybersécurité ?
KPMG est un cabinet d'audit et de conseil qui accompagne essentiellement les fonctions de direction des entreprises : directions générales, financières, des risques, du contrôle interne… La cybersécurité est un sujet et un enjeu qui concerne l'ensemble de ces fonctions au sein d'une entreprise quelle que soit sa taille.
Les cyberattaques sont devenues une réalité qui peut paralyser une entreprise pendant des semaines, exposer ses données, stopper ses activités, impacter ses résultats financiers et nuire à sa notoriété.
Notre positionnement historique auprès des entreprises et de leurs directions nous permet de les conseiller et de les accompagner face à ce défi et ce risque avec pertinence et efficacité.

Au travers de nos interventions, nous proposons :

- L'audit, le diagnostic et l'évaluation pour aider les entreprises à faire le point sur leur niveau de sécurité, les risques auxquels elles sont exposées, leurs vulnérabilités, afin d'identifier ensuite les processus, outils et mécanismes de protection à déployer ;
- Un accompagnement et du conseil sur les questions stratégiques, de gouvernance et d'organisation ;
- Ces prestations sont basées sur des expertises techniques et technologiques pointues. Nous avons notamment des hackers éthiques au sein de nos équipes qui vont, par exemple, réaliser des tests d'intrusion pour mettre à l'épreuve la sécurité du système d'information de nos clients afin d'identifier les failles éventuelles que les cyberattaquants pourraient exploiter.

Sur ce sujet autour de quelles problématiques êtes-vous sollicités ?
Le principal besoin des entreprises est de pouvoir identifier, évaluer et prioriser les cybermenaces. En effet, une entreprise peut compter des dizaines de milliers de postes, de serveurs, de sites web… À cela s'ajoute un volume colossal de données qui sont collectées, traitées et/ou stockées dans les entreprises. Un niveau de protection maximal pour l'ensemble de ces éléments est complexe à déployer et à mettre en place, d'où la nécessité de prioriser les efforts et les investissements financiers afin de privilégier les systèmes les plus critiques. Et pour ce faire, il est impératif de pouvoir s'appuyer sur une cartographie détaillée des risques cyber. Vient ensuite la mise en place des mesures de sécurisation préventives et détectives.
L'explosion des cyberattaques visant la supply chain des entreprises est un nouveau risque auquel elles sont confrontées. Dans ce cas de figure, au lieu de s'en prendre directement à un groupe ou grande entreprise, le cyber-attaquant va cibler un de ses fournisseurs ou prestataires. De plus en plus, les entreprises cherchent à mieux contrôler et quantifier ce risque en mettant en place des référentiels pour leurs sous-traitants… C'est, d'ailleurs,

"Si le risque zéro n'existe pas, il s'agit de pouvoir anticiper et limiter l'impact d'une cyberattaque. On parle alors de cyber résilience. Cela se traduit notamment par la préparation de plans de reprise, de programmation d'exercices de gestion crise pour être opérationnels le jour où surviendra une attaque…"

un sujet sur lequel nous pouvons intervenir. Ces actions doivent protéger les entreprises sans impacter le travail au quotidien des collaborateurs. Il faut pouvoir trouver le bon niveau de sécurité et faire en sorte que la cybersécurité soit abordée de la manière la plus transparente possible pour embarquer toutes les parties prenantes de l'entreprise.
Si le risque zéro n'existe pas, il s'agit de pouvoir anticiper et limiter l'impact d'une cyberattaque. On parle alors de cyberrésilience. Cela se traduit notamment par la préparation de plans de reprise, de programmation d'exercices de gestion crise pour être opérationnels le jour où surviendra une attaque...

Quel regard portez-vous sur l'évolution de ce secteur ?
Face à une menace qui ne faiblit pas, c'est un sujet critique au cœur des préoccupations des entreprises, qui n'hésitent, d'ailleurs, pas à allouer des budgets considérables et des ressources significatives afin de mettre en place des programmes visant à garantir leur sécurité.
C'est aussi un domaine qui évolue très vite avec des cyberattaquants qui se professionnalisent et qui structurent de mieux en mieux leurs attaques pour en amplifier l'impact. L'enjeu est de ne pas se laisser distancer par les attaquants qui innovent et utilisent les dernières technologies pour être plus efficaces. Côté entreprise, cela demande une veille permanente et le suivi des risques afin de garantir que les actions déployées sont toujours pertinentes vis-à-vis de la menace.
Aujourd'hui, l'impact d'une cyberattaque dépasse le périmètre de l'entreprise. Ces attaques sont de plus en plus médiatisées. Au-delà des conséquences au niveau de la notoriété et de l'image, se pose aussi la question de la confiance entre cette dernière et l'ensemble de ses parties prenantes. Et cela est encore plus vrai dans des secteurs sensibles comme les banques qui sont, d'ailleurs, un domaine très règlementé.

En parallèle, se pose également la question des compétences et des talents. Qu'en est-il et comment appréhendez-vous cet enjeu au sein de KPMG ?
Pour mettre en place une stratégie de cybersécurité efficiente, les entreprises ont besoin de pouvoir s'appuyer sur des compétences et des talents. Or, il y a, aujourd'hui, une vraie pénurie des ressources cyber sur le marché du travail français : consultants, ingénieurs, experts de la cybersécurité...
Grands groupes, ETI et PME peinent véritablement à recruter et à renforcer leurs équipes. Ces compétences sont aussi recherchées par les états et leurs différents services (renseignement, armée, police, entités dédiées à la cybercriminalité ...). Le monde du conseil aussi recrute massivement pour développer leur expertise et proposer de nouveaux services.
Face à ce constat, de nombreuses initiatives visent à solutionner ce problème. Des écoles spécialisées dans la cybersécurité ouvrent leurs portes. En interne, les entreprises proposent également des programmes et campagnes de reconversion à leurs collaborateurs pour les former et les positionner sur des métiers relatifs à la cybersécurité. Sur un plan plus opérationnel, les acteurs de la cybersécurité s'intéressent aussi de plus en plus à l'IA et aux perspectives qu'elle porte en termes d'automatisation notamment.

Quelles pistes de réflexion pourriez-vous partager avec notre lectorat sur ce sujet ?
Je pense qu'il est important de bien avoir en tête que l'ensemble des acteurs d'une entreprise, du dirigeant au manager en passant par les chefs de projets ou les ingénieurs, va être confronté à cette menace. Ce sont donc toutes les stratégies de l'entreprise, mais aussi tous ses métiers qui doivent être sensibilisés à cet enjeu.
Un autre point d'intérêt concerne la dimension technologique de la cybersécurité. Le sujet a émergé avec le développement de l'informatique. Toutefois, les dernières technologies sont aussi concernées par ce risque : le cloud, l'IA, la blockchain et demain les ordinateurs quantiques... Il ne faut donc pas oublier de les intégrer dans sa stratégie cyber.