ENQUÊTE

La Cybersécurité, un enjeu de taille pour les entreprises

Le développement fulgurant de l'intelligence artificielle a pour conséquence directe celui de la cybersécurité. Le volume croissant des datas et leur circulation de plus en plus rapide, nécessitent des investissements à la hauteur de l'enjeu, au sein d'un marché de la cybersécurité de plus en plus sophistiqué. Selon une récente étude publiée cet été par Xerfi Precepta, le marché français de la cybersécurité (logiciels, conseil et infogérance) a doublé depuis 2012.

« Les dépenses en logiciels, matériels et services de sécurité ont ainsi dépassé 2,7 milliards d'euros en 2018, soit plus de 5% de l'ensemble du marché IT. Et il devrait progresser au rythme de 8,5% par an en moyenne d'ici 2022 pour frôler la barre des 4 milliards, selon les prévisions des experts de Xerfi Precepta.

De nouvelles contraintes réglementaires (comme par exemple auprès des opérateurs de services essentiels) et la diversification des acteurs vers les TPE/PME doperont en effet les dépenses en matériels, logiciels et autres services de sécurité IT. Jusqu'ici les grands comptes constituaient le principal débouché des spécialistes de la cybersécurité. Le secteur financier, l'industrie et, dans une moindre mesure, les services publics figureront parmi les débouchés les plus dynamiques.

Par ailleurs, les cartes vont être redistribuées à la faveur des ruptures technologiques, telles que l'essor de l'intelligence artificielle et la généralisation du cloud computing, mais aussi en raison de la pénurie de main-d'œuvre. Quant aux récentes attaques d'Altran puis d'Airbus, elles ont montré que même les entreprises françaises les plus en pointe sont des cibles pour les hackers. Dans ce contexte, le recours aux services managés (externalisation) auprès de SOC (centre opérationnel de sécurité) va devenir la norme. Or, les géants du numérique (Google, Amazon ou Microsoft) se tiennent déjà en embuscade ».

COMMENT S'ORGANISE LE MARCHÉ ?

Dans l'Hexagone, le paysage concurrentiel est éclaté entre une multitude d'acteurs issus d'horizons variés avec des positionnements différents, constate-t-on chez Xerfi Precepta. *« La cybersécurité est en effet au cœur de la transformation digitale des organisations et regroupe un nombre toujours plus grand d'intervenants. Il se caractérise également par un vivier de plus de 130 start-up. Pour financer leur développement, ces jeunes pousses ont levé 100 millions d'euros ces douze derniers mois.*

Au total, les experts de Xerfi Precepta ont identifié six groupements stratégiques sur ce

... / ...

marché : les leaders mondiaux de l'édition de logiciels de sécurité, les prestataires de services informatiques généralistes, les spécialistes de la cybersécurité de nationalité française (Inside Secure, I-Tracing...), les opérateurs de télécoms (Orange, SFR, BT ou NTT)), les acteurs de la défense (Airbus Thales, Idemia) et les fournisseurs de solutions de cloud computing. Compte tenu de la forte segmentation du marché et des opportunités offertes par les menaces et les vulnérabilités d'organisations toujours plus nombreuses, la rivalité entre les acteurs reste limitée. Mais pour s'imposer sur un marché en constante mutation, tout l'enjeu est de rééquilibrer les rapports de force avec les clients.

En clair, face au risque de banalisation des solutions de sécurité, les opérateurs s'efforcent de participer à la création de valeur des entreprises clientes ».

LES GÉANTS AMÉRICAINS DANS LES STARTING-BLOCKS

Forts de leur avance technologique en intelligence artificielle et big data, ainsi que de leur incommensurable capacité de traitement et de stockage des données, les géants du cloud computing (Google, Microsoft et Amazon) semblent les mieux placés pour gagner rapidement des parts de marché ces prochaines années.
A tel point qu'ils risquent bel et bien de rebattre les cartes du marché de la cybersécurité à moyen terme. A condition de rassurer sur les enjeux de privacy (notamment pour Google).

Grâce à leur image d'expert et aux certifications obtenues ces dernières années, les acteurs de la défense auront, eux, une carte à jouer d'ici 2022. Thales pourra notamment compter sur l'intégration de Gemalto pour proposer des solutions complètes de sécurité critique.
Son expertise technique pour l'intégration de projets complexes et ses investissements en R&D seront également des atouts majeurs pour conserver durablement sa place dans le peloton de tête des leaders français de la cybersécurité.
De son côté, Orange Cyberdéfense mettra un coup d'accélérateur

... / ...

DSAGENCY
CREATIVE & DIGITAL STRATEGY

L'AGENCE CRÉATIVE & DIGITALE DE DATASOLUTION

#01 STRATÉGIE

Audit, études
Recommandations stratégiques
Transformation digitale
Consulting

#02 CRÉATION

Concepts créatifs
Direction Artistique
Expérience utilisateurs
Motion design

#03 PRODUCTION

Développements HTML5 / CSS3
Développement Open Source
Développements sur mesure
Hosting, infogérance

#04 ACTIVATION

Social Marketing
SEO / SEM
Plan média
Influenceurs

WWW.DS-AGENCY.COM | HELLO@DS-AGENCY.COM | +33 (0) 1 88 32 77 58
DS AGENCY 224 RUE DU FAUBOURG SAINT-ANTOINE 75012 PARIS

CUSTOMER RELATIONSHIP & MARKETING MEETINGS

Le Salon-Meetings de la relation & connaissance client, du marketing digital et des études

6 & 7 NOV. 2019

PALAIS DES FESTIVALS ET DES CONGRÈS DE CANNES

2 JOURS EN IMMERSION TOTALE AVEC DES DÉCIDEURS PORTEURS DE PROJETS

un événement weyou group

#CRMMMEETINGS

www.customer-relationship-and-marketing-meetings.fr

à sa stratégie ambitieuse afin de s'imposer comme un acteur de référence en Europe. Ses moyens financiers conséquents lui permettent en effet de faire ses emplettes sur le Vieux continent. Il misera également sur une diversification auprès des TPE/PME et des industriels.
A l'inverse, les leaders mondiaux des logiciels de sécurité IT seront les grands perdants de l'arrivée de nouveaux opérateurs. Déjà, l'activité de Symantec est en recul depuis 2017. Ils chercheront dès lors à se repositionner sur les services managés pour profiter de nouveaux relais de croissance.

LES SERVICES MANAGÉS, NOUVEL ELDORADO ?

Faute de formations suffisantes et avec la concurrence des autres métiers de l'information, les besoins en responsables de la sécurité des SI, chefs de projet et autres développeurs, sont loin d'être couverts. Une pénurie de compétences qui risque d'ailleurs de perdurer encore de nombreuses années, de l'avis des experts de Xerfi Precepta. Dans ces conditions, l'externalisation de tout ou partie de la cybersécurité dans des centres d'infogérance mutualisant les experts va se généraliser. En outre, ces SOC proposent des solutions de défense à la pointe de l'innovation. C'est d'autant plus vrai que l'adoption des services managés est une solution pour assurer une mise en conformité rapide face à l'inflation réglementaire émanant de l'Union européenne.

Dans le même temps, les entreprises prennent conscience de l'impact des cyberattaques (risques juridiques et économiques) et du besoin de cyber-résilience. Elles n'hésitent donc plus à débloquer des budgets dans ce domaine. Autant de raisons qui expliquent

... / ...

l'engouement pour les services managés ».

LA CYBERSÉCURITÉ, UNE PRIORITÉ POUR LES ENTREPRISES

Face à ce marché de plus en plus expert et sophistiqué, selon une étude du Capgemini Research Institute publiée également cet été, *« deux entreprises sur trois prévoient de déployer des systèmes IA dès 2020 afin renforcer leur défense. »*

Selon cette étude, *« les entreprises accélèrent le rythme des investissements dans les systèmes IA en vue de se protéger contre la prochaine génération de cyberattaques. Deux tiers d'entre elles (69%) estiment que, sans l'IA, elles ne seront pas en mesure de réagir en cas de cyberattaque majeure.*
Avec les avancées technologiques dans les domaines de cloud, de l'IoT, de la 5G et des interfaces conversationnelles, le nombre d'appareils connectés, de réseaux et d'interfaces utilisateur ne cesse d'augmenter. Dans ce contexte, les organisations doivent passer à la vitesse supérieure en matière de cybersécurité.

L'étude *« Reinventing Cybersecurity with Artificial Intelligence: the new frontier in digital security »*, a été menée auprès de 850 cadres dirigeants travaillant dans l'informatique (cybersécurité, sécurité de l'information et des opérations IT), à travers 10 pays et 7 domaines d'activité. En parallèle, le Capgemini Research Institute a organisé des entretiens approfondis avec des experts du secteur, des start-up spécialistes de la cybersécurité et des universitaires.

Ce qu'il faut retenir de l'étude, c'est que l'IA est indissociable de la Cybersécurité liée, notamment à l'augmentation des cyberattaques dont les conséquences peuvent être dramatiques pour les entreprises.

En effet, *« intégrer l'IA aux solutions de cybersécurité est devenu indispensable : pour plus de la moitié (56%) des dirigeants, les analystes cybersécurité sont submergés par la multiplication du nombre de points de données à surveiller afin de détecter et de prévenir toute intrusion. En outre, les cyberattaques qui exigent une intervention immédiate ou qui ne peuvent pas être contournées assez rapidement par les analystes ont considérablement augmenté, notamment :*

- *Les cyberattaques affectant les applications pour lesquelles la rapidité est essentielle (42% des personnes interrogées déclarent qu'elles ont augmenté, et en moyenne, de 16%) ;*
- *Les attaques automatisées, extrêmement rapides, évoluent à un rythme tel que les systèmes d'intervention traditionnels ne parviennent pas à les neutraliser (43% des personnes interrogées déclarent qu'elles ont augmenté, et en moyenne, de 15%).*

L'étude montre que face à ces nouvelles menaces, » une grande majorité des entreprises (69%) estiment qu'elles ne seront pas en mesure répondre aux cyberattaques sans l'aide de l'intelligence artificielle. Elles sont 61% à affirmer avoir besoin de l'IA pour identifier les menaces majeures. Un dirigeant sur cinq a d'ailleurs connu une faille de cybersécurité en 2018. Dans 20% des cas, l'incident a coûté plus de 50 millions de dollars à l'entreprise ciblée ».

L'autre enseignement repose sur les investissements croissants des dirigeants. *« Les dirigeants investissent de plus en plus dans l'IA pour renforcer la cybersécurité de leurs organisations : une grande majorité de dirigeants reconnait que l'IA représente sans aucun doute l'avenir de la cybersécurité :*

- *64% estiment que l'IA réduit le coût de la détection et de la correction des incidents, de l'ordre de 12% en moyenne.*
- *74% considèrent que l'IA permet un délai de réponse plus rapide avec une réduction de 12% en moyenne du temps nécessaire pour la détection des menaces, la correction des failles et le déploiement des correctifs.*
- *69% déclarent que l'IA améliore la précision de la détection des brèches de sécurité, et 60% d'entre eux estiment qu'elle*

renforce l'efficacité du travail des analystes cybersécurité, en réduisant le temps qu'ils consacrent à l'analyse des faux positifs et en améliorant la productivité.

En conséquence, près de la moitié des dirigeants (48%) indiquent que les budgets consacrés à l'IA pour la cybersécurité augmenteront de près d'un tiers (29%) au cours de l'exercice 2020. En ce qui concerne le déploiement, 73% testent actuellement des cas d'utilisation de l'IA dans le domaine de la cybersécurité. Seule une organisation sur cinq utilisait déjà l'IA avant 2019, mais les taux d'adoption s'apprêtent à grimper en flèche : près de deux entreprises sur trois (63%) prévoient de déployer l'intelligence artificielle d'ici 2020 pour renforcer leur défense ».

« L'IA offre énormément d'opportunités en matière de cybersécurité », explique **Oliver Scherer,** responsable de la sécurité des systèmes d'information (RSSI) chez Media Markt Saturn Retail Group, leader européen de l'électronique grand public. *« Aujourd'hui, le processus de détection, d'intervention et de correction est principalement manuel. Grâce à l'IA, nous allons pouvoir automatiser la correction. C'est l'objectif que toute organisation souhaite atteindre au cours des trois à cinq prochaines années. »*

Il existe des freins au déploiement de l'IA à grande échelle : 69% des dirigeants interrogés déclarent ne pas savoir comment déployer les cas d'utilisation, en phase test (Proof Of Concept), à grande échelle.

Selon **Geert van der Linden,** responsable de l'offre cybersécurité au sein du groupe Capgemini, *« Les entreprises doivent faire face à un volume sans précédent de cybermenaces de grande complexité et ont pris conscience de l'importance de l'IA comme première ligne de défense.*
Les analystes cybersécurité sont débordés, et près d'un quart d'entre eux ne sont pas en mesure de résoudre tous les incidents identifiés. Il est donc essentiel pour les organisations d'intensifier les investissements et de se concentrer sur les avantages métier que l'IA peut apporter pour améliorer la cybersécurité. »

De plus, la moitié des organisations interrogées a indiqué être confrontée à des défis d'intégration avec leurs infrastructures, systèmes de données et environnements applicatifs actuels. Bien que la majorité des dirigeants aient des objectifs précis concernant l'utilisation de l'IA dans le domaine de la cybersécurité, seulement la moitié (54%) a identifié les ensembles de données nécessaires pour rendre les algorithmes IA opérationnels.

Anne-Laure Thieullent, responsable de l'offre AI and Analytics du groupe Capgemini, conclut : *« Les entreprises doivent d'abord s'attaquer aux défis sous-jacents d'implémentation qui empêchent de maximiser le potentiel de l'IA dans le domaine de la cybersécurité. Pour cela, il faut établir une feuille de route pour surmonter ces principaux obstacles et se focaliser sur les cas d'utilisation qui peuvent être mis à l'échelle le plus facilement et offrir le meilleur retour sur investissement. Ce n'est qu'en adoptant ces mesures que les organisations pourront s'armer correctement pour s'adapter à l'évolution rapide des cybermenaces. Ce faisant, elles économiseront de l'argent et réduiront la probabilité d'être la cible de violations de données majeures. »*