SE PRÉPARER À L'INCONNU : la cybersécurité autrement

Comme les cybercriminels ne font pas de pause et que le monde s'interconnecte chaque jour davantage, les entreprises doivent s'armer d'outils de plus en plus sophistiqués pour passer de la cybersécurité à la cyber résilience. ***Interview de Marie Le Pargneux (E18), Chief Development Officer (CDO) au sein de TEHTRIS.***

Marie Le Pargneux (E18)

"Aujourd'hui, il y a environ 300 000 nouveaux types d'attaques chaque jour à travers le monde."

Autrefois traitée au niveau de la DSI, la question de la cybersécurité est devenue au cours des dernières années un sujet central pris en compte par le ComEx des entreprises. Dites-nous en plus sur cette évolution.

Ce changement reflète une vraie prise de conscience de l'importance de la sécurité informatique qui émane d'un double phénomène. D'une part, il y a une accélération accrue des attaques qui ont été quadruplées depuis le début de 2020. Cela représente environ 2 milliards de dollars de dommages par an, sans compter tous les dégâts collatéraux. En effet, aux États-Unis uniquement, plus de 18 000 entreprises ont été atteintes par des cyberattaques à la fin de 2020. Un décès a également été lié à une attaque menée contre un hôpital. D'autre part, nous remarquons une médiatisation de plus en plus forte de ces incidents, ce qui contribue à une meilleure compréhension générale des risques. Ce double phénomène est lui-même le résultat de l'interconnexion de la cyber sphère dans laquelle nous vivons. Nous sommes de plus en plus connectés, notamment à travers les réseaux sociaux, la messagerie instantanée, l'IoT, la 4G, et prochainement la 5G. Cette proximité ainsi que la multiplication des attaques et de leurs dégâts ont transformé le centre décisionnel des entreprises, notamment celles ayant des activités sensibles. En effet, de nombreux experts ont compris que l'enjeu de la cybersécurité n'est ni uniquement sur les endpoints, ni uniquement sur la périphérie, mais plutôt sur tout le parc, dans sa globalité. Il faut donc une solution étendue pour combiner tous les moyens nécessaires et disposer d'une sécurité mature. Aujourd'hui, la cybersécurité se place au cœur de la vie de l'entreprise et nécessite de ce fait l'implication de toutes les parties prenantes à tous les niveaux : CEO, ComEx, DSI, RSSI, etc. Puisque tous ces acteurs n'ont pas le même niveau d'expertise technique au sujet de la cybersécurité, nous avons conçu notre plateforme unifiée, la TEHTRIS XDR Platform, dans l'objectif de présenter une approche modulaire et holistique de la sécurité numérique.

Plus particulièrement, avec le passage au télétravail, l'année 2020 a renforcé la criticité de la cybersécurité pour les entreprises de toute taille. Qu'avez-vous pu observer à ce niveau ?

Avec le déploiement massif du travail à distance et la migration de plusieurs entreprises vers le Cloud, il y a eu une accélération inédite du nombre et de l'envergure des cyberattaques. En effet, les emails de phishing sont maintenant si bien déguisés qu'ils ressemblent à des emails de plateformes RH par exemple, et s'inscrivent donc bien dans la thématique du télétravail. De plus, les collaborateurs utilisent aujourd'hui des appareils externes pour se connecter au réseau de l'entreprise ce qui les expose d'autant plus à ces menaces. Le travail à distance a donc remis en question la notion de « château fort » où les frontières de l'entreprise sont fermées et bien protégées.

En parallèle, le fait que même les personnalités politiques peuvent être victimes de ces agressions a alerté un grand nombre de personnes à travers le monde. Par conséquent, il y a un besoin de réduire la surface d'attaque au sein des systèmes d'information des entreprises ainsi que le temps de détection et de remédiation des menaces afin

d'empêcher les pirates de les infecter dans leur globalité.

Comment expliquez-vous la sophistication, qui ne cesse de croître, de ces cyberattaques ?

Aujourd'hui, il y a environ 300 000 nouveaux types d'attaques chaque jour à travers le monde. Ce chiffre illustre bien la capacité des cybercriminels à construire leurs ransomwares à l'aide de plusieurs briques logicielles disponibles en open source à des montants relativement faibles. À l'image des pièces de Lego, ils sont capables d'assembler différents composants afin de cibler diverses parties des systèmes d'information de leurs victimes. Ils exploitent également les failles humaines ou logicielles pour installer progressivement plusieurs modules malveillants sur plusieurs machines jusqu'au lancement de l'attaque. Il s'agit d'une véritable invasion invisible et silencieuse. La cybersécurité s'est ainsi soudainement transformée en un véritable enjeu qui menace la stabilité et l'existence même des entreprises. Puisque le volume, la vélocité et la variété des attaques sont croissants, il y a plus que jamais un besoin de sécurisation automatique de bout en bout, et c'est ce que nous proposons au sein de TEHTRIS.

Comment accompagnez-vous les entreprises sur l'ensemble de ces dimensions et problématiques ?

Nous sommes un éditeur français de solutions de cybersécurité avec la seule plateforme Extended Detection and Response (XDR) européenne et entièrement native. Agissant en temps réel et avec une technologie 100 % développée en France, les menaces, connues et inconnues, sont identifiées, voire neutralisées dès leur arrivée. En effet, nous nous appuyons sur des composants réunis avec un pilotage fin et de nouvelles fonctionnalités de « hunting », couvrant la sécurisation des systèmes IT et OT, des réseaux et du Cloud. Nous proposons une plateforme qui permet aux entreprises d'orchestrer l'ensemble de leurs mesures de cybersécurité de manière proactive. Notre solution, TEHTRIS XDR Platform, est désormais déployée dans une centaine de pays dans le monde, essentiellement chez les grands groupes et les ETI. Après 10 ans de R&D, nous avons récemment levé 20 millions d'euros de série A, ce qui représente la plus grosse levée de fonds en cybersécurité européenne. Pour améliorer la lutte internationale contre les menaces cyber, nous sommes également fiers de rejoindre l'association Cyber Threat Alliance et d'être ainsi les premiers français à y adhérer, signe de reconnaissance de nos capacités.

Vous vous appuyez également sur une couche de solutions basées sur l'IA et l'automatisation des solutions de sécurité numérique. Qu'en est-il ?

En matière de cybersécurité, orchestrer les événements et réagir aux menaces avec efficacité et célérité représente un enjeu fondamental. Pour cela, nous nous appuyons sur la dernière génération d'algorithmes d'intelligence artificielle pour doter nos solutions d'une hyper automatisation particulièrement puissante. En effet, notre outil Security Orchestration Automation and Response (SOAR) est intégré à la TEHTRIS XDR Platform. Ensemble, ils permettent de gérer les différentes API internes natives qui sont utilisées entre nos produits comme EDR (Endpoint Detection and Response), EPP (antivirus nouvelle génération), SIEM (Security Information and Event Management), etc. et l'antivirus de nos clients par exemple. Cette fluidité d'action nous permet donc de neutraliser les cybermenaces en temps réel. Simultanément, la Cyber Threat Intelligence (CTI), qui est un composant interne faisant partie de la TEHTRIS XDR Platform, est utilisé par nos robots logiciels automatiquement et par les humains manuellement. En effet, grâce aux API internes, les composants de TEHTRIS peuvent demander à TEHTRIS CTI s'il existe une information sur une opération en cours. De ce fait, si un logiciel malveillant est signalé à New York, il sera par exemple partagé à Tokyo en quelques secondes. L'IA se positionne ainsi comme un stimulateur de performance pour les SOC face à la recrudescence des cybermenaces.

Pour conclure, quel message adressez-vous aux entreprises ?

Puisque le champ global de la cybersécurité aujourd'hui a été bouleversé en termes de gouvernance, d'organisation, de technologie, et d'équipes en capacité d'accompagner les entreprises, il faut s'orienter davantage vers des outils intégrés qui proposent une protection de bout en bout, automatisée et rapide. Il faudra donc opter pour un écosystème de cybersécurité. Enfin, la cyber résilience s'impose aujourd'hui comme un sujet d'actualité inévitable, surtout pour les ComEx. Pour cela, il est impératif d'intégrer ces enjeux dans le schéma organisationnel et de gouvernance des entreprises avec un tiers de confiance.