QUESTIONS À… **KAVISH DUSSOYE, «EXECUTIVE-TECHNOLOGY AND SERVICES» CHEZ BIRGER**

«L'innovation doit être encouragée tant qu'elle ne met pas à risque les données sensibles des individus et des entreprises»

Elle est certes extrêmement séduisante, la technologie, en particulier celle qui, comme l'intelligence artificielle (IA), ambitionne de repousser toujours plus loin la capacité des machines à remplacer l'homme. Mais elle peut devenir dangereuse aux mains de malfaiteurs. Cette situation a favorisé le partenariat entre Mastercard, prestataire international de services financiers numériques et BIRGER, qui, depuis son incorporation en 1953, est reconnu comme un fournisseur de solutions technologiques dans la région océan Indien-Afrique de l'Est. Kavish Dussoye explique la raison d'être de ce partenariat.

■ Quels sont les facteurs associés aux risques de pratiques criminelles et malveillantes visant à perturber le fonctionnement des systèmes informatiques ou réseaux de données, qui ont été déterminants pour favoriser ce partenariat entre Mastercard et BIRGER ?

La transformation numérique accélérée est aujourd'hui une nécessité à laquelle toutes les entreprises devraient recourir pour rester compétitives et répondre aux attentes du marché. La contrepartie est que de telles initiatives augmentent drastiquement les points d'entrée des systèmes informatiques et génèrent un volume considérable de données, offrant en même temps un terrain d'exploitation idéal pour les cybercriminels. C'est une situation qui a entraîné une montée de menaces ciblées et générées à grande échelle en ayant recours aux potentiels de l'intelligence artificielle (IA). D'où l'importance d'une approche centrée sur les risques dans la stratégie de cybersécurité.

■ En quoi Mastercard et BIRGER contribuent à ce projet de partenariat ?

Dans le cadre de cette collaboration, Mastercard apportera son expertise mondiale et ses capacités en matière de cyber-renseignements par rapport à la prévention de fraude, à la cybersécurité et à l'identité numérique pour sécuriser l'économie de la région. Cette expertise de Mastercard va bien au-delà de son écosystème de paiement pour englober tant la gestion des risques qui découlent de l'usage des technologies numériques que la sécurité informatique des entreprises. BIRGER, en tant que pionnier en conception de solutions et de services technologiques avec une présence établie dans la région de l'Afrique de l'Est, assurera des services de proximité dans le déploiement des solutions de Mastercard. BIRGER s'appuiera sur l'expertise de ses spécialistes expérimentés et formés en cybersécurité, de sa connaissance du marché régional et de son centre d'opérations de sécurité, opérationnel depuis 2016 sur une base 24h/7, pour offrir des services adaptés aux besoins spécifiques du marché.

■ Quels sont les risques les plus à même d'occasionner d'importantes perturbations aux systèmes informatiques des entreprises ?

Il existe en effet plusieurs types de risques qui peuvent exposer les entreprises aux dangers des cyberattaques. Je placerai en première position la complexité accrue des systèmes informatiques. Cette situation nécessite la mise à jour des logiciels existants. Cependant, le nouvel environnement peut être difficile à gérer. L'une de ses principales caractéristiques est qu'il peut parfois exposer des situations de vulnérabilité des entreprises, qui peuvent être exploitées par des cybercriminels. La deuxième catégorie de risques qui peuvent mettre en danger la cybersécurité des entreprises peut avoir pour point de départ l'environnement informatique des parties prenantes, incluant les partenaires externes. Une faille dans l'écosystème d'un partenaire peut constituer un danger pour un système de protection des données sensibles. Elle peut même perturber la continuité des activités. La troisième catégorie de risques concerne ceux qui ciblent les ressources financières des entreprises. Les fraudes financières peuvent être occasionnées par l'erreur car il est impossible d'écarter la possibilité que des erreurs puissent s'infiltrer dans l'exécution des tâches confiées à des hommes. Les fraudes financières peuvent aussi avoir pour origine la présence de lacunes au niveau des procédures internes.

■ Venons-en aux solutions que vous proposez. Quelles sont-elles ?

Les principales fonctionnalités des solutions proposées par Mastercard sont : la Cyber Quant : un outil automatisé et complet qui peut quantifier les cyber-risques, permettant ainsi aux équipes d'analyser leurs infrastructures informatiques afin de recommander des actions concrètes ; les Cyber Insights : une plateforme qui permet d'évaluer en temps réel des menaces dynamiques offrant ainsi une visibilité sur les tendances d'attaques actuelles et futures, une voie indispensable pour la prise de décisions stratégiques ; le système de surveillance proactive des cybermenaces RiskRecon : destiné aux entreprises qui ont une présence en ligne et qui leur permet de repérer l'existence de risques avant qu'ils ne puissent être exploités.

Par ailleurs, l'identification et la défense contre les menaces potentielles les plus importantes grâce à des simulations d'attaques sont la mission de la solution CyberFront. Elle a deux objectifs. Le premier aide une entreprise à identifier les situations où elle ne dispose pas de moyens pour repérer ses points faibles. Le second vise à tester la capacité de réaction d'une entreprise si de telles menaces se matérialisent. Le Cyber Crisis exercice est un service de conseil et d'accompagnement qui permet de reproduire des scénarios de crise pour tester la capacité de rebond d'un client, améliorer le niveau de coordination et limiter l'impact d'incidents sur les opérations d'une entreprise.

La *threat protection* assure la protection de la confidentialité, l'intégrité et la disponibilité des systèmes informatiques, des réseaux et des données contre les cyberattaques et les accès non autorisés ; et le *Brighterion*, un logiciel qui peut détecter, en temps réel, l'émergence de situations à risques et de fraudes dans l'environnement informatique où se déroulent des transactions financières ; et peut réduire l'intrusion de fausses alertes et minimiser le niveau de risques où des pertes peuvent avoir lieu. Il s'agit d'une prédisposition qui peut contribuer à renforcer le niveau de confiance des clients dans les activités d'une entreprise qui a adopté cette solution.

■ Selon vos études, quels facteurs contribuent au développement de ces outils en violation des droits fondamentaux tant des individus que des organisations qui utilisent des plateformes informatiques ?

L'IA est une technologie innovante qui est aujourd'hui utilisée par les cybercriminels pour concevoir rapidement des outils malveillants de plus en plus sophistiqués. Certains de ces outils sont même disponibles sur le *dark web*. Qu'à cela ne tienne, l'IA dispose parallèlement d'atouts majeurs susceptibles de renforcer le niveau d'efficacité des mesures mises en place pour lutter contre la cybercriminalité, automatiser le système de détection des menaces et améliorer l'efficacité des systèmes pour assurer la protection de l'environnement informatique où évoluent tant les individus que les entreprises. L'absence d'une campagne permanente pour l'adoption de bonnes pratiques qui contribueraient à renforcer les mesures pour lutter contre la cybercriminalité encourage les auteurs de ces délits à concevoir, développer et perfectionner ces outils de travail plus rapidement et à une plus grande échelle.

■ La difficulté des stratégies de lutte contre la cybercriminalité réside dans le recouvrement des biens perdus car les fraudeurs sont partout et nulle part. Comment y remédier ?

En général, les pratiques de cybersécurité s'appuient sur des outils de sécurité, des cadres de référence reconnus et la souscription aux obligations des réglementations en cours, bien que cette approche constitue une base essentielle qui nécessite d'être complétée par des solutions plus adaptées aux réalités spécifiques de chaque entreprise. La stratégie de Mastercard repose sur une approche holistique et orientée vers les risques pour sécuriser les données, renforcer la posture de sécurité et guider la prise de décision stratégique adaptée au contexte spécifique des entreprises. Pour allouer efficacement les ressources et prioriser les actions, il est essentiel de vérifier le contrôle des mesures de sécurité déjà en place, de contextualiser et de quantifier les risques.

Le cyber-renseignement généré par la plateforme Recorded Future de Mastercard fait partie intégrante des solutions proposées à cet effet, telles que les sept plateformes mentionnées dont nous avons déjà fait état. Une approche basée sur les risques ne se limite pas à l'existant. Elle anticipe les menaces émergentes. La gestion des risques ne concerne pas uniquement la technologie mais concerne également celle des processus et le mode d'opération des équipes. Pour compléter cette approche, le recours à un plan de cyber-résilience s'impose afin d'assurer la continuité des opérations et de permettre un rétablissement rapide en cas d'incident. En combinant protection et cyber-résilience, l'entreprise renforce sa sécurité globale et consolide sa pérennité dans un environnement numérique en constante évolution.

■ La réponse aux nombreux risques de cybercriminalité ne se situe-t-elle pas plus au niveau de la réglementation par rapport à l'utilisation ou la classification des applications inspirées de l'IA que dans la conception de solutions qui est votre domaine d'exploitation ?

La réglementation joue un rôle essentiel en imposant des normes de sécurité et en encadrant la protection des données. Cependant, elle reste souvent statique et rigide face aux cybermenaces en constante évolution. Avec 3,5 milliards de cartes émises à travers plus de 210 pays et territoires, 200 cyberattaques détectées et neutralisées chaque minute et 159,4 milliards de transactions traitées en 2024, Mastercard a mis en place son réseau de cyber renseignement sur lequel elle s'appuie pour la mise en œuvre de solutions de protection adaptées afin de compléter le respect des normes et des réglementations.

■ Comment trouver un juste équilibre entre la liberté d'innover et la nécessité de protéger la vie privée des individus et les données sensibles des entreprises et organisations tant publiques que privées ?

L'innovation doit être encouragée tant qu'elle ne met pas à risque les données sensibles des individus et des entreprises pour faire avancer notre société. Tant que les entreprises sont bienveillantes et conformes aux lois et normes existantes, elles doivent avoir la liberté d'innover tout en adoptant le principe de sécurité dès la conception. Il existe de nombreuses lois, telles que le Règlement général sur la protection des données (RGPD) en Europe et la *Data Protection Act* à Maurice, tous deux en vigueur depuis 2018, qui ont pour but d'assurer la protection des données des individus et des entreprises.

■ Est-ce une utopie de vouloir mettre de l'ordre dans le secteur des technologies qui ressemble plus à une jungle qu'à autre chose ou bien la meilleure posture serait de laisser faire ?

Le laisser-faire n'est certainement pas une option. Il faut encourager l'innovation tout en s'assurant que les solutions n'entravent pas les règles de la société mais permettent son avancement.

n Comment réguler la situation si la conception de pratiques frauduleuses sont l'œuvre des créateurs d'applications technologiques ?

Ce risque peut être géré à travers la régulation et autres mesures telles que le renforcement des cadres légaux et des sanctions, l'audit indépendant et obligatoire des codes source et des procédures et la certification de conformité validant la sécurité des applications. L'éducation et la sensibilisation des utilisateurs, ainsi que la promotion de l'éthique numérique, constituent des valeurs universelles permettant de distinguer les intentions malveillantes et de réduire les risques liés à l'usage des technologies.

Propos recueillis par
Lindsay PROSPER