POUR UNE MEILLEURE APPRÉHENSION ET GESTION du risque cyber

Sandra Maury, Chief Information Security Officer France ; Emmanuel Barrier, Core Practice Leader Security & Resiliency France ; Niamkey Ackable, Deputy Practice Leader Security & Resiliency France, au sein de Kyndryl, répondent à nos questions sur la cybersécurité.

Sandra Maury

Emmanuel Barrier

Niamkey Ackable

La cybersécurité est au cœur des préoccupations depuis plusieurs années. Quelles sont les évolutions que vous avez pu observer dans ce cadre ?
Le contexte géopolitique actuel, La COVID-19, la complexité et l'hétérogénéité des systèmes, l'accès immédiat et sans limitation à la donnée sans oublier la pénurie des compétences en matière de cyber sécurité ont amplifié le risque cyber dans le monde entier.
L'indisponibilité des environnements de production IT due à l'explosion en nombre et en amplitude des cyberattaques tel le ransomware, a mis en évidence l'impact économique et la fragilité des entreprises ainsi que la nécessité de repenser leur modèle de protection en intégrant dans leur stratégie de sécurité, des mesures de résilience opérationnelle.
L'évolution du paysage des risques de sécurité et l'industrialisation des cyberattaques ont entraîné un nombre croissant d'incidents de sécurité, la motivation liée aux gains avec un « retour sur investissement » rapides générés par les rançons ont transformé nos systèmes d'information en « cash-machine », des organisations cybercriminelles.
Les approches de sécurité conventionnelles ne sont plus suffisantes pour prévenir et contenir toutes les failles de sécurité.

Dans ce secteur, quel est votre positionnement ?
Fort d'une expérience de plus de 30 ans dans la gestion opérationnelle des systèmes d'information critiques de nos clients et leur résilience, nous avons développé une expertise unique et en profondeur de la sécurité opérationnelle en capitalisant sur un modèle « Glocal » avec des capacités locales (14 datacenters et centres de services en France) et une organisation globale au ser-

vice de nos clients internationaux. Notre rôle est de les accompagner dans leur transformation digitale et de leur permettre d'assurer, tout en même temps, un haut-niveau de sécurité et de résilience adapté à leurs enjeux métiers.

Il existe aujourd'hui sur le marché un nombre grandissant de solutions et d'outils en sécurité. De par notre expertise éprouvée, fort de plus de 8000 experts en cyber résilience répartis à travers le monde et en nous appuyant sur un écosystème unique de partenaires stratégiques au niveau mondial, nous nous positionnons en tant que « vendor agnostic » pour aider nos clients à construire une vision et une roadmap stratégique de leur cyber sécurité, en rationalisant les solutions existantes et en les accompagnant dans la déclinaison opérationnelle de ces choix comme la définition, l'intégration et l'administration des solutions durant tout le cycle de vie de leur exploitation.

Pour répondre aux nouveaux enjeux et à l'évolution rapide des menaces auxquels font face nos clients, nous nous sommes transformés, en capitalisant sur notre ADN issu de la production informatique et de la sécurité opérationnelle, pour faire évoluer naturellement notre organisation autour de notre proposition de valeur. Nous avons le plus grand centre de résilience d'Europe avec des experts passionnés et une capacité de reconstruction complète des environnements de production de nos clients dans un environnement externe, étanche, sécurisé, isolé physiquement comme logiquement. Nous mettons au service des entreprises des environnements et des équipes dédiées à la restauration des systèmes d'information. C'est un atout indispensable pour se préparer à tout évènement disruptif et réagir efficacement lors d'une cyberattaque pour optimiser la continuité de service.

Aujourd'hui, autour de quels enjeux et problématiques êtes-vous sollicités ?

Du fait du positionnement de Kyndryl sur les activités historiques d'infogérance auprès de nos 400 clients en France issues de différents secteurs d'activités du tissu économique français avec des tailles et des chiffres d'affaires variés – nous avons une légitimité en tant qu'expert sur le domaine de gestion de la production informatique et de sécurité opérationnelle, et accompagnons nos clients sur les problématiques et les challenges actuels du marché cyber et de la transformation digitale.

Par ces différentes sollicitations, nous observons les enjeux stratégiques de la transformation digitale suivants :

- La différenciation grâce au digital ;
- L'innovation et la simplification des systèmes d'information ;
- Le développement de services davantage orientés « utilisateur final » ;
- L'agilité et l'adaptation ;
- La sobriété et la souveraineté ;
- La régulation avec un renforcement du cadre règlementaire autour de la cyber sécurité et la résilience opérationnelle ;
- Le concept de cyber résilience.

Aujourd'hui, la principale sollicitation de nos clients et de nos partenaires, réside autour des problématiques de reconstruction post-attaque cyber. En effet, la multiplication des menaces cyber et le nombre croissant des cyberattaques, influence de manière significative les préoccupations des entreprises et place, aujourd'hui, le risque cyber au cœur des enjeux et des préoccupations de toutes directions d'entreprise, institutions et organismes.

Quelles sont les tendances qui se dessinent actuellement ? Comment les anticipez-vous ?

La cyber résilience a commencé à faire son entrée comme thématique « mainstream », car il ne s'agit plus seulement de sécuriser les frontières du système d'information au sein d'un écosystème grandissant, mais de s'assurer que toute organisation et toute activité Métier peut se remettre de tout évènement disruptif majeur incluant une cyberattaque, grâce à des pratiques de cyber résilience.

Nous remarquons également l'ascension de la résilience à la table des comités de direction avec l'évolution du métier et des responsabilités du Chief Information Security Officer (CISO) allant jusqu'à l'émergence de nouveaux rôles dédiés comme celui du Chief Resiliency Officer (CRO).

Les impératifs de résilience opérationnelle font évoluer naturellement les stratégies de sécurité des organisations. Les cyberattaques gagnent en volume, en variété, en complexité et en précision. Tout cela positionne la cyber résilience comme un impératif stratégique et représente la top-priorité pour toute direction d'organisation à court et moyen terme. Chez Kyndryl, nous avons élaboré nos offres et nos services Cyber Resilience de notre practice Security & Resiliency en se basant sur le framework du NIST et associant la cyber sécurité et la résilience autour d'une approche unique reposant sur 4 piliers pour aider nos clients à anticiper (Security Assurance Services), se protéger (Zero Trust Services), résister (SOC & Response Services) et se remettre de situations défavorables (Incident Recovery Services).

En outre, pour aider nos clients à faire face à ces enjeux, challenges et menaces, nous nous sommes dotés de plusieurs capacités de services en :

- Conseil – avec des services d'assessment en sécurité, résilience, maturité cyber résilience, stratégie, conformité, gestion de crise et mesures de détections avancées ;
- Intégration – avec une expérience opérationnelle forte de capacités d'accompagnement dans les phases de projets, de déploiement de solutions, de méthodes et d'outils ;
- Services managés – disposant d'une expertise éprouvée en secourabilité, à travers des services de reconstruction des environnements sur des infrastructures sécurisées et hébergées dans nos datacenters interconnectés entre eux et avec la plupart des fournisseurs de services Cloud.

Entre autres, nous proposons une solution dédiée de sanctuarisation des actifs vitaux et critiques d'une entreprise et nous sommes en train de décliner cette solution en mode mutualisé afin de permettre à des organisations avec des budgets plus modestes de pouvoir avoir une assurance raisonnable quant à leur capacité à se remettre d'un évènement disruptif tel que le ransomware.

Et pour conclure ?

La cyber résilience est la réponse pragmatique à l'évolution des enjeux liés à la fois à l'accélération de la transformation digitale et de la menace cyber, croissante et protéiforme qui pèse sur nos entreprises.

Kyndryl en tant que leader en cyber résilience et partenaire de confiance – à travers ses talents, son écosystème, ses services et ses solutions, continue d'investir et innove pour compléter son portfolio d'offres afin d'accompagner nos clients pour leur permettre de poursuivre leurs objectifs de transformation tout en continuant de proposer de la valeur et en atténuant les impacts de tout évènement disruptif.