ATOS

LA PAROLE À SOPHIE HOUSSIAUX ET ALEXIS CAURETTE

Quels sont les enjeux liés à la cybersécurité ?

On observe une professionnalisation des organisations mafieuses et des attaques qui ciblent davantage les banques. Les acteurs malveillants qui récoltent des millions d'euros, réinvestissent fortement dans la R&D et se dotent de moyens avancés.

L'environnement est très complexe et difficilement maîtrisable pour les banques qui sont ciblées sur tous les canaux : web, monétique, DAB… Mais aussi sur les réseaux interbancaires comme Swift.

Autre élément, face à ces risques qui montent de manière forte, les régulateurs, l'Europe et les États, par exemple en France avec la loi sur la programmation militaire, imposent aux acteurs d'importance vitale un haut niveau de sécurité adapté à la menace et des capacités de détection, de notification et de réaction aux attaques avancées,. Les exigences en matière de cybersécurité sont relevées et cela engendre une transformation.

Dernier point. Les montants investis par les banques et assurances ne sont pas à la hauteur des enjeux. Les investissements dans la sécurité physique sont 10 fois supérieurs à ceux de la cybersécurité. Les établissements sont dotés de techniques qui ne sont plus suffisamment efficaces par rapport à la multiplication des canaux : monétique, réseaux sociaux, web, mobile… Il y a un changement de posture et organisationnel de la part des banques notamment impulsé par les régulateurs. Les banques doivent être accompagnées, transformer leurs approches et compléter leurs dispositifs par des systèmes de détections informatiques avec des scénarios métiers et des analyses comportementales.

De quelle manière accompagnez-vous vos clients ?

Il y a une tendance aux changements. On parle de nouvelles capacités en cybersécuri-

té qui touchent la sécurisation des canaux, les détections des attaques, le déploiement de réactions et la reconstruction rapide des SI. Il faut accélérer pour protéger les systèmes les plus sensibles et stratégiques. On a des solutions de gestion d'accès interconnectées avec le SOC qui permettent une authentification contextuelle et qui peuvent demander une double authentification pour une confiance supplémentaire. Nous proposons ainsi une défense contextuelle.

Nous sommes fournisseurs de services d'audit, de conseil, de services de sécurité opérée de confiance et nous sommes un éditeur de logiciel et de matériels de confiance conforme aux exigences de la loi de programmation militaire. Nous adressons l'implémentation de la sécurité avec un niveau très élevé répondant aux exigences de souveraineté en France et en Europe.

Gérer des attaques sensibles demande un haut niveau de sécurité et un système de collecte et de détection qui soit pointu et de rendu totalement transparent pour l'attaquant.

Nous développons des technologies de gestion des identités, de chiffrement des canaux de communication et des données, d'échanges de clés de sécurité… Qui s'intègrent dans les dispositifs traditionnels et permettent la mise en conformité avec les exigences réglementaires. Nous accompagnons nos clients dans les ruptures technologiques à travers le big data, par exemple, qui entraînent une centralisation des données et de nouveaux besoins en matière de contrôle d'accès et de chiffrement. C'est aussi le cas pour la blockchain qui est un système de confiance décentralisé, encore peu mature et sujet à des détournements. Il s'agit d'analyser ces technologies et d'évaluer précisément leurs risques.

Quels sont les risques et les opportunités de l'ordinateur quantique ?

Le sujet quantique existe depuis 90 ans ! Nous assistons à une nouvelle approche dans le domaine du quantique. Il y a de nombreux domaines d'applications intéressants. Atos a ouvert un laboratoire quantique qui réalise des travaux de recherche dans trois domaines. La programmation quantique pour trouver des solutions innovantes et de nouveaux algorithmes pour le big data, l'intelligence artificielle, les calculs haute performance, la cybersecurité principalement. Le travail sur les machines à simulation de circuits quantiques. Et les algorithmes post-quantiques avec aujourd'hui notamment celui de Shor qui offre de nouvelles perspectives dans l'amélioration de la résistance et pourrait décupler les capacités de traitement. Progressivement, nos travaux de recherche apportent des briques d'innovation incrémentale qui nous permettent d'apporter toujours plus de valeur à nos clients afin de les aider à faire face aux nouveaux défis et particulièrement en matière de cybersécurité. ■