Parwez Bhugalee (Birger)
« En matière de cybersécurité, il faut être proactif »

L'entreprise mauricienne Birger vient de publier sa deuxième enquête régionale sur la cybersécurité des entreprises qui identifie toujours des lacunes importantes. L'analyse de Parwez Bhugalee, exécutif en charge du marketing et du développement des affaires chez Birger.

Propos recueillis par J.Rombi - j.rombi@ecoaustral.com

L'Eco austral : Pourquoi Birger a-t-il décidé de réaliser des enquêtes auprès des entreprises de la région ?

Parwez Bhugalee : Notre enseigne existe depuis plus de 65 ans et a accompagné tous les cycles de la technologie et l'émergence des TIC dans notre région. Nous avons été des pionniers dans différents secteurs avec, par exemple, l'introduction des GAB dans les îles de l'océan Indien ou encore l'installation du premier ordinateur à Maurice. Notre spécialisation dans la cybersécurité est aujourd'hui la suite logique de cette aventure. Cela fait plus de quinze ans que nous nous intéressons à la sécurité avec des solutions de type *firewall*, antivirus, protection des données et autres. Mais avec l'évolution des cyber-menaces et les demandes du marché, nous avons élaboré en 2015 une stratégie de cybersécurité avec des partenaires qui sont leaders du secteur comme l'Américain Symantec qui nous accompagne à Maurice, dans les îles de l'océan Indien et en Afrique. Cette stratégie a culminé avec l'ouverture du premier centre de cyberdéfense à Maurice, à Phoenix. Il fait référence dans la région proche mais aussi dans toute l'Afrique et nous proposons aujourd'hui des solutions qui reposent sur trois éléments clés : Technologie - Sécurité - Résilience. Il nous fallait accompagner cette croissance par des référents nous permettant de comprendre la nature des risques, leurs origines et les solutions proposées. D'où cette enquête sur la cybersécurité.

Jusqu'en 2017, il n'y avait donc pas vraiment d'évaluation des cyber-menaces ni des moyens de défense ?

En effet et c'était d'autant plus problématique que, même s'il y a beaucoup de similitudes avec les autres régions dans le monde, les enquêtes nous ont montré qu'il y avait certaines spécificités à prendre en compte. D'où l'intérêt de comprendre les menaces qui sont les plus pertinentes dans la région et de mettre en place des solutions et des méthodologies adaptées.

En outre, nous avons affiné ces résultats de façon à mesurer le degré de maturité des entreprises en cybersécurité en utilisant le *CYIndex.* Celui-ci se base sur cinq fonctions clés : Identifier - Protéger - Détecter - Répondre - Reprise. L'index peut être décliné par pays, secteurs ou segments d'activité. Le *CYIndex* est aussi utilisé pendant les audits de sécurité. Par exemple, une grande banque internationale vient de nous faire une demande d'audit de sécurité dans 16 pays à l'issue de la publication de cette enquête. Ils nous ont choisis pour notre connaissance pointue des écosystèmes de la région.

DR

Après avoir débuté sa carrière à l'extérieur de Maurice en tant qu'ingénieur système junior, Parwez Bhugalee a travaillé pendant trois ans sur les marchés étrangers avant de rejoindre Birger en 2003.

Comment s'est déroulée l'enquête et quels en sont les résultats ?

Dès 2017, nous avons fait appel aux services du cabinet DCDM Research, spécialisé dans ce type d'enquête. La méthodologie, pour être fiable, devait prendre en compte au moins 200 répondants et, pour cette dernière enquête de terrain, nous en avons eu 211 pour 142 entreprises. Cela signifie que pour certaines entreprises, il fallait questionner plusieurs personnes comme le responsable informatique et le directeur de la production. L'enquête s'est déroulée au troisième trimestre 2018 sur neuf pays qui sont Maurice, Madagascar, les Comores, les Seychelles, le Rwanda, l'Ouganda, la Tanzanie, le Kenya et le Swaziland.

Les résultats indiquent que Maurice est toujours numéro en Afrique en matière de cybersécurité, suivie de près par le Rwanda. Cela est en marge de l'index international GCI–ITU. Quant à la nature des attaques dans notre région, elles sont dues principalement au facteur humain, avec une carence des ressources humaines liée à un manque de formation du personnel en place, le manque de budget alloué à la cybersécurité, ainsi qu'à l'évolution rapide des cyberattaques et le manque de cyberintelligence. D'où l'intérêt d'être proactif plutôt que réactif comme c'est trop souvent le cas. ■