INTENSIFICATION DES CYBERATTAQUES
LE SECTEUR FINANCIER À RISQUE

BUSINESS FILES

LA CYBERCRIMINALITÉ, QUI FAIT FI DES FRONTIÈRES, EST RESTÉE TRÈS INTENSE ET A TRÈS FORTEMENT TOUCHÉ LES ENTREPRISES MAURICIENNES. SELON LE CHECK POINT SECURITY THREAT INTELLIGENCE SUMMARY, CES DERNIÈRES AURAIENT SUBI ENTRE DEUX ET TROIS FOIS PLUS DE CYBERATTAQUES QUE LE RESTE DU MONDE AU DEUXIÈME SEMESTRE 2021. CETTE TENDANCE S'EXPLIQUE EN GRANDE PARTIE PAR LA CRISE DE LA COVID-19, QUI A VU S'INTENSIFIER LES ACTIVITÉS EN LIGNE, ET EN CONSÉQUENCE LES ACTIVITÉS CYBERCRIMINELLES.

EVE FIDÈLE / RICHARD LE BON

LE TAUX croissant de transformation numérique au sein de l'île Maurice et de la région africaine facilite l'émergence de nouveaux vecteurs d'attaque et d'opportunités pour les cybercriminels. Comme le souligne Krishna Radhakeesoon, Partner chez BDO, à Maurice, la cybercriminalité est en hausse avec plus de 1 000 plaintes signalées au Computer Emergency Response Team (CERT-MU) depuis le début de l'année. Cette statistique n'est que la partie émergée de l'iceberg ; il y a tant de cas non signalés de cyberintimidation, d'usurpation d'identité, d'attaques par ransomware, de piratage, etc., qui ne font pas la une des journaux car les victimes (personnes et organisations) préfèrent protéger leur image et leur réputation.

«*La même tendance est observée dans la région de l'océan Indien et sur le continent africain. Selon l'African Cyberthreat Assessment Report 2021 d'Interpol, les cybercriminels développent et renforcent leurs attaques à un rythme alarmant, exploitant la peur et l'incertitude causées par la situation sociale et économique instable créée par la Covid-19. On constate donc une augmentation du niveau de créativité et de sophistication des cyberattaques. Le coût des cybercrimes est donc en*

ON ASSISTE À UNE AUGMENTATION CONSIDÉRABLE DES CYBERATTAQUES AU COURS DES DERNIÈRES ANNÉES AVEC UNE MULTIPLICATION DES ESCROQUERIES EN LIGNE

hausse, avec une augmentation notable du nombre de cyberattaques très médiatisées», explique Krishna Radhakeesoon.

Kevin Mulliah, Business Development & Sales Manager chez Harel Mallac Technologies, ajoute qu'il est bien de faire ressortir que la portée de la cybercriminalité dépasse les cadres nationaux, et Maurice n'en est pas une exception. Internet a aboli les frontières et les cybermenaces sont bel et bien réelles. Une cyberattaque peut avoir un impact direct et indirect sur n'importe quel pays du monde. Selon ses observations, à Maurice, nous ne pouvons malheureusement pas chiffrer le niveau de cybercriminalité à ce jour, mais d'après The Mauritian Cybercrime Online Reporting System (MAUCORS), à peu près de 1 200 cas ont été enregistrés par le grand public à travers plusieurs plateformes digitales. Cela n'indique en aucune manière le niveau de la cybercriminalité dans le secteur professionnel où la majorité des cas ne sont pas mis à découvert pour des raisons strictement professionnelles.

«*Depuis ces deux dernières années, et surtout suite à une dépendance accrue des activités en ligne liée à la période de pandémie, le monde a assisté à un regain des activités liées à la cybercriminalité souvent dû aux pertes d'emplois et à la crise économique où les organisations criminelles ont trouvé de nouvelles opportunités. L'Afrique ainsi que les pays de la région, dont Maurice, émergent rapidement au niveau de l'adoption des plateformes digitales et technologiques dans plusieurs secteurs d'industries. Et ils en deviennent par conséquent beaucoup plus vulnérables face aux cybercriminels. Cette demande grandissante pour la technologie, couplée à un manque de principes fondamentaux de la cybersécurité, nécessite une bonne gouvernance afin d'anticiper les risques et de bien protéger les entreprises. Certains pays africains avancent à grands pas tandis que d'autres peinent à établir les infrastructures nécessaires dans un cadre de loi adéquat*», souligne Kevin Mulliah.

CYBERCRIMINALITÉ EN HAUSSE

Le nombre croissant de cas de cybercriminalité est un sujet de préoccupation dans le monde entier, y compris en Afrique et à Maurice. En ce qui concerne la situation à Maurice, Ashiss Soobhug, Head of Cybersecurity Advisory chez Rogers Capital, abonde dans le même sens que Krishna Radhakeesoon et Kevin Mulliah. Il dit avoir constaté une augmentation considérable des cyberattaques au cours des dernières années avec une multiplication des escroqueries en ligne, des e-mails de phishing, des attaques de ransomware et de la compromission des e-mails professionnels qui ont déjà fait quelques victimes.

Ashiss Soobhug fait ressortir que selon un rapport d'évaluation des cybermenaces d'Interpol publié pour l'Afrique en 2021, Checkpoint Software Technologies, qui est un leader des solutions de cybersécurité, a rapporté que les organisations africaines ont connu la plus forte augmentation d'attaque, de janvier à avril 2021, soit plus de 34 % de hausse. Le rapport a mis en lumière une situation de plus en plus inquiétante en matière de risques, en particulier pour les plateformes bancaires en ligne contre lesquelles une augmentation de 238 % des cyberattaques a été estimée pour 2020. Les services liés à Internet, en particulier les services jugés critiques pour les entreprises financières, ont une valeur de piratage importante et restent dans le radar des cybercriminels.

Face à ces menaces constantes, Shanah Bucktowar, Information Security Officer à ENL, rappelle que selon la dernière évaluation menée par l'Union internationale des télécommunications (UIT) couvrant la période 2019 - 2020, le score global montre un engagement croissant dans le monde entier pour lutter contre et réduire les menaces de cybersécurité. Le développement de chaque pays est évalué selon cinq piliers stratégiques : mesures juridiques, mesures techniques, mesures organisationnelles, renforcement des capacités et coopération internationale.

MENACES SUR LE PLAN LOCAL

Depuis le début de l'année 2022, des milliers d'incidents de sécurité divers ont été enregistrés à Maurice. Les types d'incidents signalés comprennent le harcèlement en ligne, la fraude et les escroqueries en ligne, le vol d'identité, la cyberintimidation et la sextorsion. Les entreprises mauriciennes sont plus susceptibles d'être victimes de deux types d'attaques pouvant entraîner des dommages financiers élevés. La première est le ransomware, qui crypte les données et oblige les entreprises à payer en cryptomonnaies, principalement en bitcoins, pour récupérer leurs données. La deuxième catégorie est l'usurpation d'identité par courriel, qui consiste à envoyer des demandes de transfert d'argent.

Effectivement, les progrès de la transformation numérique ont inévitablement entraîné de nouvelles menaces pour la cybersécurité. Les cybercriminels profitent de la pandémie de la Covid-19, notamment en ciblant les organisations et entreprises travaillant à distance. À Maurice, Kevin Mulliah précise que d'autres cyber-risques auxquels les entreprises mauriciennes sont confrontées sont les malware (un logiciel qui déclenche un processus qui affecte un système) ; les menaces liées aux e-mails (cela vise à manipuler les gens pour qu'ils soient victimes d'une attaque par e-mail) ; la désinformation/mésinformation (la diffusion d'informations trompeuses) ; les menaces contre la disponibilité et l'intégrité (attaques qui empêchent les utilisateurs d'un système d'accéder à leurs informations) ; le cryptojacking (lorsque les cybercriminels utilisent secrètement la puissance de calcul d'une victime pour générer de la cryptomonnaie) et les menaces contre les données (violations/fuites de données).

«*En Afrique, l'île Maurice se classe en tête et occupe la 17e place mondiale. Au cours des cinq dernières années, l'île a systématiquement été classée en tête des pays africains les plus engagés dans l'amélioration de leur cybersécurité. Non seulement Maurice a été le premier en Afrique dans les quatre rapports sur l'indice mondial de cybersécurité (ICG), mais son score n'a cessé d'augmenter (2014 : 58,8 %, 2017 : 82 %, 2018 : 88 % et 2020: 96,89 %). Ce classement peut être soutenu par les diverses initiatives mises en place par le CERT-MU, telles que la stratégie nationale de cybersécurité, la stratégie nationale de lutte contre la cybercriminalité et le plan national de gestion des incidents liés à la cybersécurité*», explique Shanah Bucktowar.

Elle ajoute que Maurice a aussi mis en place le comité national de cybersécurité et de lutte contre la cybercriminalité en cas de catastrophe, composé de représentants des secteurs public et privé. Cette instance facilite le suivi, le contrôle et la communication des décisions en cas de cybercrise au niveau national. C'est pour cela que le pays a été choisi pour abriter le hub africain de cyber-résilience.

Kevin Mulliah précise que l'Afrique reste un continent avec peu d'institutions bancaires mises à la disposition de certains pays africains et cela entraîne, dans bon nombre de cas, des escroqueries à travers des plateformes bancaires digitales, parfois en dehors des limites de la légalité. Il ne pense pas qu'on soit dans cette situation à Maurice car les organisations financières, et plus précisément le secteur bancaire, en sont bien averties et misent énormément sur la cybersécurité. Cela, en ayant des stratégies et des feuilles de route bien établies par des experts du domaine qui sont dans la majorité des cas des directeurs de sécurité informatique en poste dans ces organisations.

LE SECTEUR FINANCIER CIBLÉ

Par ailleurs, en tant que juridiction de renom et reconnue internationalement, le centre financier international (CFI) de Maurice héberge un certain nombre de banques internationales, de cabinets juridiques, de prestataires de services destinés aux entreprises, de fonds d'investissement et de fonds de capital-investissement. Ce qui comporte des défis en matière de cybersécurité.

Jean-Baptiste Blanc, Executive Vice-President de Catalyst Business Solutions, souligne que le secteur bancaire et financier est aujourd'hui une cible de choix pour les cybercriminels. Pendant la pandémie de la Covid-19, le passage – souvent chaotique et peu accompagné de mesures élémentaires de sécurité – au télétravail a provoqué des failles béantes de l'architecture de sécurité d'une grande majorité de banques et d'institutions financières. Sur la région Afrique / Moyen-Orient, depuis 2019, de nombreuses banques internationales ont vu leur système d'opération corrompu à la suite d'une cyberattaque.

«*L'attrait des cybercriminels pour les secteurs bancaire et financier n'est pas difficile à expliquer : c'est l'argent ! Pour aller plus loin, il faut prendre en compte que le secteur bancaire est aujourd'hui un domaine ultra numérisé (services de paiement, règlements, compensation, échange de titres financiers, etc.). L'extrême interconnexion de l'intégralité du secteur bancaire fait également craindre un ralentissement de l'activité financière globale en cas de cyberattaques coordonnées. Dans ce cadre, le Centre Financier International, par la grande concentration d'institutions financières en son sein, se doit de maintenir un niveau de sécurité maximal, autant depuis l'extérieur vers l'intérieur mais aussi entre ses différents bailleurs, de façon que la compromission d'un membre du centre n'affecte pas l'activité des autres acteurs*», fait ressortir Jean-Baptiste Blanc.

Shanah Bucktowar ajoute pour sa part que l'ingénierie sociale est l'une des plus grandes menaces pour le secteur financier. Les personnes sont souvent le maillon le plus vulnérable de la chaîne de sécurité. Effectivement, elles peuvent être amenées à communiquer des informations sensibles telles que celles liées à l'identification des personnes. Cela peut aussi bien concerner les employés d'une banque que ses clients. L'ingénierie sociale prend de nombreuses formes, qu'il s'agisse d'attaques de phishing ou de whaling ou de l'envoi de fausses factures censées provenir d'une source fiable. Il est donc important de tenir les employés informés des tactiques d'ingénierie sociale et de l'évolution constante de ces menaces.

Effectivement, le secteur financier est généralement considéré comme la principale cible des pirates informatiques. Comme le précise Krishna Radhakeesoon, les ransomwares, la compromission de la messagerie professionnelle et le déni

L'ÎLE MAURICE EST EN TÊTE DES PAYS AFRICAINS LES PLUS ENGAGÉS DANS L'AMÉLIORATION DE LEUR CYBERSÉCURITÉ

de service sont les attaques prédominantes contre les opérateurs locaux et internationaux du secteur financier. Si les banques ont généralement investi davantage pour se protéger des cyberattaques, d'autres opérateurs du secteur financier (par exemple, les sociétés de gestion offshore, les fonds d'investissement et les fonds de capital-investissement) sont moins préparés face aux cyberattaques. Alors que le volume de transactions financières effectuées par les banques est plus élevé, les autres opérateurs du secteur financier sont impliqués dans des transactions de faible volume mais de grande valeur. Ainsi, l'impact d'une mauvaise transaction financière due à une cyberattaque sur ces derniers est beaucoup plus élevé ; et la cyber assurance peut souvent ne pas suffire.

«*Si la cybersécurité est aujourd'hui à l'ordre du jour de la direction générale de la plupart des banques, elle est moins présente chez les autres acteurs du secteur financier. Le changement de mentalité selon lequel 'la cybersécurité est une question commerciale plutôt qu'une question informatique' prend encore du temps. En outre, l'accent est moins mis sur la cyber-résilience (la capacité de réagir et de se rétablir après une cyberattaque). La question n'est pas de savoir 'si' vous subirez une cyberattaque, mais plutôt 'quand' vous en subirez une et si vous saurez comment réagir*», souligne Krishna Radhakeesoon.

Ashiss Soobhug précise que les cybercriminels ont un intérêt particulier pour le secteur financier en raison de la nature de leurs actifs numériques, notamment les données. Les cybermenaces sur ce secteur ne font qu'augmenter avec des attaques en nette augmentation en raison de l'offre de services bancaires en ligne et aux applications mobiles. Il rappelle que les effets d'une cyberattaque sont dévastateurs pour le secteur financier, en particulier les systèmes bancaires. C'est pourquoi les institutions bancaires sont connues pour avoir des programmes de sécurité plus matures que d'autres secteurs industriels. Cependant, le niveau de sécurité n'est pas aussi pointu pour des secteurs aussi sensibles, tels que les cabinets d'avocats, les prestataires de services aux entreprises et les sociétés de gestion de fonds, entre autres.

«*La cybersécurité a un coût et de nombreuses entreprises ont tendance à privilégier d'abord les investissements dans les besoins opérationnels et considèrent la cybersécurité comme une option. Il y a aussi le faux sentiment de croire que cela n'arrive qu'aux autres, jusqu'à ce qu'on soit victime d'une cyberattaque. Les entreprises qui ont déjà commencé à implémenter un programme de cyber-résilience verront assez rapidement les bienfaits de cette initiative, mais pour celles qui ne l'ont pas encore fait, l'effort financier et humain pourrait être plus important lorsqu'elles y viendront par force. D'où l'importance de s'y préparer*», fait ressortir Ashiss Soobhug.

BUDGET SÉCURITÉ

Par ailleurs, de nombreux experts affirment que les entreprises devraient consacrer 10 à 15 % de leur budget informatique annuel à la cyberdéfense. Mais est-ce le cas actuellement à Maurice ? Car il en ressort que certaines entreprises ont encore du mal à en justifier ce coût. Jean-Baptiste Blanc rappelle que Maurice est un leader en termes de cybersécurité, et le pays le mieux protégé du continent africain selon le Global Security Index 2020 de l'ITU. Il constate que la grande majorité des entreprises mauriciennes prennent très au sérieux les cybermenaces, et dédient une part importante de leur budget à la cybersécurité.

Toutefois, le nombre et l'impact financier des cyberattaques augmentent considérablement. Ainsi, les entreprises sont de plus en plus vulnérables et les coûts opérationnels de la cybersécurité en termes de SOC et d'expertise explosent. Pire, le nombre de spécialistes sur le marché est trop faible pour répondre à la demande. Les entreprises ont donc besoin d'une meilleure protection à moindre coût.

Pour Shanah Bucktowar, il y a des perceptions fantaisistes sur l'état de la cybersécurité qui freinent les organisations. De nombreux dirigeants pensent que la cybersécurité est facile et que les menaces sont exagérées. Par conséquent, les entreprises n'investissent pas suffisamment pour protéger leur infrastructure informatique. «*Il est vrai que tous les événements et impacts informatiques ne sont pas égaux, et que toutes les organisations ne sont pas également capables de s'en défendre et de s'en remettre. Il est donc préférable pour les dirigeants d'optimiser les dépenses de cybersécurité en s'efforçant d'abord de quantifier le risque propre à leur organisation en termes monétaires spécifiques...*

PÉNURIE DE COMPÉTENCES

Le marché de la cybersécurité continuera à exiger de nouvelles compétences, cela non seulement d'un point de vue technologique. Selon Shanah Bucktowar, la pénurie de compétences en cybersécurité à Maurice se fait définitivement sentir. Actuellement, nous devenons de plus en plus dépendants d'entreprises ou de ressources internationales pour nous aider. Ces services sont alors coûteux.

***«Il est vrai qu'il existe un besoin urgent de protection contre la sophistication croissante des cyberattaques et que la pénurie de professionnels de la cybersécurité commence à se faire sentir. Alors que la demande de services de cybersécurité ne fera qu'augmenter dans les années à venir, la pénurie de compétences restera un facteur limitant pour cette industrie si des mesures suffisantes ne sont pas prises. Les défis et les répercussions peuvent inclure l'incapacité des fournisseurs de services à respecter les délais du projet en l'absence d'une main-d'œuvre adéquate. Bien qu'il existe une abondance de technologies avancées et émergentes telles que l'Intelligence Artificielle, le cloud et la cybersécurité, la pénurie de main-d'œuvre pour mettre en œuvre et gérer ces technologies ne fera qu'augmenter l'exposition aux risques des organisations, ce qui entraînera une guerre mondiale de talents»*, explique Ashiss Soobhug.**

Jean-Baptiste Blanc précise que la pénurie de talents dans le secteur de la cybersécurité est un constat non seulement applicable à Maurice, mais aussi au reste du monde. À l'échelle d'une entreprise, le manque de main-d'œuvre SSI peut mener à des situations critiques : un nombre réduit de personnel dédié à la cybersécurité peut entraîner des lacunes dans le maintien en conditions opérationnelles des dispositifs de cybersécurité, dans la détection et la réponse aux incidents et cyberattaques. Pour pallier cette pénurie de ressources, les organisations peuvent bien-sûr faire appel à un Responsable de la Sécurité des Systèmes d'Information (RSSI) externalisé et sous-traité.

Il ajoute que le manque de compétences en termes de cybersécurité s'observe en réalité à tous les niveaux de responsabilité. Du simple collaborateur à l'équipe dirigeante, trop de personnes ignorent les enjeux et les gestes basiques d'hygiène numérique. Et, comme dit précédemment, il suffit d'un seul maillon faible dans la chaîne de valeur pour qu'elle s'effondre. C'est pour cela qu'il est nécessaire d'investir massivement dans des campagnes de sensibilisation adaptées à chaque public, avec ses enjeux métiers et de responsabilité propres.

... À ENL, par exemple, nous avons élaboré un budget de cybersécurité qui couvre les outils et services de sécurité indispensables pour garantir notre protection. Chaque année, nous examinons notre niveau de risque et révisons ce budget.»

Kevin Mulliah souligne, lui, que pendant la pandémie, les entreprises ont dû s'adapter rapidement aux nouvelles conditions de travail et ont ainsi ouvert de nouvelles portes et plus de possibilités aux cybercriminels. Il note qu'aujourd'hui une bonne partie des grandes et moins grandes entreprises à Maurice ont déjà emboîté le pas vers l'implémentation de la cybersécurité dans leur stratégie digitale et technologique. Certains d'entre eux sont forcés de le faire afin de rester dans les limites de la loi et des règlementations fixées par les régulateurs. Par contre, d'autres arrivent difficilement à convaincre et à justifier ce besoin d'investir dans la cybersécurité. Ces derniers ne voient en aucun lieu le bénéfice financier que cela leur ramènera ou ils pensent qu'ils sont à l'abri de ces cyberattaques.

«*De nombreuses organisations – principalement celles qui n'appartiennent pas au secteur financier – ne voient pas l'intérêt de prévoir un budget de cyberdéfense, car le coût de la mise en œuvre est souvent considéré comme beaucoup plus élevé que le rendement de tels projets*», ajoute Krishna Radhakeesoon. Cependant, les conséquences des cyberattaques en termes de pertes financières et de réputation sont généralement bien plus élevées que le coût de la mise en œuvre. En général, les entreprises qui ont subi une forme de cyberattaque disposent d'un budget plus important. Cependant, ce budget est généralement orienté vers les technologies de cyberdéfense alors que le maillon faible reste le facteur humain. «*De même, on accorde moins d'importance à la mise en place de processus et de contrôles appropriés pour atténuer les cyber-risques. Si la cybersécurité n'est pas à l'ordre du jour de votre conseil d'administration aujourd'hui, elle devrait l'être avec le taux croissant de transformation numérique qui crée de nouveaux vecteurs d'attaque pour les cybercriminels.*»

ELYTIS
Plateforme de sécurité intégrée

ELYTIS étant un distributeur privilégié dans la région – Afrique, IOI avec des bureaux en Nouvelle-Calédonie et en Polynésie française – l'entreprise joue un rôle important dans ce secteur. Parmi les nombreuses marques que représente l'entreprise, on retrouve Symantec (par Broadcom), Veritas, Crowdstrike et Microsoft. Celles-ci offrent aux clients la sécurité dont ils ont besoin pour se protéger et pour rester conformes dans leurs stratégies de sécurité informatique et de continuité des affaires.


ANIROW RAMMA (HEAD OF BUSINESS UNIT - INFORMATION MANAGEMENT & SECURITY)

«*En tant que distributeur, Elytis travaille avec ses partenaires pour mettre en œuvre la bonne solution chez un client afin de le protéger contre les diverses formes de cyberattaques et les risques auxquels il peut être confronté. Les solutions mentionnées fournissent la technologie, l'intelligence télémétrique et l'expertise mondiale des marques qui sont classées comme leaders dans Garter. IDC, Forester et d'autres rapports dans le domaine de la cybersécurité, selon le type de problèmes qu'ils abordent*», explique Anirow Ramma, Head of Business Unit - Information Management & Security d'Elytis.

Le portefeuille de cybersécurité des fournisseurs d'Elytis est une plateforme de sécurité intégrée destinée à protéger les entreprises non seulement contre les nouvelles menaces et les menaces émergentes, mais également contre les réglementations de confidentialité et de conformité dont la sécurité des points d'accès, la sécurité des serveurs, la sécurité des identités, la sécurité des environnements cloud, la sécurité des e-mails (protection contre l'hameçonnage), la gestion des accès privilèges, la sécurité de l'information (prévention de la perte de données, CloudSOC CASB, accès sécurisé cloud, chiffrement, suite de contrôle de conformité), la sécurité des réseaux (portail sécurisé avancé, service de sécurité web, isolation du web, analyse de contenu et Sandboxing, services de renseignement et WebFilter, centre de gestion et rapports) et pare-feu d'application web et reverse proxy.

«*Elytis offre également une assistance commerciale et technique, prévente et après-vente à tous nos partenaires et nos clients finaux qui renouvellent leurs abonnements ou achètent de nouvelles licences via l'un de nos partenaires. Cela signifie que vos clients bénéficient d'une expérience d'assistance de haute qualité, en sachant qu'ils seront suivis par notre équipe d'ingénieurs hautement qualifiés*», ajoute Anirow Ramma.

BIRGER.

Une équipe hautement professionnelle

BIRGER. offre un service complet couvrant la technologie, la sécurité et la résilience à tous secteurs mais principalement aux banques, assurances, opérateurs télécoms, aux grandes entreprises et au secteur public.

Depuis cinq ans, BIRGER. effectue une enquête sur la Cyber Sécurité couvrant les îles de l'océan Indien (IOI) et l'Afrique. Le but est d'évaluer les menaces et les défis dans notre région ainsi que de quantifier le niveau de maturité en Cyber Sécurité par région, pays et secteur en utilisant notre indice de maturité en Cyber Sécurité, notamment le BIRGER. CYIndex. «*Les résultats nous permettent d'analyser l'évolution de la Cyber Sécurité dans les IOI et de l'Afrique et surtout de voir la tendance en comparant avec les années précédentes. Les résultats de notre enquête de cette année indiquent clairement que le niveau de cybercriminalité est en baisse à Maurice ainsi que dans l'IOI et en Afrique*», souligne Parwez Bhugalee, Executive, Business Development de BIRGER.

L'étude fait également ressortir que la nouvelle réalité oblige, et pour assurer leur survie, les entreprises ont accéléré la transformation digitale au détriment de la Cyber Sécurité, exposant ainsi leur surface d'attaque. «*Les cybercriminels prennent avantage de cette situation et nous avons répertorié parmi les plus grandes attaques cyber en 2021, notamment Log4j, Kaseya, Chromium parmi d'autres qui ont touché des milliards d'utilisateurs et continuent de faire des dégâts. Notre région et l'Afrique étaient en progression en termes de maturité en Cyber Sécurité jusqu'à l'arrivée de la Covid avec la nouvelle réalité et l'accélération de la transformation digitale qui ont fait exploser la surface d'attaque globalement et dans notre région. Nous conseillons à nos clients et aux entreprises en général dans notre région d'œuvrer pour aligner leur stratégie de Cyber Sécurité et de la transformation digitale pour se préparer à reprendre l'avantage sur les cybercriminels.*»

> UN SERVICE COMPLET COUVRANT LA TECHNOLOGIE, LA SÉCURITÉ ET LA RÉSILIENCE À TOUS SECTEURS

Les services de Cyber Sécurité de BIRGER. englobent plusieurs offres dont le conseil. BIRGER. forme et certifie de façon continue ses employés aux normes reconnues de l'industrie et recrute aussi des experts de pointe. L'entreprise a ainsi bâti une équipe expérimentée, professionnelle et capable de fournir des services de conseil en Cyber Sécurité suivant des méthodologies éprouvées. Elle accompagne et aide à diagnostiquer l'architecture de sécurité des entreprises et fait des audits de sécurité, des tests d'intrusion et de vulnérabilité.

BIRGER. offre aussi plusieurs types de formations, en présentiel et distanciel. Les formations peuvent être avec une certification type ISO 27001 ou ciblées selon les besoins des entreprises. Les formations pratiques et des simulations peuvent être alignées pour maîtriser les techniques. Des formations sont aussi offertes en mode continu en utilisant des logiciels spécialisés pour des campagnes de phishing par exemple, pour renforcer la maturité des employés dans une entreprise. Le facteur humain reste toujours le maillon le plus faible dans les systèmes de cyberdéfense et BIRGER. conseille aux entreprises d'adopter ces formations de façon continue.

«*Notre Centre de Cyber Défense (Security Operation Center (SOC)) a démarré ses opérations en 2016 en proposant divers services visant à détecter, prévenir et répondre aux attaques et incidents liés à la Cyber Sécurité. Nous utilisons des technologies de pointe pour le CDC et les Services de Sécurité Gérés (Managed Security Services - MSS en anglais) qui s'appuient sur des réseaux d'intelligence globale. Grâce à toutes nos équipes opérationnelles, nous pouvons proposer diverses solutions technologiques en sécurité qui sont mieux adaptées aux besoins de nos clients. Nous avons une grande expérience dans le déploiement de solutions de sécurité telles que des produits pare-feu et filtrage Web par le biais de partenariats clés*», fait ressortir Parwez Bhugalee.

Depuis des années, BIRGER. a mis en œuvre des technologies de sécurité d'entreprise et d'infrastructure liées à la sécurité du courrier électronique, au chiffrement des données et des disques, la prévention des pertes de données confidentielles (DLP) ainsi que les technologies antivirus avancées et de protection contre les menaces persistantes. En exploitant ses expertises technologiques et de

PARWEZ BHUGALEE, (EXECUTIVE, BUSINESS DEVELOPMENT)

cyber sécurité, BIRGER. peut surveiller et protéger les données confidentielles de ses clients qui sont stockées dans leurs centres de données (Datacentre) ou sur le cloud, ou encore transmis par Internet ou par autres réseaux.

Par ailleurs, BIRGER. accompagne ses clients en adoptant une approche structurée suivant les bonnes pratiques, les régulations et axée sur le service de proximité principalement aux banques, assurances, opérateurs télécoms, grandes entreprises et le secteur public. «*Nos collaborateurs sont formés en mode continu et nos équipes locales sont qualifiées et certifiées. Nous offrons des services de conseil et sensibilisons nos clients sur les menaces émergentes ainsi que les normes de sécurité et les règlements internationaux tels que le RGPD. Notre enquête annuelle dédiée à la Cyber Sécurité nous procure également de l'information pour mieux comprendre et évaluer les menaces ainsi que pour faire des recommandations*», explique Parwez Bhugalee.

Il ajoute que dans la dernière enquête, BIRGER. recommande que toutes les entreprises de la région reprennent l'avantage sur les cyberattaquants en renforçant leurs gouvernance, expertise, connaissances et technologies. Ainsi, les entreprises sont conseillées de commencer par avoir une vue de leur situation actuelle en matière de Cyber Sécurité à travers un audit de sécurité, par exemple, pour pouvoir ensuite travailler sur un plan pour renforcer leur maturité en Cyber Sécurité.

SWAN

Une protection optimale contre les cyberattaques

ON SE rend de plus en plus compte que les risques liés à la cybersécurité sont beaucoup plus importants que ce que l'on pensait. Des violations de données peuvent être importantes et, dans les cas extrêmes, peuvent entraîner la faillite d'une entreprise. Selon Vincent Lim, Team Leader Specialty Risks de SWAN, la sophistication des cyberattaques va accroître la demande de couverture d'assurance cybernétique sur le plan local.

«*S'il est vrai que la prime d'une assurance Cyber Risques n'est pas aussi abordable qu'on le souhaiterait, il faut néanmoins prendre en compte l'impact financier des dommages occasionnés par une cyberattaque et les conséquences d'une perte des données qui contribuent à entacher la réputation de l'entreprise, et peuvent même entraîner sa fermeture. Nous constatons que de plus en plus de chefs d'entreprises nous interrogent sur les bénéfices d'une telle couverture. Il leur paraît clair que des pertes potentiellement encourues par leur entreprise dépasseraient largement le montant de la prime à débourser. Aux conséquences d'une cyberattaque s'ajoutent les sanctions découlant de la violation des données personnelles et confidentielles des clients qui peuvent être très lourdes*», met en exergue Vincent Lim.

Il ajoute qu'en ces temps difficiles où l'économie locale vient tout juste de redémarrer, il est important de souligner que cette assurance, loin d'être une dépense, constitue surtout une protection limitant les pertes potentielles susceptibles de mettre en péril toute l'entreprise. Ainsi, la SWAN ne se positionne pas en tant que fournisseur d'assurances, mais plutôt comme partenaire dans l'accompagnement d'entreprises dans leur mission de limiter les risques liés à une cyber attaque.

«*Nous estimons qu'il ne peut pas y avoir une solution unique en termes de couverture cyber-risque pour toutes les entreprises. Chaque solution proposée est adaptée selon les besoins spécifiques de l'organisation en prenant en compte son secteur d'activités, sa structure, le nombre d'employés, ainsi que l'état et le niveau actuel de ses systèmes de sécurité informatique. Avec la croissance alarmante des cyberattaques, même les meilleurs systèmes de sécurité à la pointe de la technologie ne sont pas toujours totalement 'hackproof'. En effet, une entreprise peut toujours être victime d'une attaque : les hackers travaillent sans relâche et parviennent toujours à déjouer les meilleures stratégies de cybersécurité.*»

Pour Vincent Lim, un moyen très important de limiter les cyber-risques consiste à y sensibiliser fréquemment les employés qui risquent de manière innocente ou par inadvertance de créer une ouverture pour ces hackers. La SWAN conseille donc les entreprises sur les différentes stratégies qui pourront améliorer leur sécurité. Outre une couverture appropriée à leurs besoins, la SWAN effectue du knowledge sharing sur l'importance des mises à jour de leurs logiciels comme moyen de protection, voire comme outil de sensibilisation. Dès que l'assurance est en place, elles bénéficient alors d'un accompagnement 24/7 par le biais d'une hotline en cas d'attaques suspectes.

La question est de savoir si les entreprises mauriciennes sont conscientes du besoin de s'assurer contre les cyberattaques ? «*À mon avis, seule une poignée d'entreprises est pleinement consciente des risques liés aux cyberattaques. Pourtant, le risque est bel et bien réel : toutes les entreprises sont désormais connectées en permanence à Internet. Or, les employés y ont recours, soit pour un usage récréatif via les réseaux sociaux, soit pour des raisons professionnelles. Ce manque de prise de conscience est principalement dû à l'absence d'outils de sensibilisation.*»

LA SOPHISTICATION DES CYBERATTAQUES VA ACCROÎTRE LA DEMANDE DE COUVERTURE D'ASSURANCE CYBERNÉTIQUE SUR LE PLAN LOCAL

VINCENT LIM
(TEAM LEADER SPECIALTY RISKS)

Par ailleurs, Vincent Lim fait ressortir que les cyberattaques sont pour la plupart des attaques non ciblées qui peuvent toucher n'importe qui, que ce soit par le biais d'un courrier électronique ou un message avec un lien cliquable. «*Qui n'a jamais reçu un e-mail suspect, sorti de nulle part et nous invitant à cliquer sur un lien ? Si l'un d'entre vous l'a déjà fait, c'est que vous êtes certainement déjà dans le viseur d'un hacker qui attend juste le moment idéal pour passer à l'action.*»

Par ailleurs, parmi les clients de SWAN, l'on retrouve des entreprises qui sont les acteurs-clés de l'économie locale et qui embauchent des milliers de personnes. On y retrouve ceux opérant dans les secteurs hôtelier, financier, informatique, logistique et de l'aviation, la distribution à grande échelle, ou encore le commerce. Avec la croissance des petites et moyennes entreprises et les avantages qui leur sont offerts, Vincent Lim s'attend à ce que ce segment se tourne également vers ce type d'assurance. Il rappelle qu'il est difficile de trouver une bonne couverture cyber. Leur coût a augmenté de manière conséquente au fil des années au regard des pertes encourues liées aux cyberattaques à travers le monde. Mais l'assurance Cyber Risques demeure un élément crucial de la gestion de risques de toute entreprise à condition de ne pas perdre de vue qu'un système de sécurité informatique n'est jamais totalement infaillible.

AGILEUM
Combler les besoins des organisations en solutions de cybersécurité


HEMRAJ BOOTUN (PARTNER SECURITY SOLUTIONS & SERVICES ET CLIENT SUCCESS LEADER)

LORSQUE AGILEUM avait lancé ses services de cybersécurité il y a dix ans, l'entreprise constatait déjà à l'époque un manque d'experts en cybersécurité capables de mettre en œuvre des projets et des solutions pour leurs clients sur le marché. Les cabinets d'experts-conseils souvent ne faisaient que des évaluations et ne soumettaient que des rapports. Les clients se retrouvaient sans fournisseurs de services en matière de cybersécurité possédant l'expertise nécessaire pour mettre en œuvre les recommandations mentionnées dans les rapports.

«*Nos services en matière de cybersécurité sont positionnés pour combler ces besoins et aider des organisations à répondre à d'autres besoins commerciaux tout en atténuant les risques et en assurant la conformité quels que soient leurs secteurs d'activité. Nous nous engageons à être les partenaires de nos clients pendant toute la durée de notre engagement. Nous sommes là pour les aider dans l'évaluation, la conception et l'élaboration des stratégies en ligne avec leur business jusqu'à la mise en œuvre, la gestion et la maintenance d'un programme efficace de cybersécurité et de gestion des risques et pour appliquer les exigences réglementaires et de conformité*», explique Hemraj Bootun, Partner Security Solutions & Services et Client Success Leader d'AGILEUM.

AGILEUM a aussi construit une alliance avec des partenaires et des experts en cybersécurité en Afrique du Sud et en Europe au cours des dix dernières années. Une alliance qui leur permet de fournir des services spécialisés et de mettre en place des solutions de cybersécurité pour protéger leurs clients contre les menaces. Mais aussi pour surveiller les risques, tout en assurant une perturbation minimale et un effet de levier maximal sur des investissements existants et des acquisitions déjà réalisées par les clients. Cette alliance leur permet aussi d'assurer une formation continue pour leurs collaborateurs, ainsi que pour leurs clients et les collaborateurs de ces derniers. «*Les organisations sont désireuses d'acquérir l'agilité et la résilience qu'exige une approche moderne des technologies informatiques, et des organisations de différentes tailles et dans différents secteurs d'activité, aussi bien des start-up que de grandes organisations publiques et privées se tournent vers nous. Elles considèrent toutes la cybersécurité comme une priorité.*»

AGILEUM est à l'origine un cabinet d'expertise en Informatique qui propose et développe des systèmes informatiques. L'expérience acquise depuis la création de la société lui permet aujourd'hui de répondre aux problématiques de cybersécurité rencontrées par différentes entreprises. Et l'entreprise apporte à ses clients une expertise et des solutions qui leur permettent d'améliorer de manière significative et continue dans le temps leur niveau de sécurité et de protection. AGILEUM propose également des offres variées, des solutions d'éditeurs reconnues ou développées et customisées, parfaitement adaptées à la taille, au niveau de risque et de maturité de ses clients, de la jeune start-up Internet aux grandes organisations publiques et privées.

ENL
Une approche fondée sur le risque


SHANAH BUCKTOWAR (INFORMATION SECURITY OFFICER)

LA CYBERSÉCURITÉ exige que chacun joue un rôle. Et pour jouer un rôle, nous devons tous comprendre le risque. C'est pourquoi ENL fournit à ses entreprises des conseils et des solutions techniques de sécurité selon une approche fondée sur le risque. «*Nous travaillons avec chaque entreprise/département pour identifier les zones à haut risque et nous fournissons des conseils et des mesures techniques pour les atténuer. Ces mesures peuvent varier en termes d'outils et de contrôles de sécurité, en fonction des besoins de l'entreprise et de son niveau de risque*», explique Shanah Bucktowar, Information Security Officer à ENL.

Elle ajoute que les entreprises mesurent leur succès en analysant leurs risques, leurs forces, leurs faiblesses et leurs opportunités. C'est ainsi qu'elles ouvrent instantanément la porte aux réussites. Un consultant en sécurité pourrait apporter à l'entreprise une perspective nouvelle et impartiale sur ses problèmes dans ce domaine. Il est très facile de se rapprocher des problèmes et d'être incapable de voir les choses, mais quelqu'un qui n'est pas directement impliqué dans le quotidien de l'entreprise peut le remarquer d'emblée.

«*Nous mettons en place des formations annuelles de sensibilisation à la cybersécurité pour l'ensemble du personnel. Nous avons conçu des programmes de sensibilisation pour tous les salariés, mais nous accordons une attention particulière aux nouveaux venus dans l'organisation afin qu'ils reçoivent une formation adéquate pour savoir comment traiter les informations et les systèmes auxquels ils ont accès. Le comportement des employés est régulièrement testé par des simulations de phishing et ils reçoivent des formations à ce sujet. Par ailleurs, afin d'atteindre le plus grand nombre d'employés, nous utilisons une plateforme de formation en ligne sur la cybersécurité. En outre, d'autres canaux de communication internes tels que les courriels, les articles et les messages télévisés sont utilisés pour des actions de sensibilisation*», fait ressortir Shanah Bucktowar.

HAREL MALLAC TECHNOLOGIES

Services complets de surveillance

LE CENTRE d'Opérations de Sécurité (SOC) d'Harel Mallac Technologies fonctionne 24 heures sur 24, et 7 jours sur 7. Il offre des services complets de surveillance des incidents à ses clients à Maurice et à l'international, où il prévient, détecte, analyse et répond aux incidents de cybersécurité. «*Il est bien de noter que la cybersécurité touche tous les secteurs d'entreprises et nous essayons au maximum de conscientiser nos clients sur la nécessité d'investir et de mettre en place une structure de programme de cybersécurité et de gestion des risques. Un consultant en sécurité aide les organisations à identifier la surface d'attaque, à remapper la pile des technologies de sécurité pour faire face aux nouvelles menaces de plus en plus sophistiquées. Conseiller et recommander des solutions et services pour améliorer la posture de sécurité et faire évoluer et recadrer les pratiques de sécurité pour mieux gérer les risques cyber, c'est notre métier*», font ressortir Nishna Tanna et Kevin Mulliah, respectivement Cybersecurity Solutions Architect et Business Development & Sales Manager à Harel Mallac Technologies.

«*Nos services sont fournis pour aider les entreprises à connecter la cybersécurité ainsi que les risques commerciaux et de conformité en les plaçant au premier plan de leur prise de décision. Ensemble, nous aidons nos clients à évaluer la surface d'attaque, à concevoir, mettre en œuvre et maintenir une structure de programme de cybersécurité et de gestion des risques pour se défendre contre les attaques, gérer et surveiller les risques, et appliquer les exigences réglementaires et de conformité*», ajoute Nishna Tanna.

RECOMMANDER DES SOLUTIONS ET SERVICES POUR AMÉLIORER LA POSTURE DE SÉCURITÉ ET FAIRE ÉVOLUER ET RECADRER LES PRATIQUES DE SÉCURITÉ POUR MIEUX GÉRER LES RISQUES CYBER

KEVIN MULLIAH
(BUSINESS DEVELOPMENT & SALES MANAGER)

NISHNA TANNA
(CYBERSECURITY SOLUTIONS ARCHITECT)

Elle fait ressortir que les services de sensibilisation à la sécurité d'Harel Mallac Technologies sont conçus pour analyser les processus métier et concevoir des simulations de phishing pour mettre en évidence les risques. Mais aussi pour éduquer les employés avec une sensibilisation continue à la sécurité sur la façon d'identifier la différence entre les données personnelles et celles de l'entreprise, repérer les activités suspectes, utiliser les meilleures pratiques pour sécuriser leurs données, et voir comment les incidents doivent être signalés.

«*Je dois préciser que la surface d'attaque s'est élargie, laissant les organisations plus vulnérables aux attaques. Nous avons encadré notre approche pour identifier la surface d'attaque et provisionner nos services pour surveiller, détecter et répondre à un ensemble plus large de risques au-delà des approches traditionnelles. Notre Centre d'Opérations de Sécurité et nos services de sécurité gérés sont conçus pour empêcher tous types d'interruptions qui seraient liés à des cyberattaques, en utilisant des technologies et des cadres émergents tels que le modèle de confiance zéro, entre autres. Et cela s'est révélé efficace grâce à notre SOC qui pouvait détecter et isoler des cyberattaques imprévues pour nos clients, et grâce à nos services de sécurité gérés qui pouvaient y remédier afin d'éviter les menaces*», explique Nishna Tanna.

S'agissant de la formation, Kevin Mulliah ajoute qu'à ce jour, Harel Mallac Technologies ne propose pas de formation directe, mais sensibilise plutôt les clients sur l'importance de la cybersécurité. Des recommandations sont faites à la suite d'une analyse précise des infrastructures des clients et de leurs processus de sécurité.

BDO

Solutions sur mesure

KRISHNA Radhakeesoon, Partner chez BDO, explique qu'indépendamment de leur taille et de leur secteur d'activité, toutes les organisations connaissent aujourd'hui un rythme croissant de transformation numérique et doivent donc définir une stratégie de gestion des risques de cybersécurité. En tant que consultants en cybersécurité, BDO propose une approche sur mesure pour aider ses clients à identifier les cyber-risques auxquels sont exposés leurs joyaux de la couronne (les actifs critiques). «*Nous les conseillons sur la manière de mettre en place des contrôles pour se protéger des cyberattaques. Et nous aidons nos clients à devenir plus cyber-résilients en mettant en œuvre des solutions susceptibles de détecter et de répondre aux incidents de cybersécurité en utilisant l'apprentissage automatique et l'intelligence artificielle. Ainsi, nous contribuons à améliorer la position de nos clients en matière de cybersécurité, ce qui peut réduire considérablement l'impact des cyberattaques.*»

Krishna Radhakeesoon ajoute qu'un programme efficace de sensibilisation à la cybersécurité comprend une formation en face à face pour tous les employés et les parties prenantes concernées. «*La formation à la cybersécurité doit être continue. C'est pourquoi nous complétons nos formations en face à face par des formations en ligne à la demande via des plateformes telles que Mimecast et KnowB4. Et surtout, nous proposons des simulations d'attaques de phishing et de vishing pour évaluer l'efficacité de la formation et identifier les utilisateurs les plus faibles qui ont besoin d'une formation en face à face supplémentaire.*» Aux professionnels de l'informatique, BDO propose également une formation sur la norme ISO 27001 relative au système de gestion de la sécurité de l'information.

KRISHNA RADHAKEESOON (PARTNER CHEZ BDO)

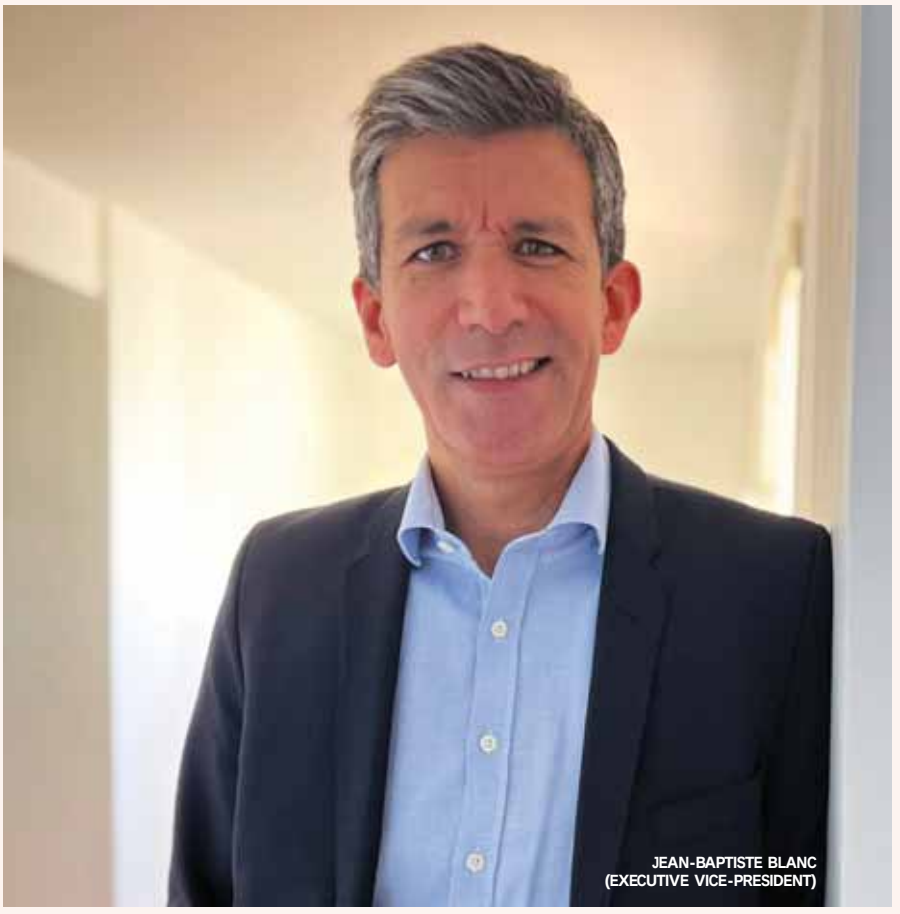
CATALYST BUSINESS SOLUTIONS

Pôle d'excellence dédié à la cybersécurité

CATALYST Business Solutions dispose d'un pôle d'excellence et propose une offre complète de services en matière de cybersécurité. Jean-Baptiste Blanc, Executive Vice-President de Catalyst Business Solutions, explique que leur approche est disruptive car elle permet d'améliorer la protection et la conformité tout en réduisant le coût de la sécurité.

«*Notre offre s'articule autour de trois objectifs : évaluation, protection, conformité. Nous proposons notamment des prestations d'hacking éthique et de sécurité offensive qui permettent à une organisation de mettre son système d'information à l'épreuve du feu en le soumettant à une série de tests d'intrusions (pentests), d'audits et de scans de vulnérabilités. Nous mettons en lumière les faiblesses du système d'information et formulons des recommandations pour les corriger et une feuille de route pour optimiser la sécurité sur la durée. Nous mettons ensuite en place un processus d'amélioration continue et d'élévation du niveau de sécurité des organisations qui nous sollicitent, et assistons les fonctions de RSSI et de Data Protection Officer (DPO).*»

Catalyst Business Solutions s'appuie sur des solutions innovantes pour l'automatisation de la posture de cybersécurité : inventaire des actifs et des vulnérabilités et quantification technique et financière du risque ; la protection des serveurs/applications contre toutes les attaques (notamment les zero day) en quelques millisecondes, réduction des faux-positifs et des coûts d'OPEX jusqu'à 70 %, cela en ne consommant que 2 % du CPU et sans nécessairement remplacer l'existant (EDR/EPP, WAF/RASP) ; la protection des équipements et applications mobiles et la conformité, confidentialité, protection de la vie privée et gouvernance des données structurées et non structurées.


JEAN-BAPTISTE BLANC (EXECUTIVE VICE-PRESIDENT)

UNE APPROCHE DISRUPTIVE EN VUE D'AMÉLIORER LA PROTECTION ET LA CONFORMITÉ TOUT EN RÉDUISANT LE COÛT DE LA SÉCURITÉ

De plus, Catalyst conçoit et anime des programmes pédagogiques personnalisés à destination de publics néophytes ou avertis en ligne ou sur site. En effet, les employés sont le plus grand atout d'une entreprise, mais ils peuvent aussi être le plus grand risque quand il s'agit de la sécurité. Selon des études, la négligence des employés est la plus grande menace pour la sécurité des informations pour 84 % des responsables et hauts cadres. Jean-Baptiste Blanc fait ressortir que le facteur humain est souvent le plus vulnérable dans un système informatique. Les membres d'une organisation doivent être sensibilisés, et cela à tous les niveaux. Catalyst Business Solutions propose ainsi des sessions personnalisées qui s'adaptent aux enjeux métiers de tous les maillons de la chaîne.

«*Les intervenants sont des experts dans leur domaine avec une expérience concrète importante. Les contenus sont coconstruits, continuellement enrichis, en lien avec les experts en Sécurité Offensive et Cyber protection. Les formations peuvent passer par des mises en situation pratiques, comme de fausses campagnes de phishing qui permettent au top management d'estimer les maillons les plus vulnérables de sa chaîne de valeur, et ainsi mieux cibler et orienter les efforts de sensibilisation. Aux dirigeants, nous proposons une gamme de sessions VIP abordant les aspects plus stratégiques de la cybersécurité. Nos experts adaptent leurs contenus à chaque contexte pour aider à définir la cybersécurité comme un élément différenciateur dans la conduite des affaires d'une entreprise. Finalement, nous délivrons également des formations techniques pointues aux équipes techniques (DSI, SSI, SOC, etc.) des entreprises. Nos experts, dotés d'une forte expérience professionnelle en entreprise, peuvent aguerrir les équipes techniques d'une entreprise et les former à mieux détecter et réagir à une cyberattaque*», ajoute Jean-Baptiste Blanc.

ROGERS CAPITAL TECHNOLOGY

Stratégie de cyberdéfense en profondeur


ASHISS SOOBHUG
(HEAD OF CYBERSECURITY ADVISORY)

LES SERVICES Cybersecurity Advisory de nouvelle génération de Rogers Capital Technology sont conçus pour améliorer la posture de cybersécurité des organisations à travers des évaluations de sécurité poussées, des programmes de gestion de risques et des formations. Les professionnels de Rogers Capital Technology combinent la force collective d'un profil d'architecte de solutions-ingénieur système et d'un profil de diagnostic de sécurité tout en suivant des méthodologies rigoureuses pour conseiller la direction et le conseil d'administration sur les expositions aux risques et les stratégies de cyberdéfense.

«*Nous nous concentrons également sur l'orientation stratégique pour guider les compagnies dans leur investissement dans la sécurité, dans leur sélection technologique et leur programme de gestion des risques. Nous pensons que la cybersécurité doit être issue d'une approche holistique axée sur la résilience. C'est pourquoi nous avons investi dans un laboratoire de cybersécurité pour la recherche et le développement afin de rester à l'affût des cybermenaces sophistiquées et les mécanismes de défense*», souligne Ashiss Soobhug, Head of Cybersecurity Advisory de Rogers Capital Technology.

Rogers Capital Technology conseille des entreprises dans différents segments de l'industrie, y compris les services financiers et bancaires, l'hôtellerie, la vente au détail, l'industrie sucrière, les voyages et le tourisme, les entreprises, l'automobile, les médias, les jeux d'argent, la santé et la gestion immobilière. Un consultant en sécurité fournit un aperçu des cyber-risques de l'organisation d'un point de vue indépendant et conseille l'organisation sur la bonne stratégie à adopter pour aligner ses objectifs commerciaux sur ses besoins de cybersécurité. Le consultant avise aussi la direction quant à la priorité des investissements de sécurité avec plus de tact, en particulier avec la sélection de la technologie. Cela à travers une solide feuille de route d'amélioration de la cybersécurité.

Par ailleurs, depuis un peu plus de trois ans, Rogers Capital Technology s'est lancée dans une série de campagnes de sensibilisation à la cybersécurité pour la communauté des affaires sur les risques et impacts des cyberattaques. Ces campagnes comprennent une série d'appels d'alerte à la cybersécurité pour les P-DG, les gestionnaires et les cadres supérieurs afin qu'ils prennent les mesures nécessaires pour protéger leurs entreprises ainsi que leurs employés alors qu'ils deviennent vulnérables lorsqu'ils travaillent à domicile. Dans de nombreux cas, Rogers Capital Technology a démontré preuves à l'appui comment les pirates exécutent leurs méthodes pour compromettre avec succès l'information et comment les techniques d'ingénierie sociale sont utilisées pour tromper les utilisateurs. L'entreprise poursuit cette initiative avec un sens de responsabilité sociale d'entreprise tout en gardant constamment à l'esprit que la bataille est longue.

AMÉLIORER LA POSTURE DE CYBERSÉCURITÉ À TRAVERS DES ÉVALUATIONS DE SÉCURITÉ POUSSÉES, DES PROGRAMMES DE GESTION DE RISQUES

«*Nous avons développé des programmes de formation en cybersécurité taillés sur mesure pour répondre aux besoins des professionnels opérant dans plusieurs secteurs de l'industrie. Nous avons des programmes de type master class qui sont conçus pour éduquer les professionnels du secteur des technologies de l'information, en particulier ceux qui ont un rôle important, visant à garantir la confidentialité des informations, la détection des menaces et la réponse aux incidents. Nos formations en 'Business Continuity Planning', 'Data protection' et cybersécurité ciblent particulièrement les cadres qui prennent des décisions, les responsables informatiques, les 'Data Protection Officers', les ingénieurs système et ceux qui sont activement dans le support technique du matériel informatique.*»

Ashiss Soobhug explique également que la situation du travail à domicile est une réalité dans le sens que, avec l'utilisateur opérant de n'importe où en utilisant un réseau public, la compagnie a moins de moyens et de visibilité pour appliquer les mêmes contrôles de sécurité que si l'utilisateur était sur le réseau de l'entreprise. L'approche de Rogers Capital Technology face à cette situation a été de réaliser une évaluation de la sécurité de la configuration liée au télétravail avec pour objectif de comprendre l'impact sur la sécurité des données. Deuxièmement, l'entreprise a également utilisé des techniques de Social engineering pour identifier ces utilisateurs étant les plus susceptibles d'être trompés par des pirates et des e-mails de types phishing. Sur la base de ces évaluations, des recommandations aux clients ont été faites afin que des actions correctives soient prises.