[INNOVATION]

PARWEZ BHUGALEE (EXECUTIVE BUSINESS DEVELOPMENT DE BIRGER)

«LES ENTREPRISES FONT FACE À DES RISQUES PLUS ÉLEVÉS AVEC LA NOUVELLE RÉALITÉ»

ENJEU MAJEUR POUR LES ENTREPRISES, LA CYBERSÉCURITÉ EST DEVENUE UN INVESTISSEMENT INCONTOURNABLE POUR PROTÉGER AUTANT LES DONNÉES PROFESSIONNELLES QUE LES INFORMATIONS PERSONNELLES. MAIS FAUT-IL ENCORE POUVOIR COMPRENDRE COMMENT, ET CONTRE QUI SE PROTÉGER. PARWEZ BHUGALEE, EXECUTIVE BUSINESS DEVELOPMENT CHEZ BIRGER., REVIENT SUR LE CYBER SECURITY REPORT 2020, QUI DONNE UN ÉCLAIRAGE SUR LA CYBERSÉCURITÉ DANS LA RÉGION.

REECHA RAMOO

Selon l'enquête de BIRGER. 2020 consacrée à la cybersécurité, Maurice a un degré de maturité de 82 en cybersécurité, alors qu'en 2019, l'indice était à 75. Qu'est-ce qui explique cette progression ?

Cette enquête, qui reflète la progression du niveau de maturité des pays et des entreprises, nous révèle qu'au fil des années, les entreprises ont mis en place une structure appropriée pour renforcer leur cyberdéfense. Les autorités ainsi que les régulateurs ont renforcé les lois et les réglementations au niveau des pays et des secteurs concernés. Cela a d'ailleurs contribué à l'amélioration du BIRGER. CYIndex de Maurice, qui est passé de 75 à 82. Pour rappel, le BIRGER. CYIndex mesure le degré de maturité des répondants en cybersécurité : 0-50 maturité faible ; 51-70 maturité modérée et 71-100 maturité élevée.

Cependant, le rapport de BIRGER. suivant son enquête dédiée à la cybersécurité nous a aussi rappelé qu'il ne faut pas dormir sur ses lauriers malgré tous les efforts déployés jusqu'ici. La pandémie de la Covid-19 est venue chambouler la stratégie des entreprises. Elle a forcé ces dernières à accélérer leur transformation digitale pour s'adapter rapidement à un nouveau mode de travail afin d'assurer la continuité de leurs activités. Toutefois, c'est très souvent au détriment des validations habituelles et de la structure de cyberdéfense déjà en place.

Il faut comprendre que cette rapide transformation digitale a exposé notre surface d'attaque beaucoup plus qu'auparavan ; notamment avec le télétravail, l'augmentation de connectivité, les transactions en ligne, l'adoption accélérée du cloud et la délocalisation des opérations sur plusieurs géographies. Ainsi, il faut dire qu'il est aujourd'hui plus que jamais important de se protéger contre les cyberattaques.

Le phishing et l'ingénierie sociale, les attaques ciblées et le ransomware font partie des incidents récurrents. Y a-t-il une raison spécifique à cela ?

Les attaques et les vecteurs d'attaques ne changent pas beaucoup d'année en année. Nous voyons que le phishing (hameçonnage) et l'ingénierie sociale, le malware (logiciel malveillant) et autre ransomware (rançongiciel) sont toujours présents dans notre région. Ces attaques ciblent le maillon faible des entreprises ; notamment le facteur humain.

Les cybercriminels savent que c'est plus facile pour un humain de cliquer sur un lien pour déclencher une attaque que d'essayer de passer les différents niveaux de sécurité des systèmes informatiques. De plus, ils utilisent les dernières technologies liées à l'Intelligence Artificielle et à l'automatisation pour déclencher un plus grand nombre d'attaques. Ce qui explique pourquoi les entreprises continuent d'être victimes de ces attaques. Nous voyons d'ailleurs cette tendance dans notre région, que ce soit dans les îles de l'océan Indien ou en Afrique.

Ces attaques continuent d'avoir des effets disruptifs. Avec la nouvelle réalité et la surface d'attaque plus exposée, les entreprises font face à des risques plus élevés.

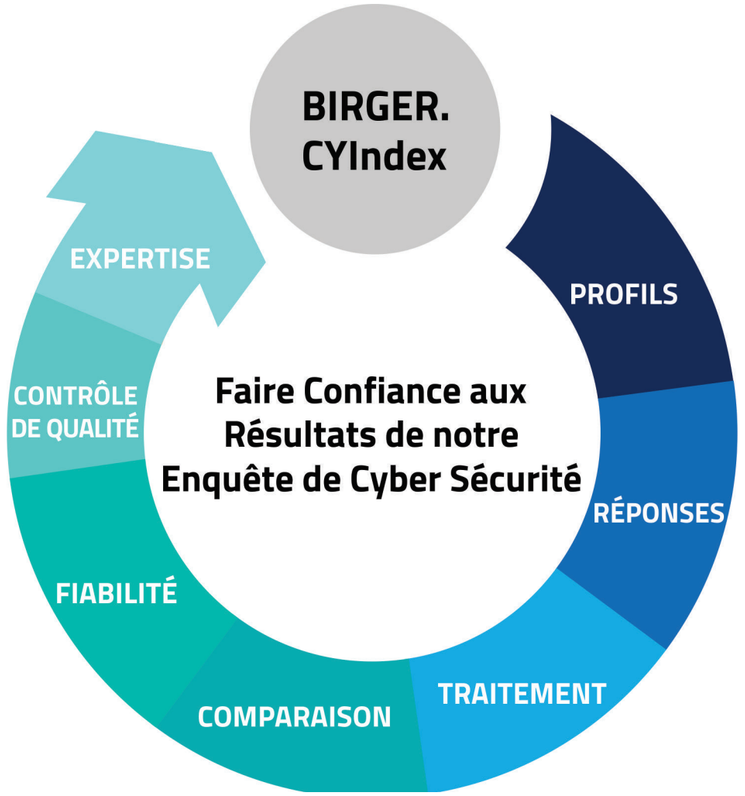
Le nombre de pays a diminué alors que le nombre d'organisations participant à l'enquête a augmenté par rapport à celle effectuée en 2019. Est-ce imputable à la pandémie et au télétravail ?

Pas forcément, bien que la nouvelle réalité avec la pandémie aurait pu avoir un effet. Chaque année, pour notre enquête, nous essayons d'avoir un échantillon de répondants représentatifs pour obtenir des résultats fiables. Il est important d'avoir des répondants qui sont impliqués dans la cybersécurité et, cette année, plus de 90 % des répondants ont satisfait ce critère. Et nous choisissons les entreprises de notre réseau de clients.

Cette année, nous avons eu la participation de 200 entreprises, avec 291 répondants ; c'est le nombre le plus élevé depuis que nous avons commencé notre enquête, en 2017. Tout cela pour dire que le ciblage des répondants est très important pour obtenir des résultats fiables.

BIRGER. a rapporté dans l'édition de 2019 que malgré l'amélioration de leur niveau de maturité, les entreprises peuvent développer un faux sentiment de sécurité. Dans le dernier rapport, les données montrent-elles une amélioration à ce niveau ?

Ce point est encore plus pertinent cette année avec la Covid-19. Bien que nous notions une amélioration générale du degré de maturité des entreprises, la Covid-19 apporte une nouvelle réalité, et nous ne nous attendons pas à retourner au modèle pré-Covid. Les entreprises ont dû adapter leur mode d'opération pour assurer la continuité de leurs opérations, cela aux dépens de la sécurité. Nous nous retrouvons aujourd'hui avec une surface d'attaque beaucoup plus exposée qu'auparavant.



Les cybercriminels s'adaptent au nouveau contexte pour orchestrer leurs attaques, comme mentionné plus haut, pour cibler le facteur humain et utiliser les technologies de l'intelligence artificielle et de l'automatisation pour générer un plus grand nombre d'attaques. Cela dit, les entreprises ne doivent pas adopter le statut quo. Il faut qu'elles s'adaptent à la nouvelle réalité et continuent à faire des efforts pour améliorer leur niveau de maturité en cybersécurité.

Les recommandations n'ont pas changé par rapport aux études menées en 2019. Pouvez-vous nous en dire plus à ce sujet ?

Les cybercriminels utilisent les mêmes vecteurs d'attaques et s'adaptent à la nouvelle façon d'opérer des entreprises dans l'ère de la Covid-19. Nous voyons que le facteur humain cette année est encore plus exploité. Le volume d'attaques généré submerge les équipes de sécurité des entreprises et le manque de ressources appropriées (financières et humaines) est un défi important mentionné par les répondants. Pour ces raisons, nous maintenons nos trois recommandations qui sont encore plus importantes dans le contexte actuel : la sensibilisation, pour pallier le maillon faible que sont les humains dans le cycle de cyberdéfense ; l'automatisation de grandes quantités d'informations et d'incidents peuvent être traitées rapidement, et actions correctives appliquées automatiquement ; les Sociétés de Services Spécialisés pour pallier le manque de compétences et de restrictions budgétaires ainsi que d'accéder aux technologies de pointe. Les entreprises doivent faire appel aux Sociétés de Services Spécialisées en Sécurité et en Résilience.

Les entreprises doivent avoir des plans de continuité d'activité qui prennent en compte les effets disruptifs qui sont causés par les cyberattaques pour être ainsi plus résilientes. D'ailleurs, pendant la Semaine de Sensibilisation à la Continuité d'Activité (Business Continuity Awareness Week), qui a lieu cette année du 17 au 21 mai, nous publierons un article approfondi sur la Résilience.

Quelles sont vos attentes concernant l'enquête de BIRGER. dédiée à la cybersécurité pour 2021 ? Les modifications proposées par l'ICTA affecteront-elles le rapport de quelque manière que ce soit ?

Nous encourageons fortement les entreprises des différents secteurs et pays de notre région de s'adapter à cette nouvelle réalité en s'appuyant sur les bonnes technologies pour mieux se sécuriser et être plus résilientes. Concernant la démarche de l'ICTA, c'est une initiative louable dans la forme pour protéger les plus vulnérables. Mais encore une fois, il faut trouver la balance entre l'application de ce modèle et la protection des données confidentielles. Si l'ICTA souhaite décrypter les messages, la chaîne de protection des données sera compromise, ce qui augmentera le risque d'être ciblé par les pirates informatiques. Il faudra aussi bien définir la démarcation des rôles et des pouvoirs associés entre les différentes institutions par cette initiative.

L'ICTA se doit d'être le régulateur pour laisser les institutions jouer leur rôle dans ce modèle. Comme avec l'application de toute nouvelle réglementation de ce genre, les données des entreprises seront plus exposées et ce sera à l'ICTA de prendre les mesures appropriées au cas où les modifications proposées soient adoptées.

BIRGER. RAPPORT 2020 DÉDIÉ À LA CYBER SÉCURITÉ

BIRGER. CYIndex 2020

57	75	76	76	82
Comores	Madagascar	Seychelles	Rwanda	Maurice

Degré de maturité - Faible : 0 – 50 | Modéré : 51 - 70 | Elevé : Plus de 70

291
Nombre de répondants

90%
Répondants impliqués dans la Cyber Sécurité

200
Nombre d'entreprises

13
Nombre de pays

Surface d'attaque

Les systèmes informatiques ont évolué d'un environnement en circuit fermé à un qui est plus exposé, car les entreprises ont numérisé leurs opérations. La pandémie de Covid-19 a accéléré cette transformation digitale et expose d'avantage la surface d'attaque aux cybermenaces.

Incidents

Afrique

63% ▲		Phishing & Ingénierie Sociale
59%		Programme Malveillant
37%		Attaques du Web
22% ▲		Cyberattaques ciblées
20%		Déni de Services
17% ▲		Ransomware

IOI

48% ▼		Programme Malveillant
46% ▼		Phishing & Ingénierie Sociale
24%		Ransomware
29%		Attaques du Web
23%		Accès non-autorisé
20%		Cyberattaques ciblées

▲ ▼ Plus haut ou plus bas comparé à 2019

Recommandations

Sensibilisation

Automatisation

Sociétés de Services Spécialisés

Conclusion

Les entreprises peuvent toujours s'améliorer, malgré leur maturité élevée en Cyber Sécurité. Dans ce nouveau contexte, les entreprises doivent redéfinir et adapter leurs stratégies de Cyber Sécurité pour minimiser les risques d'attaques.