Parwez Bhugalee : « Les entreprises ne doivent pas développer l'illusion d'être sécurisées »

Les entreprises sont recommandées de sensibiliser leurs employés continuellement pour renforcer le maillon faible qui est le facteur humain.

C'est la troisième édition de l'enquête régionale sur la cybersécurité des entreprises réalisée dans la région et en Afrique par l'entreprise BIRGER. Une mine d'informations précieuses analysées par Parwez Bhugalee, exécutif en charge du marketing et du développement des affaires chez BIRGER.

L'Eco austral : C'est la troisième enquête de ce type que BIRGER. organise dans la région et en Afrique orientale, pouvez-vous nous donner les tendances de cette année ?

Parwez Bhugalee : Pour mieux comprendre les tendances de cette année, il est important de revenir sur l'historique de notre enquête. Depuis 2017, nous menons des enquêtes annuelles dédiées à la cyber sécurité dans notre région. L'objectif est de déterminer le degré de maturité régional en cyber sécurité en utilisant notre indice de cyber sécurité, BIRGER. CYIndex. Cet indice s'appuie sur 5 fonctions clés : Identifier - Protéger – Détecter - Répondre - Reprise. Il peut être calculé par pays, par secteur et par entreprise.

Notre dernière enquête a été menée durant le dernier trimestre de 2019, dans 14 pays des Iles de l'océan Indien (IOI) et en Afrique avec 224 répondants dont plus de 90 % sont impliqués dans la cyber sécurité.

En général, le degré de maturité des entreprises en cyber sécurité s'est amélioré. Toutefois, il y a une augmentation des incidents et les cybers criminels exploitent les mêmes vecteurs d'attaques. Les attaques continuent d'évoluer rapidement pour contrecarrer les systèmes de défense mises en place comme le *Phishing & Social Engineering* qui exploitent l'erreur humaine pour compromettre les entreprises. Les répondants ont exprimé les défis principaux que leurs entreprises doivent surmonter tels que le manque de personnels qualifiés ; le volume grandissant d'attaques ; et le manque de cyber intelligence pour se défendre contre les attaques.

Pour cette année, l'île Maurice et le Rwanda ont le meilleur indice de CYIndex. Ils ont donc le degré de maturité le plus élevé dans notre région.

Le facteur humain est à nouveau la principale cause des cyberattaques, cependant quels sont les principaux incidents rencontrés en Afrique et dans nos îles de l'océan Indien ?

Les cybers criminels font des attaques ciblées pour exploiter cette faiblesse humaine comme avec le *Phishing & Social Engineering*, les *Web-based Attacks* et les *Malwares*. En analysant en détails les cinq fonctions clés, nous notons que la fonction Identifier est la plus faible car il y a des lacunes dans la gouvernance des entreprises en termes de cyber sécurité. La fonction Répondre ayant le meilleur score, on peut dire que les entreprises comprennent l'importance d'un plan bien défini pour faire face aux incidents.

Nous avons poussé notre analyse en comparant les indices de 3 secteurs : bancaire, assurance et sociétés offshore. Le secteur bancaire est le leader en degré de maturité car les banques ont mis en place des stratégies de cyber défense fondées sur une analyse et un calcul de risques. Le secteur d'assurance a progressé cette année car il implémente aussi des stratégies de cyber défense bien définies axées sur les risques encourus. Les sociétés d'offshores ont un degré de maturité moyen et n'ont pas progressé. La fonction Identifier est la plus faible et les fonctions Protéger et Reprise ont régressé cette année. Toutefois, ces compagnies font un effort en investissant dans les systèmes de détection des incidents.

Comment les entreprises font-elles face et surtout, quelles conclusions ont elles tiré des précédentes enquêtes ?

Les entreprises dans notre région comprennent l'importance de se défendre et investissent dans les ressources nécessaires. Cet effort est apparent par l'amélioration de leur degré de maturité en général avec un indice plus élevé pour les 5 fonctions clés. Toutefois, cette amélioration ne doit pas voiler l'effort qu'il reste à faire et les entreprises ne doivent pas tomber dans une illusion d'être sécurisées. Les cybers criminels d'adaptent et le nombre d'incidents a considérablement augmenté. Les défis principaux sont les manquements tant au niveau humain que des processus de cyber défense, et le nombre grandissant des canaux d'attaques. Les entreprises sont recommandées de sensibiliser leurs employés continuellement pour renforcer le maillon faible qui est le facteur humain. Ils doivent investir dans l'automatisation basée sur l'Intelligence Artificielle pour contrecarrer le volume et la variété des menaces. Ils doivent s'appuyer sur des prestataires des services spécialisés pour complémenter leur équipe interne.

BIRGER. Rapport 2019 dédié à la Cyber Sécurité

Nombre de répondants :
224

Nombre d'entreprises :
158

Répondants impliqués dans la Cyber Sécurité :
90%

Nombre de pays :
14

Les défis :

- Manque de personnel qualifié en Cyber Sécurité
- Augmentation et nouvelles menaces
- Manque d'intelligence cyber-menaces

Afrique
Incidents majeurs

- Programme Malveillant - **61%**
- Phishing & Ingénierie Sociale - **57%**
- Ransomware - **39%**

Afrique
Incident le plus disruptif

- Programme Malveillant - **25%**

BIRGER. CYIndex

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

75 Rwanda	**75** Maurice	
66 Madagascar	**64** Seychelles	**45** Comores

IOI
Incidents majeurs

- Programme Malveillant - **60%**
- Phishing & Ingénierie Sociale - **57%**
- Attaques du Web - **29%**

IOI
Incident le plus disruptif

- Phishing & Ingénierie Sociale - **31%**

BIRGER. CYIndex IOI

Bancaire	Assurance	Sociétés d'Offshore
77	75	68

Recommandations :

- **Sensibilisation**
- **Automatisation**
- **Faire appel aux Sociétés de Services de Sécurité Informatique**

Conclusion :

Régionalement, les entreprises ont investi progressivement pour améliorer leur posture en Cyber Sécurité. Les cybercriminels utilisent toujours les mêmes vecteurs d'attaques mais le nombre d'incidents augmente afin d'exploiter les nouvelles vulnérabilités. Malgré le fait d'avoir amélioré leur niveau de maturité, les entreprises peuvent développer l'illusion d'être sécurisée.

B_contacted@birger.technology | **birger.technology**