OLEA INSURANCE SOLUTIONS AFRICA - www.olea.africa - info@olea.africa

LA GIRAFE DÉCHAÎNÉE

JUIN 2023

LA CYBERSÉCURITÉ, ENJEU MAJEUR POUR VOS ENTREPRISES |
ASSURANCE CYBER : PROTÉGEZ VOS ENTREPRISES

LA CYBERSECURITE, ENJEU MAJEUR POUR VOS ENTREPRISES

Bryan Rangapanaiken, Responsable Sécurité des Systèmes Informatiques, OLEA.

Qu'est-ce que la cybersécurité et quels sont ses enjeux ?

La cybersécurité désigne l'ensemble des mesures et des pratiques mises en place pour protéger les systèmes informatiques, les réseaux, les données et les utilisateurs contre les menaces et les attaques numériques.

La dépendance croissante aux technologies numériques en Afrique a un impact majeur sur les entreprises du continent. Les avancées rapides dans les domaines des technologies de l'information et de la communication (TIC) ont transformé les opérations quotidiennes des entreprises africaines. Cependant, cette dépendance croissante présente également des défis importants. Interpol estime que la cybercriminalité coûte à l'Afrique 4 milliards de dollars par an.

Les enjeux de la cybersécurité pour les entreprises africaines sont multiples et cruciaux. Ils incluent la protection des données sensibles, la prévention des cyberattaques, la préservation de la confidentialité, de l'intégrité, de la disponibilité des informations, ainsi que la garantie de la confiance des utilisateurs et la conformité aux réglementations en matière de protection des données. La cybersécurité vise à anticiper, détecter et réagir efficacement aux risques et aux incidents de sécurité afin de maintenir un environnement numérique sûr et fiable pour les individus, les entreprises et les organisations.

Quelles sont les cybermenaces courantes pour une entreprise africaine ?

Les cinq principales cybermenaces en Afrique identifiées dans le dernier rapport d'Interpol sont :

1. **Escroqueries en ligne :** de faux e-mails ou SMS prétendant provenir d'une source légitime sont utilisés pour tromper des individus afin qu'ils révèlent des informations personnelles ou financières.

2. **Extorsion numérique :** les victimes sont amenées à partager des images compromettantes qui sont utilisées pour le chantage.

3. Compromission de messagerie professionnelle : les criminels piratent les systèmes de messagerie électronique pour obtenir des informations sur les systèmes de paiement de l'entreprise, puis trompent les employés de l'entreprise pour qu'ils transfèrent de l'argent sur leur compte bancaire.

4. Ransomware : les cybercriminels bloquent les systèmes informatiques des hôpitaux et des institutions publiques, puis demandent de l'argent pour restaurer les fonctionnalités.

5. Botnets : les réseaux de machines compromises sont utilisés comme outil pour automatiser les cyberattaques à grande échelle.

Source: Interpol African Cyberthreat Assessment Report

Comment sensibiliser les collaborateurs aux cybermenaces ?

La sensibilisation à la cybersécurité est essentielle pour protéger les entreprises contre les cybermenaces. Voici quelques mesures efficaces à mettre en place pour sensibiliser les collaborateurs et renforcer la sécurité de l'entreprise.

Formation en cybersécurité : Le facteur le plus important est la formation. Organisez des sessions de formation régulières pour familiariser les collaborateurs avec les cybermenaces courantes. En les informant sur les techniques utilisées par les cybercriminels, vous les aidez à détecter et à prévenir les attaques potentielles.

Politiques de sécurité : Établissez des politiques de sécurité claires et communiquez-les à l'ensemble du personnel. Ces politiques devraient aborder des sujets tels que l'utilisation de mots de passe forts, le partage sécurisé d'informations, l'accès aux données sensibles et l'utilisation des appareils personnels sur le lieu de travail.

Exercices de simulation : Organisez des exercices de simulation de cyberattaques pour permettre aux collaborateurs de mettre en pratique leurs connaissances en matière de cybersécurité. Ces exercices simulés peuvent inclure des attaques de phishing, des tentatives d'intrusion ou des situations d'urgence.

Communication régulière : Maintenez une communication régulière et claire sur les actualités en matière de cybersécurité. Envoyez des bulletins d'information, des courriels d'alerte ou des annonces internes pour tenir les collaborateurs informés des derniers développements et des mesures de sécurité à prendre.

En conclusion la sensibilisation à la cybersécurité est un élément crucial pour protéger les entreprises. En mettant en place des mesures telles que la formation, les politiques de sécurité, les exercices de simulation et la communication régulière, les entreprises peuvent renforcer la vigilance de leurs collaborateurs et réduire les risques liés à la cybersécurité.

La sensibilisation à la cybersécurité doit être une priorité continue et intégrée dans la culture de l'entreprise.

Que fait OLEA pour mettre en place des infrastructures solides de cybersécurité ?

Chez OLEA, les fondateurs ont vite compris l'importance d'investir dans la sécurisation de nos infrastructures et de nos outils informatiques. En partenariat avec un des leaders en matière de formation en cybersécurité, nous avons mis en œuvre différentes mesures organisationnelles destinées à renforcer la sensibilisation et la responsabilisation de tous nos collaborateurs.

OLEA démontre son engagement à avoir une sécurité optimale de ses infrastructures, notamment en ayant mis en place avec ses partenaires et fournisseurs des politiques de sécurité des systèmes d'informations répondant aux exigences de plusieurs normes et certifications : certification PCI-DSS, certification ISO/IEC 27001, certification RGPD, attestations SOC 1 TYPE II et SOC 2 TYPE II.

OLEA s'est aussi engagé auprès de partenaires certifiés Microsoft Gold Partner pour la sécurisation de son infrastructure Cloud.
Cela inclut l'implémentation de solutions de sécurité telles que :

- 1.Identity Protection
- 2.Email Protection
- 3.Mobile Device Management
- 4.Endpoint Detection and Response
- 5.Mobile Application Manangement
- 6.Data Loss Prevention

En implémentant ces différentes mesures de sécurité, OLEA renforce la protection de ses données et celles de ses clients, prévient les menaces potentielles et garantit la conformité aux réglementations en matière de confidentialité et de sécurité. En outre, OLEA continue de faire évoluer et d'améliorer ses pratiques de sécurité pour répondre aux besoins changeants de ses clients et aux défis de sécurité actuels et à venir.

ASSURANCE CYBER : PROTEGEZ VOS ENTREPRISES

Ayouba Seydou, Directeur des Placements et de la Réassurance, OLEA.

Nous faisons face de plus en plus à des violations de données qui font la une des journaux dans le monde entier, la perte de données personnelles et d'entreprise qui entraînent des conséquences considérables.
La majorité des articles concernent le type de perte de données qui a un impact sur les personnes au niveau personnel : numéros de cartes de crédit, dossiers médicaux, dates de naissance, etc.

Nous devrions également être conscients de l'impact de la perte de données et d'informations d'entreprise telles que la propriété intellectuelle qui, entre les mains d'un concurrent ou même d'un extorqueur, peuvent gravement désavantager l'entreprise.

Quels sont les caractéristiques et les avantages de l'assurance cyber ?

L'assurance cyber permet à une entreprise la continuité de son activité, ce en réduisant, l'impact financier (perte de chiffre d'affaires, frais et dépenses ; réclamations et actifs), opérationnels (Confidentialité, fiabilité et disponibilités) mais aussi les conséquences sur sa réputation et le système d'information.

Les couvertures les plus fréquentes sont de deux natures :

GARANTIES DOMMAGES :

- Pertes d'exploitation
- Frais engagés par le client
- La protection des Données Personnelles
- Frais de défense et des sanctions dans le cadre d'une enquête
- Tentatives d'extorsion informatique

GARANTIES RESPONSABILITE CIVILE :

- Réclamations à la suite d'une atteinte informatique ou une atteinte à la confidentialité des données personnelles
- Garantie multimédia

Quelles sont les entreprises éligibles à l'assurance cyber ?

Pratiquement toutes les entreprises traitent quotidiennement des données personnelles, qu'il s'agisse de numéros de cartes d'identité, profils des employés, des informations sur les cartes de crédits, informations sensibles sur les clients.
Ces mêmes entreprises sont confrontées à des responsabilités si ces données tombent entre de mauvaises mains ou tombent dans le domaine public.
Des petites entreprises aux multinationales, toutes sont concernées et éligibles.

Pourquoi les entreprises ne souscrivent pas massivement à l'assurance cyber ?

A mon avis plusieurs raisons :

1/ Le manque de connaissance des menaces, cela malgré toutes les attaques que nous voyons dans les médias. Beaucoup pensent que cela se limite à la perte des données voire perte d'exploitation.

2/ La méconnaissance des garanties, pour beaucoup les couvertures, voire l'offre cyber est inconnu. Le focus est sur les risques visibles, globale dommage, responsabilité civile et professionnelle.

Beaucoup d'entreprises estiment qu'un bon antivirus avec un pare-feu sont suffisants pour prévenir ce risque.

3/ La complexité des questionnaires cyber qui sont très spécifiques, nécessitant la collaboration entre le business et des techniciens informatiques.

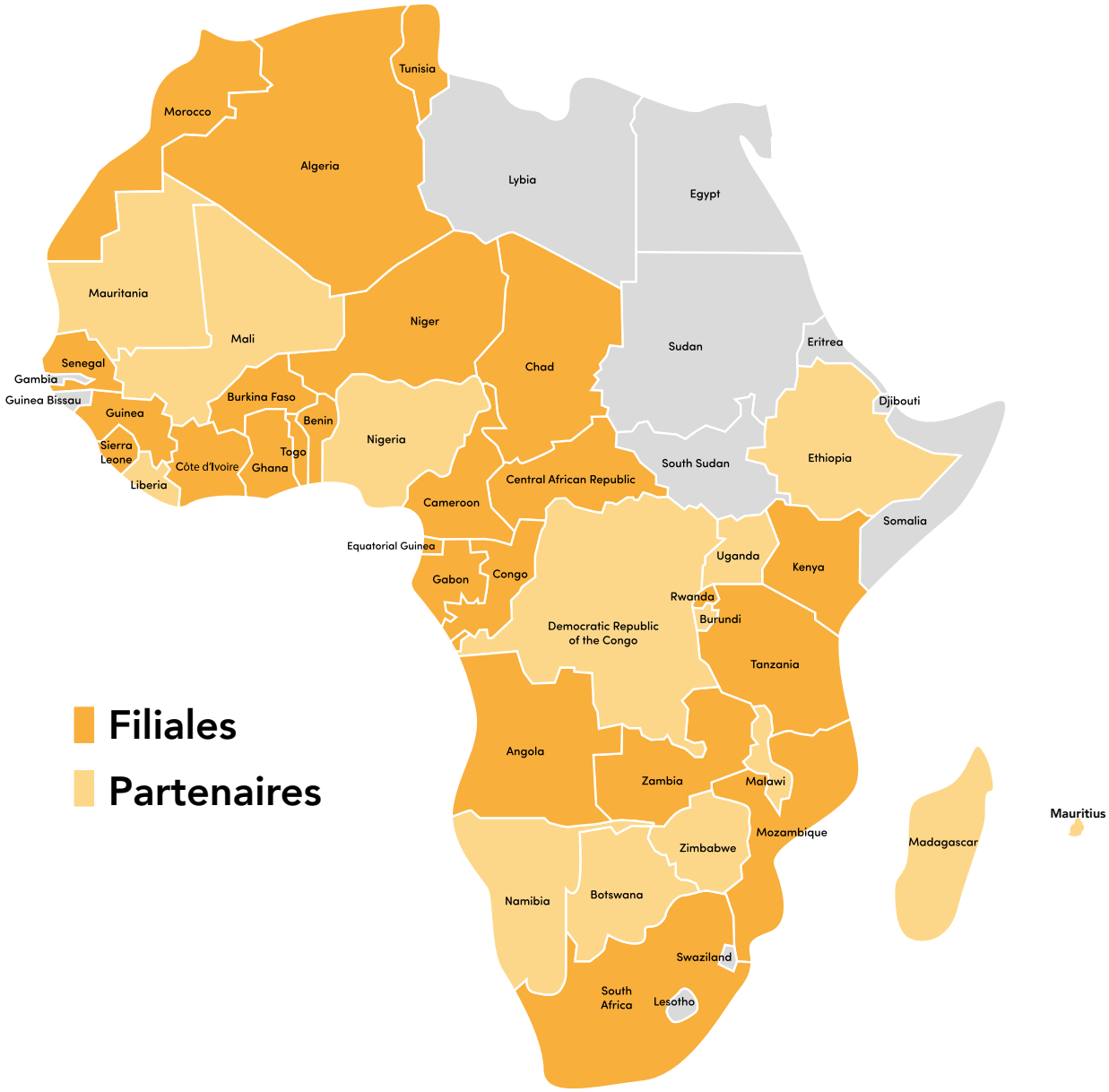
4 / Enfin, la maturité des architectures des systèmes informatiques. En effet, même quand les entreprises ont conscience de l'importance de la couverture, ces dernières ne répondent pas aux critères exigés par les assureurs en termes de prérequis. A noter d'ailleurs que la grande majorité des intrusions, failles de sécurité sont le fait d'erreurs humaines, ce qui imposent une formation / sensibilisation quasi continue des équipes pour rester vigilant. Les résultats sur ces cessions de formations sont extrêmement positifs.

C'est toute la force d'OLEA. Nous accompagnons les entreprises qui souhaitent souscrire une assurance Cyber très en amont, à travers des audits de sécurité permettant de lister tous les prérequis nécessaires à cette souscription. Nous proposons aussi des formations onlines ludiques, interactives et continues pour sensibiliser les équipes de nos clients.

Ces éléments et cette « mise à niveau » sont déterminants / discriminants pour qu'un assureur accepte de coter ce risque pour le compte de nos clients.

N'HÉSITEZ DONC PAS À NOUS CONTACTER POUR TOUS VOS BESOINS RELATIFS À LA SOUSCRIPTION DE CETTE ASSURANCE « CYBER».
INFO@OLEA.AFRICA

LE RÉSEAU OLEA
ET SES 24 FILIALES EN AFRIQUE



Afrique du Sud | Algérie | Angola | Benin | Burkina Faso | Cameroun | Centrafrique | Congo | Côte d'Ivoire | Gabon | Ghana | Guinée | Kenya | Maroc | Mozambique | Niger | Rwanda | Sénégal | Sierra Leone | Tanzanie Tchad | Togo | Tunisie | Zambie