DATAPROTECT
Security is our commitment

LA FRAUDE BANCAIRE EN AFRIQUE SUBSAHARIENNE

DATAPROTECT
Security is our commitment
(une étude Sciencetech.com)

La cybersécurité dans le secteur financier africain

Faits saillants

0. Avant-propos

Les experts DATAPROTECT ont noté avec inquiétude une recrudescence des attaques cybernétiques visant le secteur bancaire en Afrique subsaharienne depuis plusieurs mois. Cette étude est l'occasion de faire le point sur l'expérience en cybersécurité accumulée par les banques africaines au cours des dernières années. Le sondage a été très révélateur. Nous ne voulons pas garder ces données pour nous uniquement et avions décidé de les partager avec notre clientèle, pour la sensibiliser, pour leur démontrer que ce type de mésaventure n'arrive pas qu'aux autres, tout le monde est concerné, mais que ce n'est pas une fatalité, car, aujourd'hui, il y a moyen de se prémunir contre ce type de risque.

Ali El-Azzouzi
Président - DATAPROTECT

1. Tendances actuelles

Le secteur financier est entré dans une période de transformations profondes sur la terre entière. Tout a commencé avec la multiplication des néobanques qui misent sur le numérique et la téléphonie mobile pour réinventer les services financiers. Peu après est apparue une nouvelle industrie : les fintechs qui simplifient l'utilisation des comptes bancaires à bas coûts. Bousculées, les banques ont inventé le concept d'*Open Banking* qui consiste à ouvrir les systèmes d'information des banques à des tiers et à partager avec les fintechs une partie de leurs données clients.

La bancarisation de l'Afrique a enfin décollé : le nombre de nouveaux comptes augmente d'environ 3% par an. Il ne faut donc pas s'étonner si le secteur bancaire africain est un des plus dynamique au monde : le deuxième en termes de croissance et de profitabilité. Ce développement rapide du secteur financier a sa contrepartie qui est l'explosion concomitante de la cyberfraude. Or, les banques sont des cibles privilégiées des cybercriminels grâce aux programmes malveillants conçus spécialement en fonction du système financier.

La cybercriminalité se répand d'autant plus vite que le cadre législatif et réglementaire de la plupart des pays d'Afrique est inadapté et, quand il existe, il est mal appliqué. Au sein de cet environnement incertain, les banques constituent un cas à part. En effet, elles doivent respecter la réglementation internationale (accords de Bâle) et régionale (Banque Centrale des États de

l'Afrique de l'Ouest). Pour satisfaire à leurs obligations, les banques sont donc incitées à investir en cybersécurité. Elles y ont même intérêt.

2. Profil du secteur bancaire

L'enquête de DATAPROTECT a eu lieu entre février et avril 2019 auprès de 148 banques provenant de 11 pays d'Afrique de l'Ouest et centrale. Au total, 21 banques ont participé à l'enquête, ce qui fait un taux de réponse de 14%. La plupart des répondants sont des banques commerciales ou des banques de détail. La majorité sont de tailles moyennes ou petites et à capitaux africains. Pas de géant parmi les répondants, mais une des institutions financières contactées a déjà essaimé en Afrique et une autre en France.

3. La gouvernance en cybersécurité des banques africaines

Plus de 80% des institutions financières ont confié la responsabilité de leur cybersécurité à un responsable de la sécurité des systèmes d'information (RSSI), mais celui-ci relève généralement du directeur des systèmes d'information (DSI). Cela signifie que la cybersécurité n'a pas acquis le rang de discipline à part entière, elle est toujours considérée comme une composante des TI. Cela se traduit par des effectifs sous-dimensionnée : entre un employé à plein temps et trois.

Cette situation est expliquée en partie par les difficultés de recrutement de main d'œuvre qualifiée : outre le phénomène central qui est le manque de talents, les hauts salaires pratiqués et l'inadaptation de la formation sont les deux raisons les plus souvent mentionnées. Cinquante-cinq pour cent des banques ont tendance à contourner ce problème en recourant à la sous-traitance ou infogérance.

Plus de 70% des entreprises organisent des campagnes de sensibilisation et de formation. Cette forte proportion laisse cependant une minorité sans programme de sensibilisation, ni programme de formation, ce qui est inquiétant. Il s'agit d'activités peu couteuses et relativement faciles à implanter, sans lesquelles toute stratégie de cybersécurité est vouée à l'échec. Enfin, la cyberassurance est encore absente, non qu'elle soit négligée, mais parce qu'elle n'est pas disponible.

4. Le cadre sécuritaire

Près des deux-tiers des institutions financières sont dotées d'un programme écrit de cybersécurité et ce résultat diminue encore quand on vérifie plusieurs des composantes d'un tel programme, à savoir les tests d'intrusion (62%), un plan de relève (52%), une analyse de risque (52%), un audit des systèmes d'information (52%) et l'obligation d'inclure une clause de cybersécurité dans les accords de sous-traitance (14%).

Un peu plus de la moitié des institutions financières déclarent disposer d'un SOC et, dans la presque totalité des cas, il s'agit d'un SOC externe. Cette tendance à l'externalisation du SOC

correspond aux meilleures pratiques en vigueur parmi les responsables de sécurité. En effet, un SOC doit fonctionner 24/7 pour être efficace et nécessite du personnel en conséquence, toutes choses qu'il est difficile de réaliser à l'interne.

5. Les cyberattaques et leurs impacts

Au moins 85% des institutions financières consultées déclare avoir déjà été victime d'une ou plusieurs cyberattaques ayant occasionné des dommages – dans certains cas, il s'agit même d'attaques à répétition. Globalement, ce sont les fraudes sur les cartes bancaires (*carding* et *skimming*) ainsi que l'hameçonnage (*phishing*) qui sont les types de cyberattaques les plus fréquents, suivies des atteintes au système bancaire de base (*core banking*), les infections virales et les intrusions dans les systèmes d'information critiques.

La moitié des incidents signalés dans l'enquête de DATAPROTECT ont mis trois mois et plus pour être découverts. La longueur du temps de détection renvoie à la carence d'outils et de ressources nécessaires à l'identification des anomalies. À preuve, seulement 6% des incidents sont découverts par les employés de cybersécurité des institutions financières, la majorité ayant été découverts par des employés des banques ou par des intervenants extérieurs.

Le principal impact des cyberattaques est la perte d'argent, suivi de la suspension des services en ligne et de l'indisponibilité d'un ou plusieurs postes de travail – la fermeture d'une succursale entière ou des guichets automatiques demeurent peu fréquentes. Pour répondre aux cyberattaques, les institutions financières misent avant tout sur des prestataires externes, ce qui est prévisible en raison de leurs ressources humaines et techniques très limitées. La police est très rarement mise au courant.

L'impact financier des cyberattaques est en moyenne de 770 000 euros, mais bien des répondants ont refusé de répondre à la question. Parmi ceux qui n'ont pas voulu donner de chiffres, on notera des réponses parlant d'une simple question de quelques heures de travail perdues.

6. Cadre légal et réglementaire

La plupart des banques africaines déclarent souscrire aux accords de Bâle 2 ou Bâle 3 et une bonne majorité de banques a aussi adopté la norme PCI DSS relative à l'utilisation des cartes de crédit. Ce qui est anormal est que 14% d'entre elles aient déclaré n'avoir adopté aucune norme de cybersécurité. À l'inverse, le respect des normes internationales par les banques explique le succès croissant du secteur financier en Afrique. À bien des égards, on peut dire que le secteur financier joue un rôle de modèle structurant pour le reste de l'économie africaine.

7. Investissements en cybersécurité

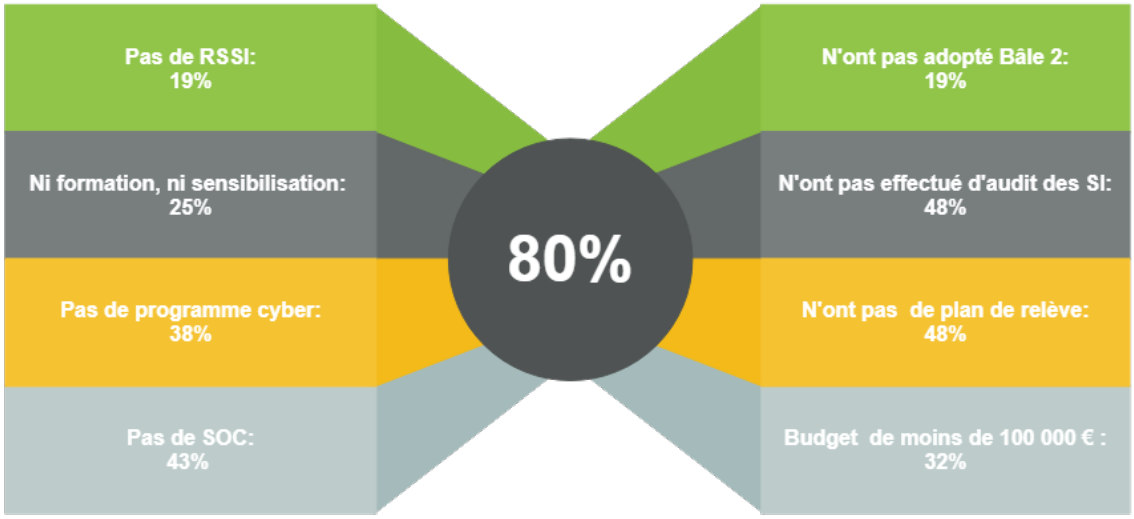
L'investissement en cybersécurité des banques africaines demeure très modeste. Quatre-vingt-cinq pour cent des banques investissent moins de 500 000 € par an en cybersécurité alors qu'elles reconnaissent avoir déjà essuyé des pertes moyennes nettement supérieures (770 000 euros, voir plus haut). Il apparaît clairement que la cybersécurité coûte cher, mais que l'absence de cybersécurité coûte encore plus cher, surtout dans le secteur financier que le risque est maximal.

Près des trois-quarts des investissements en cybersécurité sont à la hausse : il s'agit sans conteste d'un premier élément de réponse à la modestie des budgets. Les institutions financières qui prévoient des coupes budgétaires sont rares. Au total, près des deux-tiers des personnes interrogées ne jugent pas satisfaisant l'outillage de cybersécurité déployé dans leur banque.

8. Conclusion et enjeux

Environ 20% des banques africaines ayant participé à l'enquête affichent un taux de cybersécurité relativement satisfaisant (voir graphique ci-dessous). A contrario, 80% des banques africaines sont vulnérables aux cyberattaques.

PROPORTION DES BANQUES À RISQUE



Source : Étude Sciencetech/DataProtect, février-avril 2019.

Les grands enjeux de la cybersécurité sont le partage d'information, le partenariat avec les fintechs et la mutualisation des ressources (abonnement à un SOC externe).