CONFIANCE NUMÉRIQUE ET CYBERSÉCURITÉ EN AFRIQUE DU SUD

CHIFFRES CLÉS

Pop. en M	PIB/hab. (USD)	Croissance PIB (%) 2017	Croissance PIB (%) 2018	Note envt des affaires
57	**6 151**	**1,3**	**0,8**	**A4**

Sources : FMI, World Bank, COFACE, SER

CARACTÉRISTIQUES DU MARCHÉ (1/2)

Taille du marché

Fondamentaux

- Le marché de la cybersécurité en Afrique va passer de 1,7 Md USD en 2017 à plus de 2,5 Mds USD en 2020 selon le rapport « Africa Cyber Security Market » de MarketsandMarkets.
- En 2017, le FBI a classé l'Afrique du Sud comme étant le 5ème pays le plus touché par la cybercriminalité.
- Le pays est classé 56ème sur son engagement en matière de cybersécurité avec un indice global de la cybersécurité de 0,65. La France est classé 3ème avec un indice de 0,9.
- Selon le South Africa Risk Information Center, les coûts liés aux cyberattaques approcheraient les 573 M USD par an, soit 0,15 % du PIB sud-africain.
- Les acteurs les plus touchés par la cybercriminalité en Afrique du Sud sont les institutions gouvernementales (187 M USD de pertes), les sociétés de télécommunications (225 M USD) et les institutions financières (19 M USD).

Tendances et évolutions

- L'augmentation du budget alloué par les entreprises à la cybersécurité devrait atteindre 1,9 Md USD en 2019.
- L'Afrique du Sud a pris conscience de son retard en matière de cybersécurité. La mise en application en mai 2018 du règlement général sur la protection des données personnelles en Europe (GDPR) entraine des répercussions sur les sociétés sud-africaines.

CHIFFRES DU SECTEUR

Coût de la Cybercriminalité	**13 M EUR**
Place de l'Afrique du Sud dans le classement mondial des pays sujets aux cybercrimes	**5ème / 193**
Taux de croissance 2019 prévu	**20,5 %**
Part des sud-africains ayant été victimes de cybercriminalité en 2017	**77 %**

Sources : SABRIC – Exposure Index – PWC « enquête sur la criminalité mondiale 2017 » – MarketsandMarkets report – Frost & Sullivan – Observatoire 2017 de la Confiance Numérique, Business France –xGartner – IBM Security – EC-Council, ItWeb, Cyber crime & cyber security trends in africa

CONFIANCE NUMÉRIQUE ET CYBERSÉCURITÉ EN AFRIQUE DU SUD

CARACTÉRISTIQUES DU MARCHÉ (2/2)

La concurrence et positionnement de la France

La concurrence locale / internationale

Le secteur est très concurrentiel : il est notamment dominé par des sociétés américaines et sud-africaines (services de collecte de données, de décryptage et de mise en place de pare-feu).

A noter la présence de plus en plus forte d'acteurs chinois qui opèrent dans le domaine de la cybersécurité et travaillent directement avec les institutions gouvernementales dans le cadre du pacte sino-sud-africain de lutte contre la cybercriminalité.

Acteurs locaux

- Développeur de solutions de sécurité pour différents secteurs IoT : Symantec, Radware, Kaspersky, Check Point.
- Distributeurs : Consol, Amiran Communications, WestCon Group.
- Sociétés de services de cybersécurité et de gestion de solutions hébergées ou locales : EOH, Dimension Data, BCX, Vodacom.
- Revendeurs et intégrateurs : Networks Unlimited, Dimension Data, Magix Security, BCX.
- Acteurs privés : IBM, HP, Cisco, Symantec, Alliances Securities Ltd.

Le positionnement de l'offre française

- Présence d'entreprises françaises effectuant des activités de cybersécurité et de confiance numérique : Thalès, Gemalto, Egis Project, Idemia…

ATOUTS DE L'OFFRE FRANÇAISE

- Une reconnaissance à l'international sur les produits et services
- Compréhension des enjeux et forte valeur ajoutée
- Label « France Cybersecurity » de l'offre française qui garantit la qualité des services et solutions par rapport à la réalité des besoins de protection actuels

Sources : SABRIC – Exposure Index – PWC « enquête sur la criminalité mondiale 2017 » – MarketsandMarkets report – Frost & Sullivan – Observatoire 2017 de la Confiance Numérique, Business France –xGartner – IBM Security – EC-Council, ItWeb, Cyber crime & cyber security trends in africa

CONFIANCE NUMÉRIQUE ET CYBERSÉCURITÉ EN AFRIQUE DU SUD

OPPORTUNITÉS POUR L'OFFRE FRANÇAISE

Les défaillances des entreprises sud-africaines dans la défense et l'identification des cyber attaques sont importantes :

- En 2017, l'Afrique du Sud a été marquée par la fuite de données la plus importante de son histoire : « Master deeds leak », touchant presque toute la population. Au total 60 M d'enregistrements furent divulgués : adresses, salaires mensuels et numéro de carte d'identité.
- Le secteur bancaire est particulièrement touché. D'après la SA Banking Risk Information Center, la cybercriminalité représente 55 % des pertes brutes du secteur.
- Aujourd'hui, les entreprises sud-africaines mettent en moyenne 150 jours pour identifier une cyber-attaque de leurs données et 45 jours pour la contrer.
- D'après une étude d'IBM, le coût moyen d'une cyber-attaque de données est de 2,3 M EUR en 2018, contre 1,8 M EUR en 2016, soit une augmentation de 26 % en 2 ans.

Protection des données:

- **La loi sur la protection des données personnelles** (PoPI Act), entrée en vigueur en Afrique du Sud en 2018, a incité les entreprises à repenser leur politique de protection des données. Les sociétés doivent appliquer de meilleures pratiques et mettre en place des outils de sécurisation de données pour garantir la conformité à cette nouvelle loi.
- **Internet des objets** - D'ici 2020, la technologie de l'Internet des objets (IoT) sera dans 95 % de l'électronique d'après Gartner. Ceci ouvre la possibilité de cyber-attaques avec des conséquences potentiellement graves.
- **Identification et biométrie** – Il existe des opportunités en lien avec les commandes publiques de cartes d'identité (smart IDcard, permis de conduire).
- **Solutions de sécurisation des paiements effectués par mobile** – Le fort développement des paiements NFC, sans-contact et des banques sur mobile, entraîne la nécessité d'une sécurisation plus profonde de ces nouveaux types de paiement.
- **Sécurisation des terminaux de paiement des banques**
- **Introduction de nouveaux types de cartes bancaires** – Les banques sud-africaines proposent de nouveaux types de cartes plus sécurisées (carte chip), mises en place par Europay, Visa et Mastercard.
- **Sécurisation des activités de e-government** – Le développement d'une administration sud-africaine digitale et les cyber-attaques persistantes des institutions gouvernementales nécessitent des solutions de sécurisation spécifiques.

SECTEURS PORTEURS

- **Sécurité du cloud :** L'adoption croissante des services cloud en Afrique du Sud pose la question de la sécurité liée à cette technologie.
- **Technologie de cybersécurité :** Pour rattraper leur retard, les sociétés sud-africaines vont augmenter leurs dépenses pour s'équiper en outils de protection des données notamment en chiffrement et en authentification.
- **Protection de l'appareil mobile :** À la suite des récentes attaques ransomwares et de l'adoption accrue de la mobilité et du BYOD (Bring Your Own Device) au sein des organisations, les entreprises chercheront à implémenter la sécurité mobile pour empêcher l'infiltration via des réseaux externes échappant à leur contrôle.
- **Formation et sensibilisation :** 2017 a vu un boom dans les attaques ransomware. La sensibilisation à la sécurité sera essentielle pour les stratégies organisationnelles de cybersécurité.

Sources : SABRIC – Exposure Index – PWC « enquête sur la criminalité mondiale 2017 » – MarketsandMarkets report – Frost & Sullivan – Observatoire 2017 de la Confiance Numérique, Business France –xGartner – IBM Security – EC-Council, ItWeb, Cyber crime & cyber security trends in africa

CONFIANCE NUMÉRIQUE ET CYBERSÉCURITÉ EN AFRIQUE DU SUD

CLÉS D'ACCÈS

Le profil des partenaires commerciaux / Approche commerciale à privilégier

- Toute entreprise européenne qui souhaite exporter ses produits en Afrique du Sud doit se rapprocher de l'autorité de régulation Independent Communications Authority of South Africa (ICASA).
- L'Afrique du Sud dispose d'un marché de distribution très mature avec une multitude d'acteurs. La meilleure solution pour une entreprise souhaitant commercialiser ses produits électroniques est de passer par un distributeur spécialisé. Lors de la sélection du distributeur il est important de vérifier qu'il détient une bonne note BEE (Black Economic Empowerment), notamment pour adresser le secteur public.
- Il est également envisageable d'engager des échanges avec des clients finaux. Malgré des ressources encore trop faibles, il existe une réelle compréhension de la nécessité d'améliorer les systèmes de cybersécurité, notamment portée par les obligations du Popi Act 2018.

La réglementation spécifique

Le gouvernement sud-africain a pris des mesures pour enrayer la cybercriminalité. Celles-ci se traduisent par la mise en place de législations spécifiques :

- Le « Cybercrime and Cybersecurity Bill » qui impose aux fournisseurs de services de communication de transmettre les informations collectées et qui définit les infractions en lien avec la cybercriminalité et les sanctions qui les accompagnent. Validé par l'assemblée nationale sud-africaine en novembre 2018, celui-ci devrait être voté après être passé par le Concile National des Provinces.
- L'existence d'une plateforme nationale permettant la collaboration entre les acteurs institutionnels et les entreprises spécialisées du secteur (www.cybersecurityhub.gov.za/).
- Le « Protection of Personal Information Act » (PoPI Act) de 2018 qui traduit une réelle prise de conscience et de sensibilisation de la population sud-africaine, jusqu'à aujourd'hui peu informée sur l'utilisation des données personnelles. Le PoPI Act prévoit pour les entreprises : l'identification des risques et la mise en place de mesures de sécurité pour la protection de leurs données. Il les contraint également à signaler les infractions et cyber-attaques sous peine d'une forte amende, ce qui n'était pas le cas jusqu'à présent.
- « L'Electronic Communication and Transaction Act » (ECTA) qui assure la facilitation et la réglementation des communications et transactions électroniques. Il prévoit le développement d'une e-stratégie nationale, promeut l'accès universel aux communications et transactions électroniques et utilisation, assure le développement des ressources humaines dans les transactions électroniques, prévient l'abus des systèmes d'information et encourage l'utilisation des services d'administration en ligne
- Les organismes de sensibilisation et prévention : SABRIC (prévention bancaire) et Council for Scientific and Industrial Research's Cybersecurity Awareness.

NIVEAU DE TAXATION

Accords internationaux :

- World Trade Organisation (WTO)
- Southern African Customs Union (SACU)

Entités régulatrices nationales :

- International Trade Commission of South Africa (ITAC)
- South African Revenus Service (SARS)
- South African Bureau of Standards (SABS)
- South African Reserve Bank (SARB)
- Financial Sector Conduct Authority (FSCA)
- National Credit Regulator (NCR)
- Financial Intelligence Centre (FIC)
- *South Africain Internet Retailing Association (SAIRA)*

Accord avec l'Union Européenne :

- 1999: Accord sur le Commerce, le Développement et la Coopération mis à jour en octobre 2015.

Sources : SABRIC – Exposure Index – PWC « enquête sur la criminalité mondiale 2017 » – MarketsandMarkets report – Frost & Sullivan – Observatoire 2017 de la Confiance Numérique, Business France –xGartner – IBM Security – EC-Council, ItWeb, Cyber crime & cyber security trends in africa

CONFIANCE NUMÉRIQUE ET CYBERSÉCURITÉ EN AFRIQUE DU SUD

POUR ALLER PLUS LOIN

Procurez-vous le Guide des affaires Business France en Afrique du Sud

Pour comprendre les spécificités commerciales de ce pays et vous aider à faire les bons choix : de l'information très opérationnelle assortie de conseils précieux. Commandez-le…

https://www.businessfrance.fr/export-s-informer-tous-les-guides-des-affaires

Retrouvez toutes les publications Business France sur Afrique du Sud en suivant ce lien :

https://www.businessfrance.fr/export-s-informer

LES ÉVÉNEMENTS À NE PAS MANQUER

Pour connaître les grands RDV sur le secteur Confiance Numérique et Cybersécurité :

https://www.businessfrance.fr/export-agenda

NOUS CONTACTER

AUGUSTA HOUSE – INANDA GREENS
BUSINESS PARK 54 WIERDA ROAD
WEST –
SANDTON 2196

Blandine AIGRON

Tél. : +27(0)11 303 7161
blandine.aigron@businessfrance.fr