LES ENTREPRISES AFRICAINES FACE À LA CYBERCRIMINALITÉ

Salon des BANQUES et des PME
BOBO DIOULASSO
8 AU 11
NOVEMBRE 2018

PYRAMID HACKERS

Hack before you get hacked

CYBERCRIME

Un cybercrime est une infraction pénale susceptible de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau.

Il s'agit donc d'une nouvelle forme de criminalité et de délinquance qui se distingue des formes traditionnelles en ce qu'elle se situe dans un espace virtuel, le «cyberespace».

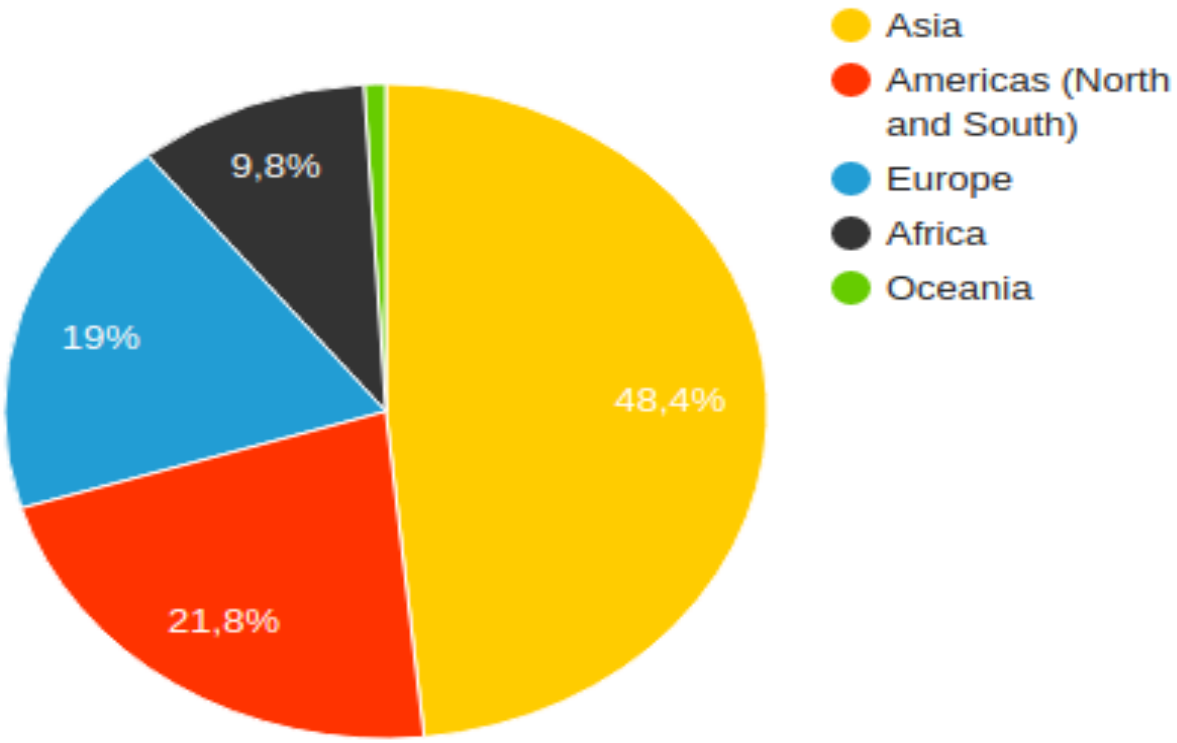
Depuis quelques années la démocratisation de l'accès à l'informatique et la globalisation des réseaux ont été des facteurs de développement du cybercrime.

POURQUOI NOUS PARLONS DE L'AFRIQUE ?

En Afrique, l'essor rapide de nouvelles technologies a entrainé le développement de nouveaux usages. Le nombre d'internautes a accru considérablement sans que ceux-ci ne soient accompagnés et sensibilisés au risques. Les statistiques des utilisateurs d'Internet de 2016 (live stats)

Pays	Population	Utilisateurs d'Internet	Pourcentages
Bénin	11.166.658	628.683	5,6%
Burkina Faso	18.633.725	1.894.498	10.2%
Cameroon	23.924.407	4.311.178	18%
Congo	4.740.992	357.471	7,5%
Côte d'ivoire	23.254.184	5.122.897	22%
Gambie	2.054.986	346.471	16,9%
Ghana	28.033.375	7.958.675	28,5%
Guinée	12.947.122	236.932	1,8%
Guinée-Bissau	1.888.249	66.984	3,5%
Liberia	4.615.222	395.063	8,6%
Mali	18.134.835	2.212.450	12.2%
Nigéria	186.987.563	86.219.965	46,1%
Sénégal	15.589.485	3.647.939	23,4%
Sierra Leone	6.592.102	160.188	2,4%
Togo	7.496.833	545.020	7,3%

L’Afrique sur le plan mondial



La cybercriminalité s’est considérablement développée ces dernières années.

Au **Nigeria**, la révolution technologique s’est accompagnée du développement d’une nouvelle criminalité. La méthode nigériane consiste à envoyer des emails à des adresses récupérées sur des listes de diffusion, en prétextant un gain à une loterie, ou un héritage débloqué à condition que l’interlocuteur débloque une certaine somme d’argent. Les hackers nigérians sont souvent jeunes et sans diplômes. Quant aux victimes, elles sont nombreuses et se trouvent principalement aux États-Unis

La cybercriminalité s’est considérablement développée ces dernières années.

La **Côte d’Ivoire** compte un nombre très important de cybercriminels. Cependant, il semblerait que les pratiques des cybercriminels ivoiriens restent à la marge par rapport à l’ampleur des méthodes nigérianes. Les brouteurs ivoiriens auraient en majorité entre 12 et 25 ans et proviendraient du Nigeria, ayant fui la répression contre les activités cybercriminelles. Ils agissent surtout depuis les cybercafés publics

La cybercriminalité s’est considérablement développée ces dernières années.

Deux méthodes sont fréquemment utilisées. La première consiste à rentrer en contact avec les victimes via un site de rencontres sur Internet. Après avoir établi une relation de confiance, les cyberesrocs réclament des sommes d’argent prétextant des frais médicaux ou bien des voyages pour leur rendre visite. Un autre type d’escroquerie consiste à recueillir de

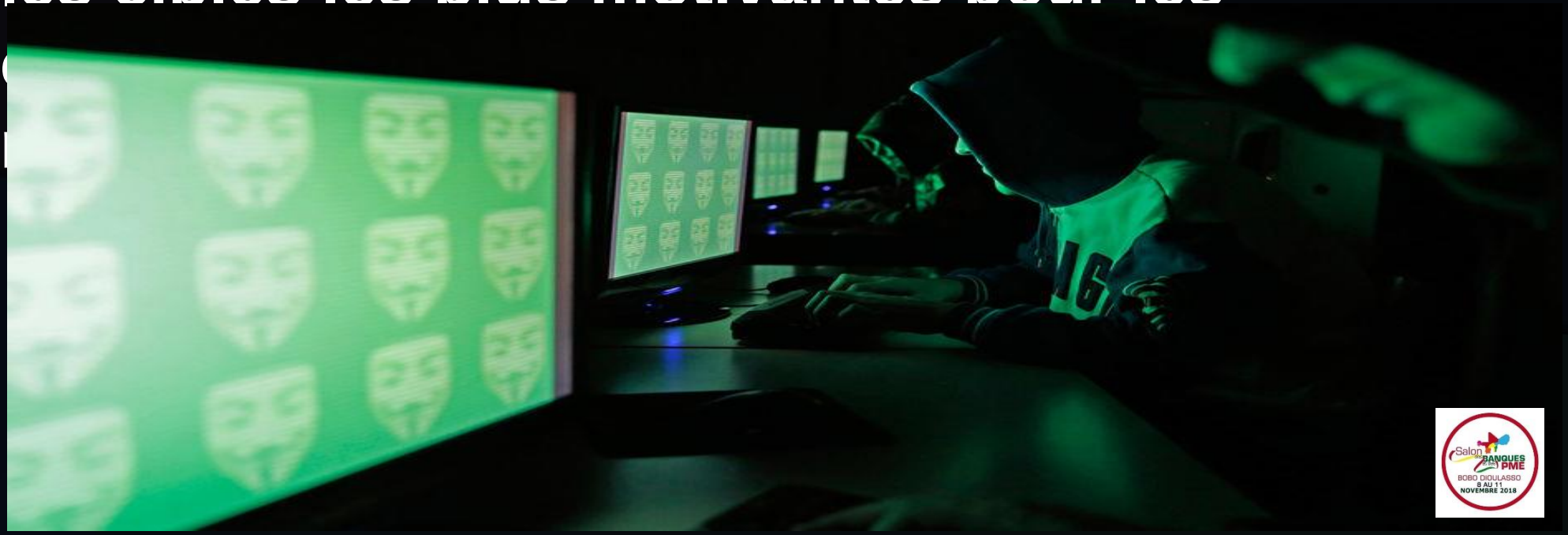
l’argent pour de faux projets humanitaires, de préservation de l’environnement ou de rénovations bâtiments religieux.

Dans un rapport publié par la société Trend Micro en 2012, « les cybercrimes en provenance de l’Afrique sont classés parmi les dix principales menaces qui pèseront sur les entreprises et le grand public dans les années à venir, car comme le cyberespace, la cyberescroquerie n’a pas de frontières.

Les Etats-Unis, inquiets des attaques venant d'Afrique, ont dressé un classement des dix premières sources mondiales de cyberarnaques : le Nigéria arrive en 3ème position, le Ghana en 7ème, et le Cameroun est 9ème du classement ».

POURQUOI NOUS PARLONS DES ENTREPRISES ?

Les entreprises sont les entités les plus victimes de la cybercriminalité. Elles constituent les cibles les plus motivantes pour les



Les attaques sont continuelles et massives. La cyberguerre se déroule sur nos écrans sans même que l'on soit au courant. Selon un rapport de FireEye, un spécialiste de la cybersécurité, **une entreprise met en moyenne deux cent cinq jours pour découvrir qu'elle a été attaquée**. Le temps de faire de nombreux dégâts, de récupérer de précieuses données et de revendre certaines informations sensibles. Personne n'est à l'abri.

LES CYBERHACKTIVISTES AFRICAINS

Le cyberhacktivisme cherche selon Patrick Chambet, à « réveiller la société et à l'éduquer sur certains sujets » . Quatre principaux groupes de cyberhacktivistes sont recensés en Afrique.

En 2013, le groupe **Anonymous Côte d'Ivoire** a attaqué les fournisseurs d'accès à internet du pays. L'attaque WAR ISP 225 réclamait aux fournisseurs la baisse des tarifs afin de démocratiser l'accès à internet à l'ensemble des ivoiriens.

En avril 2014, le serveur de l'Agence de l'Informatique de l'Etat a été attaqué par le collectif **Anonymous Sénégal**. Ainsi, 47 sites gouvernementaux (primature, ministère des finances, de l'éducation nationale, de l'agriculture…) ont été

La **Nigerian Cyber Army** attaque régulièrement les sites gouvernementaux, comme celui de l’Assemblée nationale du Nigeria. En mars 2015, le groupe a attaqué le site Internet de la Commission Electorale Nationale Indépendante

Quant à **Anonymous Africa**, ce groupe milite contre la corruption et pour la démocratie.

Ainsi, des groupes cyberhacktivistes sont bien présents en Afrique de l'Ouest mais sont globalement peu dangereux car ils disposent de faibles moyens et sont mal organisés. Les attaques menées sont principalement des attaques DDoS ou de défacement. Pour l'instant, ces groupes ne semblent pas en mesure de mener des attaques de grande ampleur.

Et comme vous le savez, plus on est connecté, plus on est cybervulnérable. Ce qui fait qu'aujourd'hui, la cybercriminalité constitue une réalité de politique criminelle en Afrique. C'est un phénomène qui se développe de façon exponentielle et qui est devenu un véritable fléau. L'exemple qu'on peut prendre pour montrer la réalité de la cybercriminalité dans nos pays, c'est l'escroquerie en ligne.

Particulièrement en Afrique de l'Ouest, cette forme de cybercriminalité a fini par prendre les proportions d'un véritable fléau.

C'est pour dire qu'aujourd'hui, en Afrique, il n'est pas possible de considérer la cybercriminalité comme un mythe ; c'est un phénomène extrêmement sérieux que non seulement les entreprises mais aussi les pouvoirs publics doivent prendre comme une préoccupation de sécurité nationale.

Maintenant, il faut comprendre que la cybercriminalité n’est pas un phénomène criminel sénégalais, congolais ou béninois ; ce n’est pas un phénomène criminel africain ; c’est un phénomène criminel mondial. C'est la raison pour laquelle la CEDEAO (Communauté Economique des Etats de l'Afrique de l'Ouest) s’est dotée d’une directive portant sur la cybercriminalité. L’Union africaine a adopté une convention africaine.

C’est la raison pour laquelle le Sénégal considère que le seul instrument international de lutte à notre disposition est la Convention de Budapest, une convention européenne, mais qui est ouverte à tous les Etats, y compris les pays non membres du conseil de l’Europe.

Ainsi, l'Afrique n'est pas à la marge de la cybercriminalité. Elle en est victime, et cela est principalement dû à la faible, voire à l'absence, de sécurité de ses infrastructures. Il est difficile d'évaluer l'impact de la cybercriminalité en Afrique. Cependant, pour les Etats d'Afrique de l'Ouest, le coût de la cybercriminalité n'est pas négligeable. Selon la dernière étude, Net losses : Estimating the Global Cost of Cybercrime, menée par McAfee, le cybercrime coûte 0,08 % du PIB par an au Nigeria. Une proportion proche de celle de la France, qui compte 0,11 % de son PIB affecté par la cybercriminalité.

L'Union Internationale des Télécommunications (UIT) soutient l'élaboration de cadres législatifs et de structures opérationnelles de lutte contre la cybercriminalité via, notamment, le développement de CERT (Computer Emergency Response Team). Aujourd'hui, 15 pays africains sur les 54 du continent disposent d'un CERT opérationnel, notamment le Bénin, le Burkina Faso, la Côte d'Ivoire, le Ghana et le Nigeria. En outre, la majorité des pays d'Afrique de l'Ouest (Bénin, Burkina Faso, Côte d'ivoire, Ghana, Nigeria, Togo, Sénégal) dispose désormais d'une législation en matière de cybercriminalité.

le **Burkina Faso** s'est doté d'un CERT en 2013 avec l'aide l'Union Internationale des Télécommunications. L'Autorité de Régulation des Communications Electroniques et des Postes (ARCEP) a par ailleurs élaboré un Plan National de Cybersécurité dont les trois principaux axes sont la réduction de la vulnérabilité du cyberespace, la gestion des incidents et le renforcement de la culture de cybersécurité. Outre ce CERT, le **Burkina Faso** s'est doté d'une Agence nationale de Sécurité des Systèmes d'Information en novembre 2013.

- Shodan

Solution :Pentesting et pourquoi Pentesting

Identifier les menaces auxquelles sont confrontés les actifs d'information d'une entreprise ou d'une organisation

Réduire les dépenses de l'entreprise en matière de sécurité informatique et améliorer le retour sur investissement de sécurité en identifiant et en corrigeant les vulnérabilités ou les faiblesses

Fournir une assurance avec une évaluation complète de la sécurité de l'entreprise ou de l'organisation, y compris la politique, la procédure, la conception et la mise en œuvre

Adopter les meilleures pratiques en conformité avec les réglementations légales et industrielles.

Pour tester et valider l'efficacité des protections et contrôles de sécurité

Pour changer ou mettre à niveau l'infrastructure existante de conception de logiciel, de matériel ou de réseau

Mettre l'accent sur les vulnérabilités de haute gravité et mettre l'accent sur les problèmes de sécurité au niveau de l'application pour les équipes de développement et la gestion

Fournir une approche globale des mesures de préparation qui peuvent être prises pour prévenir l'exploitation à venir

Évaluer l'efficacité des périphériques de sécurité réseau tels que les pare-feu, les routeurs et les serveurs Web.

Merci

Salon des BANQUES et des PME
BOBO DIOULASSO
8 AU 11
NOVEMBRE 2018