Mali Internet Next Generation Leaders
Cohorte 2

Internet Society
Chapitre Malien

La Cybersecurite : Etat Des Lieux Et Perspectives Au Mali

Superviseur :
Dr Yahaya COULIBALY
Auteurs :
Aïcha TRAORE

Rejoignez-nous

Tel : (+223) 63 46 67 38/ 76 13 02 38
Centre UVA/CISCO Sise à l'ENI
http://isoc.ml
info@isoc.ml
@isoc.ml

Mali Internet Next Generation Leaders
Présentation des Leaders

Je m'appelle Aïcha Traoré, étudiante en Master 1 Génie Informatique et Télécommunications (GIT), Spécialité : Réseau et Système Informatique à l'École Nationale d'Ingénieurs Abderhamane Baba Touré (ENI-ABT). Je suis détentrice d'une Licence en informatique et télécommunications obtenue à L'ENI-ABT.

J'ai toujours été attirée par les technologies, ce qui a orienté mes études vers les TIC et les réseaux. Je suis passionnée par les réseaux informatiques et approfondir mes connaissances là-dessus est une priorité. C'est pour cette raison que j'ai rejoint le Chapitre malien de l'Internet Society dont je suis membre il y a plus d'une année.

L'adhésion à cette association m'a ouvert la voie à plusieurs formations en ligne dont le DDCN, le NetOps1 et bien d'autres. J'ai également eu la chance de participer des séances de formation sur la Cybersécurité, l'Adressage IPv6 en présentiel. Ces formations m'ont beaucoup aidé et continuent de m' aider dans mon parcours.

J'ai eu la chance d'achever le programme « Mali internet Next Generation leaders cohorte 2 » ce qui m'a donné l'opportunité de travailler sur ce thème que j'aime tant.

Je suis fière de faire partie de cette belle organisation qui m'a offert tant d'opportunités. En plus des connaissances théorique et pratiques que j'ai acquises, j'aimerai développer des compétences pour contribuer à l'améliorations de la sécurité de l'Internet afin qu'il puisse être digne de confiance et complètement sécurisé.

Résumé :

La cybersécurité est l'ensemble des moyens qui visent à protéger les infrastructures numériques contre les cyberattaques. L'utilisation de l'internet, devenu aujourd'hui un outil presque indispensable dans les activités de tous les jours, nous expose aux risques de cyberattaques. En cas d'attaque les données privées peuvent être divulguées, c'est pourquoi la cybersécurité est nécessaire et importante. La cybersécurité est basée sur cinq (5) principes fondamentaux : la confidentialité, l'intégrité, l'authentification, la disponibilité et l'autorisation. Ne pas confondre la cybersécurité et la sécurité informatique qui a pour objectif de protéger les données contre toutes formes de menaces. Vu large utilisation du numérique au Mali, les citoyens ne sont pas à l'abri des cyberattaques. Pour minimiser les impacts négatifs de cyberattaques, les autorités maliennes ont élaboré et adopté plusieurs textes législatifs et règlementaires dans le domaine du numérique ; elles ont aussi créé des structures spécialisées dans ce domaine. Le but de cet article est d'offrir une synthèse des problématiques et des éléments de solution sur la cybersécurité des systèmes d'information au Mali. Il analyse les principales mesures techniques de la sécurité informatique et des réseaux permettant de réaliser des services et des fonctions de la sécurité informatique au Mali. Ces analyses ont montré que le Mali doit continuer à fournir plus d'effort dans le domaine de cybersécurité afin de créer un environnement numérique sûr et d'assurer une souveraineté numérique.

I. Introduction

Au fur et à mesure que le monde se transforme et se consolide, que les modes de travail évoluent, les frontières de la cybersécurité s'étendent. Avec chaque nouvel appareil connecté, découverte numérique ou processus automatisé, de nouvelles vulnérabilités et des préoccupations en cybersécurité émergent.

Avant d'évoquer pleinement la question de la cybersécurité en Afrique notamment au Mali, il convient au préalable de poser une série de constats sur le niveau de connectivité du continent africain. Rappelons tout d'abord que le taux d'accès à l'internet de la population du continent Africaine est de 43% depuis Décembre 2021 dont l'Afrique de l'ouest occupe 42% [2]. En outres, d'après DATAREPORTAL 2022, 29.9% de la population Malienne donc 6,33 millions ont accès à l'internet (612000 utilisateurs). Une nette progression de 10,7% année par année [3].

Pour autant, au-delà de ces insuffisances d'utilisation de l'internet par rapport aux autres pays dans le monde entier, il existe bel et bien un développement du numérique au Mali, caractérisé par bon nombre d'études comme porteur de croissance économique. De nombreux projets fondés sur l'utilisation du numérique vont en effet dans ce sens, facilitant une sortie de la pauvreté et un développement économique local. Pour accompagner ce mouvement, le Mali s'est dotés d'autorités chargées de piloter et promouvoir le développement des TIC au niveau national.

Le numérique au Mali est en plein essor depuis quelques années. Un exploit qui occasionne des menaces et des attaques de part et d'autre, et la question de la cybersécurité est toujours aussi préoccupante. La cybercriminalité, les attaques menées contre les réseaux informatiques par des pirates connectés et mal intentionnées sont de plus en plus fréquentes. Elles visent notamment les individus, les médias, les gouvernements, les entreprises. Face à cette menace croissante, la nécessité de renforcer les capacités en matière de cybersécurité est devenue une priorité pour le Mali.

Mais bon nombre de pays africains peinent à lutter efficacement contre la cybercriminalité, en raison notamment d'un déficit important de ressources. Ce manque touche autant la main d'œuvre qualifiée en cybersécurité, tant dans le secteur public que privé, que les formations dédiées et les ressources matérielles et technologiques adéquates. Malgré ce manque de ressources, le pays dispose par ailleurs d'une autorité dédiée à la cybersécurité, voire d'un CERT dont le rôle est de répondre aux incidents.

Le reste de cet article est organisé comme suit : la première section regroupe une étude détaillée sur les différents concepts de la cybersécurité à savoir : la définition, les principes fondamentaux, les langages informatiques à maîtriser. Dans la deuxième section, le concept général de cybersécurité ; Section 3 porte sur la description d'une étude complète de l'état des lieux de la cybersécurité au Mali, des cyberrisques, des différentes cybercriminalités et de ses impacts et des différentes initiatives qui ont été mise en place par les autorités pour renforcer la cybersécurité au Mali, ensuite, les textes réglementaires qui parle de la loi sur la cybercriminalité au Mali en vue d'améliorer la cybersécurité et les structures en charge de la cybersécurité au Mali sont élaborés dans la section 4. Et enfin, les sections 5 et 6 regroupent la conclusion générale ainsi que la perspective et des recommandations.

II. Le Concept de cybersécurité :

L'usage que nous faisons d'internet est quotidien, que ce soit dans le cadre privé ou professionnel. Parce que nous gérons quasiment l'ensemble de nos besoins sur les outils digitaux, et que ceux-ci sont connectés en permanence, les risques d'être pris par cible sont démultipliés. C'est pourquoi la cybersécurité est devenue l'enjeu de notre monde. La cybersécurité est très vaste et touche de nombreux domaines : de l'ordinateur de votre voiture au secret médical, de votre achat en ligne aux cryptages des communications satellites. En cas de cyberattaque, l'ensemble de vos données peuvent être récupérées.

La cybersécurité est très vaste et touche de nombreux domaines : de l'ordinateur de votre voiture au secret médical, de votre achat en ligne aux cryptages des communications satellites. En cas de cyberattaque, l'ensemble de vos données peuvent être récupérées.

Le but de la cybersécurité est de mettre en place une sécurité résiliente permettant aux individus, aux gouvernements, aux entreprises de protéger l'intégrité de leur activité contre les menaces et les imprévus.

1. Définition de Cybersécurité

La cybersécurité désigne l'ensemble des mesures de sécurisation de vos systèmes informatiques et de vos appareils. La cybersécurité englobe tous les moyens qui permettent d'assurer la protection et l'intégrité des données, sensibles ou non, au sein d'une infrastructure numérique. En d'autre termes, elle repose sur un ensemble de précautions matérielles et conceptuelles pour éviter l'espionnage. Mais aussi, l'usurpation d'identité et l'exploitation des informations volées. C'est une spécialité au sein des métiers des systèmes d'information. Une bonne stratégie de cybersécurité peut protéger les données sensible et confidentielle. Les langages informatiques à maîtriser pour un meilleur développement de cybersécurité sont entre autres : Python : le langage incontournable y compris dans la cybersécurité, JavaScript : un langage utilisé dans de nombreux attaques et SQL pour prévenir les attaques sur les bases de données.

2. Les principes fondamentaux de la cybersécurité

La cybersécurité se base sur 5 notions à savoir :

a. La confidentialité

La confidentialité garantie que les informations qui sont transmises entre un émetteur et un destinataire ne peuvent être lues que par l'émetteur et le destinataire. L'émetteur et le destinataire peuvent être des êtres humains ou des machines.

Afin de garantir la confidentialité, il est nécessaire de crypter l'information. C'est donc pour cela que le protocole Telnet a cédé sa place à SSH, que HTTP a cédé sa place à HTTPS, et que les serveurs de mails utilisent TLS pour crypter le flux SMTP.

b. L'intégrité

L'intégrité garantie que les informations qui sont transmises entre un émetteur et un destinataire ne peuvent pas être altérées.

c. La disponibilité

La disponibilité c'est le fait de pouvoir toujours accéder à ses propres informations, même si ces informations sont stockées ailleurs (c'est le fait de garantir l'accès aux ressources nécessaires).

d. Authentification

L'authentification consiste à vérifier votre identité. Elle s'applique aussi bien aux personnes qu'aux machines.

Une authentification peut être validée par un tiers, comme par exemple un serveur d'authentification ou une autorité tierce.

e. Autorisation

Il s'agit de définir les droits d'accès.

3. Différences entre Cybersécurité et Sécurité informatique

Bien que les termes de cybersécurité et de sécurité des systèmes d'information (SI) soient souvent utilisés de manière interchangeable, ils ne couvrent pas exactement la même réalité car chacun correspond à différents types de sécurité. Les termes de sécurité informatique et de cybersécurité sont aussi souvent confondus.

La cybersécurité vise à protéger les données, les sources de stockage, les appareils etc contre les attaques dans le cyberespace en revanche, la sécurité informatique a pour objectif de protéger les données de toute forme de menace, qu'elle soit analogique ou numérique.

III. État des Lieux de la Cybersécurité au Mali

Depuis quelques années, le Mali a connu une évolution significative en matière de cybersécurité. Alors que le pays se tourne vers une économie numérique en plein essor, de nouveaux défis et menaces sont apparus, mettant en évidence la nécessité d'une vigilance accrue pour protéger les infrastructures, les données sensibles et les citoyens.

Les cyberattaques au Mali se sont diversifiées et complexifiées au fil du temps. Des groupes de cybercriminels bien organisés et sophistiqués ont émergé, ciblant des secteurs clés tels que les institutions financières, les entreprises énergétiques, des gouvernements et des particuliers. Les pertes financières et la dégradation de la confiance des utilisateurs ont un impact direct sur le développement économique de la région, créant un défi majeur pour les gouvernements et les acteurs de la cybersécurité. Les ransomwares, les attaques par hameçonnage et les infiltrations de réseaux sont devenus monnaie courante, posant des problèmes graves en matière de sécurité et de stabilité économique. Face à cette menace croissante, la nécessité d'améliorer la cybersécurité est devenue une priorité pour le Mali. Des efforts significatifs ont été déployés pour former des experts en sécurité informatique, sensibiliser le public aux bonnes pratiques de sécurité et développer des mécanismes de réponse aux incidents. Des agences spécialisées ont été créées, des lois sur la cybersécurité ont été promulguées et des partenariats public-privé ont été établis pour renforcer la résilience face aux menaces. Cependant, il reste encore beaucoup à faire pour combler les écarts en matière de compétences et de ressources nécessaires pour faire face à cette évolution rapide du paysage de la cybersécurité. Les gouvernements, les organismes de règlementation et les entreprises doivent partager leurs connaissances, leurs bonnes pratiques et leurs ressources pour lutter efficacement contre les cybercriminels. La collaboration régionale est essentielle pour faire face aux défis complexes de la cybersécurité en Afrique de l'Ouest.

Les pays de la région ont compris qu'aucun État ne peut relever seul ces défis. C'est dans cette perspective que l'Union Africaine mise en place une convention sur la cybersécurité et la Protection des données à caractère personnel. Une nécessité urgente pour renforcer la cybersécurité et la cyberdéfense à tous les niveaux, des gouvernements aux entreprises et aux citoyens. Cette collaboration favorise une réponse plus efficace et cohérente aux menaces qui transcendent les frontières nationales [10].

Au Mali, les cas de cyberattaques augmentent de jour en jour. Les acteurs malveillants exploitent les vulnérabilités dans les systèmes informatiques des entreprises et des instituts financiers pour accéder à des informations sensibles, voler des données financières et perturber les opérations. Aucune plateforme n'est épargnée de ces attaques y compris les banques, les institutions de l'État. En effet en Février 2023, la Bank of Africa au Mali a été victime d'un piratage, c'est l'un des plus importants piratages subis par une banque Africain. Des millions de documents volés, contenant les données personnelles de clients, des informations sur les comptes. [14].

Confronté à l'augmentation de l'utilisation malveillante des réseaux sociaux, les autorités du Mali ont pris conscience de l'importance de la cybersécurité et des initiatives ont été mise en place pour renforcer la protection des systèmes d'information. Ces efforts témoignent la volonté affichée des autorités de garantir un environnement numérique sûr et sécurisé.

IV. Textes Règlementaires sur la cybersécurité au Mali

Le 5 décembre 2019, le président du Mali a promulgué la loi n° 2019-056 portant Répression de la Cybercriminalité afin de renforcer la cybersécurité au Mali [9].

La nouvelle loi s'applique à « toute infraction commise au moyen des technologies de l'information et de la communication (TIC) en tout ou partie sur le territoire de la République du Mali, toute infraction commise dans le cyberespace et dont les effets se produisent sur le territoire national ».

Les articles 20 et 21 de la nouvelle loi punissent les menaces et les insultes faites par le biais d'un système d'information, avec des sanctions allant de six mois à 10 ans d'emprisonnement, et une amende de 1 000 000 à 10 000 000 CFA (1 680 à 16 800 USD), ou les deux. De plus, les articles 55 et 56 condamnent la « diffusion publique » de « tous imprimés, tous écrits, dessins, affiches, gravures, peintures, photographies, films ou clichés, matrices ou reproductions photographiques, emblèmes, tous objets ou images contraires aux bonnes mœurs. » Les sanctions correspondantes vont de six mois à sept ans d'emprisonnement, une amende de 500 000 à 10 000 000 CFA (840 à 16 800 USD), ou les deux.

La loi est bien orientée pour garantir une utilisation sûre et sécurisée des TIC au Mali. Elle entre cependant en vigueur dans un contexte fragile. En outre, la loi impose une lourde charge aux intermédiaires de télécommunications pour suivre et surveiller l'activité du réseau.

V. Structures en charge de Cybersécurité au Mali :

Les Structures qui sont en charge de cybersécurité au Mali sont :

- L'Autorité Malienne de Régulation des Télécommunications/TIC et des Postes. Pour plus d'information, consulter le site de l'AMRTP [12] ;

- Le Ministère en charge de l'économie numérique à travers L'Agence des Technologies de l'Information et de la communication ainsi que le Service de Certification et de la Signature Électronique. Pour plus d'information, consulter le site de l'AGETIC [13].

VI. Conclusion

Nous pouvons dire que la cybersécurité joue un rôle crucial pour se tenir à distance des menaces et des personnes malveillantes. En effet, la mise en œuvre d'un solide dispositif de cybersécurité peut donc s'avérer être un véritable défi auquel les états et les communautés doivent faire face pour garantir la sécurité des utilisateurs et des ressources pour maintenir la confiance dans le cyberspace.

Aujourd'hui, le Mali a pris conscience de l'importance cruciale de la cybersécurité et en faire l'une de ces plus grandes priorités. Les Autorités ont mise en place des initiatives pour renforcer la protection des systèmes d'information afin de garantir un environnement numérique sûr et sécurisé et de préserver la confiance des investisseurs et des utilisateurs.

En perspective, le Mali prévoit d'instaurer un Pôle judiciaire national spécialisé chargé de plusieurs missions. Le Pôle devra principalement déterminés les modalités de poursuite, d'instruction et de jugement des cyber-malfaiteurs [15].

Au regard de ce qui précède, il essential que le gouvernement fournisse plus d'effort en vue d'assurer un environnement numérique fiable et sûr. A cet effet, nous recommandons entre autres :

- Créer et opérationnaliser un CERT / CSIRT national ; Un CERT (Computer Emergency Réponse Team, en français : l'équipe de réponse à l'urgence informatique ;
- Joindre le CERT régional de l'OCI (Organisation de Coopération Islamique) appelé OIC-CERT ; L'OCI-CERT s'engage à publier des articles provenant d'une grande variété de discipline de cybersécurité, allant du domaine technique, tel que l'ingénierie, l'informatique ou les systèmes d'informations, aux descriptions non techniques de la technologie et de la gestion du point de vue. Des fondamentaux et des applications de la cybersécurité.
- Investir dans l'éducation et la formation en cybersécurité ;
- Sensibiliser les populations aux bonnes pratiques des outils numériques ;
- Application stricte de la loi sur la cybercriminalité qui vise à garantir la sécurité au Mali.

ANNEXE

Table 1 :Quelques indices de Cybercriminalité au Mali [5]

INDICATEURS GÉNÉRAUX DE LA CYBERSÉCURITÉ	RÉPONSE ET TAUX DE PRÉSENCE	PRÉCISIONS SUR INDICATEURS
Indice de Développement des Nouvelles technologies	 22%	L'indice de développement des technologies de l'information et de la communication est un indice synthétique publié par l'Union internationale des télécommunications des Nations unies sur la base d'indicateurs convenus au niveau international.
Analyse et information sur les cybermenaces au sein du pays		Avec le CSIRT Mali.
Formation dans le domaine de la cybersécurité : Licence, Master ou Doctorat		Avec Higher Institute of Applied Technologies
Association couvrant la thématique de la cybersécurité		Des associations comme le Chapitre Malien ISOC, Association des Jeunes Informaticiens du Mali (AJIM) FGI MALI
Participation aux actions de coopération internationale pour la lutte contre le cybercrimes - Contribution		Le gouvernement est régulièrement représenté dans un format de coopération consacré à la cybersécurité internationale (par exemple le FIRST). » Le Mali est membre de ITU-IMPACT
Existence et mise en place d'outils pour la protection des services numériques : institutions et organismes de suivi de l'application, de protection des donnée		Loi n° 2013-015 du 21 mai 2013 Portant protection des données à caractère personnel en République du Mali
Existence d'une loi sur la protection des données et acteurs		Article 31. L'Autorité de protection des données personnelles a pour mission de veiller à la protection des données personnelles et de participer à la régulation du secteur. » Loi n° 2013-015 du 21 mai 2013 Portant protection des données à caractère personnel en République du Mali.
Existence d'un CERT ou CSIRT au niveau du pays		Le CSIRT MALI. Plus de détail sur le site officiel.

Fonctionnement des services de répression du cybercrimes au sein du pays		La section Cybercriminalité de la Brigade d'Investigation Judiciaire (BIJ) du MALI est chargé de la répression
Lutte contre la cybercriminalité Investigation Numérique		Les cybercrimes sont définis par la législation à l'article 264-271 » loi N°2019-056 du 05 décembre 2019 portant répression de la cybercriminalité. » Participation du pays au projet OCWAR-C

[1] : Deloitte_Etude-de-la-Maturité-CyberSécurité-en-Afrique-Francophone_2021-VF.pdf2
[2] : https://www.aa.com.tr/fr/afrique/afrique-46-de-la-..
[3] :https://www.spiritbko.com/chiffres-du-mois-reseaux-sociaux-au-mali-en-2022/#:~:text=En%20outres%2C%20
[4] :https://www.riskinsight-wavestone.com/2016/05/cybersecurite-en-afrique-etat-lieux-perspectives/
[5] : Indice_Cybersécurité_Mali.pdf
[6] : Feuilletage_138.pdf Solange Ghernaouti
[7] :https://www.onelogin.com/fr-fr/learn/what-is-cyber-security#:~:text=La%20cybers%C3%A9curit%C3%A9%20est%20un%20%C2%AB%20sous,Internet%20ou%20survenant%20via%20Internet.
[8] :https://www.securiteinfo.com/conseils-cybersecurite/les-5-principes-fondamentaux-cybersecurite-dican.shtml#:~:text=La%20cybers%C3%A9curit%C3%A9%20se%20base%20sur,principes%20forment%20l'acronyme%20DICAN.
[9] : https://cipesa.org/2020/02/la-nouvelle-loi-du-mali-sur-la-cybercriminalite-potentiellement-problematique-pour-les-droits-numeriques/#:~:text=Les%20articles%2020%20et%2021,USD)%2C%20ou%20les%20deux.
[10] : https://en.cybersecuritymag.africa/cybersecurite-afrique-de-louest-evolution-complexe-defis-croissants Par Koffi ACAKPO
[11] : https://www.agenceecofin.com/securite/2203-45913-mali-un-centre-de-gestion-des-cybermenaces-en-gestation
[12] : https://amrtp.ml/appel-a-manifestations-dinteret-pour-lelaboration-dune-strategie-nationale-de-cybersecurite/
[13] https://agetic.gouv.ml/
[14] https://www.jeuneafrique.com/1423263/economie-entreprises/cyberattaque-de-bank-of-africa-mali-les-dessous-dun-hacking-inedit/#:~:text=Le%2011%20f%C3%A9vrier%2C%20les%20hackers,dans%20dix%2Dneuf%20pays%20du
[15] :https://fr-sputniknews-africa.cdn.ampproject.org/v/s/fr.sputniknews.africa/amp/20221112/le-gouvernement-malien-cree-un-dispositif-special-pour-lutter-contre-la-cybercriminalite-1056798196.html?amp_gsa=1&amp_js_v=a9&usqp=mq331AQIUAKwASCAAgM%3D#ampshare=https%3A%2F%2Ffr.sputniknews.africa%2F20221112%2Fle-gouvernement-malien-cree-un-dispositif-special-pour-lutter-contre-la-cybercriminalite-1056798196.html

Internet Society
Chapitre Malien

"Mali Internet Next Generation Leaders" est un programme de formation des futurs leaders de l'Internet au Mali qui est à sa deuxième cohorte. Il est soutenu par la fondation Internet Society et l'appui de l'Internet Society au niveau global, du Complexe Numérique de Bamako et de l'Agence des Technologies de l'Information et de la Communication.

Internet Society

Internet Society Foundation

ATIC

CNB
COMPLEXE NUMERIQUE DE BAMAKO