L'authentification multifacteurs comme mesure de sécurité informatique face aux cybermenaces : Une approche à adopter par les pays et entreprises africains

Boyoko Georges Boyoko, Agneau Zunguluka Kahenga

▶ **To cite this version:**

Boyoko Georges Boyoko, Agneau Zunguluka Kahenga. L'authentification multifacteurs comme mesure de sécurité informatique face aux cybermenaces : Une approche à adopter par les pays et entreprises africains. Journal of Cybersecurity and Privacy, A paraître. hal-04492199

HAL Id: hal-04492199
https://hal.science/hal-04492199

Submitted on 20 Mar 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Copyright

L'authentification multifacteurs comme mesure de sécurité informatique face aux cybermenaces : Une approche à adopter par les pays et entreprises africains

Georges BOYOKO WANDJOLI

Enseignant – Chercheur

Assistant de 1er Mandat à l'Institut Supérieur de Développement Rural

(**ISDR/Mbandaka**)

Domaine d'étude : Sécurité Informatique

Contact : +243 852 142 546 ; +243 814 339 796

E-mail : georgesboyoko9@gmail.com

Website : https://www.geonasoft.sitw.fr

&

KAHENGA ZUNGULUKA Agneau

Enseignant – Chercheur

Assistant de 1er Mandat à l'Institut Supérieur Pédagogique de Mbandaka

(ISP/Mbandaka)

Domaine d'étude : Réseaux et Sécurité Informatique

Résumé

Depuis que le monde numérique a envahi la planète terre et depuis que l'homme est en mesure de communiquer en distance avec son prochain de l'autre bout du monde, l'homme devient vulnérable.
Depuis que les entreprises cherchent à augmenter sa productivité et des nouveaux clients potentiels en ligne, et de loger toutes les informations relatives de l'entreprise y compris de ces agents, aux serveurs, elle devient vulnérable.
Dans le continent africain, la notion de sécurité informatique pose souvent problème voire même sa vulgarisation n'est pas encore rependue au sein de quelques pays et la plupart de ces pays la fréquence de menaces informatiques est en plein essor. La population africaine souffre de problème de l'extorsion numérique, escroqueries en ligne et tant d'autres cybermenaces chaque jour.
Chaque année, près de 90% des entreprises africaines sont menace par les cyberattaques car ces entreprises la sécurité informatique n'est pas vraiment au rendez-vous.
Peu des agents des entreprises africaines, écoles, université et les gouvernements sont sensibiliser dans le domaine de cyberattaque ou cybermenace. Ce qui ouvre la voie aux cyberattaques de menacer et escroquer les gens tout en volant les données des utilisateurs. Il est à conseiller que la protection des données des utilisateurs est primordiale prioritaire pour une entreprise et l'authentification multi-facteurs constitue l'un des moyens les plus sûrs de vérifier l'identité des clients, des agents lorsqu'ils se connecte dans un système d'une entreprise ou un site web. Dans cet article, nous allons vous présenter l'importance de l'authentification à multifacteurs pour sécuriser l'accès à distance et renforcer la sécurité et diminuer les risques des attaques et les vols des informations des utilisateurs dans un système d'information d'une entreprise.

Mots clés : Authentification – Cybermenace – Sécurité – entreprise – Afrique

Abstract

Since the digital world has invaded planet Earth and since man is able to communicate remotely with his neighbor from the other end of the world, man becomes vulnerable. Since companies seek to increase their productivity and potential new customers online, and to house all the information related to the company including its agents, to servers, it becomes vulnerable.

In the African continent, the concept of computer security often poses a problem, even its popularization is not yet widespread in some countries and in most of these countries the frequency of computer threats is booming. The African population suffers from problems of digital extortion, online scams, and many other cyber threats every day.

Each year, nearly 90% of African companies are threatened by cyber attacks because these companies' computer security is not really up to date. Few agents of African companies, schools, universities, and governments are aware in the field of cyber attack or cyber threat. This opens the way for cyber attacks to threaten and scam people while stealing user data. It is advisable that the protection of user data is a top priority for a company and multi-factor authentication is one of the safest ways to verify the identity of customers, agents when they connect to a company's system or a website. In this article, we will present the importance of multi-factor authentication to secure remote access and strengthen security and reduce the risks of attacks and theft of user information in a company's information system.

Keywords : Authentication - Cyber threat - Security - Company - Africa

Introduction

Dans un monde de plus en plus numérisé, la sécurité des systèmes d'information est devenue une préoccupation majeure pour les pays et les entreprises. L'authentification multifacteurs (FMA) est une méthode de confirmation de l'identité d'un utilisateur en utilisant plusieurs preuves indépendantes. Elle joue un rôle essentiel dans la protection des systèmes d'information contre les cybermenaces. En effet, la FMA renforce la sécurité en exigeant des utilisateurs qu'ils fournissent deux ou plusieurs formes de preuves, ou facteurs, pour vérifier leur identité. Ces facteurs peuvent inclure quelque chose qu'ils connaissent (comme un mot de passe), quelque chose qu'ils ont (comme une carte à puce), et quelque chose qu'ils sont (comme une empreinte digitale).

En Afrique, la perspective de la FMA serait prometteuse si les pays et entreprises africains commencent à adopter la FMA comme mesure de sécurité informatique pour se protéger contre les cybermenaces. Cette adoption est motivée par une prise de conscience croissante de l'importance de la sécurité informatique et par la volonté de se conformer aux normes internationales en

matière de cybersécurité. Cependant, malgré ces progrès, de nombreux défis restent à relever, notamment en ce qui concerne l'infrastructure technologique, la sensibilisation et l'éducation du public, et la mise en œuvre de politiques de cybersécurité efficaces.

D'un point de vue économique, l'authentification multifacteurs (FMA) peut être considérée comme un investissement essentiel pour les entreprises et les pays. En effet, les coûts associés à la mise en œuvre de la FMA sont souvent compensés par les économies réalisées grâce à la prévention des cyberattaques, qui peuvent entraîner des pertes financières importantes. De plus, la FMA peut contribuer à renforcer la confiance des clients et des partenaires commerciaux, ce qui peut avoir un impact positif sur la réputation et la compétitivité d'une entreprise.

Dans cet article, nous expliquons comment la FMA peut renforcer la sécurité dans un système de gestion d'information d'une entreprise tout en renforçant le (la) :

- **Sécurité des comptes des utilisateurs**
- **Protection contre le phishing et autres attaques**
- **Conformité aux réglementations et**
- **Confiance des utilisateurs**

1. Les principales cybermenaces en Afrique

Selon le rapport d'INTERPOL[1] en 2021 sur la cybermenace il a recensé les menaces les plus importantes existant en Afrique à partir d'éléments communiqués par les pays membres de l'Organisation et de données fournies par des partenaires du secteur privé.

Les cinq grandes menaces de cybermenaces en Afrique recensées lors de notre recherche sont les suivantes :

- Les **escroqueries en ligne** : Les escroqueries en ligne représentent la cybermenace la plus fréquemment signalée et la plus pressante en

[1] INTERPOL, qui signifie **Organisation internationale de police criminelle**, est une organisation internationale qui a été créée en 1923 pour promouvoir la coopération policière internationale[1]. Elle compte **194 pays membres** et son siège est à Lyon, en France. INTERPOL gère **19 bases de données policières** contenant des informations sur les infractions et les criminels, auxquelles les pays membres peuvent accéder en temps réel. Elle permet aux polices de ses pays membres de travailler ensemble pour lutter contre la criminalité internationale. Elle diffuse des **notices rouges**, qui sont des documents d'alerte permettant de localiser et d'arrêter des criminels recherchés dans le monde. INTERPOL joue un rôle crucial dans la lutte contre le crime international, y compris le cybercrime, les menaces chimiques et d'autres formes de criminalité.

Afrique. Cette menace cible et exploite les peurs, les insécurités et les vulnérabilités des victimes en recourant à l'hameçonnage, aux campagnes d'envoi massif de message électroniques et à l'ingénierie sociale ;

- L'**extorsion numérique** : Cette menace a aussi été identifiée comme l'une des cybermenaces majeures dans la région africaine. L'extorsion en ligne cible les particuliers soit en alléguant de la détention d'images sexuellement compromettantes, soit par des campagnes de chantage direct.
- Les **escroqueries aux faux ordres de virement** : Ce type de menace est presque omniprésente aux entreprises où les malfaiteurs piratent les systèmes de messagerie électronique de sociétés africaines afin d'obtenir des informations sur leurs systèmes de paiement puis trompent des salariés pour les inciter à virer de l'argent sur un compte bancaire leur appartenant en guise d'exemple en République Démocratique du Congo, les entreprises suivantes sont souvent été attaquée : La CENI, EcoBank, Bralima, Vodacom, Orange, Airtel, Africell… ;
- Les **rançongiciels** : La menace des rançongiciel se répand sur le continent africain. Au cours de la seule année 2020, plus de 61% des entreprises de la région auraient subi des attaques par les rançongiciels.
  (**Lumu.IO, 2020 Ransomware Flashcard, consultable à l'adresse : https://lumu.io/ressources/2020-ransomware-flashcard/)**
- Dans ce type de menace, les cybermalfaiteurs peuvent aussi bloquent les systèmes informatiques des hôpitaux, Banques et d'institutions publiques et exigent de l'argent pour rétablir leur fonctionnement ;
    - **(Institut d'études de sécurité, Africa can 't Risk a major maritime cyber attack. Reva, D., 28 octobre 2020. Consultable à l'adresse https://www.issafrica.org/iss-today/africa-cant-risk-a-major-maritime-cyber-attack)**
- Les **botnets** : Les botnets sont des réseaux de machine infectées utilisées pour automatiser des campagnes à grande échelle comme des attaques par déni de service distribué (DDoS[2]).

[2] DDoS signifie "Distributed Denial of Service" en anglais, ce qui se traduit en français par "Attaque par déni de service distribué". C'est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser.

2. L'authentification à doubles facteurs quid ?

L'authentification est un mécanisme faisant intervenir deux entités distinctes : Un Prouveur et un Vérifieur comme illustré par la figure 1.

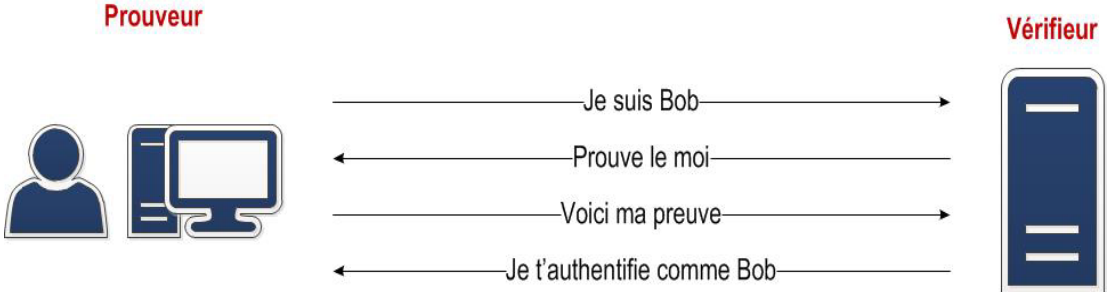

FIGURE 1 – Représentation générique d'une authentification à doubles facteurs
Source : Lumu.IO, 2020 Ransomware Flashcard

- **Un prouveur** est un utilisateur du système d'information cherchant à s'authentifier.
- **Le vérifieur** est quant à lui classiquement un serveur du système d'information qui a la charge de vérifier l'identité d'un utilisateur.

Une étape préalable à l'authentification est l'étape de l'**enregistrement**. Cette étape consiste à enregistrer un prouveur (son identité, son moyen d'authentification, etc.) auprès d'un vérifieur.
Cela correspond par exemple à la création d'un compte sur un site Web. L'authentification est précédée par une phase d'**identification** (parfois implicite) qui consiste, pour le prouveur, à annoncer son identité sans prouver cette dernière. Par exemple, il peut s'agir d'un nom d'utilisateur à renseigner.

(GUIDE ANSSI version 2.0, 08/10/2021 recommandations relatives à l'authentification multifacteurs et aux mots de passe).

3. Les avantages de l'authentification à doubles facteurs

Selon une recherche menée par Microsoft, **99,9% des cyber-attaques peuvent être bloquées** à l'aide de l'authentification multi-facteurs.
(**Matt Bromiley, Bye Password : New Ways to Authenticate, July 2019**).

Dans une attaque DDoS, plusieurs systèmes, généralement infectés par un cheval de Troie, ciblent un système particulier, provoquant une attaque de déni de service. Ces attaques utilisent plusieurs serveurs et connexions Internet pour inonder la ressource ciblée.
L'attaque DDoS peut bloquer un serveur de fichiers, rendre impossible l'accès à un serveur web ou empêcher la distribution de courrier dans une entreprise. L'attaquant n'a pas forcément besoin de matériel sophistiqué. Ainsi, certaines attaques DDoS peuvent être exécutées avec des ressources limitées contre un réseau de taille plus importante et plus moderne.
Ces attaques sont souvent réalisées à l'aide d'un "réseau zombie" d'ordinateurs infectés. Le cybercriminel contrôle les actions de chacun des ordinateurs infectés du réseau zombie, ce qui permet à l'attaque d'avoir un impact significatif sur les ressources Web de la victime.

Les pays et entreprises africains doivent adopter le mode de sécurité de l'authentification multifacteurs dans leurs systèmes informatiques pour les raisons ci-après :

- **Diminution des fraudes et vols d'identité :** Avec l'authentification multifacteurs, se procurer le mot de passe de quelqu'un ne suffit plus pour accéder à ses données sensibles. L'authentification multifacteurs complique considérablement les tentatives de piratage et réduit la fraude ainsi que le vol d'identité en utilisant des mesures de sécurité additionnelles inaccessibles pour les personnes mal intentionnées.
- **Gain de confiance de la part des clients** : Les clients aiment savoir leurs données en sécurité. Ces derniers favorisent les entreprises qui prennent la protection de leurs données au sérieux, même si les étapes de vérification additionnelles semblent parfois inutilement contraignantes.
- **Conformité** : Certaines industries doivent se plier à des **mesures de conformité spécifiques**, comme le Règlement Général sur la Protection des Données (RGPD)[3]. Les entités sanitaires, financières et gouvernementales exigent notamment que les entreprises suivent des directives strictes qui protègent les droits des consommateurs et réduisent les risques. Les exigences en matière de sécurité doivent ainsi s'aligner avec les besoins uniques des entreprises.
- **Réduction des coûts d'exploitation** : Informer les clients des activités suspectes sur leurs comptes est onéreux et chronophage. L'authentification multi-facteurs réduit les risques de fraude, soulage le service client et permet aux agents de se concentrer sur des problèmes plus complexes. Sa mise en œuvre de peut entraîner des coûts initiaux élevés, mais le retour sur investissement est assuré sur le long terme.
- **Transactions mobiles sécurisées sur tous les canaux** : Depuis le monde numérique a connu son développement, les gens utilisent de plus en plus

[3] Le RGPD, ou Règlement Général sur la Protection des Données, est un texte réglementaire européen qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union européenne (UE). Il est entré en application le 25 mai 2018.
Le RGPD a été conçu autour de trois objectifs :

- Renforcer les droits des personnes.
- Responsabiliser les acteurs traitant des données.
- Crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données.

Il s'adresse à toute structure privée ou publique effectuant de la collecte et/ou du traitement de données, quel que soit son secteur d'activité et sa taille. Le règlement s'applique à tous les organismes établis sur le territoire de l'Union européenne, mais aussi à tout organisme implanté hors de l'UE mais dont l'activité cible directement des résidents européens.
Il est important de noter que le RGPD concerne également les sous-traitants qui traiteraient ou collecteraient des données personnelles pour le compte d'une autre entité.

leurs appareils mobiles pour faire des transactions en ligne. Les **applications de messagerie OTT**[4] telles que WhatsApp et Facebook Messenger permettent aux consommateurs d'effectuer des achats directement depuis leurs canaux préférés. L'authentification multi-facteurs est alors employée afin d'augmenter le niveau de sécurité et de protéger les transactions contre la fraude.

- **Diminution de la fatigue des mots de passe** : Selon le gestionnaire de mots de passe NordPass[5], l'utilisateur moyen possède entre 70 et 80 mots de passe différents. Avec autant d'informations à retenir, nombreuses sont les personnes à utiliser un seul mot de passe pour tous leurs comptes ou à créer des identifiants trop simples. Ces deux techniques les rendent hélas vulnérables face aux attaques informatiques**.** L'ajout de l'authentification multi-facteurs soulage la fatigue des mots de passe et ajoute un niveau de sécurité supplémentaire pour éviter le piratage des mots de passe simples et répétitifs.
- **Simplification des connexions** : La méthode de connexion à authentification unique **(SSO)** permet de simplifier l'authentification multi-facteurs. Celle-ci fonctionne à l'aide d'un mot de passe à usage unique (OTP[6]) fréquemment constitué de lettres, chiffres ou caractères

[4] OTT, qui signifie Over-the-top ou service par contournement en français, fait référence à la diffusion de contenus vidéo, audio et autres médias sur Internet, en contournant les canaux de distribution traditionnels tels que la télévision par câble ou par satellite.
Cela signifie que les contenus sont proposés au moyen d'une connexion Internet, mais le fournisseur d'accès à Internet n'a aucun contrôle, ni aucune emprise sur ces contenus. Les services OTT sont donc découplés du prestataire de l'infrastructure. Les principaux prestataires d'OTT sur le marché sont Netflix, Amazon Prime, Hulu, DAZN et Eurosport Player.
Pour profiter des services de streaming, les utilisateurs doivent disposer d'une connexion Internet, et généralement installer une application proposée par le prestataire d'OTT. Avec cette application, ils peuvent accéder à tout moment au contenu souhaité, à condition de disposer d'un terminal branché sur Internet. Il pourra s'agir de reportages sportifs, de films, de séries, de streaming de jeux vidéo en temps réel ou de vidéos à la demande.
[5] NordPass est un outil de gestion des mots de passe conçu par les équipes de NordVPN. Il permet de générer, de stocker et de remplir automatiquement des mots de passe ainsi que d'autres informations sensibles en toute sécurité.
NordPass organise votre vie en ligne en offrant une solution sécurisée pour les mots de passe, les clés d'accès, les cartes de crédit et plus encore. Il génère des mots de passe forts, partage en toute sécurité vos mots de passe avec vos collègues et vous informe si vos données ont été piratées.
Il prend également en charge les clés d'accès, une nouvelle norme d'authentification sans mot de passe qui est plus sûre et plus pratique à utiliser que les mots de passe traditionnels.
En résumé, NordPass est un gestionnaire de mots de passe qui simplifie votre vie numérique, optimise votre sécurité et offre des avantages pour les entreprises et les particuliers.
[6] L'acronyme OTP signifie "One-Time Password en anglais, ce qui se traduit en français par "mot de passe à usage unique. C'est une séquence de caractères générée automatiquement qui valide une seule session de connexion ou une seule transaction.
Un OTP est généralement utilisé pour renforcer la sécurité des comptes en ligne et des transactions financières en fournissant un niveau supplémentaire de vérification de l'identité de l'utilisateur. Il est unique et créé de manière aléatoire par un algorithme. Le code OTP peut être envoyé par e-mail, par SMS, par message vocal ou encore via une application.
Il existe deux types d'OTP :
Les mots de passe à usage unique basés sur le temps (TOTP).
Les mots de passe à usage unique basés sur le hachage (HOTP).
Ces mots de passe nécessitent deux informations pour fonctionner : la graine et le facteur de déplacement. Une graine est une clé secrète détenue par le générateur de mot de passe et le serveur.

spéciaux et envoyé à l'utilisateur pour une seule tentative de connexion. Les mots de passe à usage unique peuvent être envoyés sur les appareils mobiles par SMS ou message vocal et protègent ainsi les interfaces en ligne, les identifiants privés ainsi que les données importantes. Les OTP réduisent considérablement le risque de fraude en envoyant des **codes PIN uniques et aléatoires** sur le dispositif des utilisateurs par SMS, message vocal ou notification push. Combiner la sécurité de l'authentification multi-facteurs et la commodité d'une application permet aux clients d'utiliser un seul identifiant et tout en respectant des normes de sécurité élevées. (**CM.com, cet article est disponible sur https : www.cm.com/fr-fr/blog/7-avantages-authentification-multifacteur/)**

4. Les différentes méthodes d'authentification à doubles facteurs

La méthode d'authentification traditionnelle, composée d'un identifiant et d'un mot de passe, semble aujourd'hui obsolète. En effet, d'après un rapport publié par l'entreprise de cybersécurité Hive System, un mot de passe composé de 9 caractères de toute nature (minuscules, majuscules, chiffres, caractères spéciaux) peut être forcée en à peine 6 heures par un hacker. Ainsi, la double authentification représente une solution adaptée pour apporter une protection supplémentaire à vos différents comptes, en intégrant une seconde couche de sécurité.
Ainsi, Il existe trois méthodes principales d'authentification à deux facteurs : le SMS, l'application de double authentification et la clé de sécurité.

(***Fabio Principe - stock.adobe.com disponible en ligne sur https://www.blogdumoderateur.com/double-authentification-definition-methodes-connaitre/*** **)**

- **La double authentification par SMS :** La double authentification par SMS est probablement la méthode la plus courante. Elle consiste à transmettre votre numéro de téléphone au service, qui vous enverra un SMS contenant un code à usage unique à chaque connexion à votre compte. Si cette méthode n'est pas la plus sécurisée, elle a l'avantage d'être simple à mettre en place, étant donné qu'elle ne nécessite pas de recourir à un service tiers, comme une application.
- **La double authentification par notification :** La notification de connexion permet de valider une connexion à un compte depuis un nouvel appareil. Lorsque vous vous connectez à un compte depuis un nouvel équipement, une notification est envoyée sur votre smartphone. Il vous suffit alors de valider la connexion au sein de la notification. Google

utilise cette méthode par défaut lorsque vous vous connectez à votre compte depuis un nouvel appareil.

- **L'application de double authentification :** L'application de double authentification est souvent plébiscitée pour son haut niveau de sécurité conjugué à sa simplicité d'accès. Une fois l'application installée sur votre smartphone, il vous faudra activer l'authentification à deux facteurs sur le service souhaité (Facebook, Twitter ou Instagram par exemple) et scanner le QR code qui apparaitra avec votre application. La solution génèrera alors un code de 6 chiffres à usage unique différent toutes les 30 secondes. Celui-ci ne pourra donc pas être intercepté. Ainsi, après avoir entré vos identifiants, il vous suffira d'indiquer le code qui apparaît sur l'application pour vous connecter.

(***José Billon / Publié le 12 juin 2023 à 09h40, Double authentification : définition et méthodes à connaître***).

5. L'importance de l'authentification multifacteurs dans la sécurité du système d'information d'une entreprise

Dans un paysage numérique en pleine évolution, la capacité d'utiliser son bureau en distance via le l'ordinateurs, téléphones et autres appareils fait désormais partie intégrante de la vie professionnelle dans une entreprise. Les solutions d'accès dans son bureau à distance favorisent la productivité et la connectivité, transcendant les barrières de la distance et du temps. Mais cette commodité accrue s'accompagne d'un besoin plus important en matière de sécurité.

C'est ainsi que l'authentification multifacteurs (FMA) entre en jeu. Il s'agit d'un outil simple mais puissant qui offre une couche de sécurité supplémentaire, particulièrement cruciale lorsque vous accédez à vos données à partir de différents endroits et appareils. En exigeant une deuxième forme de vérification en plus de votre mot de passe, l'authentification multifacteurs rend l'accès à vos comptes nettement plus difficile pour les utilisateurs non autorisés, même s'ils parviennent d'une manière ou d'une autre à obtenir votre mot de passe.

En pratique, la FMA fonctionne sur le principe de « quelque chose que vous connaissez et quelque chose que vous avez ou quelque chose que vous êtes ». Le premier facteur implique généralement quelque chose que vous connaissez, en général votre mot de passe. Le deuxième facteur est quelque chose que vous avez, comme un code d'accès à usage unique envoyé à votre appareil mobile ou à votre e-mail, ou quelque chose qui se rapporte à votre personne, comme un identifiant biométrique tel qu'une empreinte digitale ou une reconnaissance faciale.

Dans le cadre de l'accès à distance, la FMA. Devrait être utilisée assez souvent lorsque les entreprises permettent à leurs employés d'accéder aux données sensibles à partir de leurs propres appareils et de divers endroits, les risques potentiels pour la sécurité augmentent. Un mot de passe seul, aussi complexe soit-il, peut toujours être piraté, deviné ou hameçonné par des cybercriminels déterminés. La FMA ajoute un obstacle supplémentaire qui pourrait empêcher une fuite de données potentielle.
En mettant en œuvre la FMA, les entreprises peuvent ajouter une couche de sécurité supplémentaire à leurs protocoles d'accès à distance, garantissant que seuls les utilisateurs autorisés peuvent accéder à leurs systèmes. Cela permet non seulement de protéger les données sensibles de l'entreprise, mais aussi d'inspirer confiance aux clients et aux parties prenantes.

(Trevor Jackins, L'importance de l'authentification à deux facteurs pour l'accès à distance, Splashtop 20 septembre 2023, disponible en sur : https://www.splashtop.com/fr/blog/importance-two-factor-authentication-remote-access**)**

L'objectif principal de l'authentification multifacteurs est de créer un système de défense à plusieurs niveaux. Même si un intrus parvient à franchir une couche, le deuxième reste en place, ce qui rend l'accès au système plus difficile pour les personnes non autorisées.

6. La croissance des cybermenaces en Afrique

La croissance de cybermenaces en Afrique est fournie grâce aux données issues des pays membres d'INTERPOL, des partenaires privés et des recherches effectuées par le Desk africain pour les opérations de lutte contre la cybercriminalité, ce rapport de 2022 fournit une vision globale des tendances en matière de cybercriminalité dans la région africaine. La liste ci-après recense les principales cybermenaces identifiées dans le rapport, une tendance qui se poursuit actuellement dans la région africaine :

- **Les campagnes d'escroquerie** : Les cybermenaces piratent le système de messagerie électronique des entreprises pour obtenir les informations sur leurs systèmes de paiement, puis trompent les employés pour les inciter à virer de l'argent sur un compte bancaire qui leur appartient. Et face à ces faux ordres de virement restent prépondérantes, et ce sont les entreprises qui en paient le prix fort : c'est une activité à faible coût et faible risque, mais particulièrement rentable pour les cybercriminels. Ces derniers sont de plus en plus habiles et utilisent des outils très techniques.

- **L'hameçonnage :** Ce type de menace, il s'agit de faux e-mails ou SMS censés provenir d'une source légitime, et qui incitent les personnes à communiquer des informations financières ou personnelles. Cette attaque est une préoccupation croissante en Afrique, en raison de l'adoption rapide et de l'utilisation des technologies numériques. Plus la population se tourne vers les services et applications en ligne, plus elle est vulnérable aux attaques par hameçonnage.

- **Les attaques par rançongiciel** : Les cyberattaque pirate le système de l'entreprise pour le bloquer ensuite exigent de l'argent pour le rétablir. Et souvent ils ciblent les pouvoirs publics, des commerces et des organismes publics. Les infrastructures critiques, dont les secteurs de l'énergie et du transport, sont également dans le viseur des cybercriminels.

- **Les chevaux de Troie bancaires et les voleurs d'informations** : Ces cyberattaques représentent une nouvelle menace imminente pour les acheteurs sur Internet et sapent la confiance dans les moyens de paiement en ligne. Il est facile de se procurer différents types de chevaux de Troie et de voleurs d'informations sur des forums clandestins, et donc pour les cybercriminels de lancer leurs campagnes malveillantes.

- **Les escroqueries en ligne** : D'après nos recherches l'escroquerie en ligne se développent en Afrique rapidement à mesure que l'accès à Internet s'élargit. Cette menace est exacerbée par le peu de maîtrise numérique des victimes, ce qui en fait des cibles faciles pour les cybercriminels, qui les mettent en confiance avec de fausses promesses pour leur soutirer de l'argent.

- **La cyberextorsion :** Cette menace doit être étroitement surveillée elle va de pair avec la prolifération d'Internet et des technologies mobiles, puisque davantage de personnes sont susceptibles de recevoir des demandes de paiement et de se faire extorquer. (**Interpol, rapport d'évaluation des principales cybermenaces en Afrique** : Présentation des principales cybermenaces par le Desk Africain pour les opérations de lutte contre la cybercriminalité, Mars 2023, page 10)

- **Les logiciels criminels** : Les logiciels criminels, également appelés crimeware, sont des logiciels ou des codes délibérément créés pour faciliter les activités criminelles sur Internet. Ils peuvent englober un seul programme ou un ensemble de programmes qui permettent aux criminels de voler des informations personnelles, d'obtenir un accès non autorisé à

des appareils compromis ou d'automatiser des activités illicites comme le phishing. Une attaque de crimeware peut être très préjudiciable et entraîner de graves conséquences. Il est conçu pour mener des activités illégales, telles que le vol d'informations sensibles, la fraude financière, la diffusion de logiciels malveillants et la compromission de systèmes et de réseaux.

Il est important de noter que les logiciels criminels et les logiciels malveillants ne sont pas identiques. Le terme "malware" est un terme général qui fait référence à tout logiciel spécifiquement conçu pour nuire ou exploiter la fonctionnalité ou la sécurité d'un ordinateur, d'un réseau ou d'un appareil. D'autre part, le crimeware est un terme plus spécifique qui fait référence aux logiciels malveillants spécialement conçus pour commettre des délits financiers.

(**Christine Margret, 20 avril 2023**, Qu'est-ce qu'un logiciel criminel ? Un aperçu détaillé des chevaux de Troie malveillants, disponible sur : https ://www.fastestvpn.com/fr/blog/qu%27est-ce-qu%27un-logiciel-criminel/)
En outre, il est à noter que la transformation numérique rapide en Afrique, associée à l'absence de politiques et de normes solides en matière de cybersécurité, expose les services en ligne à des risques majeurs. Il est donc indispensable de mettre en place un cadre de cybersécurité solide pour faire face à ces menaces**. (Interpol, 2021 Un rapport d'INTERPOL recense les principales cybermenaces en Afrique 21 octobre 2021)**

7. Quelques incidents notables des cyberattaques ont été signalés en 2023

- L'armée de la Côte d'Ivoire a subi un vol de 50 Go de données à caractère personnel
- La Banque BOA du Mali a été victime d'une fuite de données en échange d'une rançon de 10 M$.

L'Autorité de Régulation des Télécommunications et des Postes du Sénégal (ARTP) a été piratée par le groupe de hackers Karakurta, avec 150 gigas de données personnelles pillées. (**Christelle HOUETO, 20 février 2023, Cybercriminalité en Afrique en 2023 : Des prédictions de plus en plus inquiétantes, publié sur Africa Cybersecurity Magazine** https://www.cybersecuritymag.africa/cybersecurite-afrique-2023-predictions-inquietantes)

8. Les conséquences économiques et sociales des cyberattaques pour l'Afrique

Les conséquences économiques et sociales des cyberattaques à la région a connu son essor dès le premier semestre de 2023, en cette année le continent africain a été le théâtre d'une augmentation significative des cyberattaques, avec une hausse de 23% par rapport à la même période en 2022, selon un récent rapport publié par African Cybersecurity Market, une entreprise spécialisée dans les services et les conseils en matière de cybersécurité, opérant principalement en Afrique de l'Ouest (notamment en Guinée, en Côte d'Ivoire, au Bénin et au Mali).

(**TELECOM ENERGIE GUINEE 17 septembre 2023, Croissance explosive des cyberattaques en Afrique en 2023)**

Selon l'entreprise, près de 90% des entreprises africaines opèrent sans protocoles de cybersécurité adéquats, les exposant ainsi davantage aux menaces en ligne.

Les cyberattaques ont des conséquences économiques et sociales significatives pour l'Afrique. Ces conséquences économiques et sociales sont les suivantes :

- **Pertes financières** : Les cyberattaques peuvent entraîner des pertes financières directes pour les entreprises et les individus. Par exemple, les escroqueries en ligne peuvent conduire à des pertes d'argent pour les victimes qui sont trompées pour transférer de l'argent ou partager des informations financières. (**INTERPOL, 21 octobre 2021, rapport sur le recense les principales cybermenaces en Afrique**)

- **Perturbation des services** : Les cyberattaques, comme les rançongiciels, peuvent perturber les services essentiels, tels que les hôpitaux et les institutions publiques, ce qui peut avoir des conséquences graves pour la société.

Perte de confiance : Les cyberattaques peuvent éroder la confiance du public dans les services numériques. Cela peut freiner l'adoption de la technologie et ralentir la transformation numérique. (**Cybersecuritymag.africa, Rapport PWC Afrique mars 2021, Les enjeux et défis de la cybersécurité en Afrique francophone subsaharienne).**

1. **Coûts de la cybersécurité** : Les entreprises et les gouvernements doivent investir dans la cybersécurité pour se protéger contre les

cyberattaques. Ces coûts peuvent être importants et représenter un fardeau pour les économies en développement.

2. **Impact sur la compétitivité** : Les entreprises qui sont victimes de cyberattaques peuvent subir des pertes de productivité et voir leur compétitivité réduite.

Pour éviter ces conséquences de cyberattaque en Afrique, Il est donc crucial aux pays africains et entreprises de mettre en place des stratégies de cybersécurité solides pour atténuer ces risques.

9. Les défis et les obstacles à la configuration de l'authentification multifacteurs (FMA)

L'authentification multifacteurs (FMA) est un processus de sécurité qui augmente la probabilité qu'une personne soit ce qu'elle prétend être. Le processus demande aux utilisateurs de fournir deux facteurs d'authentification différents avant de pouvoir accéder à une application ou un système, plutôt que d'indiquer simplement leur nom d'utilisateur et leur mot de passe**. (Fortinet, Définition de l'authentification à deux facteurs (2FA), disponible sur : https://www.fortinet.com/fr/resources/cyberglossary/two-factor-authentication)**

Cependant, la mise en œuvre de l'authentification à deux facteurs peut présenter plusieurs défis et obstacles tels que :

1. **Complexité de mise en œuvre** : La FMA est beaucoup plus difficile à mettre en œuvre que l'authentification par mot de passe uniquement. Une entreprise fournissant la FMA devra soit engager des frais d'installation, soit payer un service tiers pour fournir l'authentification à un coût permanent.
2. **Coûts commerciaux** : La FMA impose également des frais commerciaux à ceux qui gèrent le service.
3. **Récupération de compte** : Alors que les services continuent de renforcer leurs protocoles à deux facteurs ou multifacteurs et rendent la récupération de compte encore plus difficile, il devient de plus en plus impératif de configurer une authentification à deux facteurs sur vos comptes importants.
4. **Facteurs d'authentification** : Il existe plusieurs types de facteurs d'authentification qui peuvent être utilisés pour confirmer l'identité d'une personne. Les plus fréquents sont les suivants :

- Un facteur de connaissance : il s'agit d'informations que l'utilisateur connaît, par exemple un mot de passe, un numéro d'identification personnel (PIN) ou un code d'accès.
- Un facteur de possession : il s'agit de quelque chose que l'utilisateur possède, par exemple son permis de conduire, sa carte d'identification, son dispositif mobile ou une application d'authentification sur son smartphone.
- Un facteur d'inhérence : il s'agit d'un attribut personnel ou un élément inhérent à l'utilisateur, généralement une forme de facteur biométrique. Il s'agit notamment des lecteurs d'empreintes digitales, de la reconnaissance faciale et vocale, ainsi que de la biométrie comportementale comme la dynamique des frappes et les traceurs de schémas vocaux.
- Un facteur d'emplacement : il est généralement guidé par l'emplacement où un utilisateur tente d'authentifier son identité. Les organisations peuvent limiter les tentatives d'authentification à certains dispositifs situés à des emplacements spécifiques, en fonction de la manière dont les employés se connectent à leurs systèmes et de l'endroit où ils se connectent.

10. Les mesures à prendre pour promouvoir l'authentification multifacteurs en Afrique

Pour promouvoir l'authentification multifacteurs (FMA) dans tous les pays et entreprises Africains il serait mieux d'adopter une approche globale qui comprend l'éducation, la sensibilisation et l'accessibilité. Les mesures qui pourraient être prises sont les suivantes :

1. **Éducation et sensibilisation** : Il est essentiel de sensibiliser et d'éduquer les utilisateurs sur les avantages de l'authentification à deux facteurs ou multifacteurs. Cela comprend la compréhension de ce qu'est la FMA, comment elle fonctionne, et pourquoi elle est importante pour la sécurité en ligne.
   (**DUALMEDIA, Les avantages et inconvénients de l'implémentation d'une authentification multifacteurs, disponible sur : https:// www.dualmedia.fr/les-avantages-et-inconvenients-de-limplementation-dune-authentification-multi-facteurs/**)
2. **Facilité d'utilisation** : Pour encourager l'adoption de la 2FA et FMA, il est crucial de rendre le processus aussi simple et intuitif que possible. Cela peut impliquer de travailler avec des fournisseurs de

services pour intégrer la 2FA ou FMA de manière transparente dans leurs systèmes.

3. **Accessibilité** : Assurer que tous les utilisateurs ont accès aux outils nécessaires pour utiliser la FMA ou 2FA. Par exemple, si un service utilise la 2FA via SMS, il est important que tous les utilisateurs aient accès à un service mobile.

(**IBM, 2FA (authentification à deux facteurs) Découvrez comment la 2FA protège les comptes d'utilisateurs, défend les entreprises contre les cyberattaques et prend en charge une approche de sécurité Zéro Trust. Disponible sur : https://www.ibm.com/fr-fr/topics/2fa**)

4. **Support technique** : Fournir un support technique pour aider les utilisateurs qui rencontrent des difficultés avec la 2FA. Cela peut inclure des guides d'aide en ligne, des centres d'appel, et d'autres ressources.

(SURVEILLANCE SELF-DEFENSE, Guide pratique : activer l'authentification à deux facteurs, septembre 07, 2017, disponible sur : https://www.ssd.eff.org/fr/module/guide-pratique-activer-l'authentification-à-deux-facteurs)

5. **Partenariats** : Travailler avec des gouvernements, des organisations non gouvernementales, et des entreprises privées pour promouvoir l'adoption de la FMA ou 2FA. Cela pourrait inclure des campagnes de sensibilisation, des ateliers de formation, et d'autres initiatives.

(Gabriel Autran, Authentification à deux facteurs : l'implémenter pour une sécurité maximale, 16 janvier 2023, disponible en ligne sur : https://www.spendesk.com/fr/blog/authentification-a-deux-facteurs/)

Il est crucial pour les entreprises et les pays africains de comprendre que, bien que la FMA ou 2FA offre de nombreux bénéfices, elle comporte aussi des désavantages. Ceux-ci incluent une certaine complexité pour l'utilisateur, un risque potentiel de perdre l'accès, ainsi que des coûts associés à sa mise en place. Ces obstacles doivent être considérés lors de l'encouragement à l'adoption de la FMA ou 2FA.

Conclusion

L'authentification multifacteurs (FMA) est un outil essentiel pour renforcer la sécurité des systèmes d'information dans un monde numérique. Elle offre une protection robuste contre les cybermenaces en exigeant plusieurs formes de preuves pour vérifier l'identité d'un utilisateur. En Afrique, l'adoption de la

FMA est en hausse, motivée par une prise de conscience accrue de l'importance de la cybersécurité et le désir de se conformer aux normes internationales. Cependant, des défis subsistent, notamment en ce qui concerne l'infrastructure technologique, la sensibilisation du public et la mise en œuvre de politiques efficaces de cybersécurité. D'un point de vue économique, la FMA est un investissement judicieux, les coûts de mise en œuvre étant souvent compensés par les économies réalisées grâce à la prévention des cyberattaques. De plus, la FMA peut renforcer la confiance des clients et des partenaires commerciaux, améliorant ainsi la réputation et la compétitivité d'une entreprise. En somme, la FMA est un pilier de la sécurité des systèmes d'information, offrant une protection contre le phishing et d'autres attaques, assurant la conformité aux réglementations et renforçant la confiance des utilisateurs.
En outre, cet article démontre et recommande aux pays et entreprises africains l'adoption de l'authentification multifacteurs (MFA) dans leurs systèmes de gestion d'information suit à ces avantages tels que :

1. **Sécurité accrue** : La FMA réduit les risques de failles de sécurité et garde les données en sécurité.
2. **Moins de risques liés aux mots de passe compromis** : Des mots de passe faibles ou volés peuvent être utilisés pour réaliser des fraudes ou des intrusions lorsqu'il s'agit de la seule méthode d'authentification.
3. **Une solution de sécurité personnalisable** : La FMA peut être adaptée à divers cas d'usage.
4. **Compatible avec le Single Sign-On (SSO)** : La FMA peut être intégrée avec des solutions d'authentification unique (SSO).
5. **Évolutivité face à des bases d'utilisateurs changeantes** : La FMA peut s'adapter à l'évolution des besoins des utilisateurs.
6. **Conformité aux réglementations** : La FMA peut aider à se conformer aux réglementations en matière de cybersécurité.
7. **Facilite la mobilité de l'entreprise** : La FMA permet aux employés d'accéder en toute sécurité aux systèmes de l'entreprise depuis n'importe quel appareil ou emplacement.

Nous recommandons aux chefs de pays et entreprises africains de :

1. **Mener une analyse de risque** lors de la mise en place de moyens d'authentification. Cela permet de comprendre les menaces potentielles et de choisir les méthodes d'authentification les plus appropriées.

2. **Privilégier l'utilisation de l'authentification multifacteurs**. Cela renforcera la sécurité en exigeant plusieurs formes de preuves pour vérifier l'identité d'un utilisateur.
3. **Privilégier l'utilisation de l'authentification reposant sur un facteur de possession**. Cela peut inclure des éléments tels que des cartes à puce ou des jetons physiques.
4. **Adapter la robustesse d'un mot de passe à son contexte d'utilisation**. Par exemple, un système contenant des données sensibles peut nécessiter un mot de passe plus complexe qu'un site de réservation de terrain de tennis.
5. **Utiliser un coffre-fort de mots de passe**. Cela permet de stocker en toute sécurité tous les mots de passe en un seul endroit.
6. **Investir dans l'éducation et la sensibilisation**. Il est important de former les utilisateurs finaux sur l'importance de la cybersécurité et sur la manière d'utiliser correctement les méthodes d'authentification.
7. **Mettre en place des politiques de cybersécurité efficaces**. Cela peut inclure des directives sur l'utilisation de mots de passe forts, la mise à jour régulière des systèmes et la réponse aux incidents de sécurité.
8. **Investir dans l'infrastructure technologique nécessaire**. Cela peut inclure l'achat de matériel nécessaire pour l'authentification biométrique ou l'investissement dans des solutions de sécurité informatique.

Références bibliographiques

1. **Lumu.IO, 2020 Ransomware Flashcard, consultable à l'adresse : https://lumu.io/ressources/2020-ransomware-flashcard/**
2. **Institut d'études de sécurité, Africa can 't Risk a major maritime cyber attack. Reva, D., 28 octobre 2020. Consultable à l'adresse https://www.issafrica.org/iss-today/africa-cant-risk-a-major-maritime-cyber-attack**
3. **GUIDE ANSSI version 2.0, 08/10/2021 recommandations relatives à l'authentification multifacteurs et aux mots de passe**
4. **Matt Bromiley, Bye Password : New Ways to Authenticate, July 2019**
5. **CM.com, cet article est disponible sur https : www.cm.com/fr-fr/blog/7-avantages-authentification-multifacteur/**
6. ***Fabio Principe - stock.adobe.com disponible en ligne sur https://www.blogdumoderateur.com/double-authentification-definition-methodes-connaitre/***
7. ***José Billon / Publié le 12 juin 2023 à 09h40, Double authentification : définition et méthodes à connaître*.**
8. **Trevor Jackins, L'importance de l'authentification à deux facteurs pour l'accès à distance, Splashtop 20 septembre 2023, disponible en sur :** https://www.splashtop.com/fr/blog/importance-two-factor-authentication-remote-access
9. **CHRISTINE MARGRET, 20 AVRIL 2023**, Qu'est-ce qu'un logiciel criminel ? Un aperçu détaillé des chevaux de Troie malveillants,

disponible sur : https ://www.fastestvpn.com/fr/blog/qu%27est-ce-qu%27un-logiciel-criminel/

10. **Interpol, 2021 Un rapport d'INTERPOL recense les principales cybermenaces en Afrique 21 octobre 2021**
11. **Christelle HOUETO, 20 février 2023, Cybercriminalité en Afrique en 2023 : Des prédictions de plus en plus inquiétantes, publié sur Africa Cybersecurity Magazine** https://www.cybersecuritymag.africa/cybersecurite-afrique-2023-predictions-inquietantes
12. **TELECOM ENERGIE GUINEE 17 septembre 2023, Croissance explosive des cyberattaques en Afrique en 2023**
13. **INTERPOL, 21 octobre 2021, rapport sur le recense les principales cybermenaces en Afrique**
14. **Cybersecuritymag.africa, Rapport PWC Afrique mars 2021, Les enjeux et défis de la cybersécurité en Afrique francophone subsaharienne**
15. **Fortinet, Définition de l'authentification à deux facteurs (2FA), disponible sur : https://www.fortinet.com/fr/resources/cyberglossary/two-factor-authentication**
16. **DUALMEDIA, Les avantages et inconvénients de l'implémentation d'une authentification multifacteurs, disponible sur : https:// www.dualmedia.fr/les-avantages-et-inconvenients-de-limplementation-dune-authentification-multi-facteurs/**
17. **IBM, 2FA (authentification à deux facteurs) Découvrez comment la 2FA protège les comptes d'utilisateurs, défend les entreprises contre les cyberattaques et prend en charge une approche de sécurité zéro Trust. Disponible sur : https://www.ibm.com/fr-fr/topics/2fa**
18. **SURVEILLANCE SELF-DEFENSE, Guide pratique : activer l'authentification à deux facteurs, septembre 07, 2017, disponible sur : https://www.ssd.eff.org/fr/module/guide-pratique-activer-l'authentification-à-deux-facteurs**

19. **Gabriel Autran, Authentification à deux facteurs : l'implémenter pour une sécurité maximale, 16 janvier 2023, disponible en ligne sur : https://www.spendesk.com/fr/blog/authentification-a-deux-facteurs/**