MINISTERE DE L'ÉCONOMIE NUMERIQUE
ET DES TELECOMMUNICATIONS

"Les Nouvelles Formes de Menaces en Cybersécurité : Prévenir et Réagir aux Attaques Émergentes"

Présenté par M. Gérard DACOSTA
&
M. Cheikh Ahmadou Bamba FALL

A propos des intervenants

FALL Cheikh Ahmadou Bamba · 2e

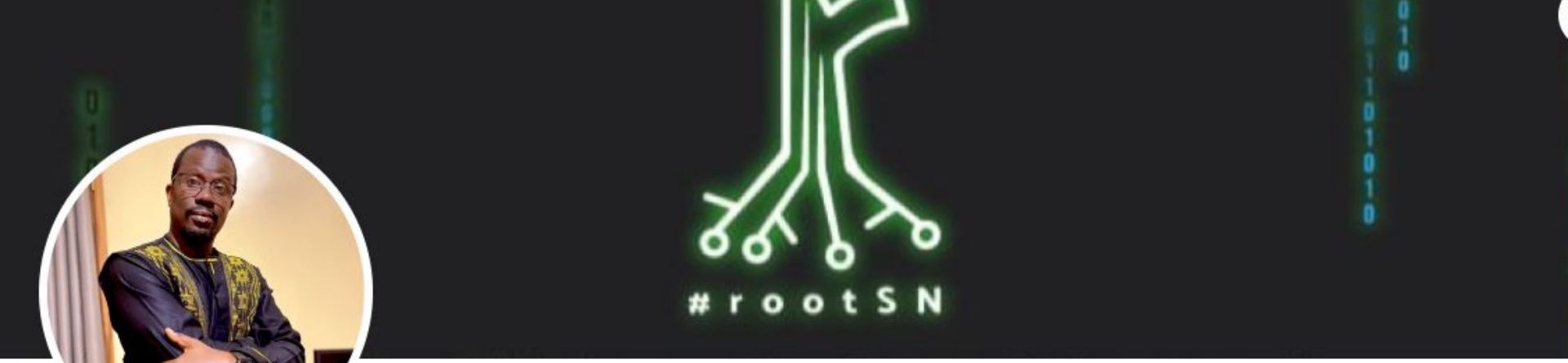
Conseiller Technique en charge de la Cybersécurité et des Tics chez Ministère de l'Economie Numérique et des Télécommunications

Sujets de prédilection : #odd, #numérique, #cybersécurité, #cybercriminalité et #transformationdigitale

Sénégal · Coordonnées

Ministère de l'Economie Numérique et des Télécommunications

Bordeaux Management School



Gérard Joseph Francisco (rootSN) DACOSTA

Computer security engineer option MSSI | founding member Nu Jang Informatique | Cyber blogger | Special Advisor Daara-IT | Founding member rootSN community | IT-Trainer | IT consultant

Sujets de prédilection : #informatique, #numériques, #cybersecurity, #cybersecurité et #securiteinformatique

Arrondissement de Dakar-Plateau, Région de Dakar, Sénégal · Coordonnées

Le Monde Du Numérique

IT4LIFE

IESMD-TECHNOLOGIE

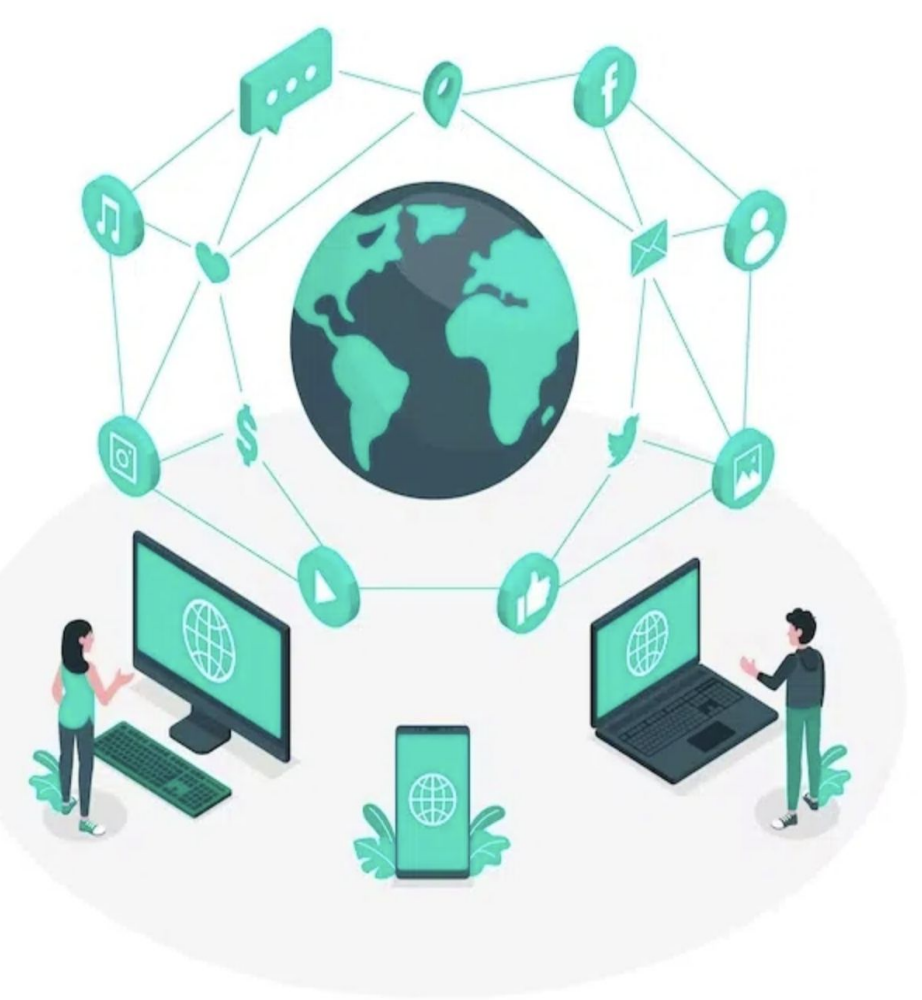
Commençons

Le réseau

Nous pouvons le définir comme un ensemble d'éléments interconnectés entre eux dans le but de traiter l'information.

Les composants d'un réseau

- Ordinateurs
- Téléphones
- Imprimantes
- scanneurs
- ...



Internet

C’est un ensemble de réseaux mondiaux interconnectés par des équipements informatique et qui permettent un vaste échange de données, d’informations.

Les composants

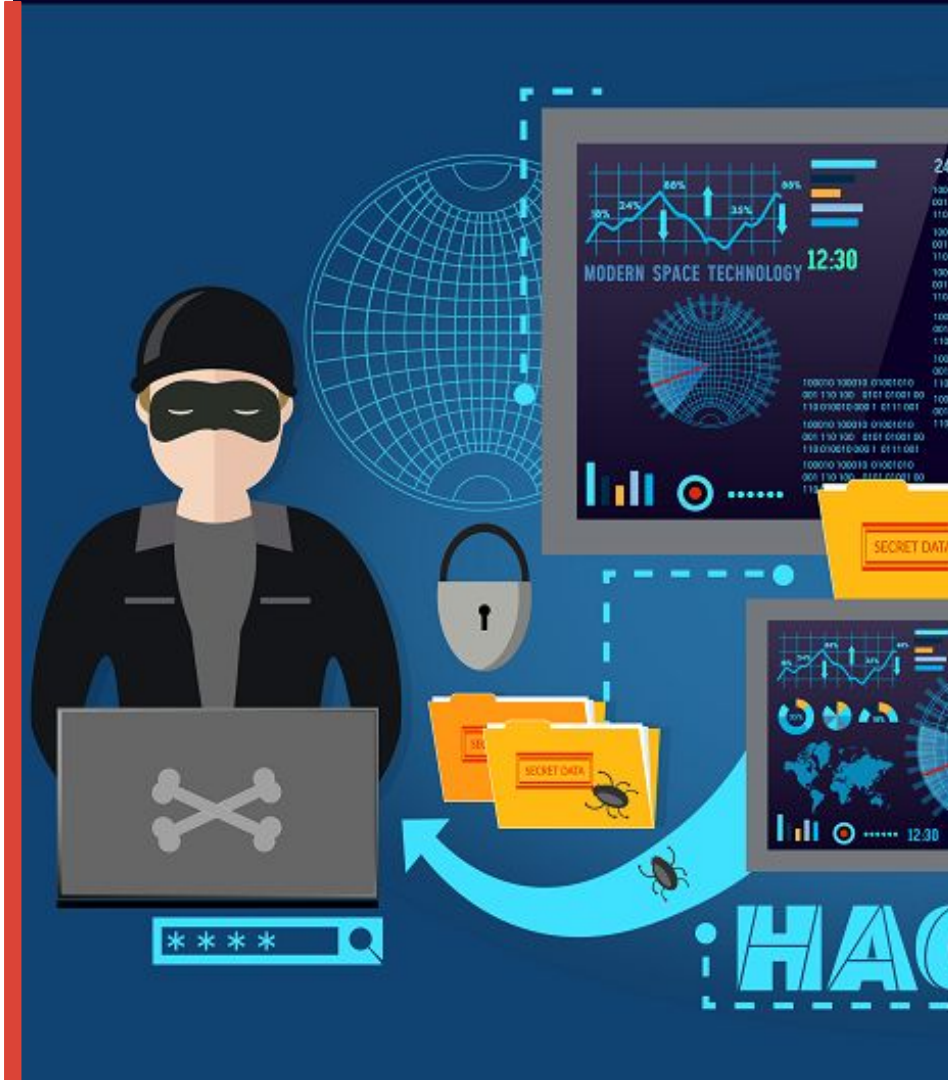
- Ordinateurs
- Téléphones
- Imprimantes
- scanneurs
- …

Cyber-Space

Espace de communication créé par l'interconnexion mondiale des ordinateurs et par les données qui y sont traitées autrement dit c'est un monde virtuel né grâce à internet.

Sécurité informatique / Cybersécurité

C'est l'ensemble des moyens techniques et non techniques permettant à une entité (Etats, Entreprises, particuliers, …) de se défendre contre les menaces venues du cyberespace.



Menace informatique

En informatique, une menace est une cause potentielle d'incident, qui peut résulter en un dommage au système ou à l'organisation.

Hacker

un hacker, francisé hackeur ou hackeuse, est un spécialiste d'informatique, qui recherche les moyens de contourner les protections logicielles et matérielles.

Données Personnelles / Sensibles

Une **donnée personnelle** est toute information se rapportant à une personne physique identifiée ou identifiable. Mais, parce qu'elles concernent des personnes, celles-ci doivent en conserver la maîtrise.

Les **données dites sensibles** sont les informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ….

La cybersécurité / Sécurité Informatique.

Les objectifs

Confidentialité

Rend les données cryptées de sorte que seules les personnes concernées aient accès à l'information.

Intégrité

Prouve que l'information reçue n'a pas subi d'altération.

Authentification

Comment prouver son identité afin de se connecter à un SI.

Non répudiation

Permet de vérifier qui est l'auteur de l'envoi d'une information.

Disponibilité

Le dernier des objectifs consiste à rendre disponible un SI 24/24, 7/7.

Les piliers

La sécurité Physique

Protéger un SI physiquement afin d'empêcher une attaque directe.

La sécurité Logique

Protéger un SI dans le cyberespace afin de limiter les attaques en ligne.

La sécurité Communicationnelle

Sécuriser les communications reste primordial, donc toute communication importante doit être chiffrée.

La sécurité Juridique

Les textes et réglementation qui permettent de poursuivre l'auteur des faits, mais aussi de punir une entité qui n'a pas su protéger les données des clients sous sa responsabilité.

La sécurité Humaine

De loin la plus importante, car l'être humain reste le maillon le plus faible d'un SI.

Les Types d’Hackers

1- Black hack

Du côté obscur, ils n'hésitent pas à vendre le talent au plus offrant

2- Grey hack

Entre la frontière du bien et du mal, pour eux tout dépend de la situation en face d’eux.

3- White hack

Les chevaliers blancs, toujours au service du bien. ils luttent tous les jours pour la sécurité dans le cyberespace.

Les Types de Hackers

4- Scripts Kiddies

Les plus dangereux mais plus prévisibles.

5- Cyberterroristes

Font des attaques de grande envergure visant des Etats.

6- Hack-activistes

Ils hackent pour défendre une idéologie, un concept, une doctrine.

Un peu d’Histoire

2007 : Estonie

- Banques,
- Hôpitaux,
- Circulation,
- Etat

2010 : Stunext

Ver créé par la NSA.

2014 : Sony Pictures

Vol de données et menace de divulgation

2017 : Wanacry

Des milliers voir milliards de postes ont été affectés.

2019 -2020 : Hameconnage

Unicef, Croix rouge font partie du lot.

2021: Cyberattaque visant les hôpitaux

Vol de données patients et autres.

Quelques chiffres

Plus de **7** entreprises sur **10**

ont été victimes **d'au moins une tentative de fraude** en 2019

Tentatives de fraudes les plus fréquentes

48%

Fraude **au faux fournisseur**

29%

Intrusion **dans les systèmes d'information**

Dispositifs ayant permis de déjouer ces tentatives de fraudes

51% **Réaction ou initiative humaine personnelle**

Dispositifs qui feront l'objet d'investissements

56% **Sensibilisation et formations internes des autres Directions**

Les Menaces avancées, c’est quoi ?

Définition

Les cybermenaces avancées, également appelées menaces avancées persistantes (Advanced Persistent Threats ou APT en anglais), désignent des attaques informatiques sophistiquées et persistantes, généralement orchestrées par des acteurs malveillants hautement qualifiés. Ces menaces diffèrent des attaques informatiques conventionnelles en raison de leur niveau d'expertise, de leur durée et de leur objectif.

caractéristiques clés des cybermenaces avancées :

- **Sophistication technique :** Les attaquants derrière les APT utilisent des techniques avancées, telles que l'ingénierie sociale, l'exploitation de vulnérabilités zero-day, la furtivité et la persistance pour compromettre des systèmes informatiques.

- **Persistance :** Les APT ont tendance à opérer sur de longues périodes, parfois pendant des mois ou des années, en infiltrant discrètement le réseau cible. Ils sont souvent capables de rester invisibles pendant de longues périodes.

caractéristiques clés des cybermenaces avancées (Suite) :

- **Objectif clair :** Les attaquants ont généralement un objectif précis, comme l'espionnage industriel, la collecte de renseignements sensibles, le vol de propriété intellectuelle ou la perturbation des opérations critiques.

- **Ciblage spécifique :** Les APT ciblent souvent des entités spécifiques, telles que des gouvernements, des entreprises, des institutions de recherche ou des organisations militaires.

caractéristiques clés des cybermenaces avancées (Fin):

- **Capacité d'adaptation :** Les attaquants sont capables de s'adapter aux contre-mesures prises par la victime, rendant la détection et la défense plus difficiles.

- **Infiltration multi-étape :** Les APT utilisent souvent des tactiques multi-étapes pour infiltrer un réseau, en passant par plusieurs couches de sécurité.

Les types de menaces

Se basant sur la signature numérique

- Vers,
- Virus,
- Cheval de troie
- Hameçonnage,
- Rançongiciel,
- Logiciels malveillants,
- DDOS.
- Entre autres.

Se basant sur comportement

Ici, nous avons l'intervention de l'IA

Types de manaces APT:

- **Malware personnalisé :** Les acteurs APT développent souvent des logiciels malveillants spécifiques à leurs cibles. Ces malwares sont conçus pour échapper aux défenses de sécurité standard.

- **Spear Phishing** : Les APT utilisent des e-mails de phishing personnalisés pour tromper les utilisateurs et les inciter à ouvrir des pièces jointes infectées ou à cliquer sur des liens malveillants.

Types de manaces APT:

- **Ingénierie sociale** : Les attaquants APT peuvent utiliser des tactiques d'ingénierie sociale pour obtenir des informations sensibles ou inciter les utilisateurs à prendre des mesures qui compromettent la sécurité de leur organisation.

- **Exploitation de vulnérabilités zero-day** : Les APT sont connus pour exploiter des vulnérabilités zero-day, c'est-à-dire des failles de sécurité encore inconnues du public, pour pénétrer dans des systèmes.

Types de manaces APT:

- **Utilisation d'outils d'administration légitimes** : Pour éviter d'éveiller les soupçons, les APT utilisent parfois des outils d'administration légitimes qui sont déjà présents sur les systèmes ciblés.

- **Tactiques de mouvement latéral** : Une fois qu'ils ont accès à un système, les APT utilisent des tactiques pour se déplacer latéralement à travers le réseau, cherchant à étendre leur influence.

Types de manaces APT:

- **Persistance** : Les APT s'efforcent de maintenir un accès continu à un système cible. Cela peut inclure l'installation de portes dérobées pour un accès futur.

- **Exfiltration de données** : L'objectif principal des APT est souvent de voler des données sensibles, qu'ils exfiltrent discrètement vers des serveurs de commande et de contrôle.

- **Capacités d'évasion** : Les acteurs APT utilisent des techniques d'évasion pour éviter la détection, telles que l'utilisation de signatures uniques pour leur malware.

Types de manaces APT:

- **Opérations à long terme** : Contrairement à d'autres menaces qui ont des objectifs immédiats, les APT opèrent sur le long terme, collectant continuellement des informations et maintenant un accès persistant.

- **Ciblage spécifique** : Les APT ciblent généralement des organisations, des gouvernements ou des entreprises spécifiques en fonction de leurs objectifs et de leurs motivations.

- **Acteurs sophistiqués** : Les APT sont souvent associés à des acteurs très sophistiqués, tels que des groupes de cyberespionnage soutenus par des États.

Exemples de menace APT coonus

- **Stuxnet** : Un ver informatique qui a ciblé les systèmes de contrôle industriels en Iran. Il est généralement attribué à une opération de cyberespionnage sponsorisée par un État.

- **Flame** : Un logiciel malveillant qui a été utilisé pour collecter des informations sur des organisations du Moyen-Orient, notamment en Iran et en Syrie.

Les menaces APT en Afrique: cas du Sénégal

Afrique

- **Cyberespionnage gouvernemental** : Les gouvernements africains sont de plus en plus préoccupés par la cybersécurité, en particulier en ce qui concerne le cyberespionnage. Les menaces APT soutenues par des États ciblent souvent des gouvernements, des entreprises et des organisations pour obtenir des informations sensibles.

- **Ressources naturelles et énergie** : En Afrique, où les ressources naturelles, telles que le pétrole et le gaz, jouent un rôle économique majeur, les APT peuvent cibler les entreprises et les infrastructures liées à ces secteurs. Le Sénégal étant récemment devenu un acteur clé dans l'industrie pétrolière et gazière, il est important de protéger ces actifs.

- **Secteur financier** : Les APT visent souvent les institutions financières en Afrique, y compris au Sénégal. Les attaques peuvent avoir des implications financières graves, notamment en cas de vol de données clients ou de fraude.

Afrique (Fin)

- **Influence politique** : Les menaces APT peuvent également être utilisées pour influencer le paysage politique en Afrique, y compris au Sénégal, en divulguant des informations compromettantes ou en perturbant les élections.

- **Opportunités d'investissement** : La croissance économique de l'Afrique attire de nombreux investisseurs étrangers. Les APT peuvent cibler des entreprises étrangères ou des institutions financières pour accéder à des informations liées aux investissements.

- **Défis de cybersécurité** : Les infrastructures de cybersécurité en Afrique, y compris au Sénégal, peuvent ne pas être aussi développées que dans d'autres régions, ce qui crée des vulnérabilités potentielles. Les APT exploitent souvent ces lacunes.

Cas du Sénégal

- **Menaces économiques** : Les groupes APT financés par des États ou des acteurs malveillants peuvent cibler les secteurs économiques clés du Sénégal, tels que l'industrie pétrolière, gazière, minière, ou le secteur de la pêche. Ils pourraient chercher à voler des informations sensibles sur les contrats, les négociations commerciales ou les réserves naturelles du pays.

- **Espionnage politique** : Les APT sont souvent utilisées pour espionner des acteurs politiques et gouvernementaux. Au Sénégal, cela pourrait inclure des tentatives de collecte d'informations sur les politiques, les élections et les mouvements de l'opposition, en vue d'influencer la stabilité politique du pays.

- **Cyberespionnage industriel** : Les entreprises sénégalaises pourraient être ciblées par des APT cherchant à voler des informations commerciales confidentielles, des plans de produits, des données de clients ou des secrets de fabrication.

Cas du Sénégal (Suite)

- **Infiltration des infrastructures critiques** : Les APT peuvent viser les infrastructures critiques, comme les réseaux électriques (SENELEC), les télécommunications (Orange SN, Free, Expresso), ou les réseaux d'eau (Seneau), pour perturber les services essentiels.

- **Cyberattaques liées au secteur de la santé** : Les APT pourraient cibler les établissements de santé au Sénégal pour accéder à des dossiers médicaux sensibles, perturber les services de soins de santé ou même voler des informations liées à la recherche médicale

- **Attaques contre les infrastructures technologiques** : Les entreprises de télécommunications (comme Orange SN, Free, Expresso) pourraient être exposées à des APT cherchant à compromettre les réseaux et à surveiller les communications.

Cas du Sénégal (Fin)

- **Influence sur les médias sociaux** : Les APT pourraient également tenter d'influencer l'opinion publique sénégalaise en diffusant de fausses informations ou en menant des campagnes de désinformation sur les réseaux sociaux, ce qui pourrait avoir un impact sur les événements politiques et sociaux du pays.

- **Fuites de données gouvernementales** : Les organismes gouvernementaux, y compris les forces de sécurité (police, armée), pourraient être vulnérables aux APT cherchant à accéder à des informations sensibles, notamment celles liées à la sécurité nationale.

Les actions gouvernementales: Cas du Sénégal

CADRE JURIDIQUE ET REGLEMENTAIRE CONVENTIONS & ACCORDS

Le Sénégal a adhéré aux instruments juridiques internationaux suivants relatifs à la lutte contre la cybercriminalité:

- CONVENTION SUR LA CYBERCRIMINALITÉ SIGNÉE LE 21 NOVEMBRE 2001 À BUDAPEST QUE LE SÉNÉGAL A ÉTÉ LE PREMIER D'AFRIQUE NOIRE À RATIFIER ET À DEVENIR LE 51ÈME ETAT PARTIE;
- CONVENTION DE L'UNION AFRICAINE SUR LA CYBERSÉCURITÉ ET LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL DIT CONVENTION DE MALABO: LE SÉNÉGAL A ÉTÉ LE PREMIER PAYS AFRICAIN À RATIFIER CETTE CONVENTION;
- TRANSPOSITION ENTIÈRE EN DROIT INTERNE DE LA DIRECTIVE DE LA CEDEAO DU 19 AOUT 2011 SUR LA CYBERCRIMINALITÉ;
- ADHÉSION À LA CONVENTION N°108 SUR LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

CADRE JURIDIQUE ET REGLEMENTAIRE-LOIS

En vertu de ce cadrage juridique, le Sénégal a adapté sa législation de la maniéré suivante:

- ✔ LOI SUR LA TRAITE DES PERSONNES ET PRATIQUES ASSIMILÉES
- ✔ LOI PORTANT LOI D'ORIENTATION DE LA SOCIÉTÉ DE L'INFORMATION
- ✔ LOI RELATIVE AUX TRANSACTIONS ÉLECTRONIQUES
- ✔ LOI SUR LA PROTECTION DES DONNÉES À CARACTERES PERSONNEL*
- ✔ LOI RELATIVE À LA CYBERCRIMINALITÉ.
- ✔ LOIRELATIVE À LA CRYPTOLOGIE
- ✔ LOI SUR LE DROIT D'AUTEUR ET LES DROITS VOISINS
- ✔ LOI PORTANT CODE PÉNAL et PORTANT CODE DE PROCÉDURE PÉNALE

ORGANES OPERATIONNELS

CADRE INSTITUTIONNEL

Le Sénégal s'est également doté d'institutions opérationnelles de lutte contre la cybercriminalité:

- COMMISSION NATIONALE DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL (CDP);
- SENUM ex AGENCE DE L'INFORMATIQUE DE L'ETAT (ADIE);
- AUTORITÉ DE RÉGULATION DES TÉLÉCOMMUNICATIONS ET DES POSTES (ARTP);
- DIVISION SPÉCIALE DE CYBERSÉCURITÉ LOGÉE AU SEIN DU MINISTÈRE DE L'INTÉRIEUR;
- PLATEFORME DE LUTTE CONTRE LA CYBERCRIMINALITÉ AU SEIN DE LA SECTION DE RECHERCHE DE LA GENDARMERIE NATIONALE;
- CADRE NATIONAL DE COORDINATION DES ACTIVITÉS DE DÉTECTIONS, D'ALERTES ER DE RÉPONSES AUX CYBERATTAQUES (CADARCA);

Processus d’élaboration et de rédaction: Adoption d’une approche multipartite sous le pilotage du ministère en charge du numérique

Plan Sénégal Emergent (PSE), stratégie Sénégal numérique (SN2025);

Evaluation de la situation de référence de la cybersécurité au Sénégal (politique et stratégie, culture et société, éducation formation et compétence, cadre juridique et réglementaire, normes organisations et technologies): modèle CMM, GCSCC,université d’oxford)

SNC2022: 49 ACTIONS SPÉCIFIQUES ET 12 PROJETS PRIORITAIRES AVEC UN BUDGET TOTAL DE 3,185 MILLIARDS DE FCFA

VISION:

« En 2022 au Sénégal, un cyberespace de confiance, sécurisé et résilient pour tous »

OBJECTIFS STRATEGIQUES (OS)

OS1: *renforcer le cadre juridique et institutionnel de la cybersécurité au Sénégal*

OS2: *renforcer la protection des infrastructures d'information critiques (IIC) et les systèmes d'information de l'Etat du Sénégal*

OS3: *promouvoir une culture de cybersécurité au Sénégal*

OS4: *renforcer les capacités et les connaissances techniques en cybersécurité dans tous les secteurs*

OS5: *participer aux efforts régionaux et internationaux de cybersécurité.*

PRINCIPES DIRECTEURS

- Etat de droit
- Responsabilité partagée
- Approche basée sur les risques
- Accès universel au cyberespace et sa pleine exploitation du cyberespace
- Coopération et collaboration entre les parties prenantes

SNC2022: 49 ACTIONS SPÉCIFIQUES ET 12 PROJETS PRIORITAIRES AVEC UN BUDGET TOTAL DE 3,185 MILLIARDS DE FCFA

VISION:

« En 2022 au Sénégal, un cyberespace de confiance, sécurisé et résilient pour tous »

OBJECTIFS STRATEGIQUES (OS)

OS1: *renforcer le cadre juridique et institutionnel de la cybersécurité au Sénégal*

OS2: *renforcer la protection des infrastructures d'information critiques (IIC) et les systèmes d'information de l'Etat du Sénégal*

OS3: *promouvoir une culture de cybersécurité au Sénégal*

OS4: *renforcer les capacités et les connaissances techniques en cybersécurité dans tous les secteurs*

OS5: *participer aux efforts régionaux et internationaux de cybersécurité.*

PRINCIPES DIRECTEURS

- Etat de droit
- Responsabilité partagée
- Approche basée sur les risques
- Accès universel au cyberespace et sa pleine exploitation du cyberespace
- Coopération et collaboration entre les parties prenantes

Comment se protéger ? / les bonnes pratiques

D’une manière Générale

- **Conscience et Formation** : La sensibilisation et la formation en cybersécurité sont essentielles. Les utilisateurs et le personnel doivent être formés pour identifier les menaces et comprendre les pratiques de sécurité.

- **Sécurité des Réseaux** : Renforcez la sécurité de vos réseaux avec des pare-feu, des outils de détection d'intrusion, des systèmes de prévention des intrusions, et surveillez en permanence le trafic réseau pour détecter les activités suspectes.

- **Authentification Multifacteur** : L'authentification multifacteur ajoute une couche de sécurité en exigeant deux formes d'authentification pour accéder aux systèmes, ce qui réduit le risque d'accès non autorisé.

D'une manière Générale (Fin)

- **Gestion des Vulnérabilités** : Identifiez et corrigez rapidement les vulnérabilités dans votre infrastructure, en mettant à jour les systèmes et les logiciels.

- **Surveillance Active** : Surveillez activement le réseau et les systèmes pour détecter les menaces, en utilisant des outils de sécurité et des SIEM (Security Information and Event Management).

- **Réponse aux Incidents** : Ayez un plan de réponse aux incidents en place pour réagir rapidement en cas d'attaque. Effectuez des exercices de réponse aux incidents pour vous préparer.

- **Collaboration** : Collaborez avec d'autres organisations, le gouvernement, les organismes internationaux et les acteurs de la cybersécurité pour partager des informations et des données sur les menaces.

L'Afrique: Cas du Sénégal

- **Législation et Réglementation** : Élaborez des lois et réglementations en matière de cybersécurité pour donner une base légale à la lutte contre les APT.

- **Coordination Nationale** : Créez des organismes de coordination nationale de la cybersécurité pour faciliter la collaboration entre les secteurs public et privé.

- **Formation et Sensibilisation** : Investissez dans des programmes de formation et de sensibilisation pour le personnel gouvernemental et le secteur privé.

- **Infrastructure de Défense** : Établissez une infrastructure de défense informatique robuste pour surveiller et protéger les réseaux gouvernementaux et les infrastructures critiques.

- **Partenariats Internationaux** : Collaborez avec d'autres pays africains et des organisations internationales pour partager des informations sur les menaces et les meilleures pratiques.

L'Afrique: Cas du Sénégal

- **Connaissance des Menaces Régionales** : Comprenez les menaces spécifiques à la région africaine, car elles peuvent différer de celles ailleurs dans le monde.

- **Développement de Talents** : Investissez dans la formation et le développement de talents en cybersécurité pour renforcer les compétences locales.

- **Soutien aux Entreprises Locales** : Encouragez le secteur privé local à jouer un rôle actif dans la lutte contre les APT, en les aidant à se conformer aux normes de sécurité.

Merci de votre attention !!!