FORUM NATIONAL SUR LA CYBERSECURITE ET

LA LUTTE CONTRE LA CYBERCRIMINALITE

Organisé par le Ministère des Postes et Télécommunications

Thème :

Protection des Données Stratégiques : enjeux et défis

Intervenant : **Thierry MINKA,** *Ingénieur en Chef d'Informatique*

Bertoua le 10 décembre 2024

Sommaire

1. Introduction

Dans cette présentation, nous essayerons d'utiliser un style simple et épurer, articulé en concepts ; explications ; exemples dans le contexte national ; recommandations.

Commençons par fixer d'entrée de jeu trois points important pour la suite :

- ☑ **Qu'est-ce qu'une données stratégique ?**
- ☑ **Pourquoi la protection des données stratégiques prend autant d'importance ?**
- ☑ **Qu'allons-nous essayer de faire dans cette présentation ?**
- ☑ **Quelques statistiques**

- ☑ On entend par **données stratégiques**, les données essentielles pour la compétitivité, la souveraineté ou la sécurité d'une organisation ou d'un État. Cette définition est large et un peu vague à souhait. Son but est de laisser une certaines flexibilité. En effet, le concept de données stratégique n'est pas figé. Un plan financier, des instruction militaires précises, un itinéraire de convoi, une technologie brevetées etc… peuvent en fonction de leur valeur pour l'entité qui les possède ou les convoite revêtir un caractère stratégique. Pour une entreprise comme la CNPS, un fichier contenant les informations de connexion sur un serveur peut ne pas sembler stratégique au premier abord, mais si je complète l'exemple en disant que ce serveur contient toutes les informations sur les pensionnés (nom, âge, numéro de compte bancaire, lieu de résidence, etc.), là, la catégorisation dudit fichier change du tout au tout, et passe donc à stratégique pour un pirate désireux d'obtenir lesdites informations.

- ☑ Avec la digitalisation accru des différents services, les données sont plus vulnérables aux attaques (interne et externe), cette nouvelle réalité exige une approche proactive pour leur protection. Plus que les autres données, d'usage commun, **la protection des données stratégiques** doit donc être adressée de manière spécifique. Si avant la digitalisation, il suffisait « juste » de bien gérer les accès physiques au bureau dans lequel les dossiers physiques des pensionnés étaient entreposés, avec la digitalisation et donc le passage de ces informations du format papier à celui numérique (fichier Excel disponible sur

un serveur et partagé sur le réseau), la complexité de l'opération c'est accrue de façon exponentielle. En effet, il faudrait à minima, sécuriser l'accès physique au serveur qui contient le fichier, mais aussi « tous » les aspects logiques à ce serveur, et sécuriser ledit fichier lui-même(copie, écriture, lecture).

- ☑ Dans cette présentation**, nous allons essayer** d'explorer les enjeux et défis liés à la protection des données stratégiques, par des exemples concrets et précis. Le personnel de la CNPS s'il y en a dans la salle, va nous pardonner de nous servir de ce cas, emblématique, comme fil conducteur le long de nos échanges.
- ☑ **Quelques statistiques** sur le sujet, produites par IBM :
    - 64 % des entreprises mondiales ont signalé des violations de données stratégiques au cours des 12 derniers mois. Le cas de la CNPS n'est donc pas anecdotique.
    - En 2024, les cyberattaques ont causé des pertes estimées à 10,5 trillions USD.
    - Le coût moyen d'une violation de données stratégiques dépasse 4 millions USD par incident.
    - Deloitte UK, a été victime d'un ransomware, qui a exfiltré plus de 1 Terra Octets de données.

2. Enjeux liés à la protection des données stratégiques

2.1. Les menaces

2.1.1. Menaces anciennes :

Espionnage traditionnel, vols de documents papier, infiltrations internes.

2.1.2. Menaces actuelles :

☑ Cyberattaques sophistiquées (comme dans le cas de la CNPS, ransomware).

☑ Espionnage numérique par des États-nations (APT[1]).

☑ Collecte massive de données par des tiers sans consentement explicite (comme dans le cas de quasiment toutes les plateformes de réseaux sociaux).

2.1.3. 2. Hypothèse des menaces futures :

☑ Cyberattaques basées sur l'IA.

☑ Piratage de données chiffrées à l'aide d'ordinateurs quantiques.

☑ Menaces liées aux technologies émergentes (comme les IoT, et le cloud computing qui restent insuffisamment protégés par les technologies actuelles).

[1] Advanced Persistent Thread

2.2. Impacts

2.2.1. Économiques :

- ☑ La perte d'avantages concurrentiels.
- ☑ L'effondrement de la valeur des actions sur les marchés financiers en cas de fuite d'informations critiques.
- ☑ La perte d'attractivité.
- ☑ Des pertes financières sèches.

2.2.2. Technologiques :

- ☑ Le ralentissement de l'innovation due au vol de secrets industriels.
- ☑ La dépendance accrue à des infrastructures potentiellement compromises.

2.2.3. Réputationnels :

- ☑ La perte de confiance des investisseurs et du public.
- ☑ Des sanctions réglementaires et amendes.

2.2.4. Géostratégiques :

- ☑ Réduction de la capacité de dissuasion militaire en cas de vol de données technologiques.
- ☑ Déséquilibre dans les relations internationales.
- ☑ La perte d'influence.

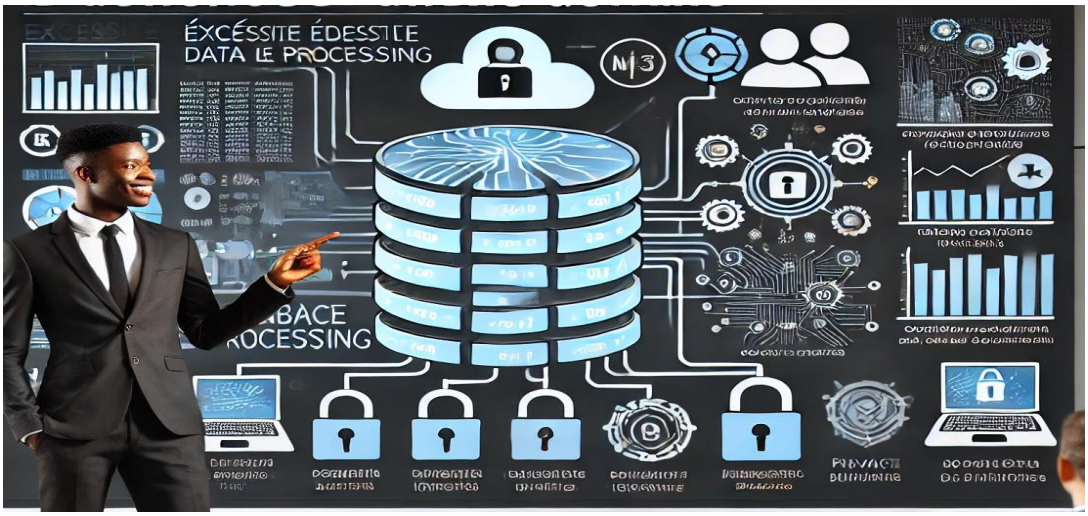
3. Défis liés à la protection des données stratégiques

Dans cette section, nous présentons les défis qui nous semblent les plus importants dans la protection des données stratégiques sous forme de question.

3.1.1. Sécurité des données

- ☑ Comment mette en œuvre des stratégies efficaces de gestion des identités et des accès (IAM Identity and Access Management) ?
- ☑ Comment mettre en œuvre des mécanismes de protection des données qui résistent à la puissance de calcul sans cesses croissante des ordinateurs classiques, et de l'usage de l'informatique quantique ?
- ☑ Comment mettre en œuvre des stratégies de sauvegarde résilientes, prenant en compte, l'indisponibilité d'une alimentation électrique stable, la faible qualité du réseau d'accès et les capacités limités de stockage internes des entreprises ?
- ☑ Comment retenir les talents locaux, et attirer d'autres en cybersécurité ?

3.1.2. Collecte et traitement excessif des données



- ☑ Comment limiter l'exploitation abusive des données collectées.
- ☑ Comment garantir la convergence des politiques de sécurité et autres chartes d'utilisation des TIC dans les entreprises vers le cadre réglementaire national (loi et règlements de la république) et des normes et standards stricts en la matière (RGPD[2], CCPA[3]).

3.1.3. Violation de données

- ☑ Comment prévenir les accès non autorisés aux données ?

[2] Règlement Général pour la Protection des Données
[3] California Consumer Privacy Act. Loi californienne sur la protection des données personnelles, d'application mondiale.

- ☑ Comment détecter et empêcher/stopper les fuite de données massives ou non ?
- ☑ Comment gérer efficacement et dans les délais les plus courts possibles, chaque incident survenu et ainsi en limiter les dégâts ?

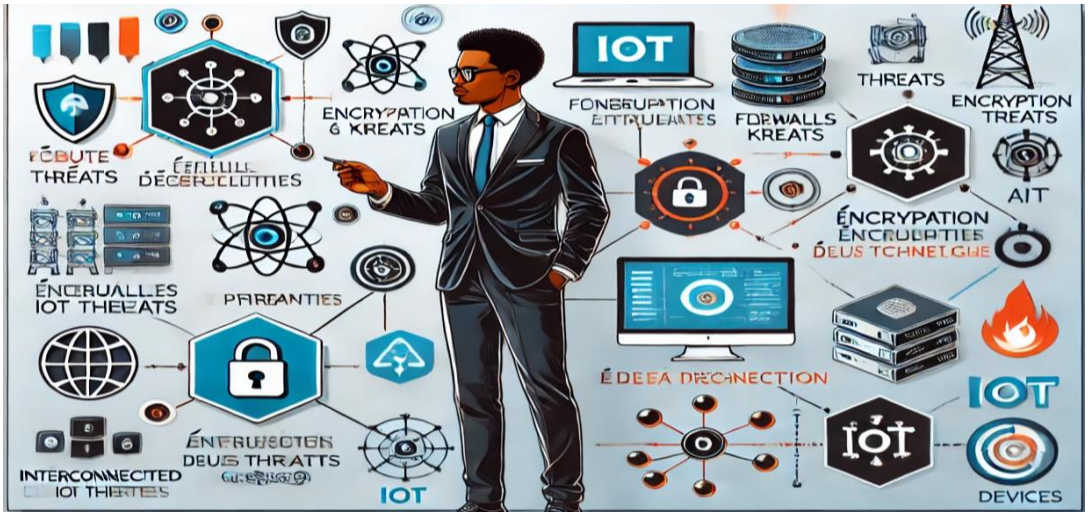
3.1.4. Gouvernance et régulation

- ☑ Comment adopter un cadre législatif et réglementaire national cohérent, à jour et en ligne avec les bonnes pratiques internationales en la matière.
- ☑ Comment mettre en place des politiques internes robustes, internalisant les bonnes pratiques nationales et internationales en la matière ?
- ☑ Comment mettre en place et maintenir une veille juridique efficace en matière de cybersécurité et de lutte contre la cybercriminalité ?

3.1.5. Éthique et vie privée

- ☑ Comment maintenir un équilibre entre exploitation des données et respect des droits des individus.
- ☑ Comment adresser la problématique de l'éthique face au nécessaire contrôle des masse ?

3.1.6. Défis techniques et technologiques



- ☑ Comment se retrouver et choisir parmi les outils de cybersécurité de plus en plus nombreux et complexes ?
- ☑ Comment sécuriser les nouvelles technologies comme les IoT, l'IA, le big data et les réseaux 5G ?

4. Cas pratique : attaque de la CNPS au Cameroun

4.1. Ce qui s'est passé

- ☑ Cyberattaque de type ransomware sur des postes no suffisamment protégés.
- ☑ Vols de données sensibles et demande de rançon importante.

4.2. Raisons de l'incident

De mon point de vue, 3 raisons majeures suffisent à expliquer ce qui s'est passé :

- ☑ Niveau de sécurité non optimal des postes de travail visés ;
- ☑ Limites de la politique de sécurité en place, notamment au niveau des conditions de stockage des données sensibles ;
- ☑ Limites dans la sensibilisation et la culture globale de cybersécurité de l'entreprise.

4.3. Ce qu'il aurait fallu faire

Pour palier les raisons avancées à la section précédentes, il aurait fallu entre autres choses :

- ☑ Mettre un accent sur l'éducation et la sensibilisation des utilisateur à :
  - le téléchargement des pièces jointes ;
  - l'ouverture de pièces jointes ;
  - la navigation sur des sites à contenu spécifique ;

- l'activation de certains liens dans les messages liés aux supposées campagnes promotionnelles et gains sensés êtres faciles/rapides ;
- le transfert de message promotionnels ;
- l'ouverture de contenu privé sur des ordinateurs de service.

☑ Renforcer la sécurité des postes de travail par la définition/relèvement du niveau de sécurité sur les postes de travail des personnel occupant des fonctions ou manipulant des fichier critiques ;

☑ Améliorer la politique de sauvegarde des données critiques/sensibles, en incluant par exemple des mesures comme leur sauvegarde exclusive sur les serveurs (mieux sécurisés que les poste de travail) ;

☑ Améliorer la sensibilisation du personnel aux comportements à risque sur les réseaux.

☑ Améliorer la sécurité du réseau :

- Rajouter des règles sur les équipements de frontière pour interdire l'exfiltration de certaines données ;
- Améliorer le suivi/contrôle des flux à destination et en partance des poste de travail de certains personnels ;

4.4. Recommandations

Les 4 recommandations suivantes me semblent suffisantes et pertinentes, en plus des éléments compris dans la section précédente (ce qu'il aurait fallu faire), pour qu'une telle chose ait probabilité quasi nulle de se reproduire.

☑ Formation continue du personnel (en charge de la sécurité informatique en générale, et de celle du réseau en particulier) à la cybersécurité.

☑ Mise en place de protocoles détaillés de réponse aux incidents.

☑ Audits réguliers et de périodicité aléatoire, des infrastructures et des procédures informatiques.

☑ Certification des systèmes et des personnels clés.

5. Recommandations et conclusion

La protection des données stratégiques devrait être au cœur des priorités des États et des entreprises.

L'évolution rapide des menaces exige des réponses proactives et innovantes. Un équilibre entre innovation technologique et régulation est essentiel pour garantir la sécurité des données stratégiques.

Au terme de cet exposé, nous pouvons formuler quelques recommandations. Certaines relèvent de la mise en place d'un cadre globale par l'Etat, les autres, de l'internalisation des bonnes pratiques par chaque entreprises.

5.1. Solutions techniques :

☑ Chiffrement avancé (quantique, end-to-end).

☑ Sécurisation des infrastructures critiques avec des firewalls de nouvelle génération.

5.2. Solutions organisationnelles :

☑ Mise en place d'un répertoire des infrastructure critiques.

☑ Renforcement de la gouvernance des données.

☑ Veille sécuritaire constante.

☑ Mise en place de plateformes public/privé d'échanges et de collaboration national sur la protection des données.

5.3. Solutions Légale et réglementaires :

☑ Mise en place d'un cadre légal et réglementaire structuré, cohérent et à jour sur la protection des donnée.

☑ Mise en place de mesures réglementaires incitatives et/ou contraignantes pour systématiser la formation continue et le renforcement des capacités des metiers de la sécurité des systèmes d'information.

5.4. Solutions collaboratives :

☑ Coopération avec des agences internationales (INTERPOL, FIRST[4]).

☑ Échange de renseignements avec d'autres organisations du même secteur d'activité.

[4] Forum of Incident Response and Security Team, créé en 1990, il vise à promouvoir la collaboration entre les organisations et les gouvernements pour répondre efficacement aux cybermenaces.

6. Questions/Réponses

7. Références

1. **IBM Security Report 2024** – Analyse des tendances de la cybersécurité.
2. **CNIL** – Rapport annuel sur la protection des données en Europe.
3. **Forbes 2024** – Impacts économiques des violations de données stratégiques.
4. **Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)** – Recommandations sur la cybersécurité.
5. Cybersecurity Ventures. (2023). "Cybercrime Report."
6. Verizon. (2023). "Data Breach Investigations Report."
7. National Institute of Standards and Technology (NIST). (2024). "Cybersecurity Framework."
8. Europol. (2024). "Annual Cybercrime Report."

8. A-propos de l'Intervenant

Thierry MINKA est un professionnel cumulant 19 ans d'expérience professionnelle dont 10 dans la cybersécurité, l'audit des systèmes d'information et l'investigation numérique.

Ingénieur en Chef d'Informatique, il est titulaire d'une quarantaine de certification dont les plus importantes sont :

- ☑ CISA ;
- ☑ CISM ;
- ☑ CGEIT ;
- ☑ CRISC ;
- ☑ CDPSE ;
- ☑ COBIT ;
- ☑ CSX ;
- ☑ ISO 27001 Lead Auditor ;
- ☑ ISO 27001 Risk Manager ;
- ☑ ISO 9001 Lead Auditor ;
- ☑ ISO 9001 Lead Implementor ;
- ☑ ISO 9001 Quality Manager ;
- ☑ ISO 22301Lead Implementor ;
- ☑ ISO 22301 Lead Auditor ;
- ☑ ISO 22301 Risk Manager.

Il enseigne l'Investigation Numérique, l'Audit des Systèmes d'Information et la Sécurité Informatique à l'Ecole Nationale Supérieure Polytechnique de Yaoundé. Par ailleurs il est expert judiciaire en cybercriminalité et investigation numérique près les Tribunaux.

C'est un consultant chevronné qui a déjà notamment travaillé sur des projets pour le compte de la Banque Mondiale, la Commission de l'Union Européenne et la Banque Africaine de Développement. Dans ce cadre, il s'implique principalement dans les problématiques de sécurisation d'infrastructures critiques, de protection de données stratégiques, de développement durable impliquant les technologies, de réduction de la fracture numérique et d'inclusion.

Ecce homo !


Merci de votre aimable attention
12
13
13%
12%
13%