Formation des délégués à la protection des données personnelles (DPO) 2022

Sécurité des données

Emery Kouassi Assogba, PhD

Novotel, Déc 2022

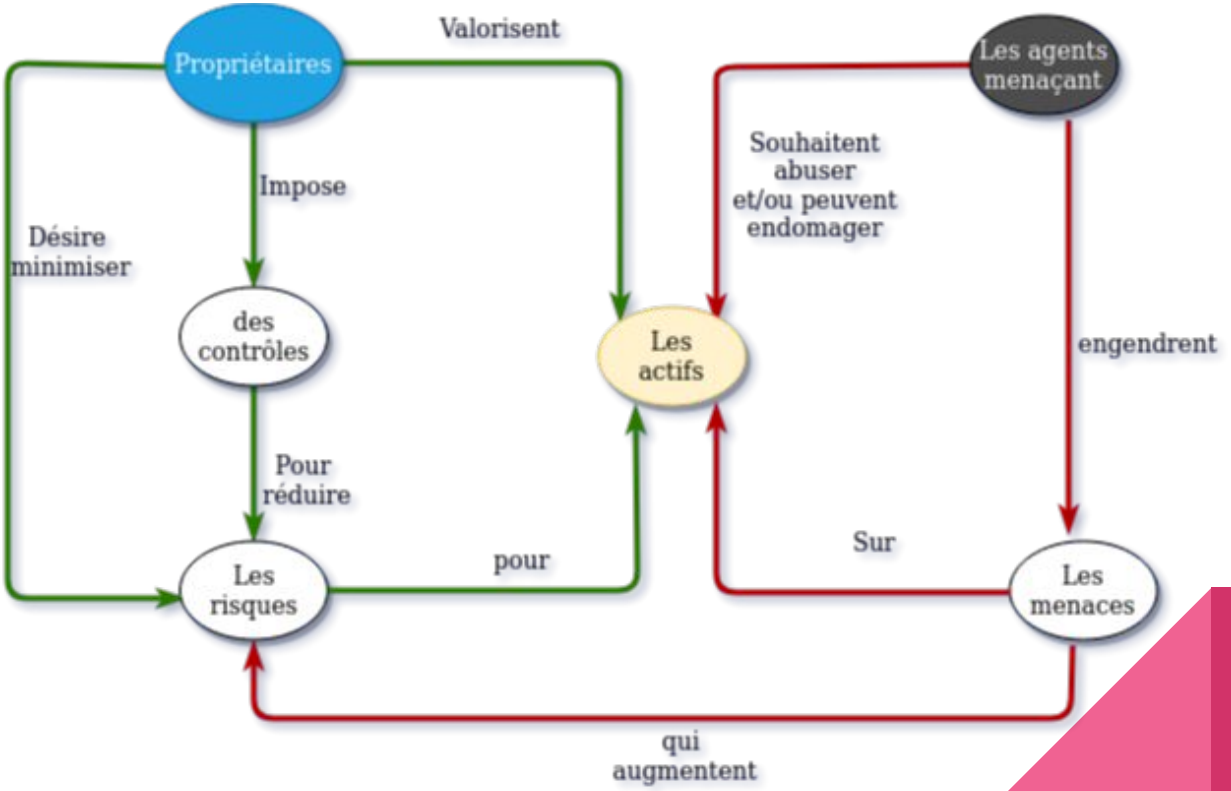
Objectifs de la sécurité informatique

- La confidentialité
- L’intégrité
- La disponibilité
- La traçabilité
- La non-répudiation
- protection de la vie privé

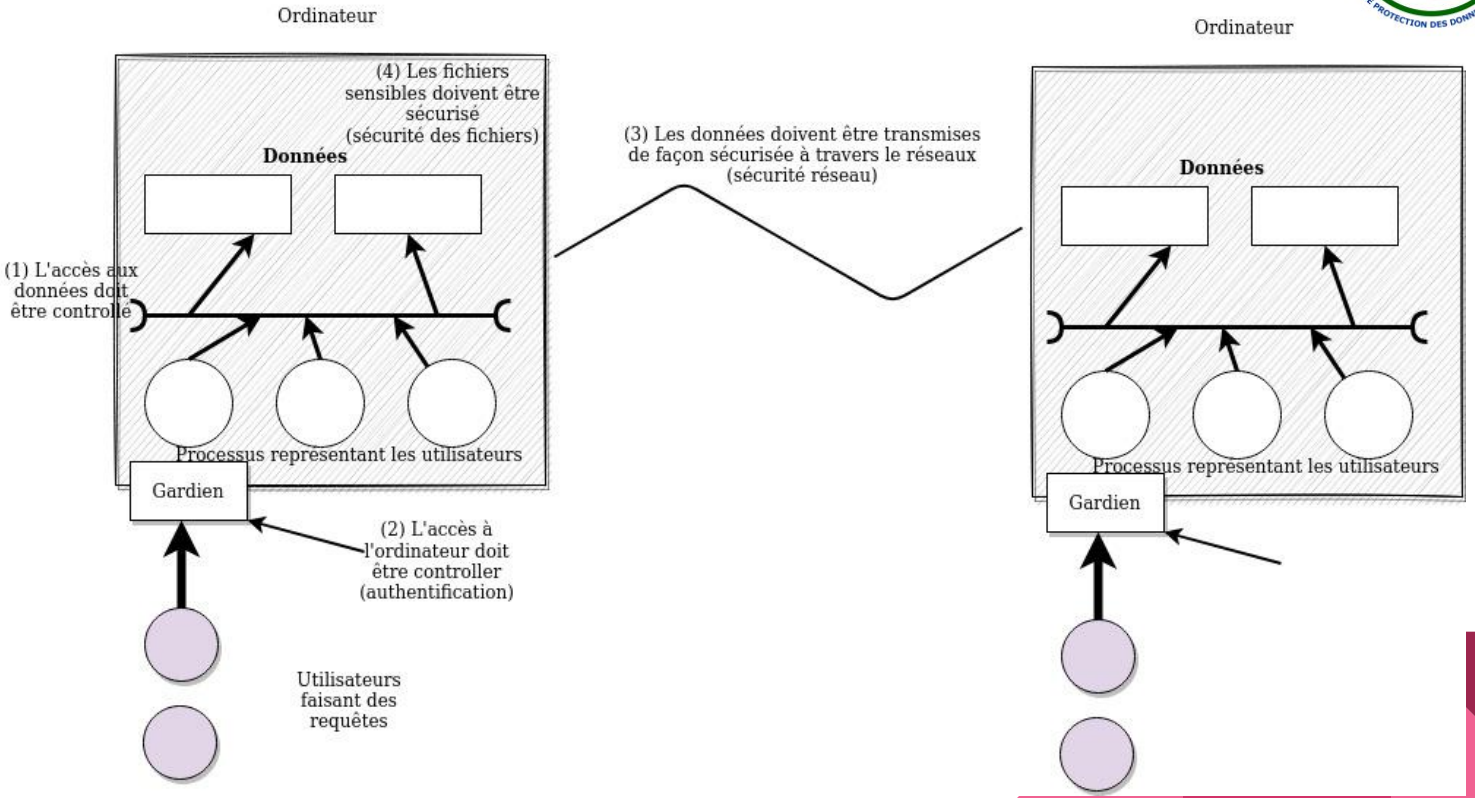
Quelques actualités sur l’exposition des données en 2022

- Coût total des pertes liées à la violation des données : de $4.24 million en 2021 à $4.35 million en 2022 soit une augmentation de 2.6%
- Plusieurs grandes entreprises touchées dont:
  - établissements publics et collectivités territoriales françaises en région normandie (9 décembre 2022)
  - Uber (16 Septembre 2022)
  - Des hôpitaux en France
  - Plus récent, la commune d’Anvers en Belgique

Concepts et relation de sécurité



Périmètre de la sécurité informatique



Pourquoi ?

Données

- mots de passe,
- numéros de carte de crédit,
- dossiers médicaux,
- informations personnelles
- et secrets commerciaux

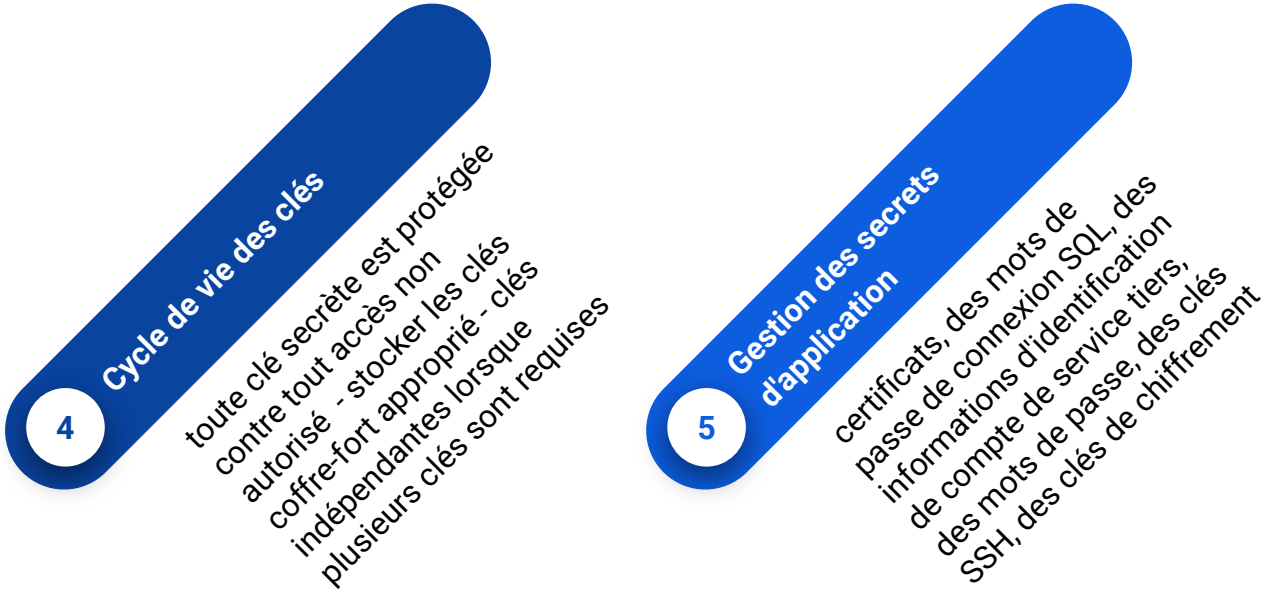
nécessitent une protection supplémentaire, en particulier si ces données relèvent des lois sur la confidentialité

- Loi du numérique au Bénin
- APDP au Bénin
- PSSIE

Comment ?

1. **Classification des données**
   - Niveaux de sensibilité - Mapper chaque catégorie de données aux règles de protection nécessaires pour chaque niveau de sensibilité.
2. **Chiffrer/Tokenizer les données en transit**
   - **TLS - k2view**
3. **Chiffrer les données au repos**
   - Eviter de stocker des données sensibles - Données sensibles protégées par la cryptographie d'une manière ou d'une autre

Comment?


4
Cycle de vie des clés
toute clé secrète est protégée contre tout accès non autorisé - stocker les clés coffre-fort approprié - clés indépendantes lorsque plusieurs clés sont requises
5
Gestion des secrets d'application
certificats, des mots de passe de connexion SQL, des informations d'identification de compte de service tiers, des mots de passe, des clés SSH, des clés de chiffrement

Des standards

- PSSIE
- Code du numérique au Bénin
- PCI DSS

Code du numérique au Bénin

- Cryptologie : LIVRE SIXIEME - TITRE III - CHAPITRE I

- L'ANSSI est en charge de la cryptologie, conformément aux dispositions de l'article 617 du présent code (Article 606)

- L'ANSSI-BÉNIN désigne en son sein une commission chargée de la cryptologie en République du Bénin, ci-après désignée la «commission cryptologie». (Article 615)

Aide-mémoire OWASP : Stockage cryptographique

- Définir le modèle de menace
- Où appliquer le chiffrement (application - base de données - système de fichiers - matériel)
- Minimiser le stockage des information sensible (**l'idéal ne pas les stocker**)
- Algorithmes
  - AES min 128 bits - 256 bits
  - ECC (Curve25519) ou RSA-2048 bits
  - Eviter les algorithmes personnalisés
- Mode de chiffrement
  - Mode sécurisé GCM CCM

https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Che .html

Aide-mémoire OWASP : Stockage cryptographique

Langage	Fonctions dangereuses	Fonctions cryptographiquement sécurisées
C	random(), rand()	getrandom(2)
Java	java.util.Random()	java.security.SecureRandom
PHP	rand(), mt_rand(), array_rand(), uniqid()	random_bytes(), random_int() in PHP 7 or openssl_random_pseudo_bytes() in PHP 5
Python	random()	secrets()
Node.js	Math.random()	crypto.randomBytes, crypto.randomInt, crypto.randomUUID

https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Che eet.html

Aide-mémoire OWASP : Protection de la couche transport

- Prendre en charge que les protocoles solides
  - TLS 1.3 ou TLS 1.2
  - bannir TLS 1.1
- Ne prendre en charge que les algorithmes de chiffrement forts
  - De préférence seul les chiffrements CGM doivent être activés
  - Bannir Null ciphers - Anonymous ciphers - EXPORT ciphers
- Utiliser des paramètres Diffie-Hellman forts
  - 2048 bits
- Désactiver la compression
- Mettre à jour les librairies crypto
- HTTP Strict Transport Security
- Tester la configuration du serveur

https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection[illegible]Sheet.html

Aide-mémoire OWASP : Stockage des mots de passe

- Hasher au lieu de chiffrer les mots de passe
- Concepts de stockage de mot de passe
  - Salt
  - Peppering
  - Work Factors
- Bannir
  - MD5 - SHA-1

https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_S[illegible]

Gestion des secrets

- Secret : login/mot de passe, Credentials de la BD, Jetons d'API, Credentials TLS - Certificats - Clé cryptographique
- Cycle de vie des secrets
  - Où sont-ils ?
  - Qui les utilise ?
  - Quand les révoquer?
- Gestion centralisée
  - Coffre fort

Outils

- SSLyze - Bibliothèque d'analyse de configuration SSL et outil CLI
- SSLLabs - Service gratuit pour scanner et vérifier la configuration TLS/SSL
- TruffleHog - Recherches de secrets publiés accidentellement
- KeyWhiz - Gestionnaire de secrets
- Hashicorp Vault - Gestionnaire de secrets