USCB15 - Sécurisation avancée des données

Mis à jour le 21-01-2025

Code : USCB15

Unité spécifique de type mixte

3 crédits

Responsabilité nationale :
EPN05 - Informatique / Nicolas PIOCH

Contact national :

Cnam Centre Régional de Bretagne

Zoopôle Les Croix
2 rue Camille Guérin
22440 Ploufragan
0 972 311 312
Isabelle Guée
bzh_master_cybersecurite@lecnam.

Présentation

Objectifs pédagogiques

Description :

Il est crucial de détecter ou d'empêcher des accès non autorisés dans des environnements critiques ou stratégiques afin d'assurer la sécurité des données pour en maintenir la confidentialité, l'intégrité et la disponibilité. Cette sécurité est d'autant plus critique que les données des entreprises et des individus sont de plus en plus stockées dans le Cloud. Cette U.S. aborde le problème de la protection des données lors du stockage, mais aussi au moment du transfert ainsi que des traitements afin de diminuer la connaissance de fournisseur de service de stockage, ou de limiter les impacts d'un vol de données.

Objectifs pédagogiques :

Ce cours présente les nouveaux enjeux de sécurités des données critiques face à la recrudescence des attaques et des modes de stockages et de traitements externalisés. Il s'agit de présenter les problématiques liées aux données (locales ou déportées dans le cloud), connaître différents éléments de protections des données en fonction de son état (transport, stockage ou traitement).

Compétences

Compétences acquises :

- Connaître les risques relatifs aux données
- Connaître différents mécanismes de protection des données en fonction de leurs états
- Mettre en application les compétences techniques protection des données

Savoirs :

- Modèles de contrôle d'accès, solutions par chiffrements, TEE, TPM, chiffrement homomorphe, blockchain

Programme

Contenu

- Introduction à la sécurisation des données
  - Risques relatifs aux données
  - Réglementation sur la sécurité des données
  - Spécificités et menaces des Clouds
  - Risques de fuites de données
- Réduction du risque
  - Minimisation des données
  - Suppression
  - Masquage
  - Définition d'une politique de sécurité
- Protection de la donnée transportée
  - Protection des échanges
  - Détection des fuites de données (Data Loss Prevention)
- Protection de la donnée stockée
  - Chiffrement appliqué aux données dans le cloud
  - Modèles de gestion des clés (modèles HSM, KMS, BYOK, CASB)
  - Principe de la Tokennisation
  - Modèles de contrôle d'accès aux données
  - Sécurisation du stockage
- Protection de la donnée utilisée
  - Calcul multipartite sécurisé
  - Chiffrement homomorphe
  - Trusted Execution Environment

    - Trusted Platform Module
- Blockchain et stockage des données
    - Principes des blockchains
    - Intégrité, performances, stabilité
    - Problème du stockage arbitraire de données

Modalités de validation

- Examen final

Description des modalités de validation

Examen de 2 heures