USCB2A - Contrôle d'accès et Gestion des Identités Numériques

Mis à jour le 12-03-2026

Code : USCB2A

Unité spécifique de type mixte

5 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.n

Présentation

Prérequis

Bac+2 informatique, BAC + 2 SI ou SHS
RSX112
L2 ou Bac+2

Il est conseillé de suivre CYB102 avant CYB105.

De bonnes bases en OS Linux (Debian ou RedHat) et en virtualisation (VirtualBox) sont nécessaires pour suivre cette UE.

Objectifs pédagogiques

- Comprendre les concepts fondamentaux de la gestion des identités et du contrôle d'accès
- Identifier les réglementations et normes en vigueur
- Maîtriser les différentes méthodes et modèles de contrôle d'accès
- Appliquer les technologies et protocoles d'authentification
- Déployer et gérer des solutions IAM adaptées aux environnements d'entreprise et cloud
- Reconnaître et contrer les menaces liées à la gestion des identités
- Appréhender le cycle de vie de l'identité numérique
- Mettre en œuvre les meilleures pratiques pour sécuriser les accès et identités numériques

Compétences

- Capacité à concevoir et mettre en place des politiques de gestion des identités et des accès
- Maîtrise des outils et technologies IAM (Microsoft Active Directory, Okta, Ping Identity, Keycloak, LemonLDAP::NG, …)
- Implémentation de protocoles d'authentification sécurisés (OAuth, OpenID Connect, SAML, MFA)
- Gestion des accès dans des environnements multi-cloud et hybrides
- Sensibilisation et formation des utilisateurs aux bonnes pratiques de sécurité

Programme

Contenu

1. Introduction au Contrôle d'Accès et à la Gestion des Identités

- Définitions et concepts fondamentaux
- Enjeux de la gestion des identités et des accès
- Réglementations et conformités (RGPD, NIST, ISO 27001, etc.)

2. Méthodes et Modèles de Contrôle d'Accès

- Modèle basé sur les listes de contrôle d'accès (ACL)
- Modèle RBAC (Role-Based Access Control)
- Modèle ABAC (Attribute-Based Access Control)
- Contrôle d'accès basé sur les rôles et politiques d'entreprise

3. Technologies et Protocoles d'Authentification

- Authentification simple vs. forte : MFA (authentification multi-facteurs), 2FA (2 facteurs)
- Protocoles d'authentification (OAuth2, OpenID Connect, SAML, CAS)
- Mécanismes d'authentification (Radius, Kerberos, etc.)
- Gestion des mots de passe et alternatives (biométrie, authentification adaptative)

4. Gestion des Identités et des Accès (IAM - Identity and Access Management)

- Cycle de vie des identités (création, gestion, révocation) et norme Supann
- Solutions IAM : Microsoft Active Directory, Okta, Ping Identity, Keycloak, LemonLDAP::NG
- Gouvernance des identités et gestion des privilèges

5. Gestion des Accès dans les Environnements Cloud et Hybrides

- IAM dans le Cloud : AWS IAM, Azure AD, Google IAM
- Gestion des accès à l’échelle de l’entreprise
- Concepts de Zero Trust et de Least Privilege

6. Menaces et Attaques sur l’Identité et les Accès

- Phishing et vol d’identifiants
- Attaques par force brute et credential stuffing
- Attaques internes et compromission des privilèges

7. Meilleures Pratiques et Stratégies de Sécurisation

- Mise en place d’une politique de gestion des identités et accès
- Surveillance et détection des anomalies
- Automatisation et gestion des identités avec l'IA

8. Études de Cas et Travaux Pratiques

- Configuration d’une solution IAM en environnement test
- Implémentation d’une authentification multi-facteurs (MFA)
- Audit et gestion des accès dans une organisation

Modalités de validation

- Contrôle continu
- Projet(s)
- Examen final

Description des modalités de validation

- Contrôle continu + TP
- Examen final