PARTIE III
Contrôle d'Accès

- Principes et Définitions
- Menaces
- Types de Contrôle d 'Accès
- Modèles de Contrôle d'Accès
- Surveillance et Administration

Principes et Définitions

- L'**ACCÈS** : définit le flux d'information circulant entre un **SUJET** et un **OBJET**. (consultation d'une donnée, exécution d'un programme, écriture d'un fichier, mais aussi ouverture d'une porte, utilisation d'un appareil spécifique, etc.).
- Un **SUJET** est une entité active (utilisateur, programme, processus, appareil, etc.) sollicitant l'accès à un objet.
- Un **OBJET** est une entité passive (fichier, base de données, programme, processus, appareil, etc.) à laquelle un sujet tente d'accéder.
- Les **CONTRÔLES D'ACCÈS** sont une collection de mécanismes qui, mis en œuvre conjointement, permettent d'assurer la protection des actifs informationnels de l'entreprise contre les accès non autorisés.

Principes et Définitions

- Les contrôles d'accès donnent au gestionnaire de la sécurité les moyens de :
  - Spécifier quels utilisateurs peuvent accéder aux ressources contenues dans un système d'informations
  - Spécifier à quelles ressources en particulier ils peuvent avoir accès
  - Spécifier quelles opérations ils peuvent effectuer sur ces ressources
  - Conserver une trace des accès effectués

Menaces

Les menaces auxquelles doit faire face un système de contrôle d'accès sont multiples et de diverses natures. En voici quelques exemples :

- **Menaces informatiques directes**
  - Déni de Service (ping de la mort, attaque par rebond, saturation de serveur par SYN flood, DDoS ou déni de service distribué, etc.)
  - Logiciels non autorisés ou malveillants (virus, vers, chevaux de Troie, bombes logiques, code mobile type ActiveX ou Applet Java ou email frauduleux, etc.)
  - Attaques externes du réseau (par force brute ou dictionnaire, scan de ports, spoofing, etc.)
  - Failles logicielles (débordement mémoire, porte dérobée, canal caché)
- **Menaces physiques**
  - Accès physique non autorisé aux données (récupération des poubelles, écoute du réseau, shoulder surfing, etc.)
  - Capture des émissions d'ondes électromagnétiques
  - Perturbations des communications
  - Perturbations des fournitures d'énergie
- **Menaces internes, ingénierie sociale**
  - Employés mécontents ou indélicats (vol de données, espionnage, vol d'identité, destruction de données, etc.)
  - Employés peu précautionneux ou naïfs (hameçonnage, communication ou affichage de mot de passe, communication de données classifiées, etc.)

Types de Contrôle d 'Accès

- Pour rappel, les contrôles d'accès sont un ensemble de moyens permettant aux gestionnaires de la sécurité d'assurer la **disponibilité**, **l'intégrité** et la **confidentialité** des actifs informationnels. Ces moyens sont classés dans trois catégories : Moyens **organisationnels,** Moyens **opérationnels et** Moyens **techniques.**

- Les contrôles d'accès sont aussi caractérisés par leur type :

  - Contrôles **directifs** : politique de sécurité, normes et standards, règlement intérieur, tous moyens informant le personnel d'une entreprise du comportement à adopter pour protéger les actifs informationnels contre les accès non autorisés.
  - Contrôles **préventifs** ou dissuasifs : mesures physiques, administratives et techniques instaurées pour prévenir les accès non autorisés au système d'information.
  - Contrôles de **détection** : pratiques, procédures et outils dont le but est de détecter, d'identifier et si possible de réagir à des tentatives d'accès frauduleux au système d'information.
  - Contrôles **correctifs** : contre-mesures physiques, administratives et techniques conçues pour réagir à des incidents de sécurité, de façon à réduire ou éliminer la possibilité d'une nouvelle occurrence de l'incident.
  - Contrôles de **récupération** : mesures de remise en état du système d'information suite à l'occurrence d'un incident de sécurité.

Types de Contrôle d 'Accès

Moyens Organisationnels - Exemples de contrôles :

	Contrôles Directifs	Contrôles Préventifs	Contrôles de Détection	Contrôles Correctifs	Contrôles de Récupération
Moyens Organisationnels	•Politiques •Directives	•Processus d'inscription des utilisateurs •Processus d'approbation des utilisateurs •Clauses de confidentialité •Séparation des pouvoirs •Bannière d'avertissement	•Vérification des journaux d'accès •Permutation obligatoire des postes •Investigations •Audits	•Sanctions •Mises à pied •Procédures de licenciement pour faute	•Plan de continuité des activités (PCA) •Plan de la reprise d'activité après sinistre (PRA)

Types de Contrôle d 'Accès

Moyens Opérationnels et Physiques - Exemples de contrôles :

	Contrôles Directifs	Contrôles Préventifs	Contrôles de Détection	Contrôles Correctifs	Contrôles de Récupération
Moyens Opérationnels et physiques	•Procédures	•Barrières physiques •Verrous et serrures •Système de badges •Vigile de sécurité •Portes à sas •Procédures d'embauche efficaces •Programme de sensibilisation	•Gardiens, surveillance des accès •Détecteurs de mouvement •Vidéo-surveillance	•Modification des comportements des utilisateurs •Modification des barrières physiques	•Reconstruction •Site de secours

Types de Contrôle d 'Accès

Moyens Techniques - Exemples de contrôles :

	Contrôles Directifs	Contrôles Préventifs	Contrôles de Détection	Contrôles Correctifs	Contrôles de Récupération
Moyens Techniques	•Normes et standards	•Moyens d'authentification •Authentification multi-facteurs •ACL •Pare-feux •Système de prévention des intrusions (IPS) •Chiffrement	•Journalisation des accès et des transactions •Conservation des journaux •Messages SNMP •Système de détection des intrusions (IDS)	•Isolation des systèmes •Blocage des connections •Modification et mise à jour des droits d'accès trop permissifs	•Utilisation des sauvegardes •Récupération des fonctions système •Reconstruction de données

Identification - Authentification

- Les contrôles d'accès déterminent **QUI** a accès à **QUOI**, **COMMENT**, **OÙ** et **QUAND** tout en conservant la trace des accès effectués ou rejetés.

- L'**Identification** et l'**Authentification** vont déterminer le QUI,
- l'**inventaire** et la **classification** des actifs vont fournir le QUOI,
- l'**Autorisation** va définir le COMMENT, le OÙ et le QUAND.
- La **Traçabilité** (ou **Imputabilité**) va permettre de conserver des enregistrements de l'ensemble des accès ou tentatives d'accès.

- **Identification :** c'est une méthode dont l'objectif est d'établir **l'identité** d'un sujet (utilisateur, programme, processus, etc.).
- Idéalement, l'**Identifiant** d'un sujet est unique, respecte une nomenclature établie, n'est pas descriptif d'une autre propriété telle que fonction ou métier, et fait l'objet d'une procédure d'attribution sécurisée et documentée.

- **Authentification :** c'est une méthode dont l'objectif est de **prouver** qu'un sujet est bien celui qu'il prétend être, donc qu'il est le porteur légitime d'un identifiant donné. C'est la clé de voûte de tout système de contrôle d'accès, puisque c'est le mécanisme qui va permettre à un utilisateur de bénéficier à l'intérieur du système d'information des droits liés à l'identité qu'il va porter.

Facteurs d'authentification

- En matière d'authentification de personnes, il existe trois grandes catégories ou facteurs d'authentification :
  - Ce que l'on **CONNAÎT**, par exemple, mot de passe, phrase de passe, code PIN, en général une donnée statique de type chaîne de caractères.
  - Ce que l'on **POSSÈDE**, par exemple clé, badge, carte magnétique, jeton RFID.
  - Ce que l'on **EST**, au moyen de mesures biométriques, telles que reconnaissance des empreintes digitales, de la voix, de l'image rétinienne, des contours du visage ou de la main, etc.
- ***Principe*** :

  « Utiliser non pas ce que l'utilisateur sait,
  mais ce qu'il a ou ce qu'il est »

- **Authentification forte :** c'est généralement une méthode qui combine plusieurs facteurs, par exemple une carte à puce et son code PIN combine la connaissance du code PIN et la possession de la carte.

Ce que l'on connaît

- Le **mot de passe** couplé à un **code utilisateur** (Userid) est la forme la plus commune d'authentification basée sur la connaissance d'une information. C'est aussi celle qui est considérée comme la plus faible.
- Cependant, si c'est la seule méthode d'authentification possible ou disponible sur un système, il est alors important d'imposer un certain nombre de règles et bonnes pratiques de gestion des mots de passe :

- **Protection et contrôle d'accès.**
  - Éviter la transmission en clair, par exemple en imposant des pages de login chiffrées par HTTPS.
  - Restreindre l'accès au fichier ou à la base de données des mots de passe et en assurer le chiffrement par un algorithme solide.
  - Limiter le nombre de tentatives autorisées par blocage après un seuil, ou pénalité de temps exponentielle.

- **Structure du mot de passe**
  - Longueur minimale imposée.
  - Complexité imposée, par exemple mélange obligatoire de minuscules, majuscules, chiffres et caractères spéciaux.
  - Usage interdit de mots couramment trouvés dans un dictionnaire, des informations personnelles…

- **Maintenance du mot de passe**
  - Expiration automatique, par exemple changement obligatoire tous les 30 jours ou 60 connexions.
  - Historique, par exemple obligation de choisir un nouveau mot de passe différent des 12 derniers.
  - Fréquence, pas plus d'un changement autorisé par jour.
  - Une phrase de passe (**Passphrase**) est aussi une séquence de caractères, mais généralement plus longue qu'un mot de passe. Elle est donc plus difficile à acquérir par un attaquant, mais également plus facile à retenir par l'utilisateur qu'un mot de passe long et complexe, car elle peut être une suite de mots présentant un sens pour lui ou elle (vers de poésie, citation, liste d'objets ou de lieux, etc.)

Ce que l'on possède

- La possession d'un objet particulier est aussi un moyen d'authentification, par exemple :
  - Un badge, une pièce d'identité,
  - Une clé physique,
  - Une carte à puce, à piste ou à mémoire,
  - Un "token" ou autre objet générateur de mot de passe à usage unique
  - Etc.
- Les principales faiblesses de ce mode ou facteur d'authentification tiennent dans la nature de l'objet utilisé.
  - Si l'objet peut facilement être reproduit, alors la valeur même de l'authentification par cet objet est mise en cause.
  - Si l'objet est volé, alors le voleur peut se faire passer pour le porteur légitime.
  - Si l'objet est perdu ou oublié par l'utilisateur, alors celui-ci n'a plus accès au système, bien qu'il puisse légitimement y prétendre.
  - Le déploiement en masse peut s'avérer coûteux, notamment du point de vue de la logistique.

Ce que l'on est

- Ce mode d'authentification exploite le caractère réputé unique d'une ou plusieurs propriétés physiques de l'être humain.
- Cette exploitation s'accomplit au moyen de techniques dites **biométriques**, mesurant et analysant des caractéristiques telles que :
  - Empreinte digitale
  - Voix (reconnaissance vocale)
  - Forme de la main
  - Forme du visage (reconnaissance visuelle)
  - Image rétinienne
  - Iris
  - Signature dynamique (forme, accélération, vitesse, pression, parcours)
- Les principaux écueils rencontrés lors de la mise en œuvre de techniques biométriques sont :
  - Ajustement du système pour obtenir des taux acceptables de faux négatifs et faux positifs
  - Aspect invasif souvent mal perçu par les utilisateurs
  - Équipement coûteux
  - Procédure d'enrôlement des utilisateurs complexe
- Les systèmes biométriques fiables nécessitent souvent une surveillance sur leur mise en œuvre, par exemple pour vérifier qu'une tentative d'imitation n'est pas en cours, et sont donc réservés aux environnements nécessitant une haute sécurité justifiant les coûts associés.

Authentification forte ou multi-facteurs

- Une technique permettant aisément d'obtenir un niveau suffisamment fiable d'authentification consiste à combiner l'usage de plusieurs facteurs, on parle alors d'authentification forte ou d'authentification multi-facteurs (en anglais MFA ou 2FA).

- La technique la plus connue en France est la **carte à puce** lorsqu'elle est employée pour effectuer un paiement sur un Terminal de Paiement Électronique (TPE). En effet, pour que le paiement soit accepté, l'utilisateur doit insérer sa carte bancaire et ensuite entrer son **code PIN**, il s'agit donc d'une authentification à 2 facteurs :
  - Ce que l'on possède, une carte bancaire à puce, réputée impossible à reproduire
  - Ce que l'on connaît, le code PIN réputé connu du seul porteur

- Il est intéressant de noter que les autres usages de la carte bancaire, par exemple lors de paiements en ligne, ne présente pas ce même niveau de sécurité, puisque seule la connaissance des informations inscrites en clair sur la carte permet d'effectuer un paiement.
- C'est pour pallier à cette faiblesse que de nombreuses banques ont mis en place un contrôle supplémentaire par envoi d'un SMS sur le téléphone portable du titulaire de la carte (système 3D Secure).

Authentification forte ou multi-facteurs

- Une autre mise en œuvre très populaire d'un système d'authentification multi-facteurs consiste en l'usage de "***tokens***" générateurs de mots de passes dynamiques, connus sous le nom d'**OTP** (One Time Password).
- Ces objets (**facteur possession**), contenant en général un processeur cryptographique et une clé secrète unique, vont permettre à l'utilisateur d'obtenir une séquence de chiffres (souvent de 6 à 8) formant un nombre pseudo-aléatoire. Il ou elle va pouvoir présenter ce nombre au système hôte sur lequel il se connecte soit en remplacement, soit en complément du mot de passe usuel (**facteur connaissance**).
- Le mot de passe généré par ces *tokens* est à usage unique et l'algorithme cryptographique utilisé pour le générer rend sa prédiction extrêmement improbable.
- Cette solution a donc pour avantage de combler les principales faiblesses du mot de passe statique tout en étant compatible en termes d'interface utilisateur, ce qui est la raison principale de son succès (plusieurs centaines de millions en service dans le monde).

Autorisation

- L'autorisation est le mécanisme qui va décider si un sujet, préalablement identifié et authentifié, va pouvoir obtenir l'accès qu'il demande sur un objet, c'est-à-dire une ressource du système d'information elle aussi correctement identifiée.

- Le mécanisme de contrôle d'accès, généralement situé au cœur d'un système, va prendre sa décision d'accorder ou de refuser l'accès demandé par le sujet en s'appuyant sur un ensemble de règles.

- La construction et l'utilisation de ces règles sont définies par un modèle de contrôle d'accès, répondant à un choix ou un impératif de sécurité.

- Les différents modèles de contrôle d'accès seront détaillés dans ce qui suit.

Traçabilité ou Imputabilité

- C'est un dispositif indispensable dans tout système de contrôle d'accès, car il permet de conserver d'une part la trace des accès effectués dans le cadre des autorisations accordées, mais aussi et surtout la trace des tentatives d'accès refusées.

- Le premier type de trace est souvent appelé piste d'audit, car il va permettre de reconstituer l'ensemble des actions effectuées par un utilisateur lors de son passage dans le système d'information.

- Le second type de trace est quant à lui une source précieuse d'information pour détecter les tentatives d'intrusion ou d'accès frauduleux.

Modèles de Contrôle d'Accès

- Les modèles de contrôle d'accès vont essentiellement définir d'une part la façon dont les administrateurs vont pouvoir concevoir les règles de contrôle d'accès, mais également les propriétés utilisées par le mécanisme de contrôle pour prendre sa décision d'autoriser ou de refuser l'accès d'un sujet à un objet.
- Ces propriétés seront par exemple :
  - Type d'action possible sur l'objet (accès simple, lecture, écriture, mise à jour, suppression, exécution, etc.),
  - Classification de l'objet,
  - Habilitation du sujet,
  - Contexte de l'accès à l'objet (provenance du sujet, date et heure de l'accès, chemin de l'accès, programme ou transaction en cours d'exécution, etc.),
  - Appartenance du sujet à un groupe ou à un rôle donné,
  - Etc.

Modèles de Sécurité

- Un certain nombre de modèles de sécurité ont été théorisés par la recherche et les institutions.
- Sauf exception, ces modèles sont rarement appliqués strictement dans les systèmes de contrôle d'accès, on retrouve plus souvent des mises en œuvre hybrides plus adaptées à la réalité des besoins des entreprises et/ou des sous-systèmes considérés.
- Le choix entre les différents modèles est en général guidé par l'objectif principal recherché : confidentialité, intégrité, adaptabilité, souplesse de gestion, etc.
- Quel que soit le modèle, le principe de sécurité fondamental devrait être que *ce qui n'est pas explicitement autorisé doit être interdit*.
- Dans la réalité des implémentations, ce principe n'est pas toujours bien respecté.
- Les principaux modèles théoriques sont :
  - MAC ou Mandatory Access Control
  - DAC ou Discretionary Access Control
  - Rule-set Based Access Control
  - Role Based Access Control

MAC (Mandatory Access Control)

- Dans ce modèle à usage essentiellement militaire, les possibilités d'accès sont prédéterminées par l'adéquation entre la classification des objets et l'habilitation des sujets.
- Les deux modèles MAC théoriques les plus connus sont le modèle **Bell-LaPadula** qui se préoccupe uniquement de confidentialité et le modèle **Biba** qui lui se focalise sur l'intégrité.
- L'usage de ces modèles impose une labellisation de tous les objets et l'affectation d'un ou plusieurs niveaux d'habilitation à tous les sujets.
- Il est aussi important de noter que ces modèles permettent d'éviter la déclassification accidentelle des objets.
  - Par exemple, un sujet agissant avec une habilitation "secret" pourra lire des objets de niveau "secret" ou "confidentiel" mais pas "très secret". Par contre, il pourra créer ou modifier des objets de niveau "secret" ou "très secret" mais pas "confidentiel" car il risquerait alors de déclassifier une information.
- L'accès aux objets d'un même niveau de classification peut également être différencié par l'attribution d'une catégorie en plus du label, qui permet d'effectuer un découpage horizontal en plus du découpage vertical apporté par les labels.

DAC (Discretionary Access Control)

- Dans un système basé sur le contrôle d'accès discrétionnaire (DAC), c'est le propriétaire d'un objet qui décide qui établit les règles donnant des droits d'accès à certains sujets.

- Ce modèle est ainsi nommé car les contrôle des accès est établi à la discrétion du propriétaire.

- L'implémentation la plus connue du modèle DAC est le système d'**ACL** (**Access Control List**) des systèmes de fichiers, où le propriétaire d'un fichier décide des droits d'accès qu'il souhaite accorder aux membres de son groupe et à l'ensemble des utilisateurs.

Rule-set Based Access Control

- Ce modèle est base sur des jeux de règles ne s'appuyant pas forcément sur une identification individuelle des sujets, mais portant plutôt sur des aspects généraux ou des circonstances particulières.

- C'est ce modèle qui est prioritairement mis en œuvre dans un pare-feu qui filtre au niveau des paquets, avec des règles du type "tout paquet entrant sur le port 22 est interdit".

Role Based Access Control

- Ce modèle se base sur la définition de **rôles** et de **droits** d'accès attachés à l'exercice de ce rôle.
- Les rôles sont ensuite affectés aux sujets, qui de ce fait héritent des droits d'accès associés au rôle.
- C'est ce modèle qui est le plus souvent rencontré en entreprise, où les droits d'accès aux actifs informationnels sont étroitement liés au métier ou à la fonction exercée par un individu.
- Il présente l'avantage de simplifier la gestion des droits, notamment lorsqu'un nouvel employé arrive dans un service et a besoin des mêmes droits d'accès que ses collègues.
- Il permet à un ou plusieurs administrateurs de la sécurité de définir un ensemble de règles dans un référentiel de type annuaire, par exemple Active Directory.

Exemples pratiques

Matrice d'autorisation :

- Selon le modèle MAC (Mandatory Access Control)

objets

utilisateurs	F1	F2	Imp1	A	F3
Jules	R	R	W		R
Joseph	RW	R		R	
Caroline	W	X	W		
Tiburce	RX	R	W		
Géraldine	W	W	W	W	W

- ➔ Inconvénient majeur : matrice énorme et creuse

Exemples pratiques

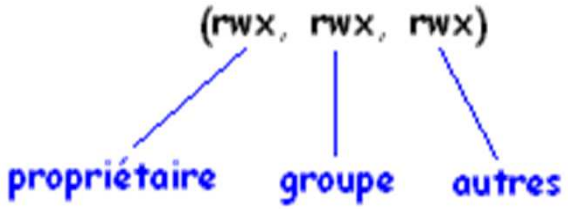
Access Control List ou ACL : selon le medèle DAC (Discretionary Access Control), consiste à stocker les colonnes de la matrice d'autorisation en ne gardant que les éléments non nuls.

- Représentation sous la forme : (uid, gid, droits).
- **Exemples**
  - 3 groupes (gid) : Système, Enseignant, Etudiant
  - 4 utilisateurs (uid) : Jules, Henri, Consuela, Marcel
  - 5 fichiers : F0, F1, F2, F3, F4, F5
    - F0 : (Jules, *, RWX)
    - F1 : (Jules, systeme, RWX)
    - F2 : (Jules, *, RW-)(Henri, Enseignant, R--)(Marcel,*,R--)
    - F3 : (*, Etudiant, R--)
    - F4 : (Consuela, *, -W-)(*, Etudiant, R--)
  - * = joker

Exemples pratiques

Unix : reprise du principe ACL d'une manière plus simplifiée

- 3 groupes d'utilisateurs :
  - le propriétaire
  - le groupe
  - les autres
- Pour chaque objet :



r = read, w = write, x = execute représenté par 0(interdit) ou 1(permis) ➔ possibilité de codage en octal sur 3 chiffres.

- Exemple :
  - **F (rwx,rw-,r--) = (111,110,100) =764**
  - le propriétaire peut lire, écrire, exécuter
  - le groupe peut lire et écrire mais pas exécuter
  - les autres peuvent seulement lire

- La commande **chmod** pour modifier ces droits

Exemples pratiques

- **Liste de capacité ou C-List** selon le modèle **Role Based Access Control**,
- Le stockage de la matrice des autorisations s'effectue par ligne.

processus n°123 →

type	droits	objets
0 fichier	R--	-> F3
1 fichier	RWX	-> F4
2 fichier	RW-	-> F5
3 imprimante	-W-	-> Imp1

- On peut rajouter des droits **génériques** :
  - Créer une nouvelle capacité
  - Copier un objet
  - Retirer une capacité
  - Détruire un objet

Application

- Confronter les méthodes de contrôle d’accès (matrices d’autorisation, ACL, Unix et C-list) aux situations suivantes :
  - a) Salah désire que ses fichiers soient lisibles par quiconque sauf Salim.
  - b) Mohamed et Ali souhaitent partager seulement entre eux l'accès total à quelques fichiers.
  - c) Sami désire que certains de ses fichiers soient publics.

Centralisé et Décentralisé/Distribué

- L'administration des contrôles d'accès peut donc se trouver dans un référentiel **unique et central** auquel tous les composants en charge du contrôle effectif des accès font appel.
- C'est le plus souvent le cas lorsque l'environnement technique du système d'information est **homogène et géographiquement concentré**.

- Par contre, dès lors que cet environnement est **hétérogène**, il devient impossible d'utiliser un mécanisme ou service unique pour l'administration et le contrôle des accès.
- On utilise alors une **architecture décentralisée** dans laquelle par exemple les sujets/utilisateurs et leur affectation à des rôles ou privilèges sont gérés à un niveau centralisé, puis l'attribution des droits d'accès aux objets/ressources liés à ces rôles ou privilèges est quant à elle gérée sur chacune des plateformes où résident les ressources.

- Ce découplage présente l'avantage d'avoir des administrateurs de la sécurité multiples et spécialisés, donc plus efficaces chacun dans leur domaine, mais aussi l'inconvénient d'être une source potentielle de discordance de droits entre les plateformes.
- L'administration décentralisée impose donc contrôles de cohérence et des audits plus nombreux afin de vérifier la bonne mise en œuvre de la politique de sécurité à tous les niveaux du système d'information.

Centralisé et Décentralisé/Distribué

- Les systèmes de gestion décentralisée sont souvent couplés avec des mécanismes de **Single Sign On (SSO)** permettant de gommer la complexité technique de l'architecture de sécurité du point de vue de l'utilisateur.
- Le plus connu est le système **Kerberos**, qui est aujourd'hui le mécanisme sous-jacent à Active Directory, mais existait depuis les années 90 dans les environnements distribués Unix.
- Un autre exemple plus adapté aux environnements très hétérogènes et issu du projet européen **SESAME** (Secure European System for Applications in a Multi-vendor Environment) est la solution de l'éditeur Evidian (anciennement Bull) initialement nommée AccessMaster.

Surveillance et Administration

- Le fonctionnement effectif des contrôles d'accès doit faire l'objet d'une surveillance permanente afin de vérifier son bon fonctionnement.

- Pour cela, une analyse attentive des journaux d'accès est nécessaire.

- Le résultat de l'analyse des journaux par les administrateurs va souvent avoir pour conséquence une mise à jour des règles de contrôle d'accès.

➔ Détection et Protection contre les Intrusions

➔ Mise à l'Épreuve et Audit

Détection et Protection contre les Intrusions

- Dans un système complexe, l'analyse des événements de sécurité est prise en charge par des outils automatisés qui vont permettre d'une part de **détecter** les intrusions ou tentatives d'intrusion, d'autre part d'essayer de les **prévenir**, en modifiant dynamiquement les règles de certains mécanismes contrôles d'accès.

Système de Détection des Intrusions (IDS)

- C'est un système à base d'outils de surveillance **passifs**, qui peuvent être placés au niveau du réseau ou sur les serveurs.
  - Sur le réseau, ces outils vont passivement **surveiller** et **analyser** les flux transmis,
  - Sur le réseau et/ou sur les serveurs, ils vont **rechercher** des signatures ou des motifs (*patterns*) connus, ou encore des anomalies par rapport à des scenarii de fonctionnement normal,
  - Sur les serveurs, ils vont analyser les signatures (MD-5 ou SHA-xxx) des fichiers afin de détecter tout changement.

Détection et Protection contre les Intrusions

Système de Prévention des Intrusions (IPS)

- Un système de prévention des intrusions effectue les mêmes analyses de trafic réseau que l'IDS, mais il a un rôle **actif**.
- Pour cela, il est installé en coupure sur les points d'entrée du réseau de l'entreprise.
- On peut voir un IPS comme un pare-feu capable **d'adapter** dynamiquement ses règles en fonction des indications fournies par son cœur IDS.

- Par exemple, s'il détecte une utilisation jugée anormale d'un protocole particulier, il va dynamiquement adaptées les règles de routage liées à ce protocole pour dévier les paquets suspects vers un point où ils pourront être mis en quarantaine ou analysés.
- L'objectif est de **détecter** et **prévenir** les attaques, en évitant ainsi leurs conséquences pour la sécurité du système d'information.
- Une difficulté majeure dans la mise en œuvre d'un IPS est d'éviter les faux positifs, qui viendraient alors perturber le fonctionnement des utilisateurs légitimes.

Mise à l'Épreuve et Audit

- Une autre méthode de validation du bon fonctionnement du système de contrôle d'accès consiste en la conduite d'audits et de mises à l'épreuve du système de contrôle d'accès, en général au moyen de tests d'intrusion.

Les Audits de Sécurité

- Ils ont pour objectif de vérifier la conformité du système de contrôle d'accès par rapport au référentiel que constituent :
  - La politique de sécurité de l'entreprise,
  - L'analyse des risques et les décisions de gestion des risques qui en sont issues,
  - Les normes et standards retenus par l'entreprise, ainsi que les obligations légales et/ou réglementaires.
- Ce type d'audit ne teste donc pas la qualité ou l'efficience intrinsèque des mesures de sécurité prises, mais il vérifie qu'à minima ce qui a été décidé est véritablement mis en œuvre, correctement géré et exploité.

- Il existe aussi d'autres types d'audit qui font en général suite à un ou plusieurs incidents de sécurité, dont le but est de remonter la **piste d'audit** afin de retrouver, de comprendre et si possible de corriger ce qui a permis la survenance de ces incidents.

Mise à l'Épreuve et Audit

Mise à l'Épreuve et Audit

- Contrairement aux audits qui sont passifs vis à vis du contrôle d'accès et interviennent à posteriori, les mises à l'épreuve du système de contrôle d'accès ont pour objectif de simuler des scenarii d'attaque afin de trouver des failles potentielles dans la mise en œuvre des mesures de sécurité déjà actives.

- On trouve plusieurs variantes et une gradualité dans la nature de ces tests :
  - Tests internes, non intrusifs,
  - Tests externes, tests d'intrusion coordonnés avec la cible,
  - Tests d'intrusion non coopératifs,

- La conduite de ces tests et notamment les tests non coopératifs demande une certaine prudence car, afin d'être réellement probants, ils se conduisent sur un système de production.
- L'équipe de **Pen Testers** doit donc être prête à mettre fin à son action si elle détecte que les tests risquent de mettre en péril le fonctionnement normal du système.
- Il est aussi très important que le résultat de ces tests reste strictement confidentiel afin de ne pas surexposer l'entreprise cible tant que les mesures correctives nécessaires n'ont pas été prises.