Version provisoire

RÉSUMÉ THÉORIQUE – FILIÈRE INFRASTRUCTURE DIGITALE

M107 – SÉCURISER UN SYSTÈME D'INFORMATION

45 heures

SOMMAIRE

MODALITÉS PÉDAGOGIQUES

1

LE GUIDE DE SOUTIEN

Il contient le résumé théorique et le manuel des travaux pratiques

2

LA VERSION PDF

Une version PDF est mise en ligne sur l'espace apprenant et formateur de la plateforme WebForce Life

3

DES CONTENUS TÉLÉCHARGEABLES

Les fiches de résumés ou des exercices sont téléchargeables sur WebForce Life

4

DU CONTENU INTERACTIF

Vous disposez de contenus interactifs sous forme d'exercices et de cours à utiliser sur WebForce Life

5

DES RESSOURCES EN LIGNES

Les ressources sont consultables en synchrone et en asynchrone pour s'adapter au rythme de l'apprentissage

Copyright - Tout droit réservé - OFPPT

PARTIE 1

DÉCOUVRIR LES NOTIONS DE BASE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (SI)

Dans ce module, vous allez :

- Découvrir les notions de base de la sécurité
- Identifier et classifier les attaques de sécurité d'un système d'information

11 heures

CHAPITRE 1

CONNAÎTRE LES CONCEPTS DE BASE DE LA SÉCURITÉ INFORMATIQUE

Ce que vous allez apprendre dans ce chapitre :

- Mettre l'accent sur l'importance de la sécurité dans un SI
- Comprendre la terminologie de la sécurité informatique
- Définir les objectifs et les propriétés de la sécurité informatique

4 heures

CHAPITRE 1

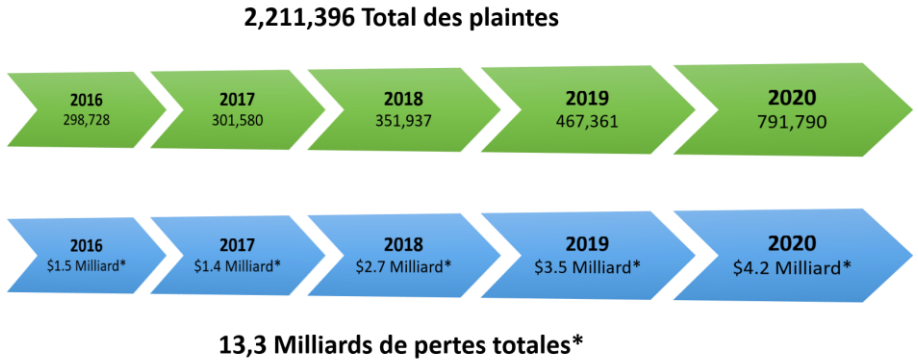
CONNAÎTRE LES CONCEPTS DE BASE DE LA SÉCURITÉ INFORMATIQUE

1. **Importance de la sécurité dans les SI**
2. Terminologie et définitions
3. Objectifs et propriétés de la sécurité
4. Quiz sur les notions de base de la sécurité informatique

Importance de la sécurité dans les SI

- De nous jours, les organisations comptent beaucoup sur l'utilisation des nouvelles technologies afin d'acquérir une meilleur efficacité et productivité dans l'exécution de leurs tâches quotidiennes. En effet, l'utilisation des équipements informatiques (tel que les ordinateurs, les supports de stockages, etc.), des systèmes d'information (tel que les systèmes d'information opérationnels, les systèmes d'aide à la décision, les systèmes de gestion, etc.), et du réseau Internet sont devenus primordiaux dans la plupart de organisations.
- Cependant, les nouvelles technologies, plus particulièrement Internet, exposent leurs utilisateurs à plusieurs attaques de sécurité. En plus des technologies (informatique, internet, et ses services) qui évoluent en parallèle avec les attaques de sécurité et leurs diversifications.

- La figure suivante illustre les statistiques annuelles et agrégées pour les plaintes et les pertes financières depuis l'année 2016 jusqu'à 2020. Au cours de cette période, Internet Crime Complaint Center (IC3) a reçu un total de 2 211 396 plaintes, faisant état d'une perte de 13,3 milliards de dollars.
- Ces statistiques illustrent l'augmentation du nombre des plaintes chaque année. Notamment, il est possible de remarquer que le nombre de plaintes a presque doublé en 2 ans (de 2018 à 2020).



Statistiques des plaintes reçues par IC3
Source: **Rapport Annuel 2020 de IC3**

PARTIE 1

Copyright - Tout droit réservé - OFPPT

Importance de la sécurité dans les SI

- Un système d'information contient généralement toutes les **informations sensibles** d'une entreprise, y compris les informations relatives à son fonctionnement, sa clientèle, ses produits, etc.
- Certaines attaques de sécurité visant les systèmes d'information peuvent causer une suppression, altération, falsification, ou diffusion des informations sensibles dont elles effectuent leurs traitements. Ce qui pourrait induire plusieurs risques graves à l'entreprise tel que pertes financières, perte de la confiance de sa clientèle, perte de son image de marque, etc.
- Par conséquent, la protection des systèmes d'information contre les attaques de sécurité est **primordiale**.
- La protection des systèmes d'information et leurs résistances aux attaques de sécurité permet à leur entreprise de :

  Garantir la protection des informations sensibles ;

  Assurer la continuité de ses activités et par conséquent préserver la confiance de ses clients ;

  Se protéger contre les risques potentiels.

Copyright - Tout droit réservé - OFPPT

CHAPITRE 1

CONNAÎTRE LES CONCEPTS DE BASE DE LA SÉCURITÉ INFORMATIQUE

1. Importance de la sécurité dans les SI
2. **Terminologie et définitions**
3. Objectifs et propriétés de la sécurité
4. Quiz sur les notions de base de la sécurité informatique

Classification de la sécurité

- La sécurité fait référence à l'ensemble des outils, méthodes, et/ou techniques permettant de protéger des actifs contre des dommages potentiels et le rendre sûr.
- Différentes classes de sécurité peuvent être distinguées :

La sécurité de l'information : adresse la protection des informations (ou des données) dans **tous les processus de traitement de l'information** contre les dommages potentiels tel que la falsification, la suppression, ou la diffusion de l'information aux entités non autorisés.

La sécurité physique : se réfère au **contrôle de l'accès physique aux ressources matérielles et/ou logicielles** et à leurs protections contre les dommages physiques et le vol, grâce à l'utilisation des outils et/ou techniques de défense.

La sécurité informatique : adresse **la protection d'un système informatique** par la prévention, la détection et la réduction des conséquences des actions non autorisées exécutées par les utilisateurs (autorisés et/ou non autorisés). Elle adresse également la protection de l'information durant son traitement et son stockage.

La sécurité des communications : consiste à protéger :

- Les systèmes informatiques **connectés à un réseau de communication** (tel que le réseau internet).
- Les informations circulant **dans un réseau informatique** contre les dommages potentiels.

La sécurité opérationnelle : consiste à **protéger les opérations d'une organisation** pour empêcher les dommages potentiels visant les informations sensibles échangés (ou traités) durant une opération.

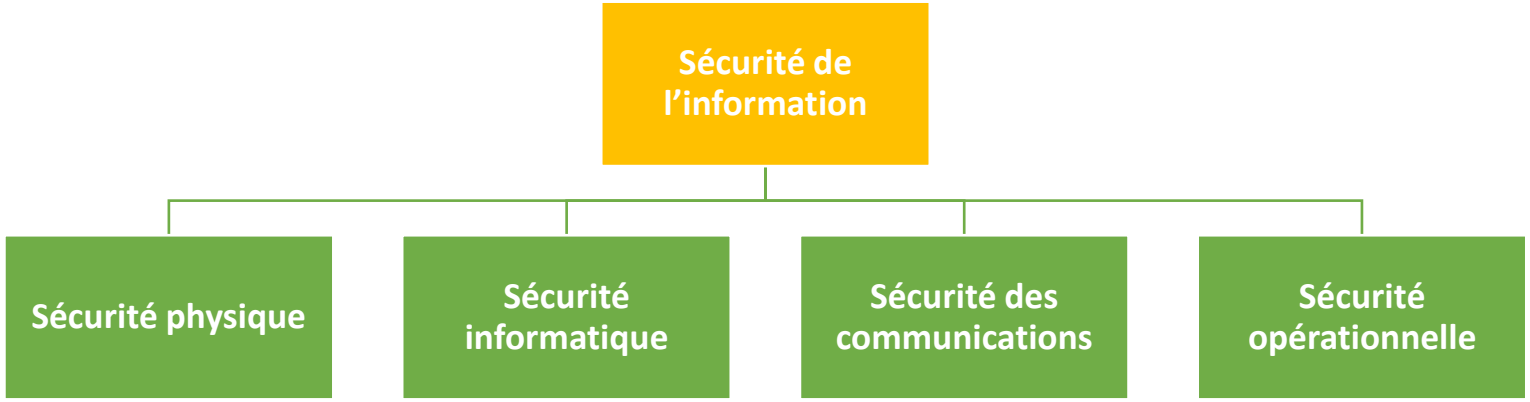
La sécurité opérationnelle se réfère à la mise en place des mesures de sécurité suite à un processus de gestion de risques.

Un processus de gestion de risque analyse les opérations d'une organisation du point de vue pirate, pour identifier les risques de sécurité.

Copyright - Tout droit réservé - OFPPT

Classification de la sécurité

- Partant des définitions précédentes, il est possible de noter que les quatre classes de sécurité (sécurité physique, sécurité informatique, sécurité des communications, et sécurité opérationnelle) sont indispensables pour assurer la sécurité de l'information. Par conséquent, ces quatre classes de sécurité peuvent être considérées comme sous-classes de la sécurité de l'information, comme illustré dans la figure suivante.



Les classes de la sécurité de l'information

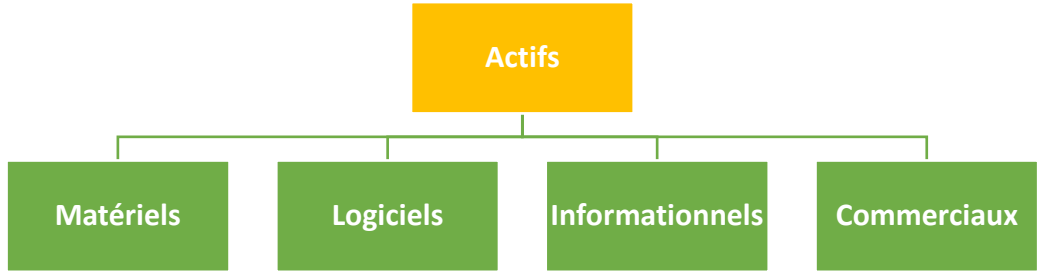
Copyright - Tout droit réservé - OFPPT

PARTIE 1

Actifs

- Un actif se réfère à tout ce qui a de la valeur pour une entité (une organisation ou une personne) et qui nécessite donc d'être protégé par des mesures de sécurité.
- Un actif peut être définit comme un bien, ayant la forme d'une donnée, appareil, ou composant, qui pourrait être consulté, utilisé, divulgué, détruit et/ou volé de manière illicite et entraîner une perte.
- Différent types d'actifs peuvent être distingués :
    - **Actifs matériels** : Ce sont les biens matériels qui exécutent des tâches spécifiques et/ou fournissent des produits. Les actifs matériels incluent des serveurs physiques, des postes de travail, des supports amovibles, des équipements de réseau, etc…
    - **Actifs logiciels** : Ce sont les bien logicielles qui exécutent des tâches de traitement des informations pour les transformer sous formes de données prêtes à être utilisées. Les actifs logiciels incluent les applications, les systèmes d'exploitation, les logiciels de virtualisation, les systèmes de gestion de base de données, les systèmes d'aide à la décision, etc…
    - **Actifs informationnels** : Ce sont les biens qui sont liés directement aux informations ou à leurs stockages, tels que les bases de données, les systèmes de fichiers, les informations de routage, etc…
    - **Actifs commerciaux** : Ce sont les autres biens d'une organisation qui ne rentrent pas dans les trois types d'actifs précédents (c.à.d., matériels, logiciels, et informationnels). Les actifs commerciaux incluent le capital humain, la réputation, l'image de l'organisation, etc…

Les types d'actifs



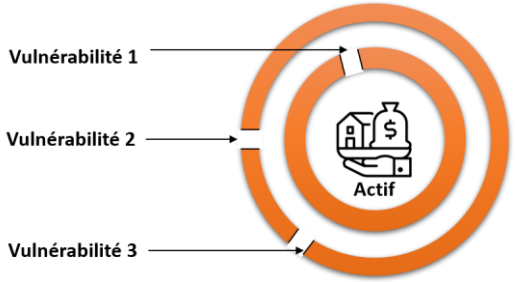
Copyright - Tout droit réservé - OFPPT

PARTIE 1

Vulnérabilité, Menace et Attaque

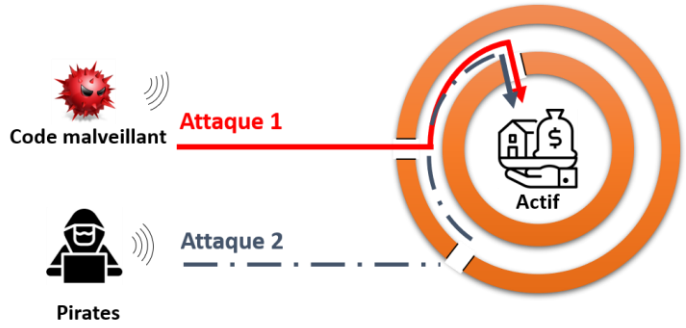
- **Vulnérabilité** : La faiblesse d'un actif (ou d'une ressource) l'expose à des menaces internes et externes pouvant entraîner des défaillances ou des violations. Les faiblesses peuvent être inhérentes à la conception, à la configuration, ou à la mise en œuvre d'un actif. Les mauvaises pratiques lors de l'utilisation d'un actif, tel que l'utilisation des mots de passes faibles pour accéder à cet actif, peuvent être aussi des sources de faiblesses.

Les vulnérabilités



- **Menace** : Un potentiel de violation de la sécurité qui pourrait exploiter une ou plusieurs vulnérabilités d'un actif pour l'endommager.

- **Attaque** : Une action ou un évènement non autorisée délibérée sur un actif pour causer son dysfonctionnement ou l'altération de l'information qu'il stocke.



Copyright - Tout droit réservé - OFPPT

Acteur de menace, Victime, Risque et Contre-mesures

- **Acteur de menace (Agent de menace)** : Une entité qui exécute et réalise une action de menace. Un agent de menace peut être :

  une personne ou groupe de personnes qui sont souvent des employés de l'entreprise ou des pirates ;

  un programme malveillant tel que les virus ; ou

  la nature lorsque la menace réalisée est une menace naturelle comme les tempêtes ou les inondations.

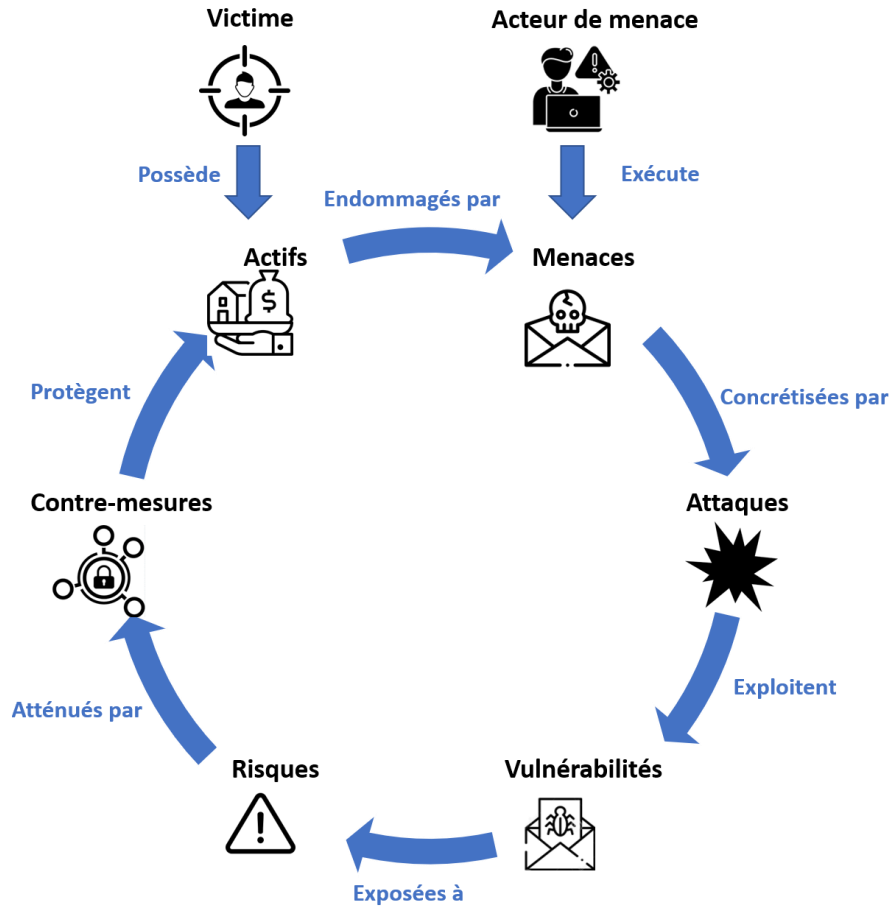
- **Victime** : La cible d'une attaque de sécurité. Elle est généralement une entité (une personne, groupe de personnes, organisations) qui possède un ou un ensemble d'actifs menacés par des attaques de sécurité.
- **Risque** : Une mesure qui évalue la combinaison du niveau de la gravité des conséquences de l'apparition d'une attaque de sécurité et la probabilité d'occurrence associée (c.à.d., la probabilité qu'une menace particulière exploite une vulnérabilité donnée).
- **Mesures de sécurité (Contre-mesures)** : Les techniques, méthodes, et/ou outils permettant la détection, la prévention ou la récupération des attaques de sécurité.

Copyright - Tout droit réservé - OFPPT

PARTIE 1

Terminologie et relations

- La figure suivante illustre les relations entre les différents termes qui ont été présentés précédemment. Ces relations sont détaillées ci-après
- Un acteur de menace exécute des menaces, qui sont généralement concrétisées par un ensemble d'attaques de sécurité, en exploitant des vulnérabilités.
- Les actifs qui souffrent de la présence des vulnérabilités sont exposés à des risques potentiels.
- Pour protéger les actifs contre les menaces de sécurité et atténuer les risques potentiels, il est possible de mettre en place un ensemble de mesures de sécurité (contre-mesures).
- Une victime est la cible d'une attaque. Elle possède des actifs qui pourraient être endommagés par des menaces de sécurité



Relations et terminologie de la sécurité

Copyright - Tout droit réservé - OFPPT

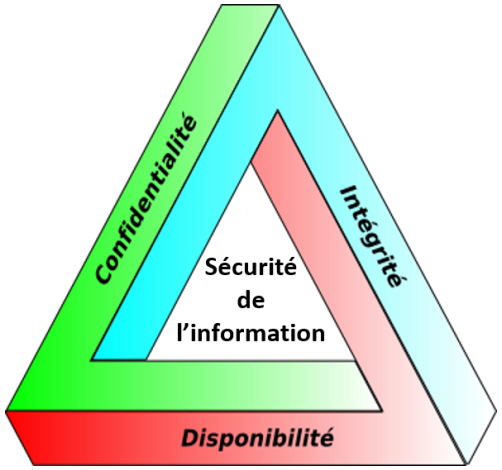
CHAPITRE 1

CONNAÎTRE LES CONCEPTS DE BASE DE LA SÉCURITÉ INFORMATIQUE

1. Importance de la sécurité dans les SI
2. Terminologie et définitions
3. **Objectifs et propriétés de la sécurité**
4. Quiz sur les notions de base de la sécurité informatique

Disponibilité, Intégrité, Confidentialité (DIC)

- Pour assurer la sécurité de l'information, au moins les trois principaux objectives de la sécurité (souvent appelés triade DIC), que sont la disponibilité, l'intégrité et la confidentialité, doivent être atteints. La définition de ces trois objectives est fournie par la suite :
    - **Disponibilité** : exige qu'une ressource soit disponible et/ou fonctionnelle lorsqu' une entité autorisée la demande ;
    - **Intégrité** : exige que les actifs n'ont pas été modifié, détruit, falsifié, ou perdu d'une manière non autorisée ou accidentelle ;
    - **Confidentialité** : exige que les données ne soient pas divulguées aux entités à moins qu'elles n'aient été autorisées à accéder et à connaitre ces données.
- Lorsqu'un objectif de sécurité est assuré, il est souvent appelé propriété de sécurité.



La triade DIC pour la sécurité de l'information

Lien source

PARTIE 1

Copyright - Tout droit réservé - OFPPT

Liste exhaustive des objectives de sécurité

- Une liste exhaustive d'objectifs relatifs à la sécurité de l'information comprend, en plus des objectives DIC, les éléments suivants :
    - **Authenticité** : exige d'être authentique et de pouvoir être vérifié, et digne de confiance. En d'autres termes, l'authenticité exige de vérifier que les identités fournies par les entités (utilisateurs ou processus) demandant accès à une ressource ne sont pas fausses et que ces entités sont bien ce qu'elles prétendent être ;
    - **Contrôle d'accès**: exige que l'accès à un actif ou une ressource soit contrôlée pour assurer que l'accès n'est possible que pour les entités autorisées ;
    - **Non-répudiation** : exige que les entités participantes à un évènement ou exécutant une action (tel que l'échange des messages , l'exécution des transactions, etc.) ne peuvent pas nier leur participation à cet évènement, ou l'exécution de cette action, respectivement. Cet objectif pourrait être atteint, en exigeant aux entités de fournir une preuve d'identité avant de participer à un évènement ou exécuter une action ;
    - **Traçabilité** : exige de suivre les actions exécutées par une entité durant son accès à un actif et de journaliser des informations décrivant les actions exécutées (tel que la durée d'accès, la nature des actions, les données utilisées, etc.) et que les actions exécutées peuvent être attribuées uniquement à cette entité, qui peut alors être tenue responsable de ses actions

Copyright - Tout droit réservé - OFPPT

CHAPITRE 1

CONNAÎTRE LES CONCEPTS DE BASE DE LA SÉCURITÉ INFORMATIQUE

1. Importance de la sécurité dans les SI
2. Terminologie et définitions
3. Objectifs et propriétés de la sécurité
4. **Quiz sur les notions de base de la sécurité informatique**

01 - Connaître les concepts de base de la sécurité Informatique

Quiz sur les notions de base de la sécurité informatique

PARTIE 1

Énoncé

- **Question 1 : Quelle est la propriété de sécurité qui garantie qu'un actif est accessible uniquement aux entités autorisées ?**
  - ❑ La confidentialité
  - ❑ L'intégrité
  - ❑ La disponibilité
  - ❑ L'authenticité
- **Question 2 : Quelle est la propriété de sécurité qui consiste à assurer qu'un actif devra répondre aux demandes des entités autorisées ?**
  - ❑ La confidentialité
  - ❑ L'intégrité
  - ❑ La disponibilité
  - ❑ L'authenticité
- **Question 3 : Un agent de menace peut être :**
  - ❑ Un employé
  - ❑ Un logiciel malveillant
  - ❑ Un pirate
  - ❑ Toutes les réponses sont correctes
- **Question 4 : Toutes les informations sensibles d'une organisation (tel que chiffre d'affaires, clientèle, produits, etc.) peuvent être considérées comme actif ?**
  - ❑ Vrai
  - ❑ Faux

Copyright - Tout droit réservé - OFPPT

Correction

- **Question 1 : Quelle est la propriété de sécurité qui garantie qu'un actif est accessible uniquement aux entités autorisées ?**
  - ◙ La confidentialité
  - ❑ L'intégrité
  - ❑ La disponibilité
  - ❑ L'authenticité
- **Question 2 : Quelle est la propriété de sécurité qui consiste à assurer qu'un actif devra répondre aux demandes des entités autorisées ?**
  - ❑ La confidentialité
  - ❑ L'intégrité
  - ◙ La disponibilité
  - ❑ L'authenticité
- **Question 3 : Un agent de menace peut être :**
  - ❑ Un employé
  - ❑ Un logiciel malveillant
  - ❑ Un pirate
  - ◙ Toutes les réponses sont correctes
- **Question 4 : Toutes les informations sensibles d'une organisation (tel que chiffre d'affaires, clientèle, produits, etc.) peuvent être considéré comme actif ?**
  - ◙ Vrai
  - ❑ Faux

Copyright - Tout droit réservé - OFPPT

CHAPITRE 2

IDENTIFIER LES ATTAQUES DE SÉCURITÉ VISANT UN SI

Ce que vous allez apprendre dans ce chapitre :

- Classifier les attaques de sécurité et les hackers
- Présenter les attaques internes et les attaques externes
- Mettre l'accent sur le besoin de l'identification des vulnérabilités

7 heures

CHAPITRE 2

CONNAÎTRE LES CONCEPTS DE BASE DE LA SÉCURITÉ INFORMATIQUE

1. **Classification des attaques et des hackers**
2. Attaques internes
3. Attaques externes
4. Besoin d’identification des vulnérabilités

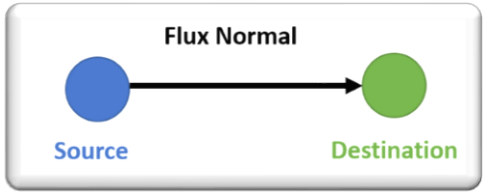
Classification des pirates

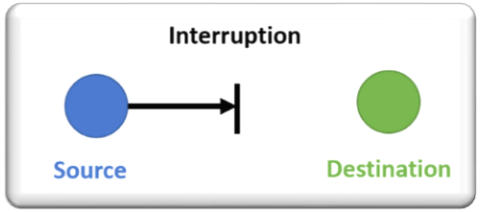
- Différents types de pirates peuvent être distingués selon leurs **niveau d'expertises** et/ou leurs intentions, lors de l'exécution des attaques :
    - **Les White hat hackers (les pirates chapeau blanc)** : ce sont souvent des **experts en sécurité** qui explorent en profondeur les systèmes d'information, afin de **découvrir les vulnérabilités** des ses systèmes et de les reporter aux responsables afin de les améliorer.
    - **Les Black hat hackers (les pirates chapeau noir)** : ce sont des pirates, qui ont des **mauvaises intentions** et dont la principale motivation est de **nuire aux systèmes d'information visés**
    - **Les Crackers** : ce sont des pirates dont la principale motivation est de **surmonter les outils de protections des logiciels payant**, grâce à des programmes logiciells (appelés souvent crack) développés. En effet, un crack permet de patcher un logiciel payant pour surpasser les protections mises en place.
    - **Les script-kiddies** : ce sont souvent **des pirates non experts en sécurité** qui réalisent leurs attaques de sécurité avec des outils et des logiciels existants. Les principales motivations de ces pirates sont **la destruction des systèmes d'information et le gain financier.**
    - **Hacktivistes** : ce sont des pirates dont la motivation principale est **idéologique**. Ils recourent généralement à l'attaque par déni de service. Anonymous est un exemples de Hacktivistes
- Après avoir classé les pirates, passons maintenant à la présentation des différentes classes d'attaques de sécurité qui peuvent être exécutées par les pirates.

Copyright - Tout droit réservé - OFPPT

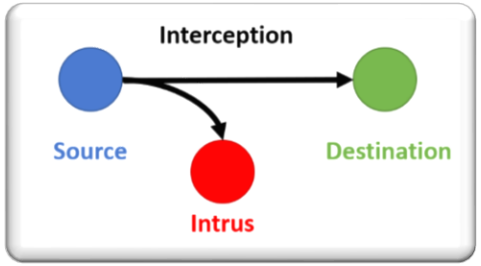
Classification des attaques

Les attaques de sécurité peuvent être classées en fonction de la propriété de sécurité visée. Quatre catégories d'attaques peuvent être distinguées : l'interruption, l'interception, la modification et la fabrication.

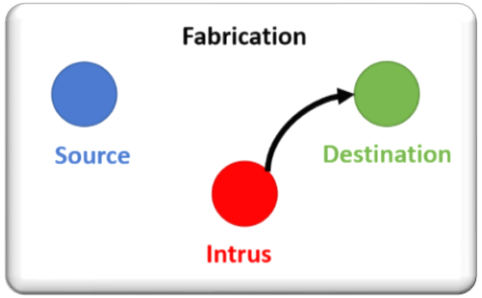




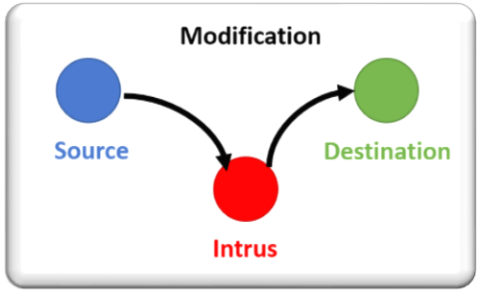
Un actif est détruit devient indisponible.
C'est une attaque qui vise la disponibilité.



Un intrus (une entité non autorisée) accède à un actif.
C'est une attaque qui vise la confidentialité.



Un intrus (une entité non autorisée) insère un faux objet dans un actif.
C'est une attaque qui vise l'authenticité.



Un intrus (une entité) non autorisée accède à un actif et le modifie.
C'est une attaque qui vise l'intégrité.

PARTIE 1

Copyright - Tout droit réservé - OFPPT

Classification des attaques

- Un autre moyen de classification d'attaque de sécurité, qui a été utilisée à la fois dans **X.800** et **RFC 2828**, classifie les attaques de sécurité en fonction de leurs **effets sur les ressources visées**. Dans cette classification, deux classes d'attaques de sécurité sont distinguées : les attaques *passives* et les attaques *actives.*
- **Les attaques passives :**

  Dans ce type d'attaque, l'objectif de l'intrus est de collecter des informations concernant les ressources et les actifs sans réaliser aucune modification affectant l'information ou la ressource visée. Deux types d'attaques passives peuvent être distinguées, qui sont :

  La lecture du contenu des messages et **l'analyse du Traffic.**
- **Lecture du contenu des messages :**

  Ce type d'attaque est possible lorsque **le contenu des messages échangés** entre deux entités est un **texte en claire** (c.à.d., un texte non chiffré). Dans ce type d'attaque, l'intrus peut collecter et lire des messages (ou écouter une communication vocale) échangés entre deux entités (Alice et Bob, comme illustré dans la figure ci-dessous.).

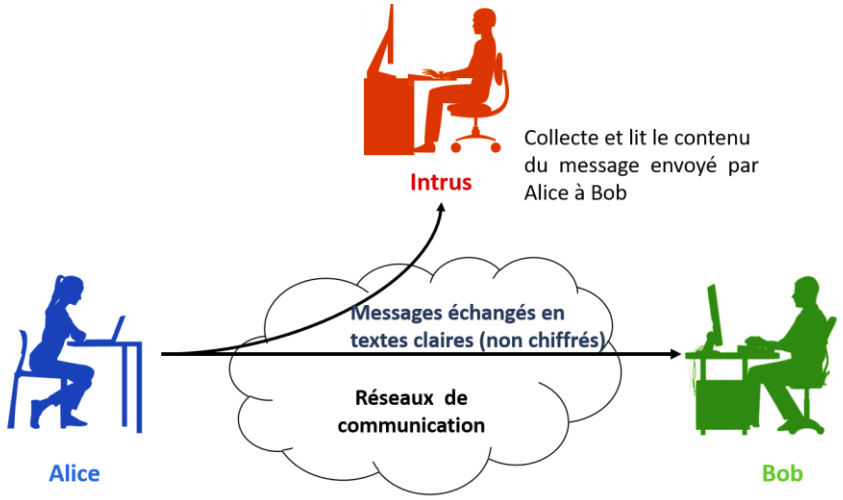


Illustration de l'exécution de l'attaque passive « lecture du contenu des messages »

PARTIE 1

Copyright - Tout droit réservé - OFPPT

Classification des attaques

Analyse du trafic : ce type d'attaque est exécuté lorsque **le contenu des messages échangés est masqué** (souvent en utilisant le cryptage). En fait, même en implémentant des mesures permettant de masquer le contenu des messages, l'intrus reste en mesure de collecter les messages, d'observer et d'analyser leurs structures, leurs motifs et/ou la fréquence des échanges. Le résultat de l'analyse lui permet de deviner la nature de la communication et d'exécuter d'autres attaques de sécurité plus sophistiquées.

Les attaques passives sont **difficiles à détecter**, puisqu'elles n'induisent aucune altération des données. Cependant, ce type d'attaques pourrait être **empêché** au moyen du **cryptage**. Par conséquent, le traitement des attaques passives doit être basé sur la prévention plutôt que sur la détection.

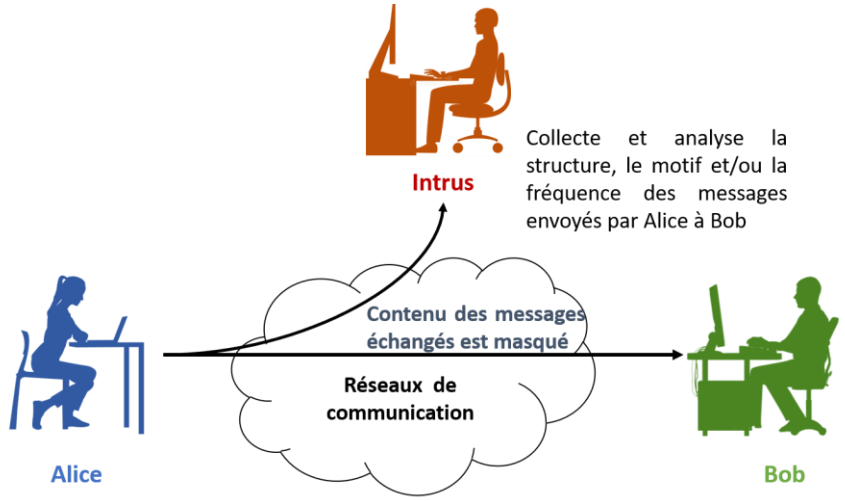


Illustration de l'exécution de l'attaque passive « Analyse du trafic»

Copyright - Tout droit réservé - OFPPT

Classification des attaques

- **Les attaques actives** : Dans ce type d'attaque, l'objectif de l'intrus est de modifier les ressources et/ou d'affecter leur fonctionnement. Cela consiste souvent à une modification du flux de données ou à la création d'un faux flux. Quatre catégories d'attaques actives peuvent être distinguées : **mascarade, rejeu, modification des messages et déni de service.**

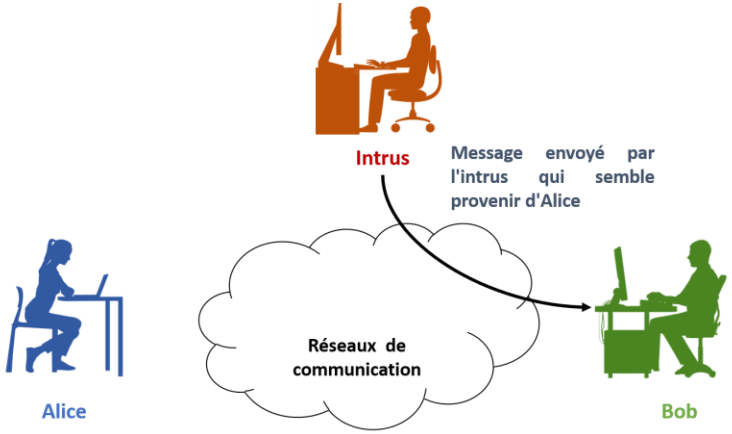


Illustration de l'exécution d'une attaque de mascarade

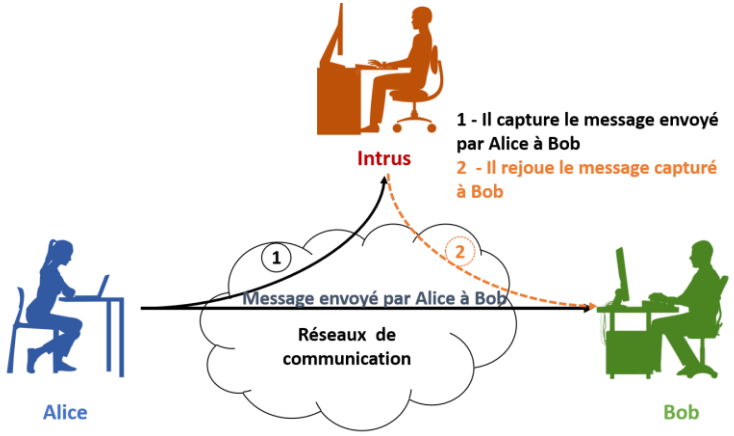


Illustration de l'exécution d'une attaque de rejeu

Mascarade : Cette attaque se réalise lorsqu'une entité fait semblant d'être une entité différente. Malgré le fait que le message reçu par Bob ait été envoyé par l'intrus, Bob croit que Alice est à l'origine du message.

Rejeu : L'attaque de rejeu consiste à capturer une unité de données (ou un trafic de données) et la retransmet ensuite, sans effectuer aucune modification, pour réaliser un effet non autorisé. L'intrus exécute une attaque passive et capture le message envoyé par Alice à Bob. Par la suite, l'intrus renvoie le message capturé à Bob. L'exécution d'une attaque pourrait faire croire à Bob que ce message est envoyé par Alice.

Copyright - Tout droit réservé - OFPPT

PARTIE 1

Classification des attaques

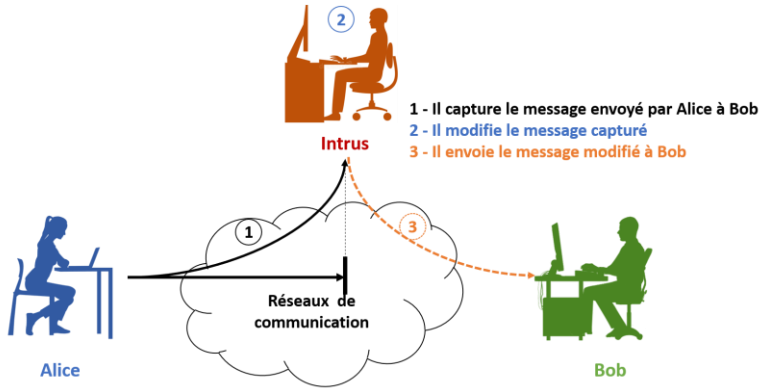


Illustration de l'exécution d'une attaque de modification des messages

Modification des messages : pour réaliser cette attaque, l'intrus modifie une partie d'un message capturé, ou retarde ou réorganise un ensemble de messages qui ont été capturés pendant une session légitime, pour produire un effet non autorisé.

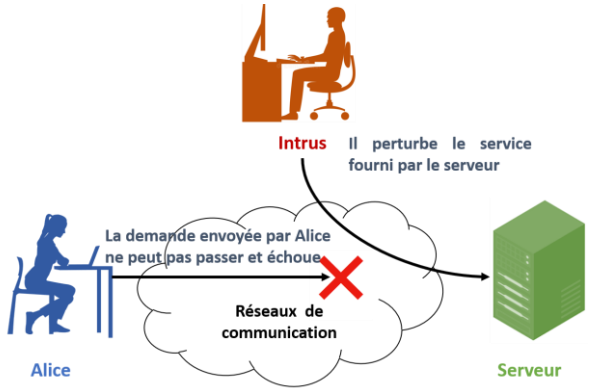


Illustration de l'exécution d'une attaque de déni de service

Déni de service : c'est une attaque qui pourrait se présenter sous plusieurs formes. Son objectif principal est d'empêcher ou d'entraver l'exécution des services visées. Exemples de formes d'attaques de déni de services :

- la suppression de tous les messages dirigés vers une destination particulière (le serveur dans notre exemple).
- la surcharge d'une destination particulière avec des faux messages pour dégrader ses performances et l'empêcher de répondre aux messages légitimes.
- l'interruption de l'ensemble du réseau (en le désactivant, le surchargeant, ou en provoquant une interférence) pour empêcher la réception des messages envoyés par des entités autoriséEs (la non réception du message d'Alice dans notre exemple).

Copyright - Tout droit réservé - OFPPT

Classification des attaques : Attaques internes et Attaques externes

- Un autre moyen de classification des attaques de sécurité se base sur **le périmètre et l'entité responsable** de l'exécution de l'attaque de sécurité par rapport au **périmètre de l'organisation**. Dans cette classification, deux classes d'attaques de sécurité peuvent être distinguées : les attaques internes et les attaques externes.
- **Les attaques internes** : Ce type d'attaque est exécutée ou bien par une entité interne à l'organisation ou par une entité étroitement liée à cette organisation via un accès direct ou indirect à ses actifs afin de les endommager.

  Les entités internes à une organisation sont souvent ses employés qui peuvent avoir des intentions malicieuses ou qui négligent les bonnes pratiques et les mesures adéquates de la sécurité.

  Les entités liées à l'organisation peuvent être des clients, des prestataires, des partenaires, des collaborateurs, etc...

  Le point commun des deux types d'entités cités précédemment est qu'ils peuvent bénéficier d'un accès direct ou indirect aux ressources de l'organisation victime.
- **Les attaques externes** : Ce type d'attaque est exécuté par une entité externe à l'organisation (c.à.d., qui ne dispose d'aucun lien avec cette organisation). Cependant, pour mener des attaques de sécurité, cette entité externe exploite les failles des réseaux de communication (tel que internet) et/ou celles des systèmes informatiques mis en place dans l'organisation.
- En ce qui suit, ces deux classes d'attaques (attaques internes et attaques externes) vont être abordés avec plus de détails

Copyright - Tout droit réservé - OFPPT

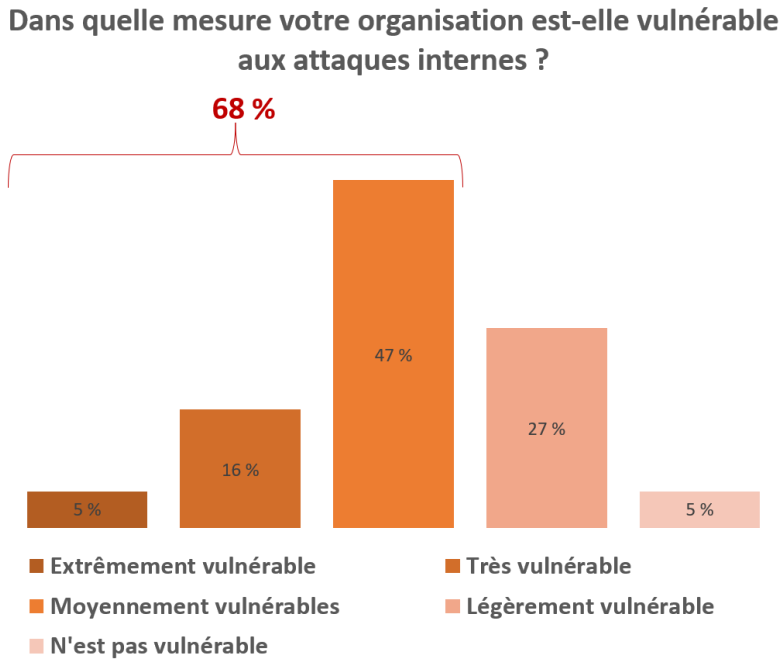
CHAPITRE 2

CONNAÎTRE LES CONCEPTS DE BASE DE LA SÉCURITÉ INFORMATIQUE

1. Classification des attaques et des hackers
2. **Attaques internes**
3. Attaques externes
4. Besoin d’identification des vulnérabilités

Attaques internes : Statistiques

- Comme défini précédemment, les attaques internes sont les attaques exécutées par des entités internes à l'organisation ou ayant un lien avec elle.
- La majorité des experts en sécurité admettent que le grand risque pour une organisation provient des attaques internes. En fait, selon le rapport annuel INSIDER THREAT de l'année 2020, la majorité des experts de la sécurité (environ 68%) ont affirmé que leurs organisations sont modérément à extrêmement vulnérables aux attaques internes. Tandis que uniquement 5 % ont affirmé que leurs organisations ne sont pas vulnérables aux attaques internes.



Le niveau de vulnérabilité des organisations aux attaques internes en chiffres selon les experts de sécurité

PARTIE 1

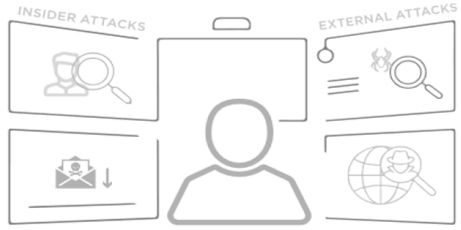
Copyright - Tout droit réservé - OFPPT

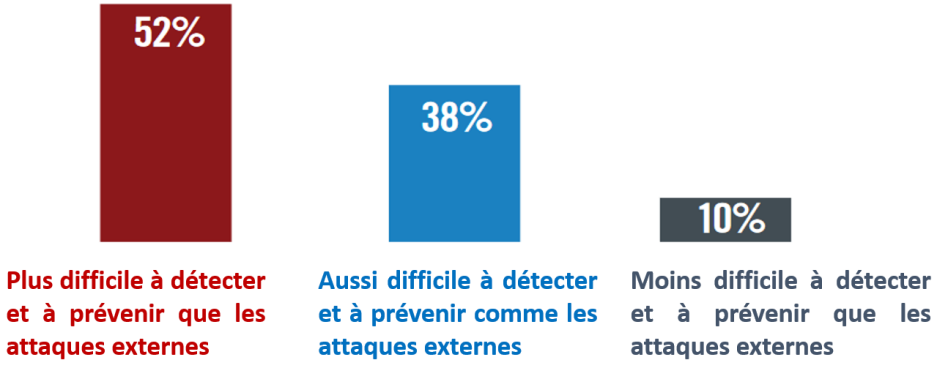
PARTIE 1

Attaques internes : Statistiques

En comparant les attaques internes aux attaques externes, la majorité des experts de la sécurité (environ 52 %) confirment que les attaques internes sont plus difficiles à détecter et à prévenir que les attaques externes. Notamment que les responsables de l'exécution de ce type d'attaques de sécurité ont des privilèges d'accès approuvés ce qui rend la distinction entre les activités légitimes et les attaques malveillantes très difficiles.

Est-il difficile de détecter et de prévenir les attaques internes par rapport aux attaques externes ?





Le niveau de difficulté de détection et prévention des attaques internes par rapport aux attaques externes en chiffres selon les experts de sécurité

Source : **Rapport annuel INSIDER THREAT de l'année 2020**

Copyright - Tout droit réservé - OFPPT

Attaques internes : Classification

Les attaques internes peuvent être classifiées selon le type d'employés qui sont à l'origine des attaques internes. Ci-dessous une figure qui présente quatre types d'employés pouvant être la cause principale de l'apparition d'une attaque interne dans une organisation. Dans ce qui suit, les types d'employés sont détaillés.

- **Employé inconscient** : c'est un employé qui a souvent un accès privilégié aux données sensibles (c.à.d., des données commerciales précieuses) de l'entreprise et qui ne reconnaît pas la valeur de ces données, ne comprend pas l'importance de la sécurité, et souvent n'applique pas les bonnes pratiques de la sécurité.
- **Employé Négligent** : c'est un employé qui n'a pas été formé et ne connaît pas les menaces de sécurité potentielles ou qui contourne simplement les mécanismes de sécurité pour des raisons d'efficacité dans le travail (il partage ses mots de passe avec des collègues afin de réduire le temps de réalisation de certaines tâches, par exemple). Ce type d'employé est généralement le type d'employé le plus vulnérable à l'**ingénierie sociale**.
- **Employé Malveillant** : c'est un employé qui vole **intentionnellement** des données des l'entreprise, les détruit ou les publie pour se venger (par exemple, un employé qui supprime les données de l'entreprise avant de quitter son poste actuel).
- **Employé professionnel** : c'est un employé qui a un bon niveau d'expertise dans la sécurité pour pouvoir dépasser les mesures de sécurité mise en place. En fait, ce type d'employé exploite les vulnérabilités de l'entreprise et revend des informations privées à des concurrents.

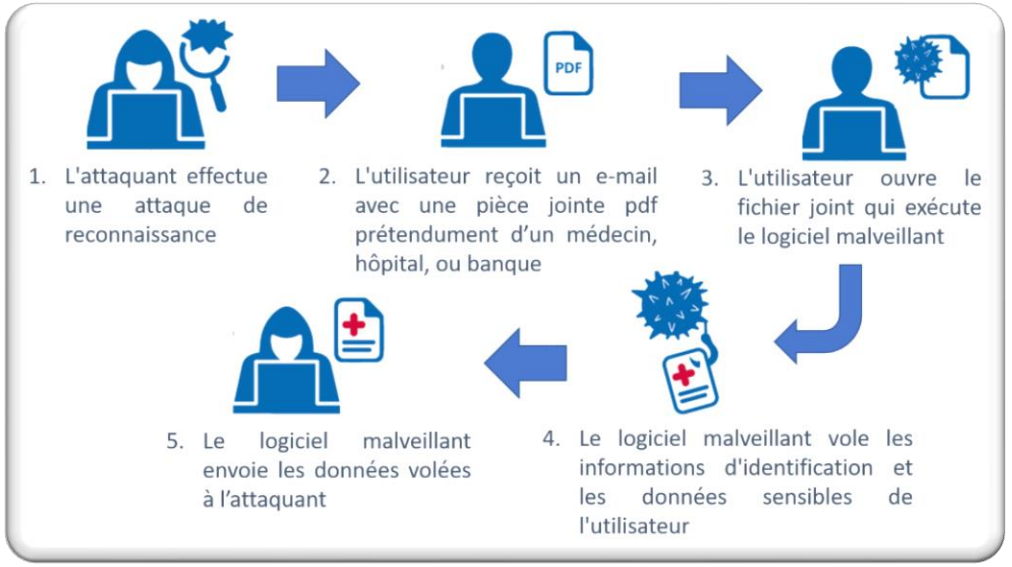
Les quatre types d'employés pouvant induire la réalisation des attaques internes
Lien source : https://deltalogix.blog/wp-content/uploads/2021/07/Cyber-Attacks-2-English-1-1398x800.png

PARTIE 1

Copyright - Tout droit réservé - OFPPT

Exemple d'attaque interne : Ingénierie Sociale et Hameçonnage

- L'attaque d'ingénierie sociale (Social engineering, en anglais) est parmi les attaques internes qui visent à tromper ou à manipuler les employés de l'entreprise pour les amener à enfreindre les procédures de sécurité mises en place.
- Le principe de l'attaque de l'ingénierie sociale consiste à :
    - Induire les employés à partager leurs informations confidentielles ;
    - Installer des logiciels malveillants (malwares) dans les ordinateurs des employés ou même le système de l'information de l'entreprise.
- Plusieurs scénarios d'attaques d'ingénierie sociale peuvent être distingués. Un exemple de scénario d'une attaque d'ingénierie sociale est illustré dans la figure ci-contre.



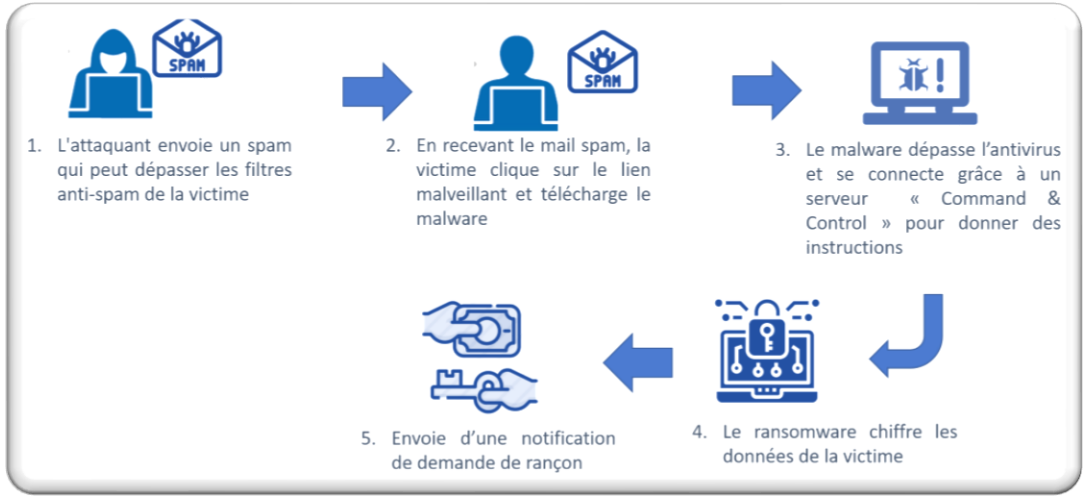
Exemple de réalisation d'une attaque Social Engineering
Lien source : https://www.researchgate.net/profile/Julio-Mayol/publication/310844589/figure/fig5/AS:432806523346946@1480200524238/Social-engineering-attack-on-hospital-staff.png

PARTIE 1

Copyright - Tout droit réservé - OFPPT

Exemple d'attaque interne : attaque du Ransomware

- L'attaque du ransomware est parmi les attaques internes les plus répandus actuellement. Selon le rapport de l'ANSSI publié en mars 2021, il y a eu une augmentation de 255% des alertes de signalement d'attaque par rançongiciel en un an.
- L'attaque du ransomware se base sur l'utilisation des rançongiciels (appelés souvent ransomwares) qui sont des logiciels malveillants (malwares) qui prennent en otage les données de l'entreprise au profit d'un pirate.
- Le principe de l'attaque du ransomware, comme illustré dans la figure contre, consiste à cacher dans un lien (ou une pièce jointe), envoyé via un spam, un **malware.** Ce dernier s'installe dans l'ordinateur de la victime et se connecte à un serveur « Command & Control » qui permet à l'attaquant de contrôler l'ordinateur victime. Ensuite, l'attaquant envoie des instructions au malware pour chiffrer tous les fichiers stockés dans un ordinateur victime. Il envoie ensuite une notification de rançon à la victime et déchiffre les fichiers infectés uniquement après la réception de la somme d'argent demandée.



Exemple de réalisation d'une attaque du Ransomware

PARTIE 1

Copyright - Tout droit réservé - OFPPT

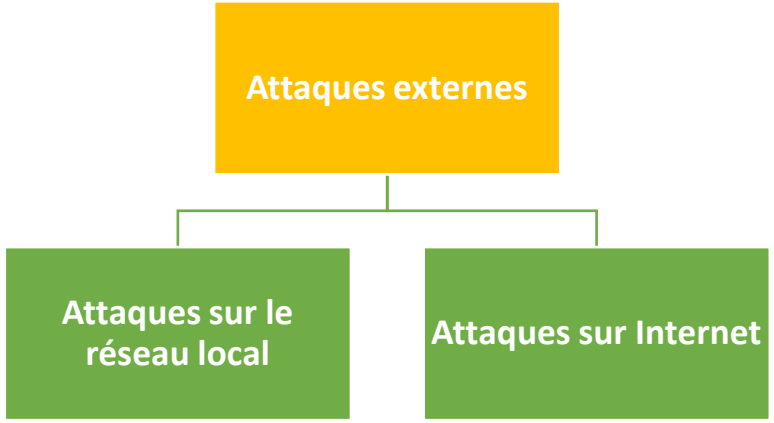
CHAPITRE 2

CONNAÎTRE LES CONCEPTS DE BASE DE LA SÉCURITÉ INFORMATIQUE

1. Classification des attaques et des hackers
2. Attaques internes
3. **Attaques externes**
4. Besoin d'identification des vulnérabilités

Attaques externes : Classification

- Après avoir présenté les attaques internes, nous abordons maintenant les attaques externes. Comme défini précédemment, les attaques externes sont des attaques exécutées par des entités n'ayant aucun contact avec l'organisation victime
- Il existe une large variété d'attaques de sécurité externes. En fait, le nombre ainsi que la nature de ce type d'attaques évoluent chaque année. En ce qui suit, nous allons présenter uniquement les attaques externes les plus courantes.
- Avant de détailler certains exemples d'attaques externes, ces derniers vont être classifiées en deux catégories : les attaques externes sur le réseau local et les attaques externes sur Internet.



Les classes des attaques externes

Copyright - Tout droit réservé - OFPPT

PARTIE 1

Attaques externes sur le réseau local

- Le modèle OSI (Open Systems Interconnection) est un modèle en couche qui a été conçu afin de permettre à ses différentes couches de fonctionner séparément les unes des autres. Ce qui fait que même si l'une des couches est piratée, les communications seront compromises sans que les autres couches ne soient conscientes de l'apparition de l'intrusion. Par conséquent, il faut veiller à la sécurité des différents protocoles des couches réseau.
- En réseau, la couche liaison de données (niveau 2) peut être un maillon faible en terme de sécurité. Il est donc nécessaire de renforcer la sécurité à ce niveau
- Avant de présenter les attaques de sécurité visant la couche liaison de données, faisons un petit rappel sur le fonctionnement du protocole ARP (Address Resolution Protocol) , qui est un protocole de la couche 2 permettant de mapper une adresse de couche réseau (adresse IP) à une adresse physique (adresse Media Access Control, MAC) d'une machine donnée.
- **Fonctionnement du Protocole ARP :**
    1. **Une requête ARP** est diffusée lorsqu'une machine "A" veut identifier l'adresse MAC d'une adresse IP donnée (figure ci-dessous à gauche) ;
    2. Uniquement l'hôte "B" ayant cette adresse IP répond avec **un message de réponse ARP unicast** intégrant son adresse MAC (figure ci-dessous à droite) ;
    3. L'hôte "A" apprend l'adresse MAC de B et l'écrit dans son cache ARP (figure ci-dessous à gauche).

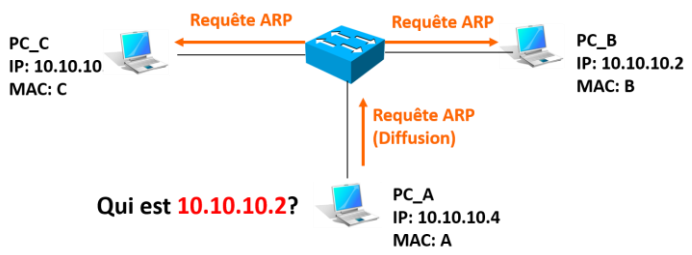


Illustration de la diffusion d'une requête ARP

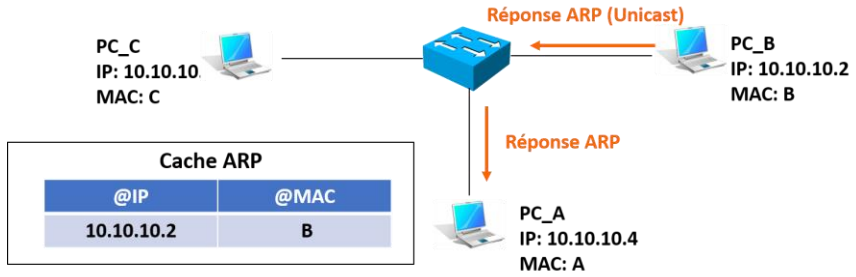


Illustration de la réception de la réponse ARP et le mappage d'adresses

Copyright - Tout droit réservé - OFPPT

Faiblesses du protocole ARP et attaques

- Le protocole ARP présente plusieurs **faiblesses** qui le rend vulnérable à certaines attaques de sécurité, parmi ces faiblesses, nous citons :

  ARP est un **protocole sans état** qui n'implémente pas le concept d'établissement de session. En effet, la cache ARP est mis à jour chaque fois qu'une réponse ARP est reçue, même si la machine hôte n'a pas envoyé une requête ARP.

  ARP n'implémente **aucun mécanisme d'authentification** et par conséquent les intrus peuvent usurper les informations IP et MAC dans les paquets ARP pour mener certaines attaques.

- À cause des faiblesses citées précédemment, une attaque de sécurité peut cibler le protocole ARP qui est l'attaque d'usurpation (ARP spoofing attack, en anglais).

Copyright - Tout droit réservé - OFPPT

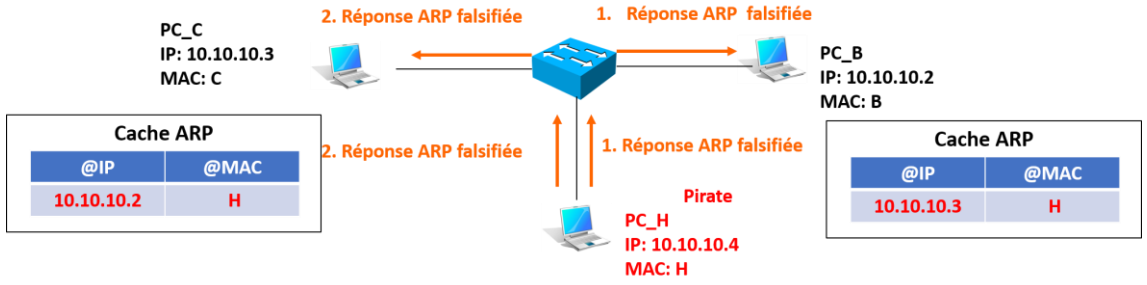
PARTIE 1

Attaque d'usurpation (ARP spoofing attack)

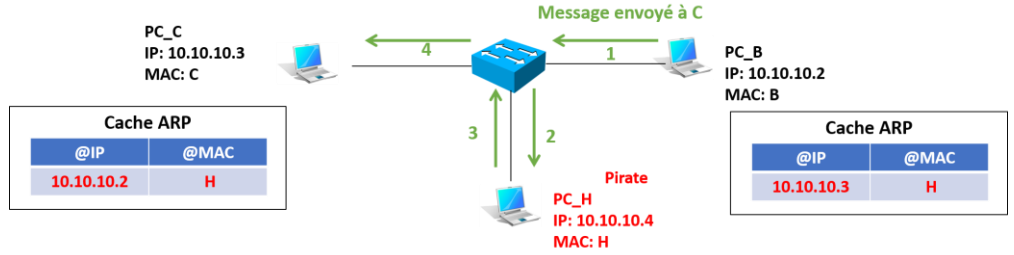
- Les étapes de l'exécution de l'attaque ARP spoofing sont les suivantes :
    1. Le pirate envoie une réponse ARP contrefaite avec l'adresse IP de l'hôte C et son adresse MAC à l'hôte B ;
    2. Il envoie également une réponse ARP falsifiée avec l'adresse IP de l'hôte B et son adresse MAC à l'hôte C ;
    3. Par conséquent, l'hôte de l'attaquant est insérée entre le chemin de communication des hôtes "B" et "C ". En fait, comme illustré dans la figure ci-dessous à gauche.

        La machine B a enregistré dans son cache ARP le mappage entre l'adresse IP de la machine C et l'adresse MAC de l'attaquant ;

        La machine C a enregistré dans son cache ARP le mappage entre l'adresse IP de la machine B et l'adresse MAC de l'attaquant.
- Après la réalisation de l'attaque ARP spoofing, l'attaquant relaie les messages de communication entre les deux hôtes victimes "B" et "C ", sans que ces derniers soient conscient de sa présence. En fait, comme illustré dans la figure ci-dessous à droite, tout message envoyé passe par le pirate puis il atteint sa destination finale.



Étapes d'exécution de l'attaque ARP spoofing



Résultat de l'exécution d'une attaque ARP spoofing

Copyright - Tout droit réservé - OFPPT

PARTIE 1

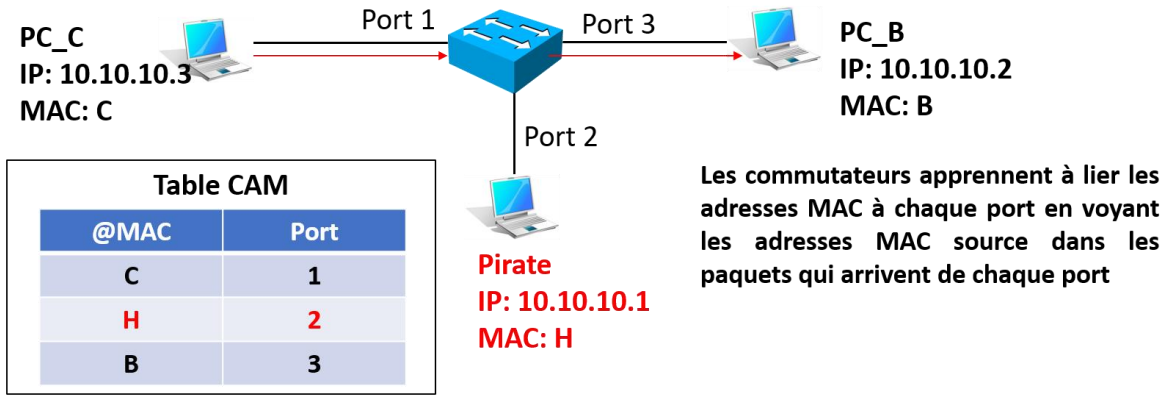
Attaque par inondation d'adresses MAC (MAC Flooding Attack)

- Un deuxième exemple d'attaque de sécurité ciblant la couche liaison de données est l'attaque par inondation d'adresses MAC. Avant de détailler le principe et les étapes de la réalisation de cette attaque, nous présentons un petit rappel sur la mémoire adressable par le contenu d'un commutateur.
- **Principe de la mémoire adressable par le contenu d'un commutateur :**

  Chaque commutateur Ethernet (Switch, en anglais) possède une mémoire adressable par le contenu, souvent appelé une table CAM (Content-Addressable Memory), qui lui permet de stocker les adresses MAC des hôtes, les numéros de port et d'autres informations, et qui possède une taille fixe.

  Un commutateur remplit sa table CAM en liant les adresses MAC des paquets reçues et les port de réception des paquets.

  Comme illustré dans la figure ci-dessous, le commutateur transfère les trames entre le PC_C et le PC_B sans inondation, grâce à sa table CAM qui contient les mappages port/adresse MAC. Dans une telle situation, un pirate qui est connecté à ce même commutateur ne peut pas recevoir une copie du trafic échangé.



Fonctionnement normal d'un commutateur

Copyright - Tout droit réservé - OFPPT

PARTIE 1

Attaque par inondation d'adresses MAC (MAC Flooding Attack)

- La vulnérabilité exploitée par le pirate pour qu'il puisse réussir son attaque, est le fait que la table CAM d'un commutateur ait une taille fixe. Dés qu'elle sera pleine, le commutateur passe en mode concentrateur et diffuse le trafic dont son adresse MAC ne figure pas dans la table CAM.
- **Étapes de l'exécution de l'attaque par inondation MAC :**
    1. Le pirate inonde le commutateur à l'aide des paquets ARP falsifiés qui contiennent des adresses MAC sources différentes ;
    2. Les fausses adresses MAC sont ajoutées à la table CAM ;
    3. La table CAM se remplit et le commutateur diffuse le trafic, qui n'a pas d'entrée dans la table CAM, vers tous les ports ;
    4. Le pirate est maintenant capable de recevoir toutes les trames qui n'étaient destinées qu'à un hôte spécifique.

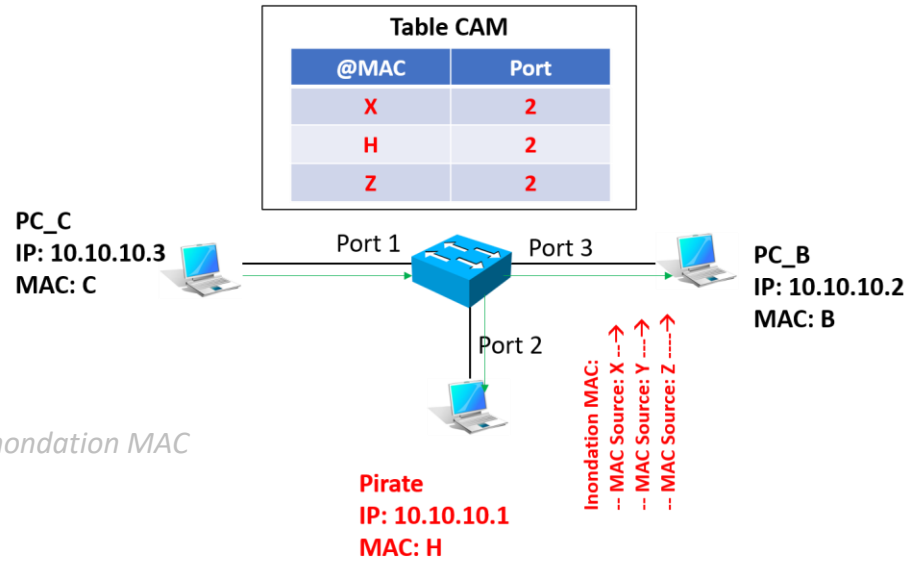


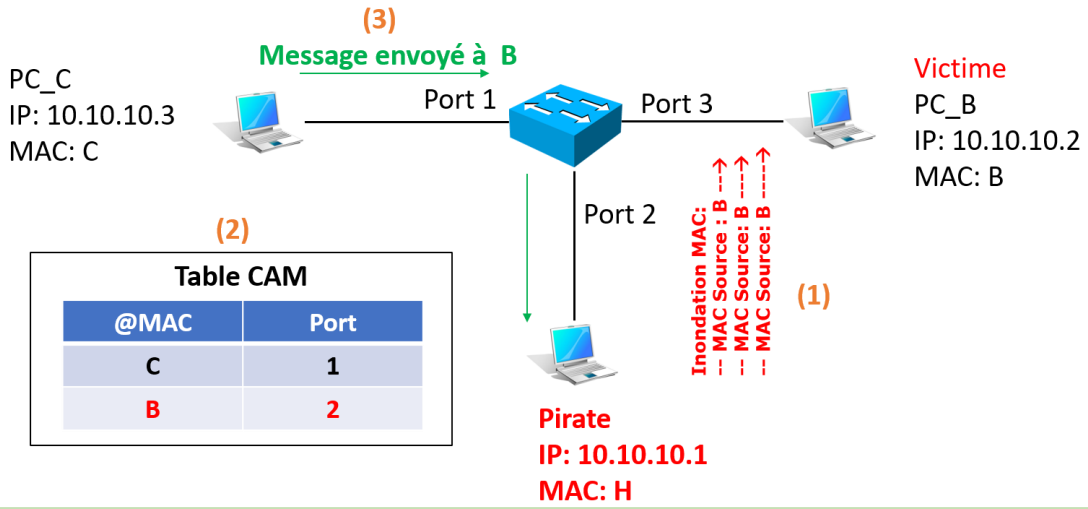
Illustration de l'attaque par inondation MAC

Copyright - Tout droit réservé - OFPPT

PARTIE 1

Attaque du vol de port (Port Stealing)

- Une deuxième attaque de sécurité qui exploite les vulnérabilités liées au remplissage de la table CAM d'un commutateur est l'attaque du vol d'un port commutateur. Le principe d'une telle attaque consiste à voler le port des commutateurs d'un hôte victime afin de recevoir le trafic envoyé à l'hôte victime.
- **Étapes de l'exécution de l'attaque du vol de port :**
    1. Le pirate inonde le commutateur avec des paquets ARP falsifiés qui incluent comme :
        - Adresse MAC source celle de l'hôte victime ;
        - Adresse MAC de destination celle du pirate.
    2. Comme illustré dans la figure ci-dessous, le commutateur mappe l'adresse MAC de l'hôte victime B sur le port du pirate (le port 2 dans notre exemple).
    3. Lorsqu'un hôte C envoie un paquet à l'hôte victime B, le commutateur le transfère sur le port du pirate (qui est le port 2).

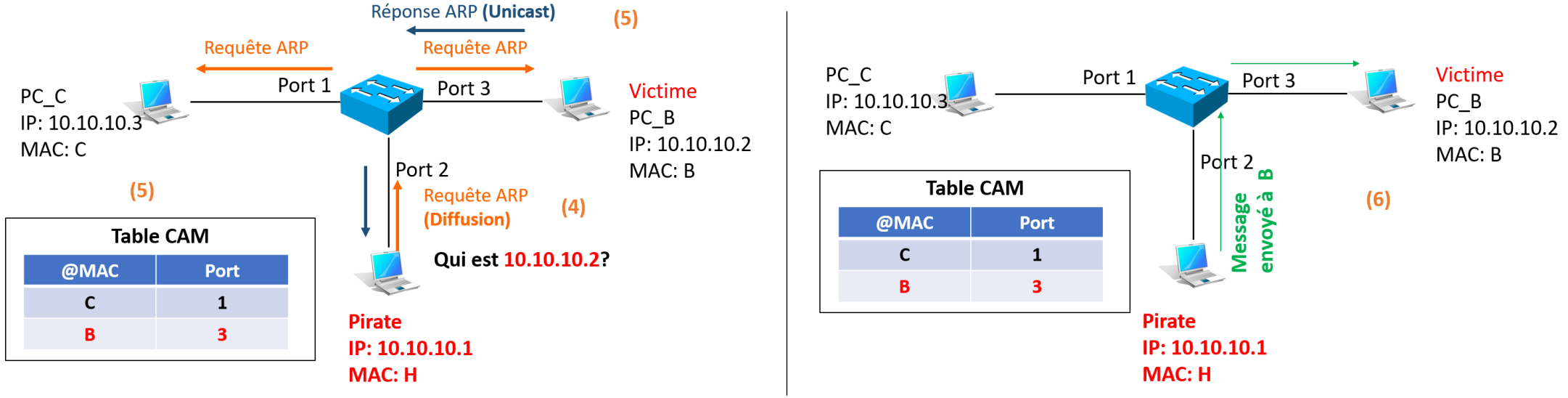


Étapes d'exécution de l'attaque Port Stealing

Copyright - Tout droit réservé - OFPPT

Attaque du vol de port (Port Stealing)

4. Lors de la réception d'un message qui est destiné à la machine victime B, le pirate l'enregistre dans une mémoire tampon et envoie une requête ARP pour demander l'adresse IP de l'hôte victime.
5. Comme illustré dans la figure ci-dessous à droite, lorsque l'hôte victime B répond à la requête ARP reçu, le commutateur remappe l'adresse MAC de la victime à son port réel (le port 3 dans notre exemple).
6. Comme illustré dans la figure ci-dessous à droite, le pirate transmet le message envoyé qui a été mis en mémoire tampon à l'hôte victime B.



Étapes d'exécution de l'attaque Port Stealing

PARTIE 1

Copyright - Tout droit réservé - OFPPT

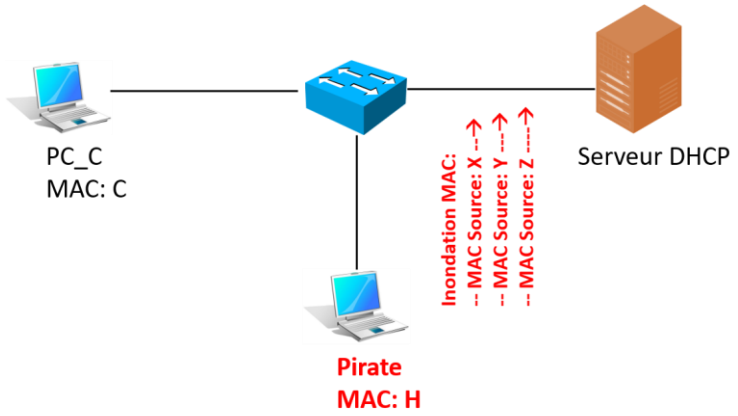
Attaques ciblant le protocole DHCP (Dynamic Host Configuration Protocol)

- Les attaques ciblant le protocole DHCP sont des attaques qui peuvent s'exécuter dans le réseau local. Un petit rappel du protocole DHCP avant de détailler ces attaques.
- **Aperçu du protocole DHCP** : DHCP est un protocole de la couche réseau (niveau 3) qui permet l'attribution dynamique des adresses IP aux machines, grâce à un serveur DHCP. L'attribution dynamique se déroule comme suit :

  Le client DHCP envoie une requête dans laquelle il demande des informations (tel que l'adresse IP, la passerelle par défaut, etc.) à un serveur DHCP ;

  À la réception d'une requête valide, le serveur attribue à ce client une adresse IP et d'autres paramètres de configuration IP.
- Le protocole DHCP est vulnérable à deux attaques de sécurité qui sont : DHCP Starvation (attaque par épuisement de ressources) et DHCP spoofing (attaque d'usurpation).
- **Principe de l'attaque DHCP Starvation** : Pour réaliser cette attaque, le pirate épuise les adresses IP disponibles dans le serveur DHCP, en lui envoyant un grand nombre de requêtes avec des adresse MAC falsifiés. Cela induit la production d'un déni de service. En effet, le serveur DHCP ne peut plus attribuer des adresses IP aux hôtes légitimes.

Exécution de l'attaque DHCP Starvation



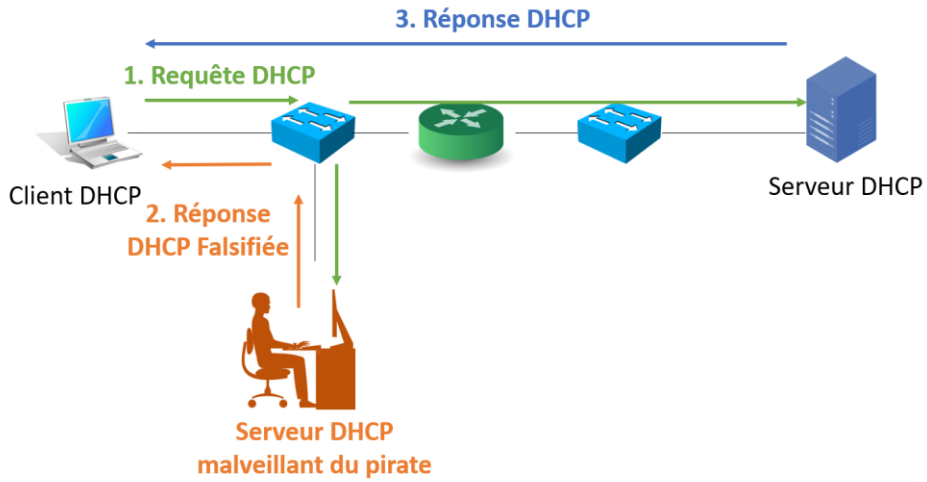
PARTIE 1

Copyright - Tout droit réservé - OFPPT

PARTIE 1

Attaques ciblant le protocole DHCP (Dynamic Host Configuration Protocol)

- **Principe de l'attaque DHCP Spoofing :** Pour réaliser cette attaque, le pirate exécute souvent les étapes suivantes :
    - Il déploie un serveur DHCP malveillant pour fournir des adresses IP aux client et attend la réception des requêtes DHCP ;
    - À la réception d'une requête DHCP, le pirate envoie une réponse DHCP falsifiée à ce client, avant que la réponse DHCP autorisée puisse lui parvenir. La fausse réponse DHCP inclue souvent l'adresse IP du pirate comme passerelle par défaut du client ;
        - Pour s'assurer que sa réponse DHCP falsifiée arrive en premier lieu, le pirate peut se positionner dans un emplacement physique plus proche que le serveur DHCP (comme illustré dans la figure ci-contre), ou bien il essaie d'exécuter en parallèle une attaque de déni de service ciblant le serveur DHCP autorisé afin que ce dernier ne puisse pas répondre aux requêtes de ses client ;
    - À la réception de la première réponse DHCP (qui est celle du pirate), le client considère l'adresse IP du pirate comme sa passerelle par défaut. Par conséquent, tout le trafic qu'il envoie passe par le pirate. Dans une telle situation, le pirate est appelé souvent "man-in-the-middle" (l'homme du milieu).
    - Le pirate peut intercepter tous les paquets et choisir entre répondre à la passerelle réelle ou les supprimer.



Exécution de l'attaque DHCP Spoofing

Copyright - Tout droit réservé - OFPPT

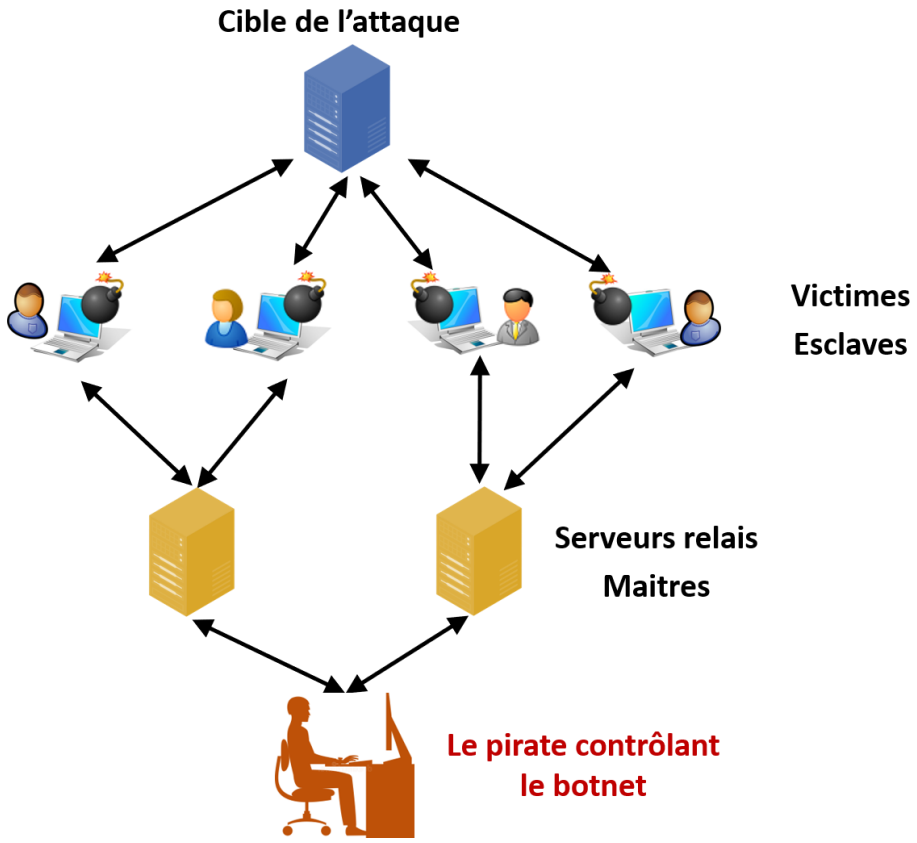
Attaques externes sur le réseau Internet

- Après avoir présenté un ensemble d'attaques externes qui peuvent être exécutées dans un réseau local, passons maintenant à des exemples d'attaques externes qui peuvent être réalisées quand le réseau local d'une organisation est connecté au réseau Internet.
- Parmi les attaques externes les plus courantes qui s'exécutent via le réseau Internet, nous citons les attaques de déni de service (Denial of Service attacks, en anglais et son abréviation est DoS).
- Le résultat d'une attaque de déni de service est une interruption des services. Pour réaliser avec succès une telle attaque, il suffit de procéder à :
    - **L'envoi d'un volume de trafic très important**. En fait, une ressource (tel qu'un réseau, un serveur ou même une application) sera épuisée (c.à.d., ne peut plus fournir les services attendues) à la réception d'un large volume de messages ou données dans une courte période ;
    - **L'envoi d'un ensemble de paquets formatés de manière malveillante**. En effet, un paquet malveillant peut inclure des malwares ou des requêtes malveillantes qui visent à bloquer le fonctionnement de la ressource ciblée (réseau, serveur, ou application).
- L'exécution d'une attaque de déni de service peut être réalisée sous plusieurs formes, tel que le SYN flood , le ping of death, etc.
- En plus, une attaque de DoS peut être menée par une seule machine ou simultanément par plusieurs machines et dans ce cas elle est appelée DoS distribué (Distributed DoS en anglais, et son abréviation est DDoS).
- En ce qui suit, nous détaillerons les attaques suivantes : DDoS et SYN flood.

Copyright - Tout droit réservé - OFPPT

DoS distribué

- La déni de service distribué (DDoS) est une attaque qui vise à saturer une ressource (serveur, application, site web etc.) pour la mettre hors-service à l'aide des **botnets**.
- Botnet est un réseau de machines zombies (machines infectées) contrôlées par des pirates, sans que leurs propriétaires en soient conscients. Ces machines sont souvent appelées des esclaves puisqu'elles reçoivent les commandes des pirates et les exécutent pour cibler une victime précise.
- Le scénario typique d'une attaque DDoS est le suivant: Comme illustré dans la figure ci-contre, le pirate utilise des serveurs relais (qui sont considérés comme des maitres) pour diffuser une commande spécifique à l'ensemble des machines esclaves. À la réception de cette commande, toutes les machines esclaves (qui sont à l'ordre de milliers ou millions de machines), réagissent et envoient des paquets volumineux, falsifiés, ou autres selon le type de l'attaque DDoS.



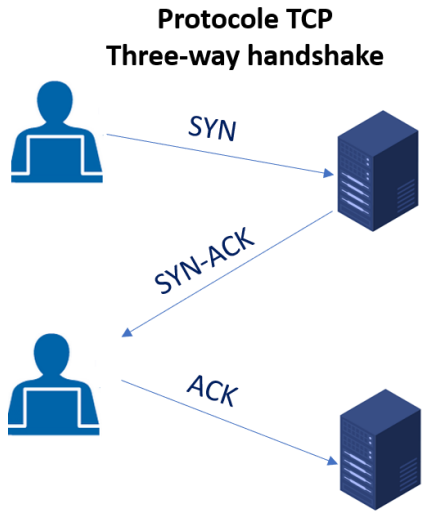
DDoS attaque

PARTIE 1

Copyright - Tout droit réservé - OFPPT

SYN flood attaque

- **Principe d'une connexion TCP** : Avant de commencer l'échange de données, l'émetteur (client) et le récepteur (Serveur) sont tenus d'établir une "connexion". Comme illustrées dans la figure, les étapes de l'établissement d'une connexion sont comme suit :
    1. Le client envoie un segment TCP SYN au serveur ;
    2. Le serveur reçoit SYN et répond par sagement SYN-ACK ;
    3. Le client reçoit SYNACK du serveur et répond par ACK qui peut contenir des données.



Principe d'une connexion TCP

Copyright - Tout droit réservé - OFPPT

SYN flood attaque

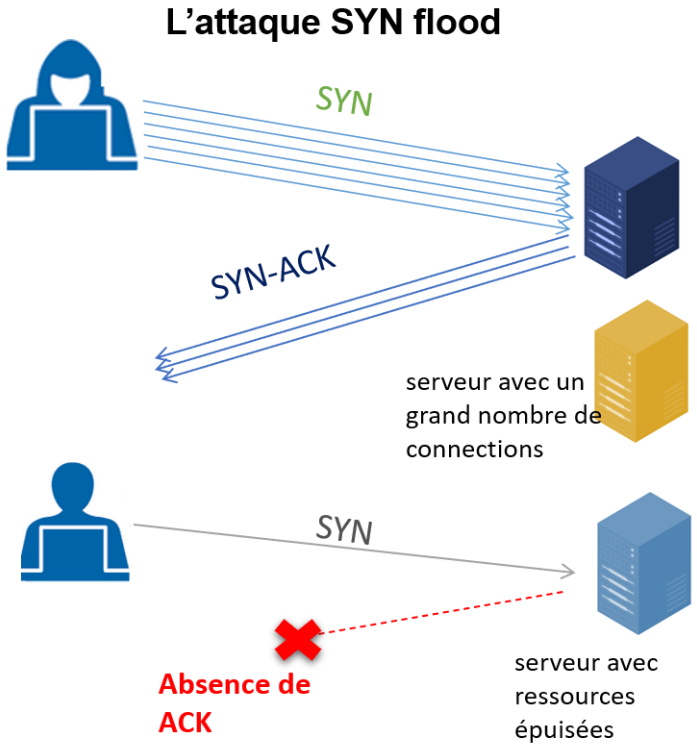
- **Principe de l'attaque SYN flood** :

Pour réaliser ce type d'attaque, le pirate prend la position du client et envoi un volume très important des requêtes SYN à la victime. Pour ne pas être épuisé avec les réponse un SYN/ACK, les requêtes envoyées par le pirate incluent généralement de fausses adresses source (c.à.d., adresses différentes à celle du pirate).

Comme illustré dans la figure ci-contre, le serveur victime répond alors avec un SYN/ACK à un réseau inexistant (cela est due au fait que les adresses sources dans les requêtes SYN sont fausses).

La victime attend le ACK du client qui n'arrive jamais. Par conséquent, les ressources de la victime peuvent être épuisées par le traitement du large volume des requêtes SYN reçues et l'attente des ACK.

Au bout d'un certain temps, la victime ne plus répondre à aucune demande de connexions, notamment celles envoyés par les clients autorisés.



Principe de l'attaque SYN flood

PARTIE 1

Copyright - Tout droit réservé - OFPPT

CHAPITRE 2

CONNAÎTRE LES CONCEPTS DE BASE DE LA SÉCURITÉ INFORMATIQUE

1. Classification des attaques et des hackers
2. Attaques internes
3. Attaques externes
4. **Besoin d'identification des vulnérabilités**

Besoin d'identification des vulnérabilités

- Après avoir présenté les attaques de sécurité visant une organisation ainsi que les notions de bases de la sécurité, la principale question à poser est : **Comment empêcher la réalisation des attaques de sécurité ?**
- La réponse à cette question est la mise en place de mécanismes de **prévention** et de **protection** afin de réduire les attaques de sécurité.
- Avant de choisir les mécanismes de **prévention** appropriés à mettre en place, il est nécessaire d'identifier les actifs d'une organisation et les vulnérabilités qui les menace. Cela pourra être réalisé à l'aide des audits de sécurité récurrents que nous allons découvrir dans la suite du cours.

Copyright - Tout droit réservé - OFPPT

PARTIE 2

PROTÉGER LE SYSTÈME D'INFORMATION (SI)

Dans ce module, vous allez :

- Découvrir la politique de sécurité
- Présenter les règles et les droits de sécurité
- Identifier les composants et les outils logiciels permettant la sécurisation de l'accès physique et des équipements informatiques

18 heures

CHAPITRE 1

PRÉSENTER LA POLITIQUE DE SÉCURITÉ DU SI

Ce que vous allez apprendre dans ce chapitre :

- Décrire la démarche de la mise en place d'une politique de sécurité du SI
- Présenter des normes et méthodes de gestion des risques
- Définir l'approche PDCA et la veille technologique

6 heures

CHAPITRE 1

PRÉSENTER LA POLITIQUE DE SÉCURITÉ DU SI

1. **Démarche de la mise en place d'une politique de sécurité du SI et gestion des risques**
2. Normes et méthodes de gestion des risques
3. Approche PDCA
4. Veille technologique
5. Quiz sur les notions de base relatives à l'assurance d'une amélioration continue de la sécurité SI

Politique de Sécurité du Système d'Information (PSSI)

- Comme présenté dans la première partie de ce cours, la sécurité du système d'information est primordiale pour une organisation.
- Pour faire face aux attaques de sécurité et protéger le système d'information (SI), toute organisation devra élaborer soigneusement une stratégie de sécurité, appelée souvent Politique de Sécurité du Système d'Information.
- Une PSSI est traduite par l'élaboration d'un référentiel (document) de sécurité pour une organisation. Il inclut essentiellement les objectifs et les règles de sécurité à appliquer ainsi que les actions à réaliser afin de fournir un niveau de sécurité acceptable.
- Une PSSI traite la sécurité de toutes les activités et les informations sensibles d'une organisation. Elle couvre plusieurs catégories de la sécurité de l'information :
    - La sécurité des systèmes d'information ;
    - La sécurité de la communication ;
    - La sécurité physique ;
    - La sécurité organisationnelle.
- Les principaux objectifs d'une PSSI :
    - Définir les objectives de sécurité pour une organisation et élaborer les règles de sécurité à mettre en place ;
    - Définir une approche homogène, garantissant un degré de sécurité élevé ;
    - Définir les responsabilités en matière de la sécurité des systèmes d'information.

Copyright - Tout droit réservé - OFPPT

Démarche de la mise en place d'une PSSI

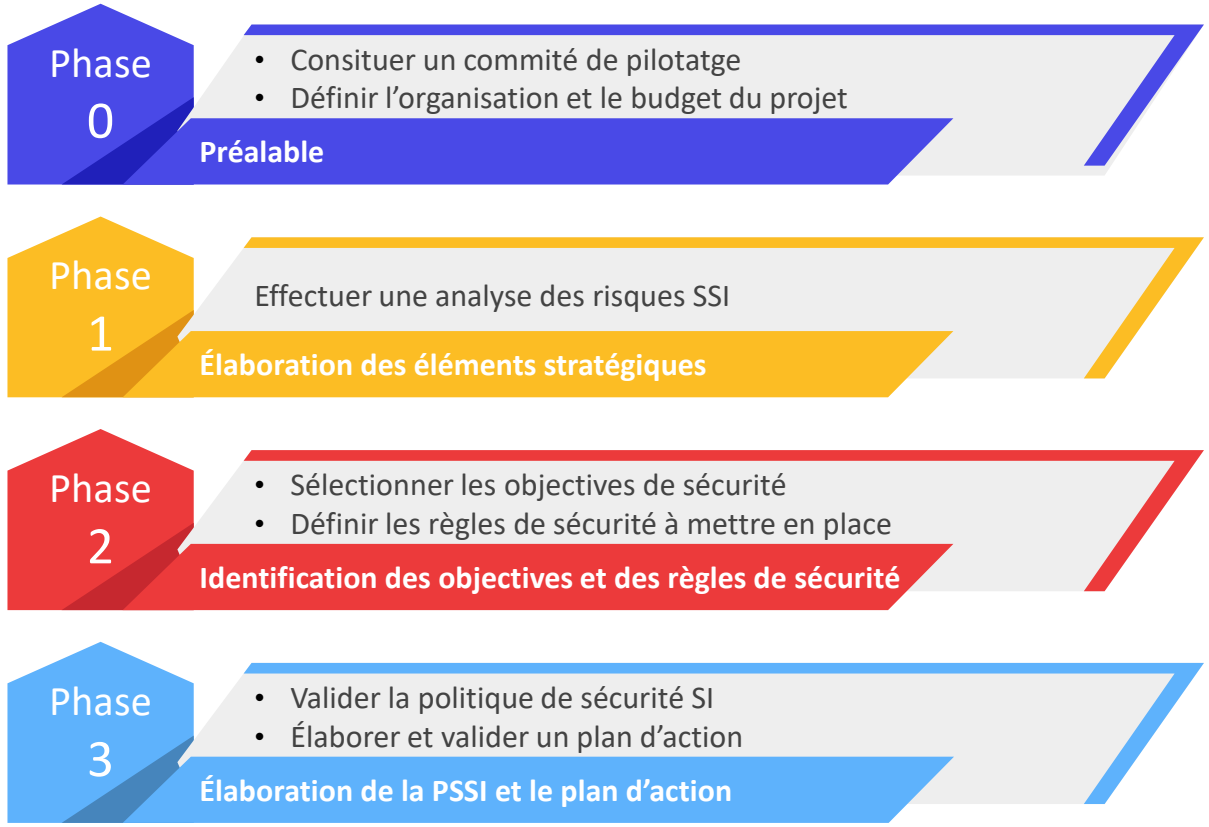
- Pour élaborer une PSSI offrant les objectifs décrits précédemment, il faut suivre une démarche bien organisée et planifiée.
- Comme illustré dans la figure ci-contre, une démarche PSSI, suivant les meilleurs pratiques de sécurité, est organisée en quatre phases :

  Phase 0 : Préalable ;

  Phase 1 : Élaboration des éléments stratégiques ;

  Phase 2 : Identification des objectives et des règles de sécurité ;

  Phase 3 : Élaboration de la PSSI et le plan d'action.
- Chacune de ces phases incluent un ensemble de tâches qui doivent être effectués soigneusement.
- En ce qui suit, nous détaillerons les tâches à effectuer durant chacune des quatre phases.



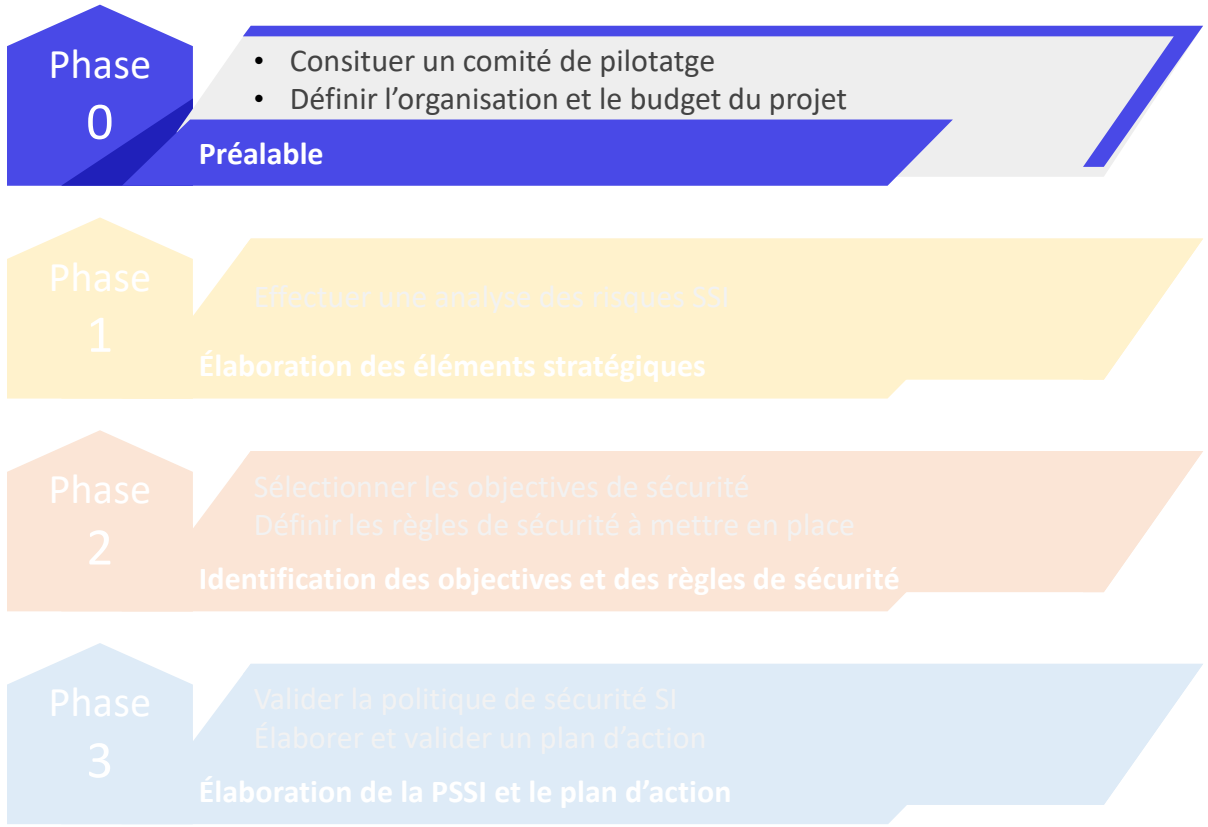
Les phases d'élaboration d'une PSSI

PARTIE 2

Copyright - Tout droit réservé - OFPPT

Démarche de la mise en place d'une PSSI

- La phase 0 est une phase préliminaire qui doit être menée pour déterminer l'ensemble des éléments nécessaires pour l'élaboration de la PSSI.
- Comme illustré dans la figure ci-contre, cette phase inclue deux tâches :
    - **Constituer un comité de pilotage** : consiste à désigner une équipe qui sera responsable de l'élaboration de la PSSI, cette équipe inclut :
        - Un responsable de sécurité système d'information ;
        - Des représentants des unités opérationnels : sont des employés maitrisant les opérations de l'organisation. Chaque représentant est responsable d'une unité opérationnelle ;
        - Des experts de différents domaines (Sécurité, Réseaux, Juridiques, etc…).
    - **Définir l'organisation et le budget du projet** : consiste à spécifier le budget, le temps et les ressources nécessaires pour l'achèvement de l'élaboration de la PSSI.



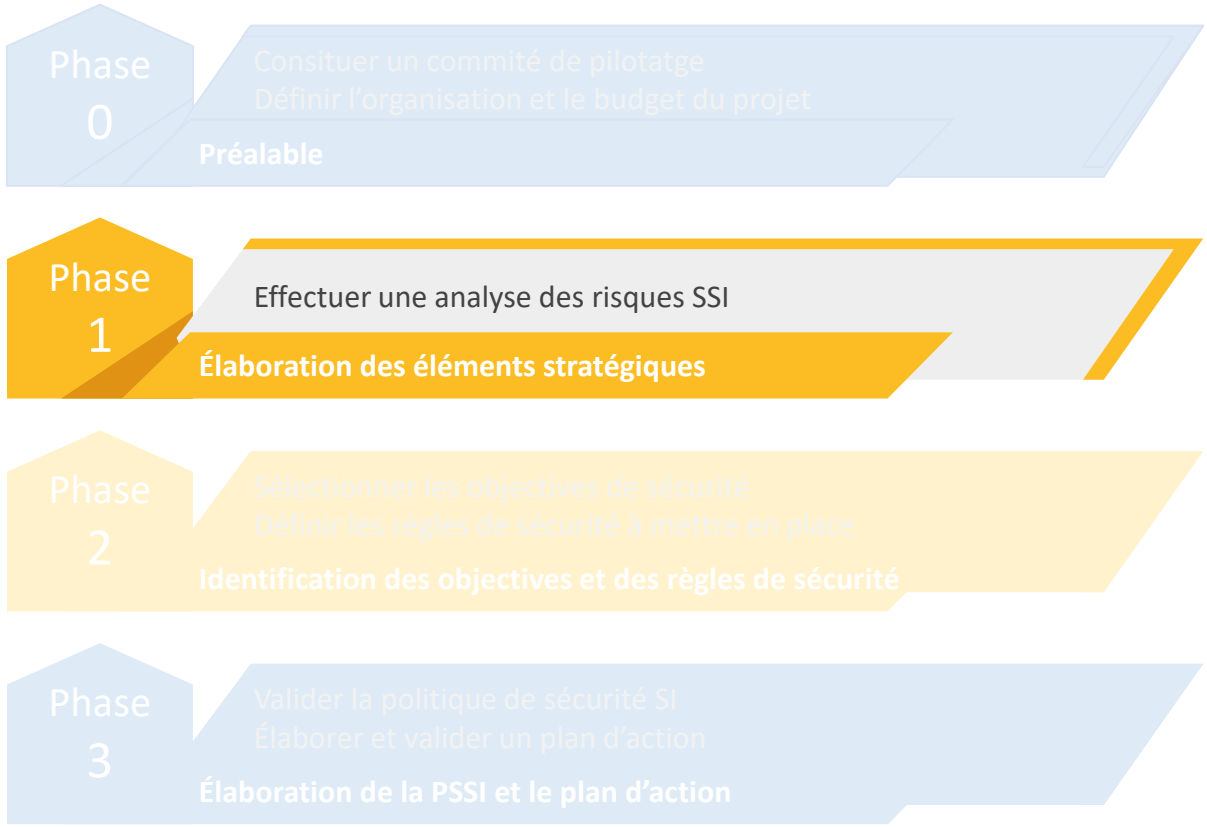
Les phases d'élaboration d'une PSSI

PARTIE 2

Copyright - Tout droit réservé - OFPPT

Démarche de la mise en place d'une PSSI

- La phase 1 est la première phase de l'élaboration d'une PSSI.
- Durant cette phase, le Responsable de Sécurité Système d'Information (RSSI), avec le comité du pilotage, mènent une analyse des risques de la Sécurité du Système d 'Information (SSI).
- Une analyse des risques SSI inclue plusieurs étapes (ou tâches à effectuer). Le nombre, l'appellation, et le processus d'exécution de ces étapes diffère en fonction de la norme ou de la méthode de gestion du risque utilisée. En fait, l'analyse des risques est incluse dans le processus de gestion des risques
- Parmi les étapes d'analyse des risques SSI, nous citons :
    - Délimiter le périmètre d'analyse du risque ;
    - Définir des échelles de besoins en termes d'objectifs de sécurité (tel que disponibilité, intégrité, confidentialité, etc.) ;
    - Identifier les actifs à protéger ;
    - Identifier les failles de sécurité et les menaces visant les actifs à protéger ;
    - Exprimer les besoins de sécurité des actifs à protéger.



Les phases d'élaboration d'une PSSI

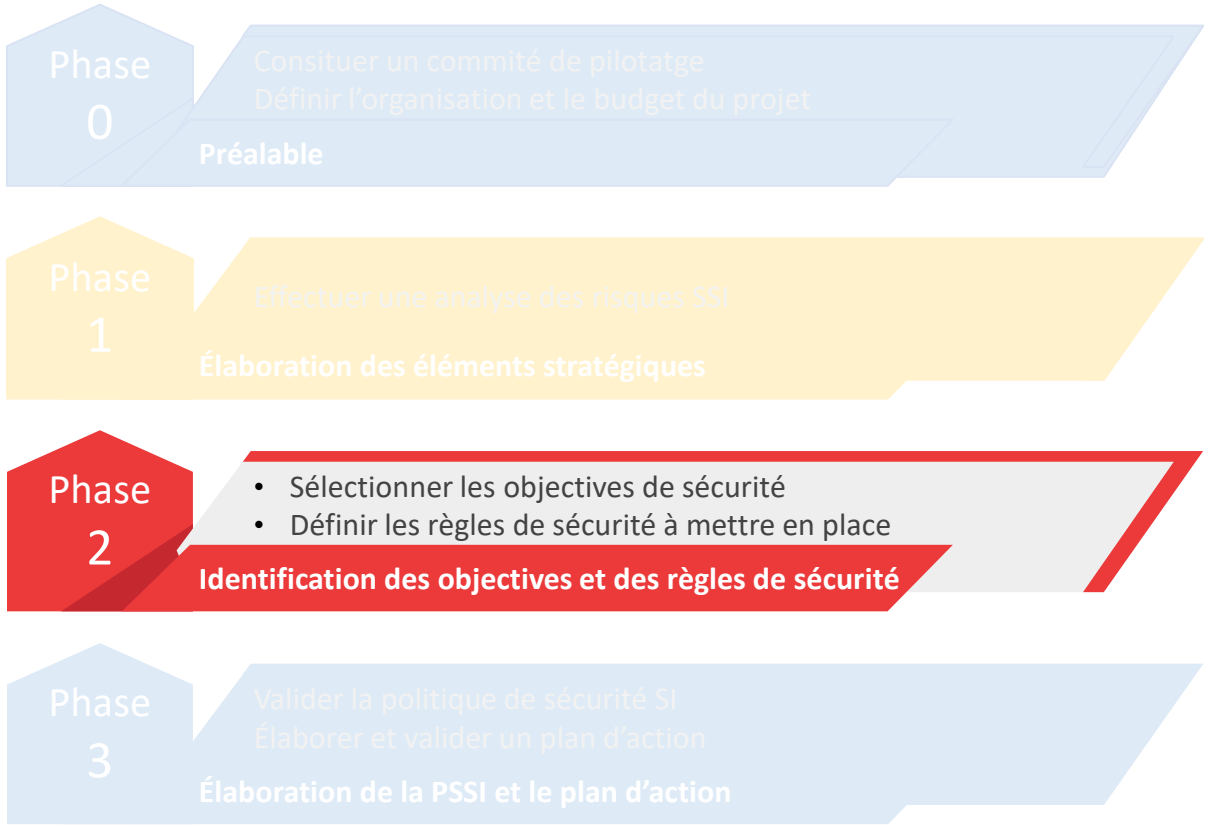
PARTIE 2

Copyright - Tout droit réservé - OFPPT

PARTIE 2

Démarche de la mise en place d'une PSSI

- Après avoir effectué l'analyse des risques SSI, le comité du pilotage passe à la réalisation de la phase 2
- Comme illustré dans la figure ci-contre, la phase 2 inclue deux tâches :
  - **Sélectionner les objectives de sécurité** : durant cette tâche, le comité de pilotage sera en charge d'analyser les objectives de sécurité de chaque actif (identifié dans la phase précédente) afin de :
    - retenir certaines objectives de sécurité qui seront instancier en règles de sécurité durant la tâche suivante.
    - écarter quelques objectives de sécurité, tout en justifiant les raisons.
  - **Définir les règles de sécurité à mettre en place** : pour chaque objective de sécurité retenu, un ensemble de règles de sécurité doit être défini. La réalisation d'une telle tâche demande de l'expertise pour fournir des règles efficaces. De plus, la définition des règles de sécurité doit être accompagnée par des rapports d'estimation des coûts relatifs à la mise en place de ces règles



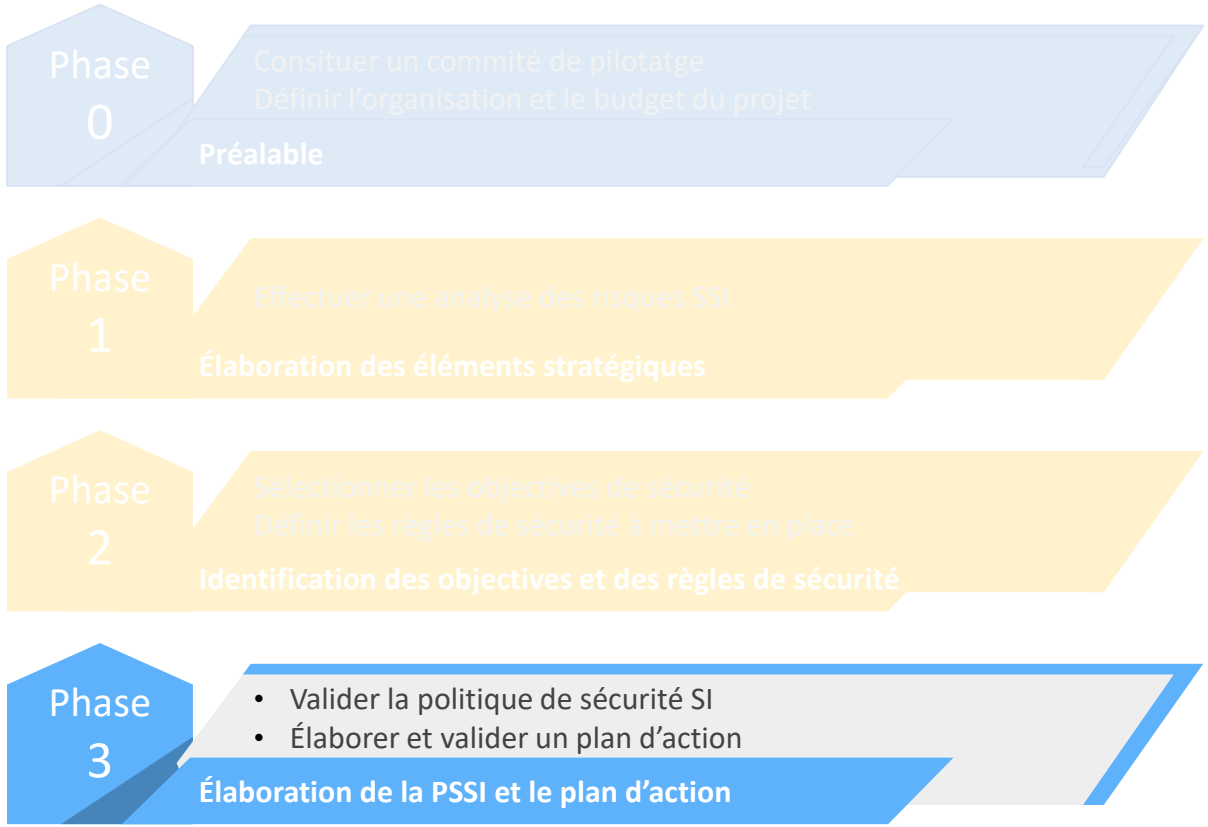
Les phases d'élaboration d'une PSSI

Copyright - Tout droit réservé - OFPPT

PARTIE 2

Démarche de la mise en place d'une PSSI

- La phase 3 est la dernière phase de l'élaboration d'une PSSI.
- Comme illustré dans la figure ci-contre, la phase 3 inclue deux tâches :
  - **Valider la politique de sécurité SI** : l'objectif de cette tâche est de fournir un document valide décrivant la PSSI. Pour ce faire, cette tâche veille sur la rédaction d'un tel document ainsi que la vérification de la cohérence des règles de sécurité (définies durant la phase précédente) et leurs applicabilités au sein de l'organisation.
  - **Élaborer et valider un plan d'action** : cette tâche consiste à définir un plan d'action pour appliquer la PSSI élaborée. Les principales étapes à réaliser, durant cette tâche, sont :
    - Établir un plan d'action adéquat pour chaque unité organisationnelle ;
    - Rédiger une charte de sécurité qui définit un ensemble de règles à appliquer par les employé durant l'interaction avec les actifs de l'entreprise ;
    - Communiquer la PSSI auprès des employés ;
    - Former et sensibiliser les employés à l'importance de la sécurité et l'application de la PSSI.



Les phases d'élaboration d'une PSSI

Copyright - Tout droit réservé - OFPPT

CHAPITRE 1

PRÉSENTER LA POLITIQUE DE SÉCURITÉ DU SI

1. Démarche de la mise en place d'une politique de sécurité du SI et gestion des risques
2. **Normes et méthodes de gestion des risques**
3. Approche PDCA
4. Veille technologique
5. Quiz sur les notions de base relatives à l'assurance d'une amélioration continue de la sécurité SI

Définition et objectifs de gestion des risques

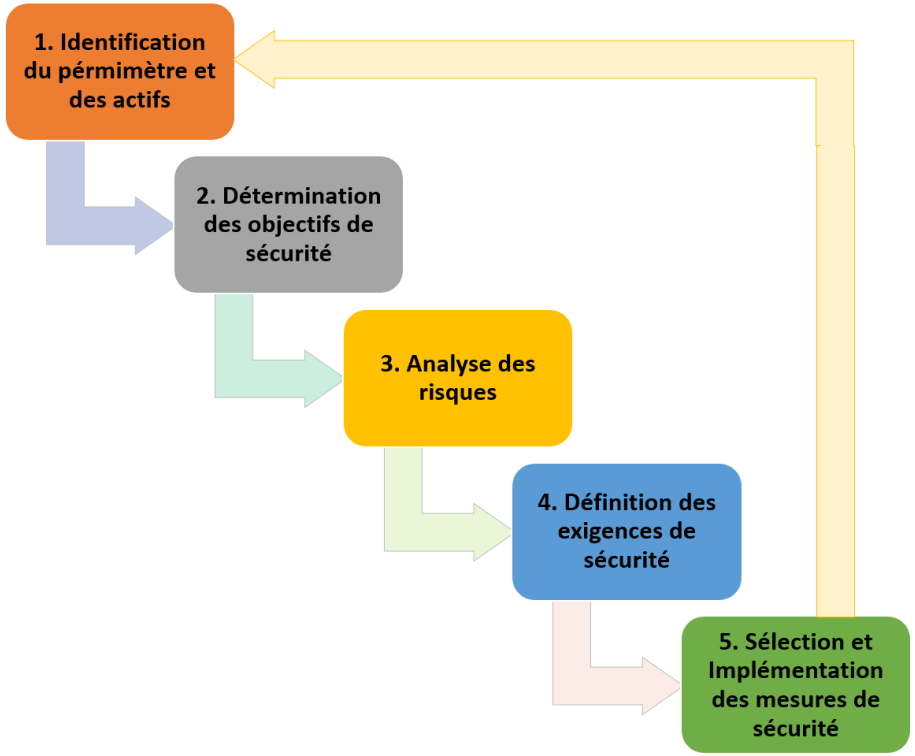
- La gestion des risques est un processus permettant d'identifier, évaluer et prioriser les menaces et les risques visant une organisation et son SI afin de :
    - Sélectionner les mesures de sécurité et les plans d'action à mettre en place.
    - Proposer des ajustements pour les solutions de sécurité déjà mises en place.
- Selon l'organisation internationale de normalisation (International Organization for Standardization ISO, en anglais), la gestion des risques est une démarche composée d'un ensemble d'activités permettant de guider une organisation face aux risques possibles.
- Les principaux objectifs d'une démarche de gestion des risques SI :
    - Amélioration de la sécurité de l'organisation et de son SI ;
    - Justification du budget nécessaire pour sécuriser un SI ;
    - Preuve de crédibilité du SI grâce aux analyses réalisées.
- La gestion des risques SI est un instrument important d'une PSSI efficace.
- En ce qui suit, nous détaillerons :
    - Une démarche typique de la gestion des risques ;
    - La méthode EBIOS comme exemple de méthodes de gestion des risques ; et
    - La norme ISO 27005.

Copyright - Tout droit réservé - OFPPT

PARTIE 2

Processus de la gestion des risques

- Généralement, un processus de gestion des risques est un processus itératif, qui inclut essentiellement cinq étapes primordiales :
    - Identification du périmètre et des actifs d'une organisation ;
    - Détermination des objectifs de sécurité (disponibilité, confidentialité, intégrité, etc.) ;
    - Analyse des risques, qui est le cœur du processus de gestion des risques, permet de :
        - Identifier les vulnérabilités et les menaces associés à chaque actif ;
        - Estimer l'impact des risques associés à chaque actif ;
        - Prioriser les risques (apprécier le niveau d'impact de chaque risque).
    - Définition des exigences de sécurité qui permet de spécifier les risques de sécurité à traiter ;
    - Sélection et implémentation des mesures de sécurité en fonction des résultats des étapes précédentes.
- Le processus illustré dans la figure ci-contre est admis par la majorité des méthodes et normes de gestion des risques. La différence majeure c'est que chaque norme ou méthode utilise une terminologie appropriée. De même, certaines normes/méthodes adoptent le principe de l'amélioration continue et d'autres non.

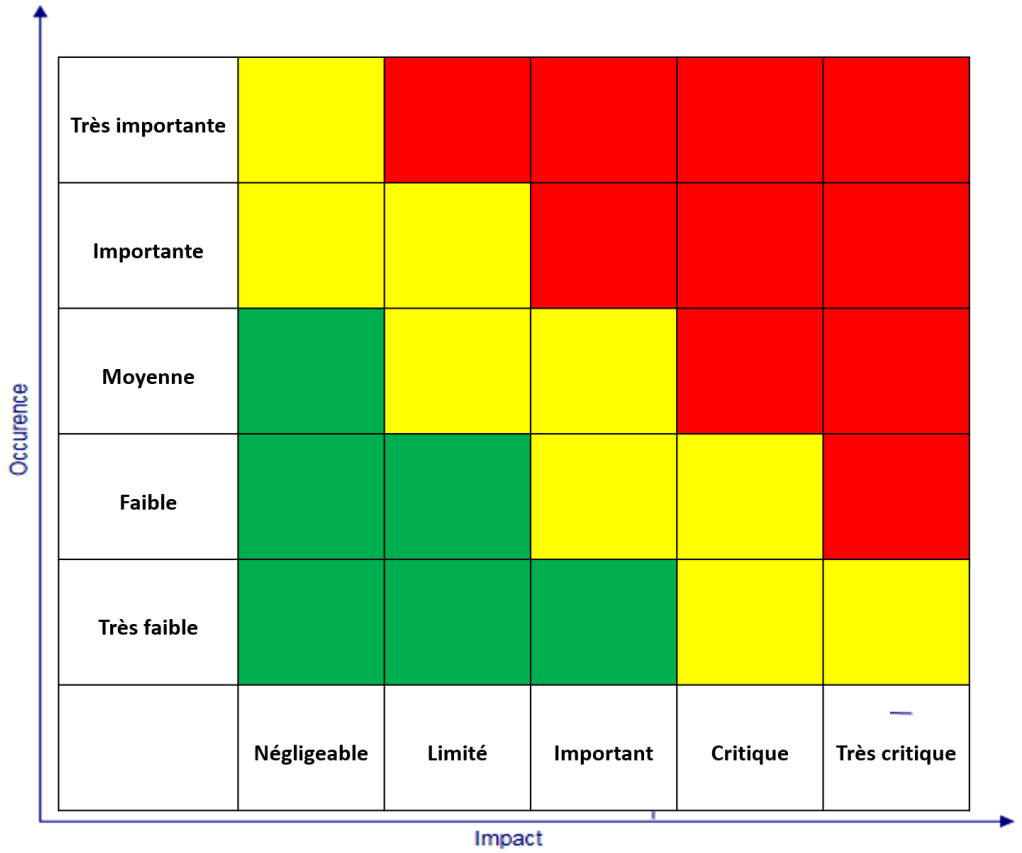


Étapes primordiales dans le processus de la gestion des risques
Source : https://www.nmayer.eu/publis/NMA-JPH_MISC24.pdf

Copyright - Tout droit réservé - OFPPT

Priorisation des risques

- Elle fait partie du processus de gestion des risques, plus particulièrement de la phase d'analyse des risques.
- Elle consiste à classifier les risques identifiés par ordre de priorité afin de pouvoir les raffiner dans l'étape suivante en choisissant les risques à traiter. Notamment qu'il est impossible de traiter tous les risques.
- Le concept clé permettant la priorisation des risques est d'évaluer son **niveau de criticité.**
- La **criticité d'un risque** est généralement **estimée** en fonction de :
    - La **fréquence d'apparition** (occurrence) d'un risque ;
    - Le niveau d'**impact** d'apparition d'un risque.
- La fréquence d'apparition et l'impact d'un risque sont présentés sous la forme d'une échelle à différents niveaux. Dans la figure ci-contre, une échelle à cinq niveaux est choisie.
- La **criticité d'un risque** ne peut pas être une valeur exacte, c'est **une valeur relative** qui dépend essentiellement de l'expertise de l'équipe menant le processus de gestion des risques, et du niveau de la granularité des échelles utilisées.



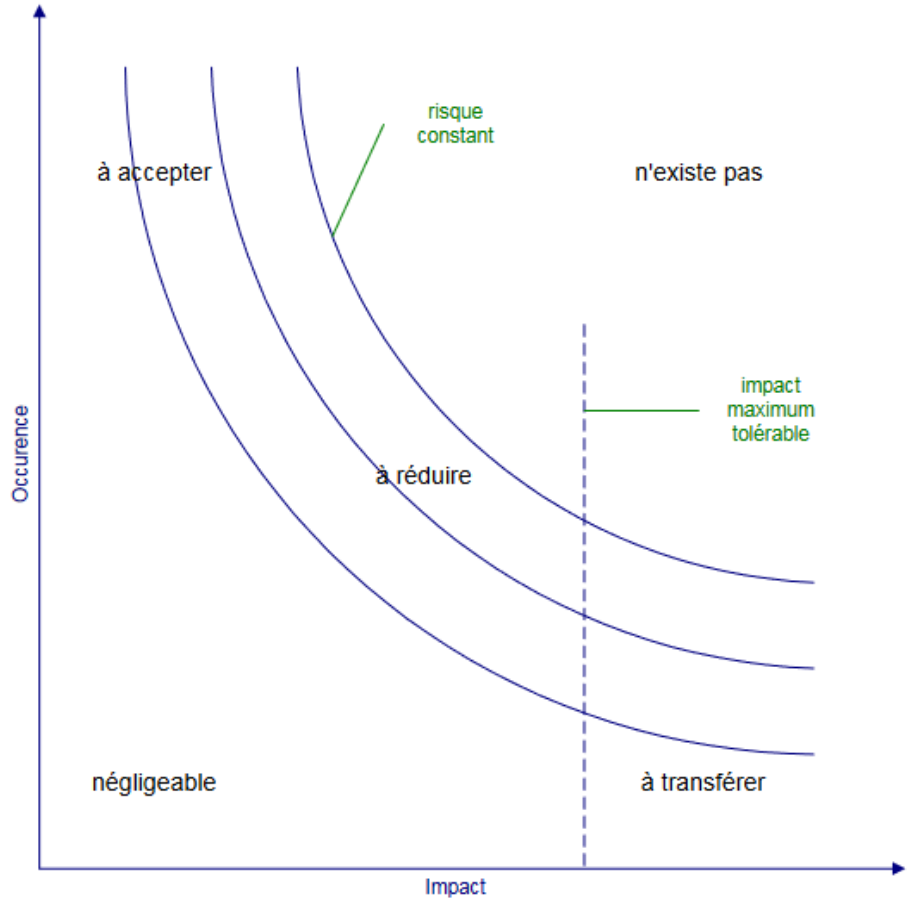
Exemple de matrice de priorisation des risques

PARTIE 2

Copyright - Tout droit réservé - OFPPT

Priorisation des risques

- Comme illustré dans la figure ci-contre, les risques peuvent être organiser en cinq catégories :
    - **Risques négligeables** : sont caractérisés par une faible occurrence et un niveau d'impact négligeable ;
    - **Risques à éviter (Risk avoidance, en anglais)** : possèdent une forte fréquence d'apparition et un niveau d'impact important. Ces risques ne doivent pas exister. Autrement dit, les activités de l'organisation doivent être mises en causes ;
    - **Risques acceptés** : sont des risques très fréquents (occurrence importante) et un niveau d'impact faible ;
    - **Risques à transférer** : possèdent une occurrence minimale et un niveau d'impact très importants. Ce type de risque est généralement à transférer pour être couverts par un tiers ou une assurance ;
    - **Risques à traiter (Risk mitigation, en anglais**) : ce sont les risques qui n'appartiennent à aucune des catégories de risques précédentes. Cette catégorie de risques doit être traité par le processus de gestion des risques afin de leurs diminuer leurs criticités via la mise en place des mécanismes de sécurité.



Les différentes zones de risque

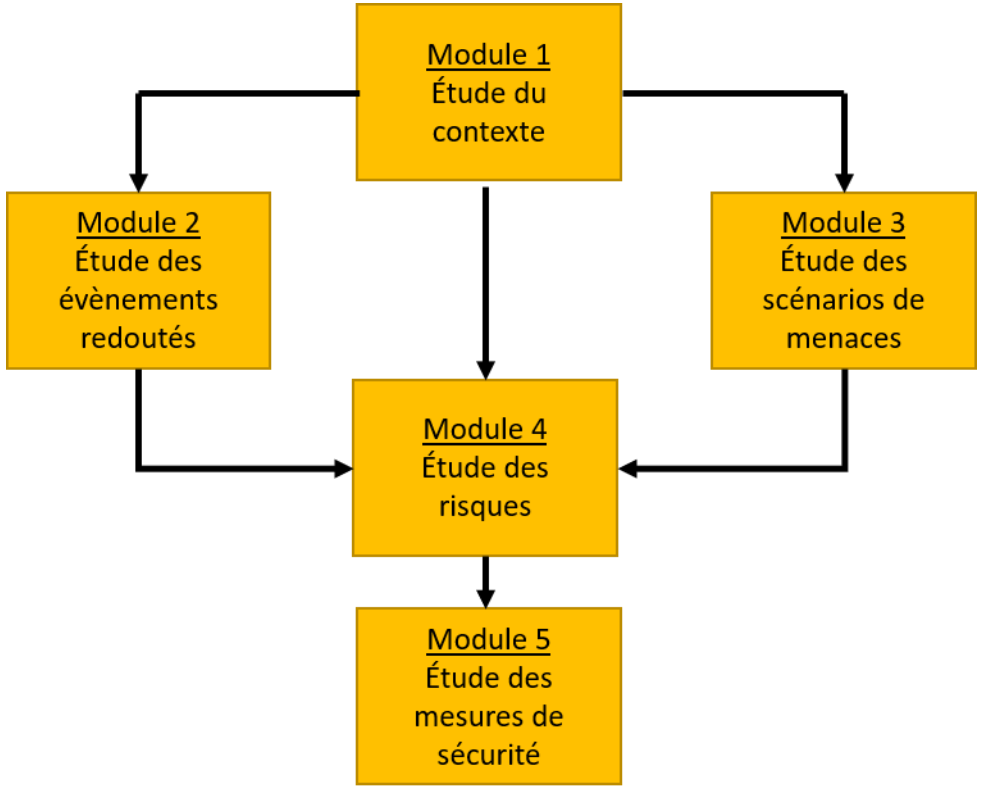
Source : https://www.nmayer.eu/publis/NMA-JPH_MISC24.pdf

PARTIE 2

Copyright - Tout droit réservé - OFPPT

Méthode EBIOS

- La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) est une méthode formelle de gestion des risques qui est organisé en cinq modules :
    1. Étude du contexte ;
    2. Étude des événements redoutés ;
    3. Étude des scénarios de menaces ;
    4. Étude des risques ;
    5. Étude des mesures de sécurité.
- EBIOS décrit une démarche itérative qui est mise à jour d'une manière continue. En fait, chaque module peut être examiné plusieurs fois afin d'en améliorer le contenu.
- En ce qui suit, nous détaillerons les activités effectuées dans chaque module de la démarche EBIOS, en se basant sur le référentiel officiel de la méthode EBIOS.



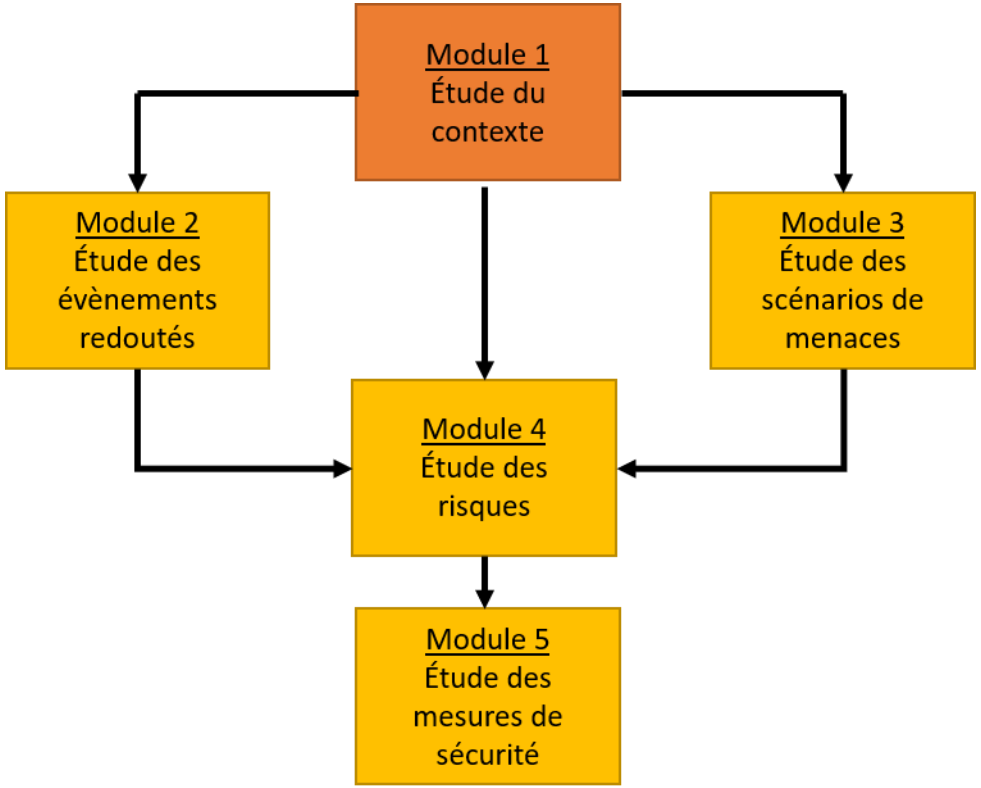
Démarche itérative de la méthode EBIOS
Source : https://www.ssi.gouv.fr/uploads/2011/10/EBIOS-1-GuideMethodologique-2010-01-25.pdf

PARTIE 2

Copyright - Tout droit réservé - OFPPT

Démarche de la méthode EBIOS

- Le premier module de la démarche EBIOS est intitulé **Étude de contexte**.
- Ce module permet de formaliser le cadre de l'étude et déterminer les éléments nécessaires pour mener le processus de gestion des risques.
- Ce module est composé de trois activités :
    - **Activité 1.1 Définir le cadre de la gestion des risques.** L'objectif de cette activité est de définir le périmètre d'étude, le contexte d'étude et les sources de menaces ;
    - **Activité 1.2 Préparer les métriques**. L'objectif de cette activité est de définir les échelles et les objectifs de sécurité qui seront utiliser par la suite pour l'étude des risques ;
    - **Activité 1.3 Identifier les biens**. L'objectif est de déterminer les biens (les actifs) au sein du périmètre de l'étude.



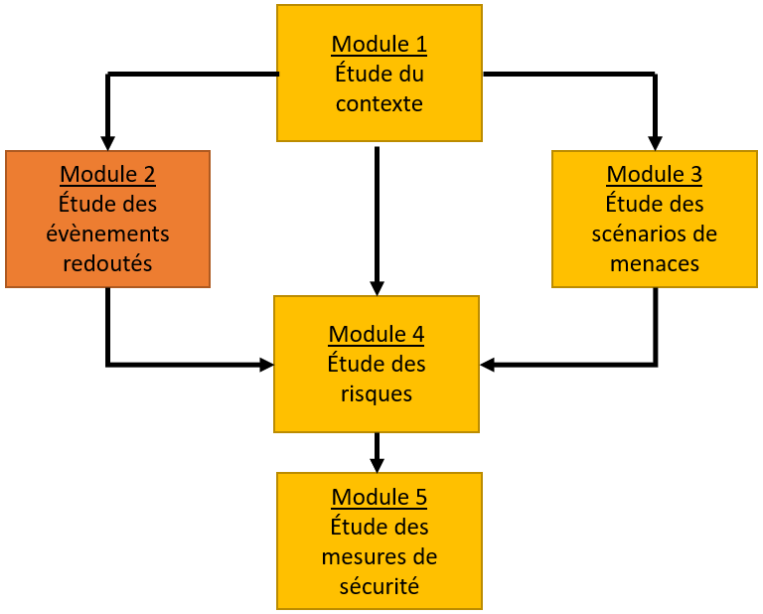
Démarche itérative de la méthode EBIOS
Source : https://www.ssi.gouv.fr/uploads/2011/10/EBIOS-1-GuideMethodologique-2010-01-25.pdf

PARTIE 2

Copyright - Tout droit réservé - OFPPT

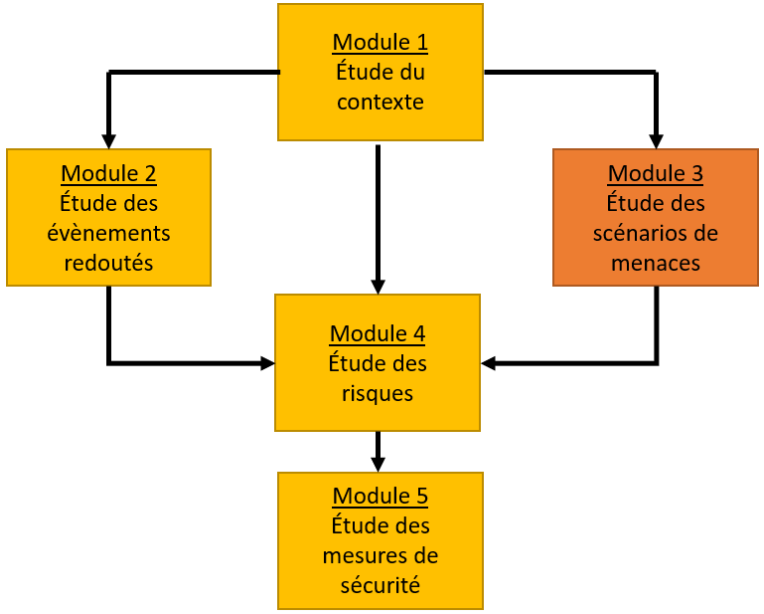
PARTIE 2

Démarche de la méthode EBIOS



- Le deuxième module est intitulé **Étude des évènements redoutés**.
- Ce module permet d'étudier tous les événements redoutés en estimant le niveau de gravité de chaque événement redouté :

  Un événement redouté est un événement indésirable dont la survenu n'est pas souhaité en regard des exigences de sécurité.
- Ce module est composé d'une seule activité : **apprécier les événements redoutés.**

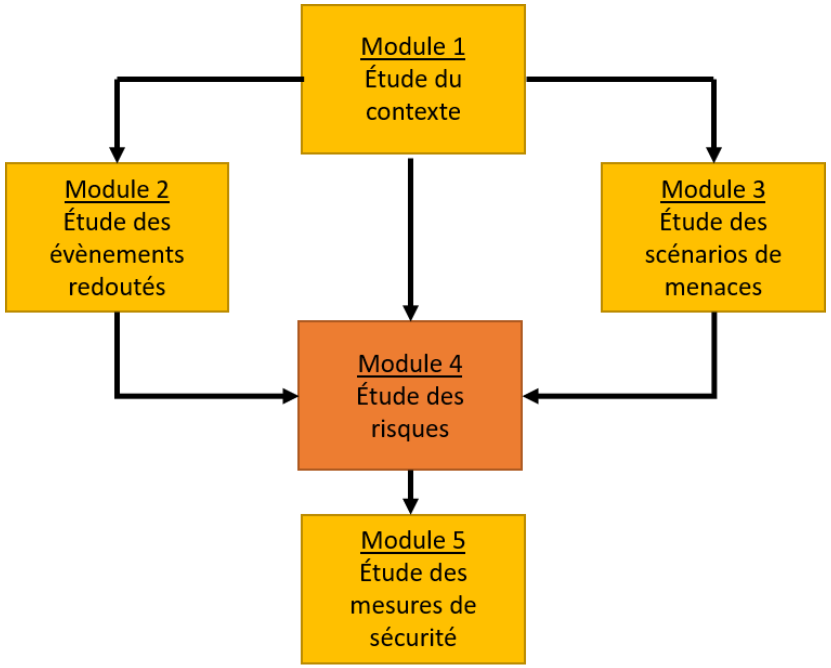


- Le troisième module est intitulé **Étude des scénarios de menaces**.
- Ce module permet d'étudier tous les scénarios de menaces en estimant la vraisemblance de chaque scénario de menaces :
  - La vraisemblance et la fréquence de l'apparition d'un scénario de menace.
- Ce module est composé d'une seule activité : **Apprécier les scénarios de menaces.**

Copyright - Tout droit réservé - OFPPT

Démarche de la méthode EBIOS

- Le quatrième module est intitulé **Étude des risques.**
- Ce module permet d'identifier les scénarios des risques qui peuvent apparaître dans le périmètre d'étude en réalisant une corrélation entre les événements redoutés et les scénarios des menaces. L'appréciation (priorisation) des risques est également réalisée dans ce module, afin de choisir les mesures de sécurité adéquate dans le cinquième module.
- Ce module est composé de deux activités :
    - **Activité 4.1 Apprécier les risques**. L'objectif principal de cette activité est de mettre en évidence et de caractériser les risques réels.
    - **Activité 4.2 Identifier les objectifs de sécurité.** L'objectif principal de cette activité est de spécifier la manière du traitement du risque en fonction du résultat de son évaluation



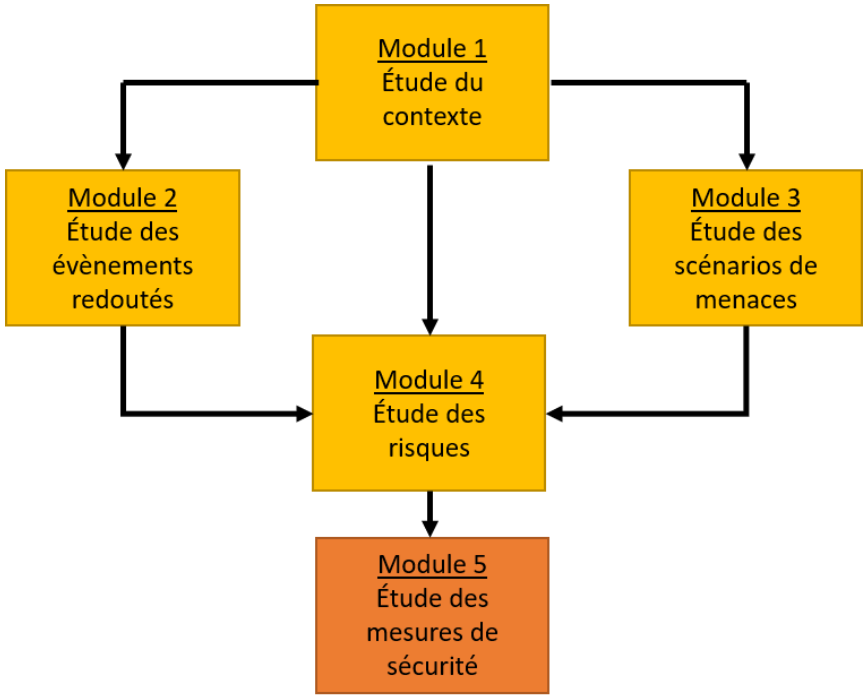
PARTIE 2

Copyright - Tout droit réservé - OFPPT

Démarche de la méthode EBIOS

- Le cinquième module est intitulé **Étude des mesures de sécurité.**
- Ce module permet de sélectionner les mesures de sécurité permettant de traiter les risques, conformément aux objectifs de sécurité qui ont été définis dans les modules précédents. Il permet également de fournir une planification de la mise en place et la validation de ces mesures de sécurité.
- Ce module est composé de deux activités :
    - **Activité 5.1 Formaliser les mesures de sécurité à mettre en œuvre.** Les objectifs de cette activité sont : identification des mesures de sécurité offrant les critères de sécurité définis dans les modules précédents, spécification des risques résiduels et validation des choix effectués.
    - **Activité 5.2 Mettre en œuvre les mesures de sécurité.** L'objectif de cette activité est la planification et le suivie de la mise en place des solutions de sécurité.

.



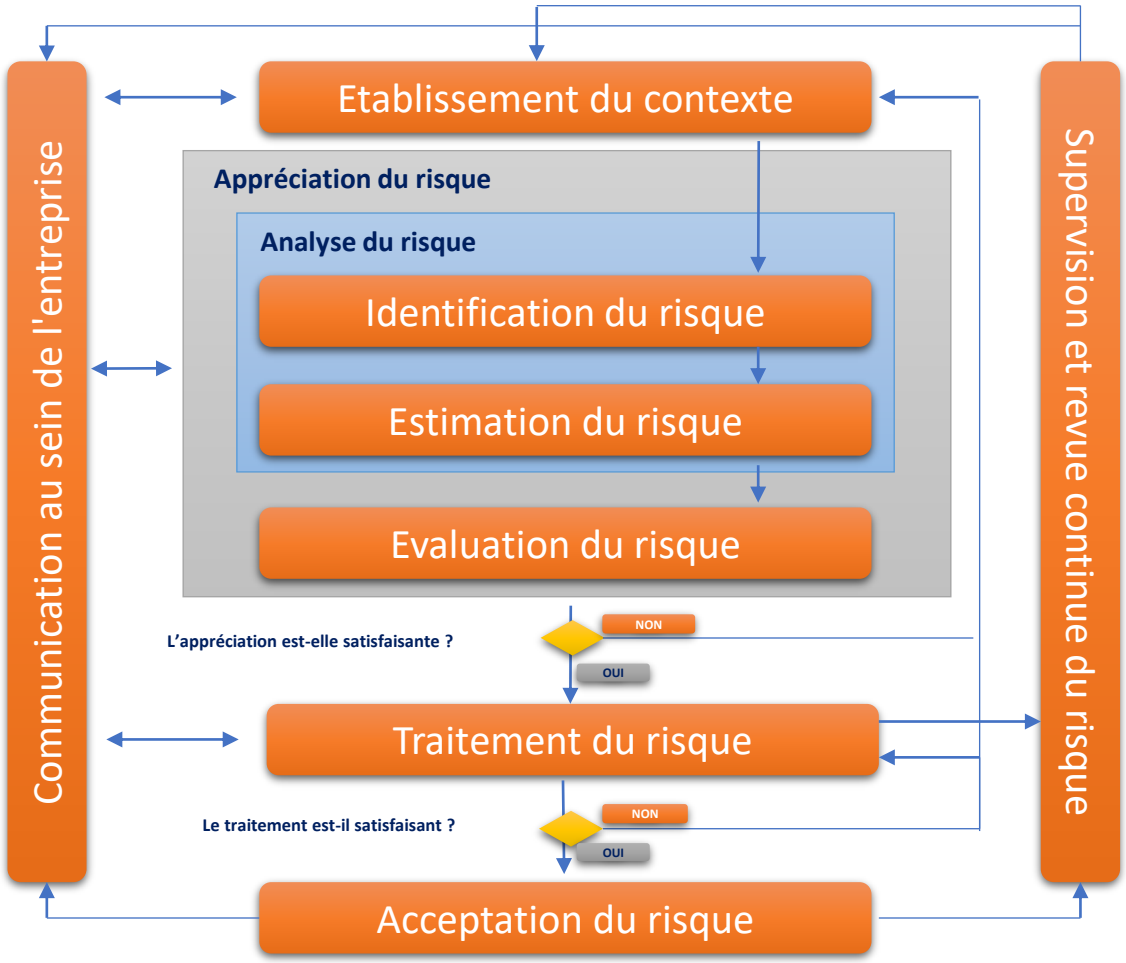
PARTIE 2

Copyright - Tout droit réservé - OFPPT

PARTIE 2

Norme ISO 27005

- La norme ISO 27005 est une norme internationale décrivant les grandes lignes d'un processus de gestion des risques.
- Elle définit une démarche de gestion des risques mais ne constitue pas une méthode. Ce qui fait que chaque organisation peut utiliser sa propre méthodologie.
- Souvent, la norme ISO fait référence à la méthode EBIOS.
- Comme illustré dans la figure ci-contre, la norme ISO 27005 propose un processus organisé en quatre phases principales :
    - **Etablissement du contexte** : peut être effectuée grâce à un questionnaire détaillé et une étude préliminaire du contexte de l'organisation et son SI ;
    - **Appréciation du risque :** inclut l'analyse et l'évaluation du risque en fonction des enjeux de l'organisation ;
    - **Traitement du risque** : réalisé via la mise en place des mesures de sécurité ;
    - **Acceptation du risque après traitement.**
- Parallèlement à ces quatre phases, deux autres activités sont réalisées :
    - Communication au sein de l'entreprise.
    - Supervision et revue continue du risque.



Copyright - Tout droit réservé - OFPPT

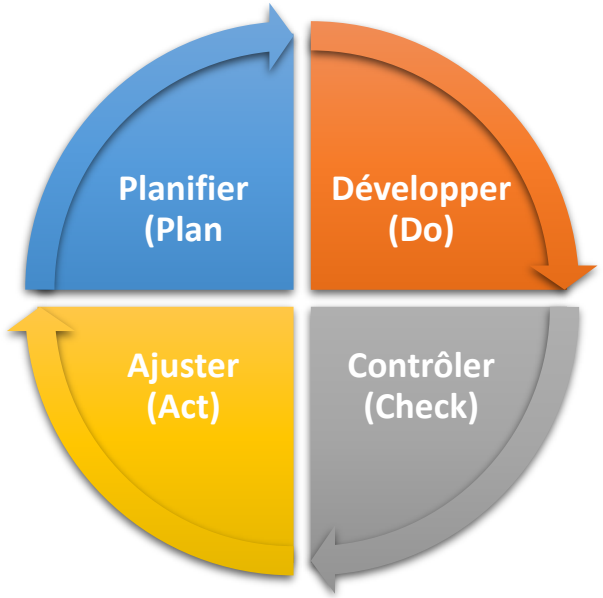
CHAPITRE 1

PRÉSENTER LA POLITIQUE DE SÉCURITÉ DU SI

1. Démarche de la mise en place d'une politique de sécurité du SI et gestion des risques
2. Normes et méthodes de gestion des risques
3. **Approche PDCA**
4. Veille technologique
5. Quiz sur les notions de base relatives à l'assurance d'une amélioration continue de la sécurité SI

Approche PDCA

- Pour veiller à l'efficacité de la politique de sécurité du système d'information et faire face aux nouveaux logiciels malveillants et attaques, il faut suivre une démarche d'amélioration continue.
- L'approche PDCA, souvent appelée la roue de Deming, est l'acronyme de : Planifier, Développer, Contrôler, et Ajuster (Plan, Do, Check and Act, en anglais).
- L'approche PDCA consiste à réaliser d'une manière continue les quatre étapes :
  - **Planifier (Plan)** : consiste à élaborer une politique de sécurité des SI. Cette action est finalisée par un document de référence et un plan d'action ;
  - **Développer (Do)** : se réfère à exécuter le plan d'actions défini dans l'étape précédente via la mise en place des mesures de sécurité, sensibilisation et formation des employés, etc. ;
  - **Contrôler (Check)** : consiste à réaliser des audit et contrôles internes récurrents afin de vérifier l'efficacité des actions réalisées durant l'étape précédente, en particulier les mesures de sécurité mises en place. L'identification d'une ou plusieurs actions inefficaces fait appel à la réalisation des ajustements qui seront définies et planifier durant les deux étapes suivantes (Ajuster et planifier).
  - **Ajuster (Act)** : consiste à
    - La mise en place des actions correctives pour certaines actions inefficaces détectés dans l'étape précédente, qui n'exige pas une planification, ou
    - La suggestion des d'amélioration pour certaines actions qui seront planifiés dans l'étape suivante (c.à.d., Planifier).



Roue de Deming

PARTIE 2

Copyright - Tout droit réservé - OFPPT

CHAPITRE 1

PRÉSENTER LA POLITIQUE DE SÉCURITÉ DU SI

1. Démarche de la mise en place d'une politique de sécurité du SI et gestion des risques
2. Normes et méthodes de gestion des risques
3. Approche PDCA
4. **Veille technologique**
5. Quiz sur les notions de base relatives à l'assurance d'une amélioration continue de la sécurité SI

Veille technologique

- Les technologies, en particulier dans le domaine de la sécurité, suivent une évolution très rapide. Par conséquent, la veille technologique en sécurité informatique est primordiale afin de :
    - Assurer une meilleur protection de l'organisation et son système d'information.
    - Garantir une réactivité efficace, en temps réel face aux intrusions.

- La veille technologique en sécurité informatique consiste à :
    - Suivre les évolutions réglementaires et techniques dans le domaine de l'organisation ;
    - Acquérir des informations à propos les nouvelles technologies de sécurité ainsi que les nouvelles vulnérabilités identifiés dans les systèmes informatique ;
    - Veiller sur la mise en place des nouvelles technologies afin de garanti une meilleur sécurité logique et physique du système d'information de l'organisation ;
    - Prendre des mesures de sécurité pour éviter les risques associés à l'exploit des vulnérabilités récemment identifiées.

- L'adoption d'une démarche PDCA accompagné des outils assurant la veille technologique peuvent garantir une amélioration continue de la politique de sécurité du système d'information de l'organisation, ce qui permet de garantir son efficacité.

- Passons maintenant à découvrir dans les trois chapitres suivants les mesures de sécurités qui peuvent être mis en place dans le cadre de d'une PSSI.

Copyright - Tout droit réservé - OFPPT

CHAPITRE 1

PRÉSENTER LA POLITIQUE DE SÉCURITÉ DU SI

1. Démarche de la mise en place d'une politique de sécurité du SI et gestion des risques
2. Normes et méthodes de gestion des risques
3. Approche PDCA
4. Veille technologique
5. **Quiz sur les notions de base relatives à l'assurance d'une amélioration continue de la sécurité SI**

01 - Présenter la politique de sécurité du SI

Quiz sur les notions de base relatives à l'assurance d'une amélioration continue de la sécurité SI

Énoncé

- **Question 1 : Quelles sont les domaines de sécurité qui peuvent être couvert par une politique de sécurité système d'informations (PSSI) ?**
  - ❑ La sécurité physique uniquement
  - ❑ La sécurité organisationnelle uniquement
  - ❑ La sécurité de la communication uniquement
  - ❑ Les domaines de sécurité relatifs à toutes les activités d'une organisation, y compris la sécurité physique, informatique, organisationnelle, etc.
- **Question 2 : Une politique de sécurité système d'informations (PSSI) doit être :**
  - ❑ Typique afin d'être partagé entre plusieurs organisations appartenant aux mêmes domaines d'activités
  - ❑ Spécifique à une seule organisation et ne peut pas être partagé avec d'autres organisations
- **Question 3 : Quel est la norme qui a fourni une description haut niveau du processus de gestion des risques ?**
  - ❑ EBIOS
  - ❑ ISO 27000
  - ❑ ISO 27005
- **Question 4 : L'acronyme PDCA signifie**
  - ❑ Plan, Do, Check , Act
  - ❑ Plan, Design, Control, Approve
  - ❑ Planifier, Développer, Contrôler, Ajuster
  - ❑ Protéger, Développer, Concevoir, Améliorer

Copyright - Tout droit réservé - OFPPT

01 - Présenter la politique de sécurité du SI

Quiz sur les notions de base relatives à l'assurance d'une amélioration continue de la sécurité SI

Correction

- **Question 1 : Quelles sont les domaines de sécurité qui peuvent être couvert par une politique de sécurité système d'informations (PSSI) ?**
  - ❑ La sécurité physique uniquement
  - ❑ La sécurité organisationnelle uniquement
  - ❑ La sécurité de la communication uniquement
  - ▣ Les domaines de sécurité relatifs à toutes les activités d'une organisation, y compris la sécurité physique, informatique, organisationnelle, etc.
- **Question 2 : Une politique de sécurité système d'informations (PSSI) doit être :**
  - ❑ Typique afin d'être partagé entre plusieurs organisations appartenant aux mêmes domaines d'activités
  - ▣ Spécifique à une seule organisation et ne peut pas être partagé avec d'autres organisations
- **Question 3 : Quel est la norme qui a fourni une description haut niveau du processus de gestion des risques ?**
  - ❑ EBIOS
  - ❑ ISO 27000
  - ▣ ISO 27005
- **Question 4 : L'acronyme PDCA signifie**
  - ▣ Plan, Do, Check , Act
  - ❑ Plan, Design, Control, Approve
  - ▣ Planifier, Développer, Contrôler, Ajuster
  - ❑ Protéger, Développer, Concevoir, Améliorer

PARTIE 2

Copyright - Tout droit réservé - OFPPT

CHAPITRE 2

APPLIQUER LES DROITS NÉCESSAIRES POUR SÉCURISER L'INFORMATION

Ce que vous allez apprendre dans ce chapitre :

- Définir les principes relatifs au contrôle d'accès
- Découvrir les différentes méthodes d'authentification (mot de passe, biométrique, renforcée, etc.)
- Présenter les règles d'autorisation et le besoin de la traçabilité

4 heures

CHAPITRE 2

APPLIQUER LES DROITS NÉCESSAIRES POUR SÉCURISER L'INFORMATION

1. **Contrôle d'accès**
2. Méthodes d'authentification
3. Règles d'autorisation et traçabilité
4. Quiz sur les notions de la sécurisation de l'information

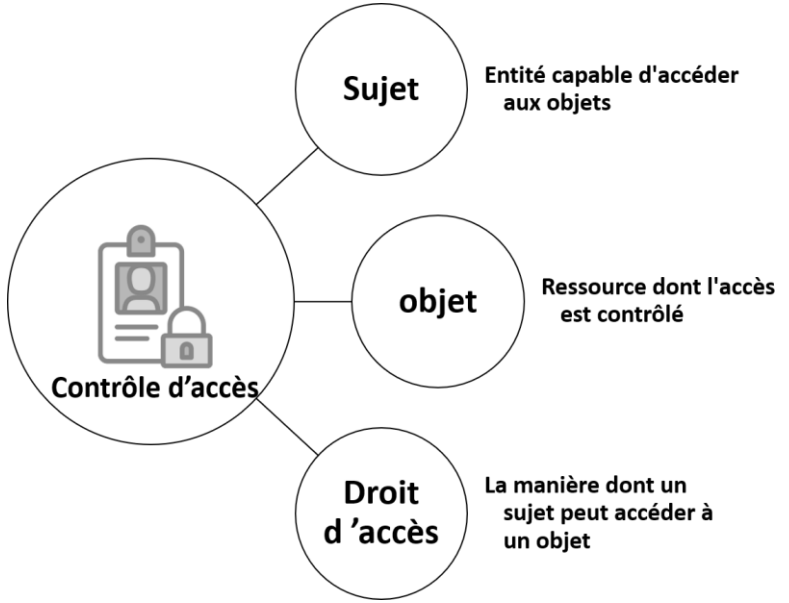
Contrôle d'accès

- Le contrôle d'accès est un concept fondamental de la sécurité de l'information.
- Il dicte qui ou quoi est autorisé à utiliser des ressources dans un environnement informatique.
- Deux types de contrôle d'accès peuvent être distingués :

  Le contrôle d'accès physique : limite l'accès aux lieux (bâtiments, salles, etc.) et aux ressources informatiques physiques (serveurs, disques durs, etc.).

  Le contrôle d'accès logique : limite les connexions aux systèmes informatiques, aux réseaux, aux fichiers et aux données.

- Comme illustré dans la figure ci-contre, les éléments de base du contrôle d'accès sont trois :
  - **Sujet** : entité capable d'accéder à un objet. Généralement, un sujet est tenu d'être responsable des actions qu'ils exécutent sur un objet. Trois classes de sujets peuvent être distingués : groupe, propriétaire, tout le monde ;
  - **Objet** : ressource généralement utilisée pour contenir et/ou recevoir des informations sensibles. Pour cette raison, l'accès à cet objet est contrôlé pour le limiter aux sujets autorisés ;
  - **Droit d'accès** : décrit la manière d'accès à un objet. Les principaux droits d'accès à un objet sont : lire, écrire, exécuter, supprimer, créer, et rechercher.



Les éléments de base du contrôle d'accès

PARTIE 2

Copyright - Tout droit réservé - OFPPT

Étapes de gestion de contrôle d'accès

- Le contrôle d'accès peut être assuré via trois étapes primordiales, qui sont : Authentification, Autorisation, et Traçabilité (Accounting, en anglais). L'abréviation de ces étapes est **AAA**.
- **Authentification** : processus de vérification de l'identité d'une entité (utilisateur, application, etc.) qui demande d'accéder à une ressource. Comme illustré dans la figure ci-contre, une entité, qui s'est authentifiée avec succès (c.à.d., il a pu prouver son identité), peut passer à la deuxième étape du contrôle d'accès ;
- **Autorisation** : processus de vérification des permissions accordées à l'entité en question vis-à-vis de la ressource sollicitée. Généralement, la vérification utilise les informations de preuve d'identité fourni dans l'étape d'authentification. Après vérification, une entité autorisée pourra accéder à la ressource sollicitée. Dès que l'entité bénéficie de l'accès à la ressource, la troisième étape sera lancée ;
- **Traçabilité** : processus de suivi des activités d'une entité durant son accès à une ou plusieurs ressources, tel que la durée d'accès, les modifications effectuées, etc. Les informations collectées durant ce processus, souvent appelés traces numériques, sont conservées dans des fichiers journaux (log).

Les étapes de gestion du contrôle d'accès

PARTIE 2

Copyright - Tout droit réservé - OFPPT

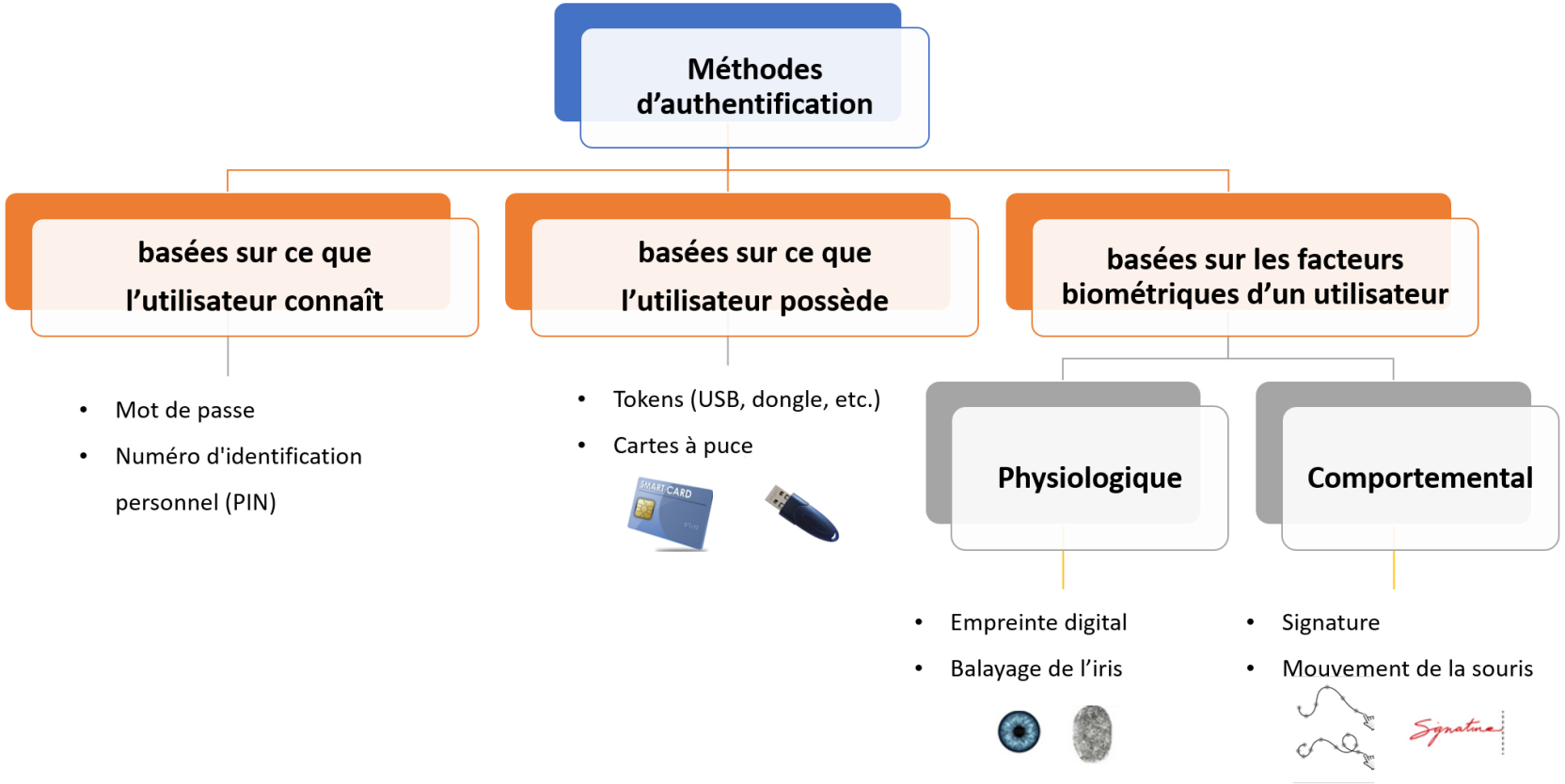
CHAPITRE 2

APPLIQUER LES DROITS NÉCESSAIRES POUR SÉCURISER L'INFORMATION

1. Contrôle d'accès
2. **Méthodes d'authentification**
3. Règles d'autorisation et traçabilité
4. Quiz sur les notions de la sécurisation de l'information

Méthodes d'authentification

Trois grandes classes de méthodes d'authentification peuvent être distinguées. Ces trois classes ainsi qu'un ensemble d'exemples sont illustrés dans la figure ci-dessous.



Classification des méthodes d'authentification

PARTIE 2

Copyright - Tout droit réservé - OFPPT

Authentification avec mot de passe

- L'authentification avec mot de passe est une méthode d'authentification qui est basée sur la vérification d'un secret partagé avec l'utilisateur.
- C'est la méthode d'authentification la plus répandue, pour les raisons suivantes :
    - La plus simple à mettre en œuvre ;
    - La moins gourmande en consommation d'énergie (à cause de la simplicité des algorithmes de vérification) ;
    - La moins couteuse (ne nécessite pas des équipements de vérification spécifiques).
- Toutefois, l'authentification avec mot de passe offre un minimum de sécurité qui dépend essentiellement de la robustesse du mot de passe (longueur, niveau de complexité, caractères aléatoires, etc.).
- L'authentification avec mot de passe présente plusieurs risques qui reposent sur :
    - L'utilisation des mots de passe simples (vulnérable aux attaques par dictionnaire) ;
    - L'échange des mots de passe sur les réseau informatique (vulnérable aux attaques d'interception de trafic) ;
    - Le stockage des mots de passe en claire ;
    - L'utilisation fréquente du même mot de passe pour une longue période (vulnérable aux attaques par force brute).
- **Attaque par dictionnaire** : une attaque qui profite de l'utilisation des mots courant et des mots de passe courts. Elle consiste à essayer une liste de mots courants et un dictionnaire de mots de passe. Généralement, exécuté à l'aide d'un logiciel tel que John the ripper.
- **Attaques par force brute** : une attaque qui profite de l'utilisation d'un mot de passe pour une longue période. Elle consiste à tester toutes les combinaisons possibles jusqu'à la découverte du mot de passe

Copyright - Tout droit réservé - OFPPT

Authentification par Jeton

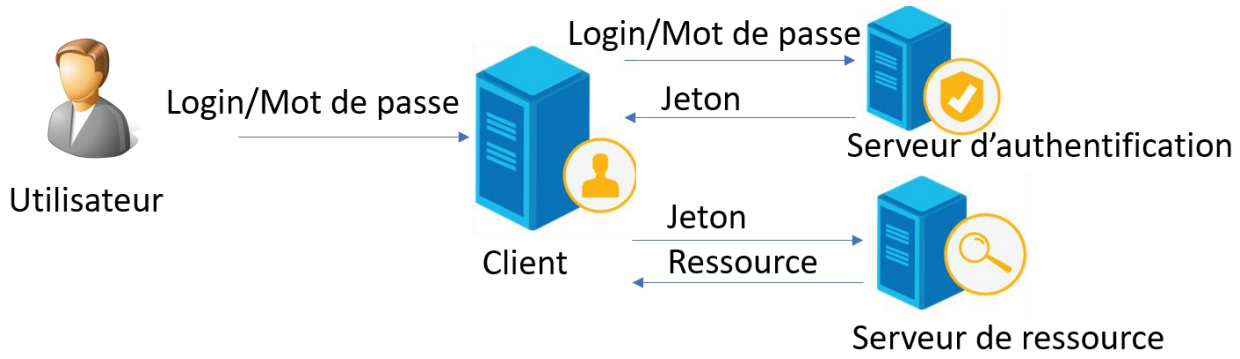
- L'athentification par jeton est une méthode basée sur l'authentification avec mot de passe. Toutefois, elle permet de faire face à certaines limites de l'authentification avec mot de passe (utilisation fréquente des mots de passe et échanges dans le réseau) tout en bénéficiant de ses avantages.
- Le principe de l'authentification par jeton est le suivant :

  Un utilisateur qui désire accéder à une (aux) ressource(s) dont l'accès est contrôlé, fournit ses identifiants (le couple login/mot de passe) via une interface affichée par un client ;

  Ce couple est transmis à un serveur d'authentification qui vérifie l'authenticité de l'utilisateur ainsi que l'autorisation d'accès accordée ;

  Un utilisateur autorisé qui s'est authentifié avec succès, reçoit un jeton d'accès unique (un code aléatoire) pour une durée limitée via le client ;

  Grâce au jeton reçu, l'utilisateur bénéficie d'un accès à la (aux) ressource(s) demandée(s), pendant la durée de vie du jeton. Ce qui permet de réduire l'utilisation fréquente et l'échange du mot de passe dans le réseau.

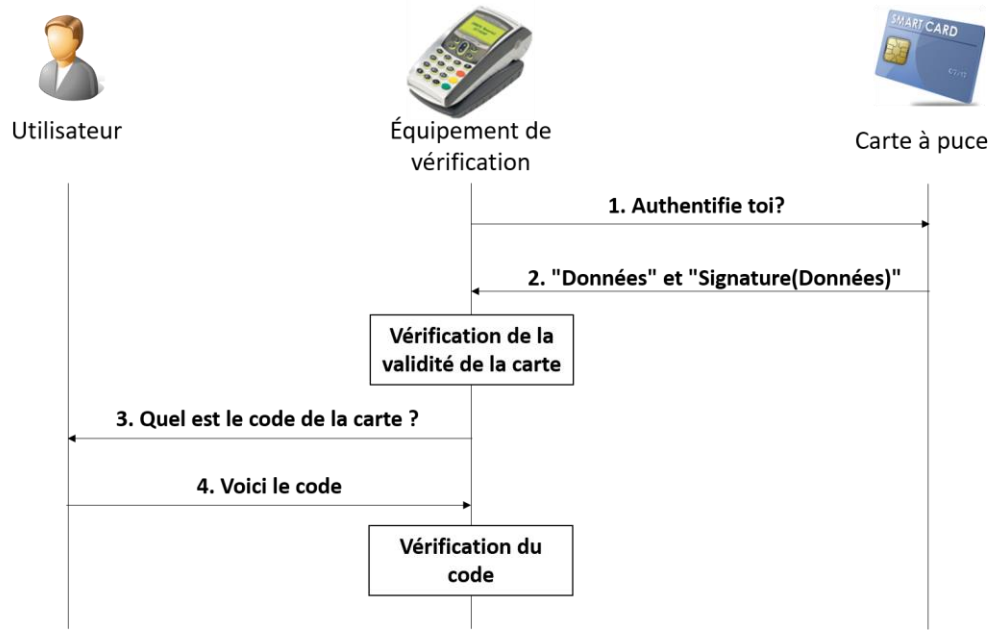


Processus d'authentification par jeton

Copyright - Tout droit réservé - OFPPT

Authentification par carte à puce

- Une carte à puce est une carte contenant des circuits intégrés comprenant des composants de stockage de mémoire non volatile pour stocker :
    - Des certificats numériques prouvant l'identité de l'utilisateur porteur de la carte.
    - Des permissions et des informations d'accès.
- Le principe de l'authentification par carte à puce est le suivant :
    - Un utilisateur qui désire s'authentifier insère (ou approche) sa carte à puce à l'équipement de vérification approprié. Ce dernier envoie alors une requête à la carte qui demande les informations d'authentification ;
    - La carte à puce répond par l'envoie des informations qu'elle stocke ;
    - À la réception de ces informations, l'équipement vérifie la validité de la carte (souvent, il envoie une requête de vérification à l'autorité délivrant cette carte). Une fois vérifiée, l'équipement demande à l'utilisateur de saisir un code secret ;
    - L'utilisateur saisit alors le code secret ;
    - À la réception du code, l'équipement vérifie le code fournit qui sert à prouver que l'utilisateur est le propriétaire de la carte. Une fois vérifié, l'utilisateur accède à la ressource demandée.



Processus d'authentification par carte à puce

PARTIE 2

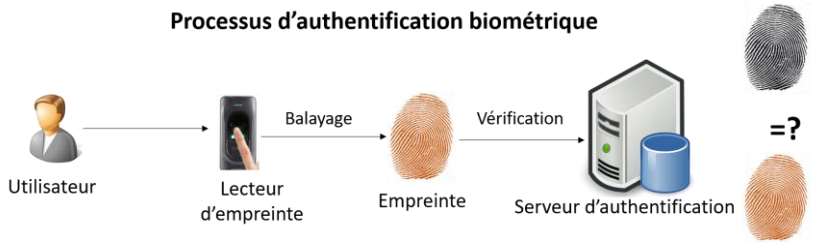
Copyright - Tout droit réservé - OFPPT

Authentification biométrique

- Comme vu précédemment, l'authentification biométrique peut être basée sur des facteurs physiologiques ou des facteurs comportementaux.
- Quel que soit la nature du facteur biométrique utilisé, ce type d'authentification exige deux phases primordiales :

Collecte des facteurs biométriques : consiste à collecter les facteurs biométriques (tel que l'empreinte) d'un utilisateur grâce à un équipement de collecte spécifique (lecteur d'empreinte) et les stocker dans une base de données pour les utiliser plus tard dans la phase d'authentification. Cette phase s'exécute une seul fois par un utilisateur qui désire utiliser ses facteurs biométriques pour s'authentifier.

Phase d'authentification : pour s'authentifier, un utilisateur fournit ses facteurs biométriques (empreinte) grâce à un équipement spécifique (lecteur d'empreinte qui assure le balayage de l'empreinte). Les facteurs collectés sont envoyés au serveur stockant les facteurs stockés (collectés durant la phase de collecte). Le serveur vérifie alors la similitude entre les facteurs fournies et stockés grâce à des algorithmes de vérification spécifique.



PARTIE 2

Copyright - Tout droit réservé - OFPPT

CHAPITRE 2

APPLIQUER LES DROITS NÉCESSAIRES POUR SÉCURISER L'INFORMATION

1. Contrôle d'accès
2. Méthodes d'authentification
3. **Règles d'autorisation et traçabilité**
4. Quiz sur les notions de la sécurisation de l'information

Règles d'autorisation et traçabilité

- Après avoir été authentifié avec succès, la deuxième phase du contrôle d'accès est de vérifier les permissions accordées à l'utilisateur authentifié pour la ressource sollicitée. Souvent, la vérification des permissions se fait en se basant sur une liste de contrôle d'accès (Access Control List, en anglais, et l'abréviation est ACL).
- Une liste de contrôle d'accès est composée de règles qui autorisent ou refusent l'accès à un objet.
- Les deux types d'ACL les plus courants sont :
    - ACL pour les systèmes de fichiers qui gère l'accès des utilisateurs aux répertoires ou aux fichiers. Elle spécifie au système d'exploitation les utilisateurs autorisés à accéder au système, ainsi que les privilèges accordés.
    - ACL réseau qui gère l'accès à un réseau. Souvent, elle fournit des instructions aux commutateurs et/ou aux routeurs quant aux types de trafics autorisés à circuler dans le réseau. Elle dicte également les autorisations accordées aux utilisateurs (appareils) qui sont connectés au réseau.
- L'efficacité des ACL pour la protection des actifs dépends essentiellement des règles d'accès définies. Par conséquent, pour assurer une meilleure efficacité, il faut veiller sur l'application des règles de base suivantes durant la définition des règles d'accès dans une ACL.
    - **Interdiction par défaut** : Tout ce qui n'est pas autorisé explicitement est interdit.
    - **Moindres privilèges** : Autoriser que le strict nécessaire.
- Toutefois, fournir l'accès à un utilisateur authentifié est insuffisant, il faut surveiller les actions exécutées par les utilisateurs. En fait, pour garantir une protection efficace des actifs, il faut mettre en place des outils assurant la traçabilité.
- Pour garantir la non répudiation (c.à.d., garantir qu'aucun utilisateur ne peut nier sa responsabilité de l'exécution des actions collectés sous forme de trace numérique), il faut veiller à protéger les fichiers journaux. Autrement dit, les fichiers journaux doivent être accessible en lecture uniquement afin d'éviter le risque de falsification des traces numériques.

Copyright - Tout droit réservé - OFPPT

CHAPITRE 2

APPLIQUER LES DROITS NÉCESSAIRES POUR SÉCURISER L'INFORMATION

1. Contrôle d'accès
2. Méthodes d'authentification
3. Règles d'autorisation et traçabilité
4. **Quiz sur les notions de la sécurisation de l'information**

Quiz sur les notions de la sécurisation de l'information

Énoncé

- **Question 1 : Le contrôle d'accès :**
  - ❑ Est basé sur un modèle AAA (Authentication, Autorisation, and Accounting)
  - ❑ Assure uniquement le contrôle d'accès aux données numériques
  - ❑ Vérifie l'identité d'une entité qui demande d'accéder à une ressource
  - ❑ dicte qui est autorisé à utiliser des objets (des ressources)
- **Question 2 : Un objet est :**
  - ❑ Une ressource utilisée par un sujet
  - ❑ Une ressource dont l'accès est contrôlé
  - ❑ Une ressource dont l'accès n'est autorisé qu'aux administrateurs
- **Question 3 : L'authentification par carte à puce est une méthode d'authentification basée sur :**
  - ❑ Ce que l'utilisateur connait
  - ❑ Ce que l'utilisateur possède
  - ❑ Les facteurs biométriques d'un utilisateur
- **Question 4 : Parmi les propositions suivantes, quels sont celles qui peuvent être des facteurs biométriques permettant l'authentification ?**
  - ❑ Empreinte
  - ❑ Jeton
  - ❑ Voix
  - ❑ Code secret

Copyright - Tout droit réservé - OFPPT

Correction

- **Question 1 : Le contrôle d'accès :**
  - ◘ Est basé sur un modèle AAA (Authentication, Autorisation, and Accounting)
  - ❑ Assure uniquement le contrôle d'accès aux données numériques
  - ❑ Vérifie l'identité d'une entité qui demande d'accéder à une ressource
  - ◘ dicte qui est autorisé à utiliser des objets (des ressources)
- **Question 2 : Un objet est :**
  - ❑ Une ressource utilisée par un sujet
  - ◘ Une ressource dont l'accès est contrôlé
  - ❑ Une ressource dont l'accès n'est autorisé qu'aux administrateurs
- **Question 3 : L'authentification par carte à puce est une méthode d'authentification basée sur :**
  - ❑ Ce que l'utilisateur connait
  - ◘ Ce que l'utilisateur possède
  - ❑ Les facteurs biométriques d'un utilisateur
- **Question 4 : Parmi les propositions suivantes, quels sont celles qui peuvent être des facteurs biométriques permettant l'authentification ?**
  - ◘ Empreinte
  - ❑ Jeton
  - ◘ Voix
  - ❑ Code secret

Copyright - Tout droit réservé - OFPPT

CHAPITRE 3

SÉCURISER L'ACCÈS PHYSIQUE

Ce que vous allez apprendre dans ce chapitre :

- Décrire les composants permettant le contrôle d'accès physique
- Définir la vidéoprotection et ses composants

2 heures

CHAPITRE 3

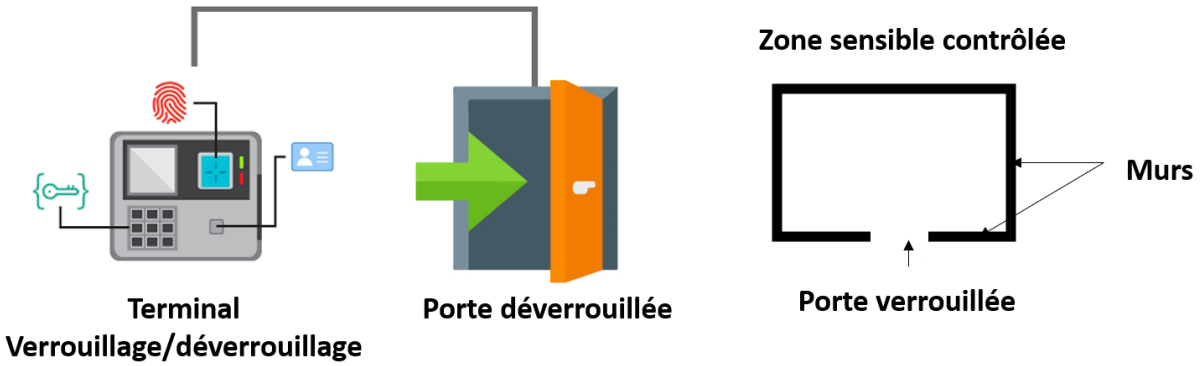
SÉCURISER L'ACCÈS PHYSIQUE

1. **Contrôle d'accès physique : description des composants et des phases de contrôle d'accès**
2. Vidéoprotection : définition et composants
3. Autres outils pour sécuriser l'accès physique

Contrôle d'accès physique : description des composants et des phases de contrôle d'accès

- Le contrôle d'accès physique est l'une des catégories du contrôle d'accès qui contrôle l'accès aux lieux et ressources physiques d'une entreprise.
- Les principales fonctions du contrôle d'accès physique sont :
  - Limiter l'accès aux zones sensibles et ressources physiques de l'entreprise aux personnels autorisés ;
  - Surveiller les activités du personnels autorisés dans les zones sensibles ;
  - Interdire tout type de modification ou destruction des ressources physiques.
- Par conséquent, le contrôle d'accès physique consiste à la mise en place d'un ensemble de mécanismes et équipements offrant les fonctions citées précédemment.
- Un système de contrôle d'accès physique pour les zones sensibles est souvent composé de :
  - Un outil de fermeture (tel qu'une barrière, une porte, des vitres etc.) et des murs pour fermer une zone sensible ;
  - Un outil de verrouillage pour verrouiller/déverrouiller la porte, par exemple ;
  - Un terminal pour vérifier l'identité des personnes désirant avoir accès à la zone contrôlée.

Composants du système de contrôle d'accès physique
Source : https://s3-eu-west-1.amazonaws.com/files.visiotech.es/images/stories/news/TIPOS_CONTROL/imagen-04.jpg



PARTIE 2

Copyright - Tout droit réservé - OFPPT

Phases de contrôle d'accès physique

- Le processus du contrôle d'accès physique est composé des phases suivantes :
    1. Un utilisateur désirant avoir accès à une zone contrôlée devra s'authentifier. Pour ce faire, il fournit sa preuve d'identité au terminal. La preuve d'identité peut être sous la forme d'une clé secrète, d'une empreinte digitale, d'une carte à puce ou autre.
    2. Le terminal authentifie l'utilisateur et vérifie s'il est autorisé à accéder, en se basant sur la preuve d'identité fournie et la base de données stockant la liste des utilisateurs autorisés.
    3. Si l'utilisateur s'est authentifié avec succès et qu'il est autorisé à accéder, le terminal envoie une instruction de déverrouillage à l'outil de verrouillage.
    4. L'outil de verrouillage ouvre donc la porte (ou la barrière) et l'utilisateur peut alors accéder à la zone contrôlée.
- Le verrouillage est souvent automatique et se réalise immédiatement suite à l'entrée de l'utilisateur et la fermeture de la porte.
- Le système de contrôle d'accès physique, détaillé précédemment, peut uniquement limiter l'accès aux zones contrôlées. Toutefois, pour garantir la surveillance des activités réalisés dans les zones contrôlées, il faut équiper le système de contrôle d'accès physique par des composants de vidéoprotection.
- En ce qui suit, nous détaillerons le principe et les composants de la vidéoprotection.

Copyright - Tout droit réservé - OFPPT

CHAPITRE 3

SÉCURISER L'ACCÈS PHYSIQUE

1. Contrôle d'accès physique : description des composants et des phases de contrôle d'accès
2. **Vidéoprotection : définition et composants**
3. Autres outils pour sécuriser l'accès physique

Vidéoprotection : définition et composants

- Pour surveiller une zone contrôlée, il est possible de mettre en place un système de vidéosurveillance (souvent appelé aussi vidéoprotection).
- Toutefois, dans certains pays les deux termes peuvent avoir des désignations différentes.
    - En France, par exemple, la vidéoprotection est un cas particulier de la vidéosurveillance. Elle se réfère à la vidéosurveillance appliquée dans les lieux publics et soumise aux réglementations de la Commission nationale de l'informatique et des libertés (CNIL).
- La vidéosurveillance (ou la vidéoprotection) est un système de surveillance qui vise à :
    - protéger les actifs d’une organisation
    - surveiller les activités des personnes dans les zones contrôlées
- Plusieurs composants peuvent être inclus dans un système de vidéosurveillance selon le besoin de l’organisation. En ce qui suit, nous définirons les principaux composants qui sont souvent inclus dans un système de vidéosurveillance.

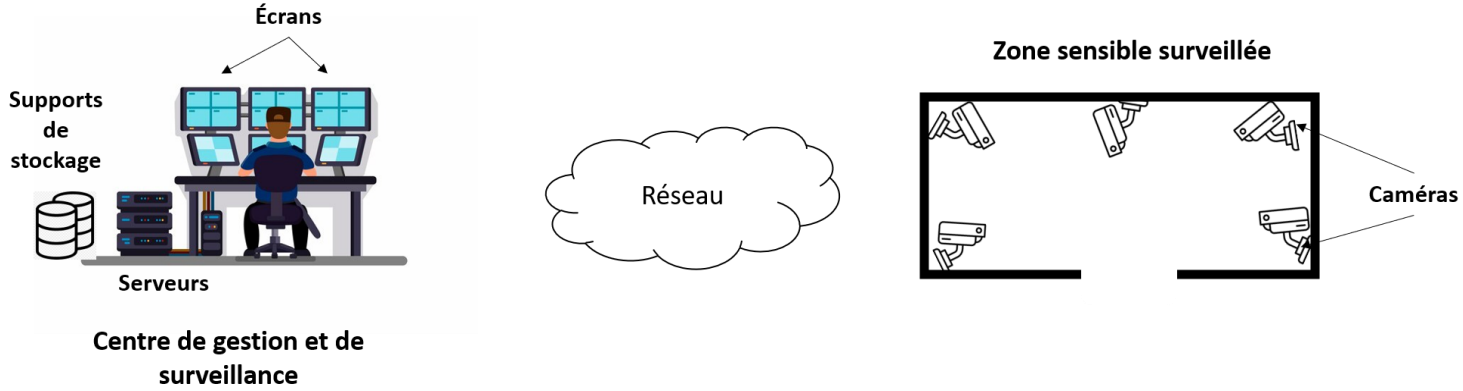
Copyright - Tout droit réservé - OFPPT

PARTIE 2

Les composants typiques d’un système de vidéosurveillance

Un système de surveillance typique est généralement composé de :

- Un ensemble de caméras installées dans des positions et orientations adéquates afin d’avoir une visibilité efficace sur la zone et les actifs contrôlés ;
- Un centre de gestion et de surveillance qui est souvent composé de :
  - Une batterie d'écrans permettant la surveillance en temps réel de l’ensemble des images collectées par les caméras installées
  - Un ou plusieurs serveurs permettant le traitement automatique des images afin qu’elles soient analysées, filtrées, archivées ou détruites, grâce à un ensemble d’algorithmes de traitement (tel que reconnaissances faciales, détection de mouvements, etc.)
  - Des supports de stockage pour le stockage les images après avoir été traitées par les serveurs.
- Un réseau informatique pour interconnecter les caméras installées et le centre de gestion. Il sert comme un moyen de transfert des images et vidéos collectés depuis les caméras vers le centre de gestion..



Composants d’un système de vidéosurveillance typique

Copyright - Tout droit réservé - OFPPT

CHAPITRE 3

SÉCURISER L'ACCÈS PHYSIQUE

1. Contrôle d'accès physique : description des composants et des phases de contrôle d'accès
2. Vidéoprotection : définition et composants
3. **Autres outils pour sécuriser l'accès physique**

Autres outils pour sécuriser l'accès physique

- Comme vu précédemment, pour sécuriser une zone sensible (équipée souvent avec des équipements à protéger), il est possible de mettre en place **conjointement :**

  Un système de contrôle d'accès physique aux zones sensibles pour limiter l'accès aux personnes autorisées.

  Un système de vidéosurveillance pour surveiller les activités des personnes ayant accès aux zones surveillées.

- Pour fournir une meilleure protection des zones sensibles, il est possible d'ajouter d'autres outils et composants aux deux systèmes cités précédemment afin de fournir une meilleure efficacité en termes de sécurité.
- Exemples d'outils et/ou composants incluent :

  Des capteurs spécifiques permettant la détection des événements précis dont certains peuvent être considérés comme risqués. Exemples de capteurs :

  Des capteurs de détection de mouvement : permettent de notifier le centre de gestion lors de la détection d'un mouvement dans une zone sensible.

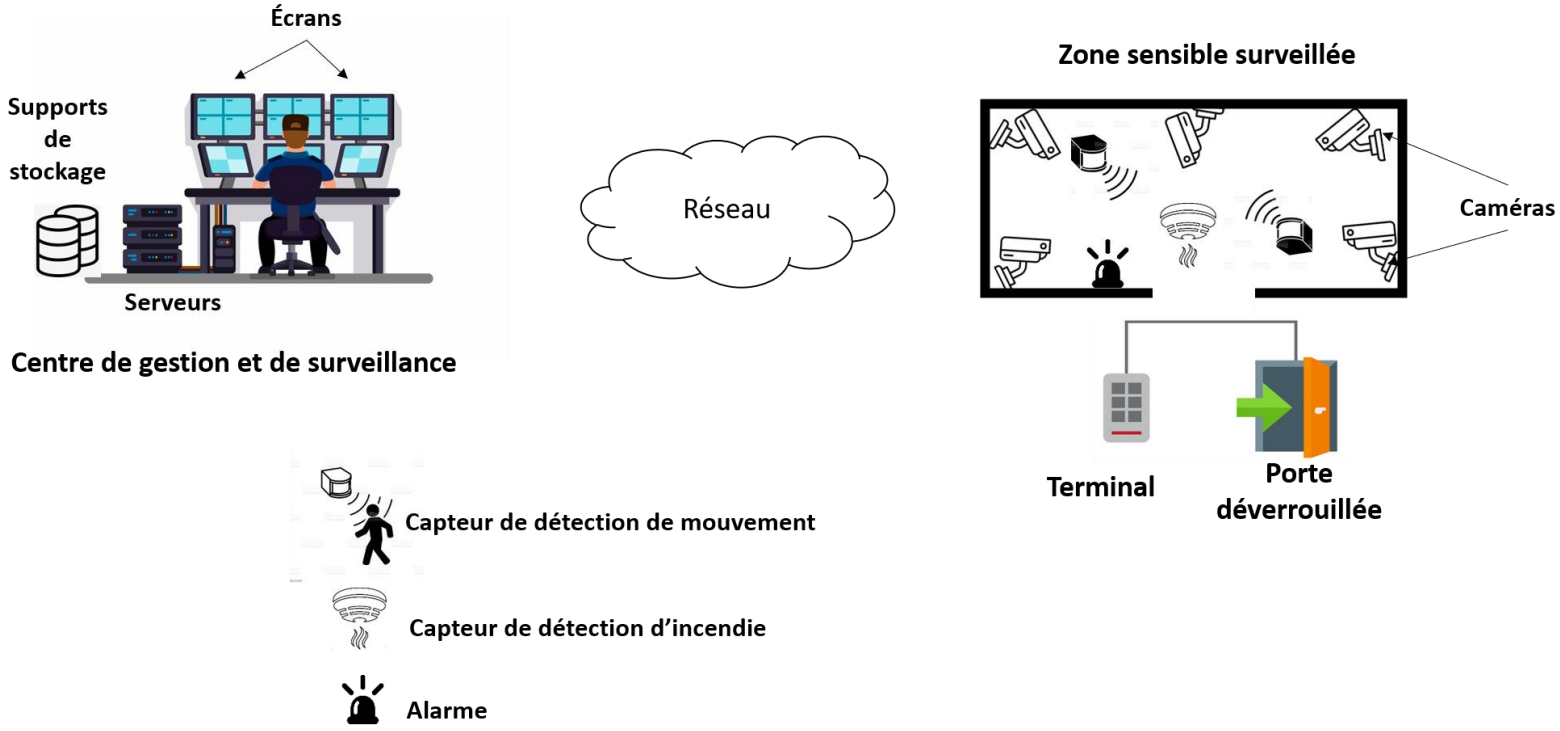
  Des capteurs de détection d'incendie : permettent de notifier le centre de gestion lors de la détection d'un dégagement de chaleur élevé et de la fumée.

  Des alarmes : génèrent un effet sonore lors de la réception d'une instruction de détection d'une intrusion de la part du centre de gestion.

Copyright - Tout droit réservé - OFPPT

Autres outils pour sécuriser l'accès physique

La figure ci-dessous est un exemple de système permettant de sécuriser l'accès physique à une zone sensible



Composants d'un système sécurisant l'accès physique à une zone sensible

PARTIE 2

Copyright - Tout droit réservé - OFPPT

CHAPITRE 4

SÉCURISER LES ÉQUIPEMENTS INFORMATIQUES

Ce que vous allez apprendre dans ce chapitre :

- Spécifier les règles et les bonnes pratiques pour sécuriser les équipements informatiques tel que les postes de travail, les serveurs, les commutateurs et les routeurs
- Décrire le fonctionnement et les techniques des anti-Virus
- Présenter le filtrage du trafic avec des Pares-feux logiciels

6 heures

CHAPITRE 4

SÉCURISER LES ÉQUIPEMENTS INFORMATIQUES

Introduction

- La sécurisation des équipements informatiques (tel que les serveurs, les postes de travail, les routeurs, etc.) peut être assurée, grâce à :
    - La protection physique via la mise en place des mécanismes de contrôle d'accès physique, tel que présentés précédemment.
    - La protection logique (ou logicielle) que nous détaillerons dans ce chapitre .

- La protection logique des équipements informatique consiste au :
    - Renforcement des systèmes d'exploitation installés dans les équipements informatique.
    - Déploiement des mesures de sécurité telles que des pares-feux, des antivirus, des systèmes de détection d'intrusion, etc..

- Dans ce contexte, nous détaillerons dans ce chapitre :
    - Les bonnes pratiques à appliquer pour sécuriser les équipements informatiques (les serveurs, les postes de travail, les commutateurs et les routeurs).
    - Des exemples de mesures de sécurité : les antivirus et les pares-feux.

Copyright - Tout droit réservé - OFPPT

CHAPITRE 4

SÉCURISER LES ÉQUIPEMENTS INFORMATIQUES

Sécurisation des postes de travail et des serveurs

- La sécurisation logique des postes de travail ainsi que des serveur consiste essentiellement au renforcement du système d'exploitation installé dans ces équipements.
- Le renforcement du système d'exploitation (hardening operating system, en anglais) est le processus de mise en place de mesures de sécurité et de correctifs pour les systèmes d'exploitation.

- Le renforcement d'un système d'exploitation comprend généralement :
    - L'application des meilleures pratiques de sécurité pour assurer une configuration sécurisée du système d'exploitation ;
    - La veille sur la mise à jour automatique du système d'exploitation avec des correctifs et des service packs ;
    - Le déploiement de mesures de sécurité supplémentaires telles que les antivirus et les pares-feux.

- Procéder au renforcement des systèmes d'exploitation après l'installation permet de :
    - Limiter les risques de compromission à distance.
    - Élévation de privilèges des utilisateurs favorisant l'exécution des attaques de sécurité.

- Bien que chaque système d'exploitation possède ses propres caractéristiques, il existe plusieurs pratiques de renforcement communes à tous les systèmes d'exploitation. En ce qui suit, nous présenterons une liste des bonnes pratiques permettant le renforcement de la sécurité des systèmes d'exploitation.

Copyright - Tout droit réservé - OFPPT

Bonnes pratiques pour une configuration sécurisé

- Après avoir installé un nouveau système d'exploitation, il est recommandé de :
    - Configurer des mots de passe complexes et robustes, notamment pour le compte administrateur ;
    - Supprimer les comptes utilisateurs inutiles ;
    - Renommer les comptes utilisateurs par défaut ;
    - Désactiver/arrêter les partages et les services inutilisés ;
    - Désinstaller les programmes inutiles et inutilisés ;
    - Vérifier les privilèges accordés aux utilisateurs ainsi qu'aux applications installées et veiller à l'attribution du **moindre privilège.**
        - Par exemple, un utilisateur n'a pas besoin d'avoir des privilèges lui permettant d'installer de nouveaux logiciels ou de modifier la configuration du poste de travail. Ce sont les privilèges d'un compte administrateur.
    - Utiliser des modèles de sécurité afin de gérer et appliquer les configurations de sécurité d'une manière centralisée.
- Il est notamment recommandé de :
    - Veiller sur l'application des mises à jour du système d'exploitation ;
    - Maintenir les programmes à jour et installer la dernière version ;
    - Appliquer les correctifs de sécurité: peut être réalisé via la planification, les tests et l'audit continu afin de s'assurer que les systèmes d'exploitation et les programmes installés soient mises à jour.

Copyright - Tout droit réservé - OFPPT

Application des mesures de sécurité supplémentaires

- L'application des mesures de sécurité est l'une des pratiques de renforcement communes à tous les systèmes d'application. Elle consiste à :
    - Ajuster la configuration du pare-feu afin qu'il puisse agir avec efficacité.
        - Souvent, les systèmes d'exploitation n'ont pas de pare-feu configuré par défaut. En fait, même s'il existe un pare-feu en cours d'exécution, généralement, il faut ajuster ses règles et modifier sa configuration.
        - Une configuration idéale d'un pare-feu consiste à autoriser uniquement le trafic provenant d'adresses IP et de ports connus et approuvés. En effet, les ports ouverts inutiles représentent un risque pour la sécurité.
    - Utiliser des modules de sécurité complémentaires tel que AppArmor et SELinux pour les systèmes Linux afin d'améliorer le contrôle d'accès.
        - L'intérêt de ces modules c'est qu'ils permettent l'application automatique d'un nombre de meilleures pratiques de sécurité efficaces.

        - SELinux (Security-Enhanced Linux) est un module de contrôle d'accès fourni dans le noyau Linux permettant la définition d'une politique de contrôle d'accès pour les applications, processus et fichiers d'un système.

        - AppArmor est un système de contrôle d'accès permettant l'association d'un profil de sécurité à chaque application pour restreindre ses privilèges.
    - Isoler les données et applications sensibles. L'isolation pourra être effectué en :
        - exécutant les bases de données et les applications sensibles dans des machines virtuelles ou conteneurs.
        - limitant l'accès au réseau aux machines exécutant ce type d'applications.

Copyright - Tout droit réservé - OFPPT

CHAPITRE 4

SÉCURISER LES ÉQUIPEMENTS INFORMATIQUES

Sécurisation des commutateurs et des routeurs

- L'administration de tout équipement réseau (commutateur ou routeur), faisant parti du réseau connecté au système d'information, doit respecter un ensemble de recommandations de sécurité.

PARTIE 2

Copyright - Tout droit réservé - OFPPT

Mesures de sécurité supplémentaires dans un commutateur

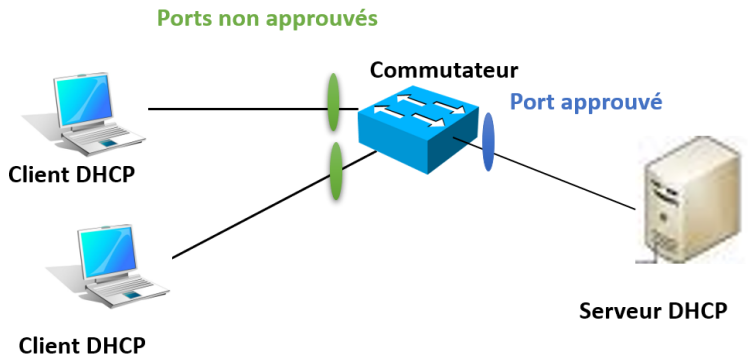
- Les commutateurs peuvent aussi être configurés pour implémenter des mesures de sécurité supplémentaires permettant la protection contre certaines attaques de sécurité discutées précédemment :
    - Port-security pour empêcher l'attaque par inondation d'adresses MAC
    - DHCP Snooping pour faire face à l'attaque DHCP spoofing

- **Port Security :**
    - Une fonctionnalité de sécurité au niveau de la couche liaison de données du modèle OSI disponible sur les **commutateurs Ethernet intelligents**. Cette fonctionnalité permet de restreindre l'accès à un port du commutateur à une liste d'adresses MAC des hôtes autorisés.
    - Une attaque de sécurité est identifiée lorsque :
        - Le nombre maximal d'adresses MAC sécurisées est atteint.
        - Une station, dont l'adresse MAC n'est pas stockée dans la liste des adresses autorisées tente d'accéder à un port du commutateur.
    - Trois types de réactions à une violation de sécurité peuvent être distingués :
        - **Protéger (Protect)** : Les adresses sources inconnues sont supprimées et aucune notification de violation de sécurité n'est générée ;
        - **Restreindre (Restrict)** : Les adresses sources inconnues sont supprimées et une notification de violation de sécurité est générée ;
        - **Fermer (Shutdown)** : Le port devient désactivé et le voyant du port s'éteint. De plus, une notification de violation de la sécurité est générée.

Copyright - Tout droit réservé - OFPPT

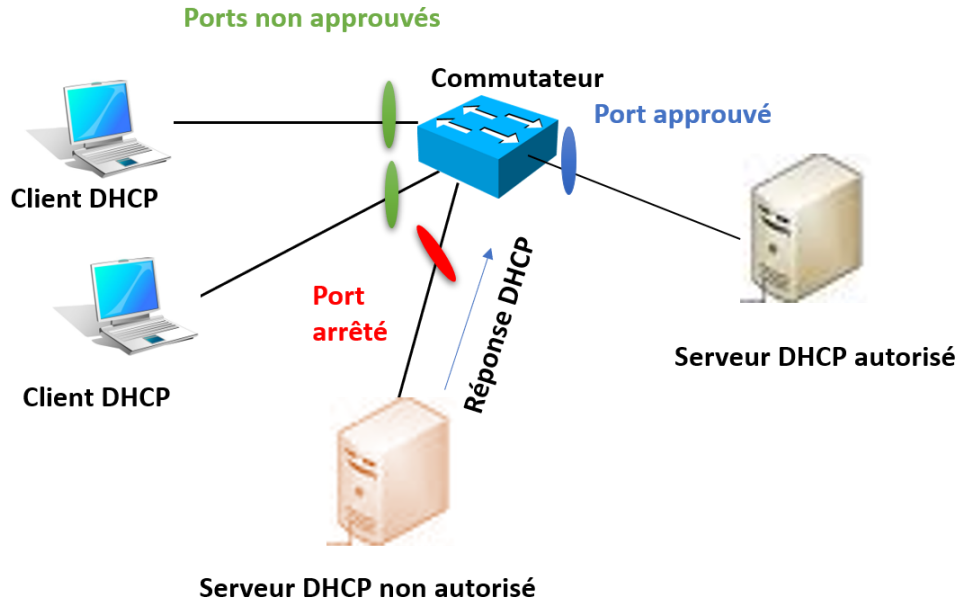
DHCP Snooping

- Une fonction de sécurité disponible sur les commutateurs et permettant de configurer les ports du commutateur en tant que ports approuvés et non approuvés :
    - **Ports approuvés** (trusted ports, en anglais) sont les ports connectés à un serveur DHCP autorisé et capables de répondre aux requêtes DHCP
    - **Ports non approuvés** (untrusted ports, en anglais) sont les ports autorisés à envoyer uniquement des requêtes DHCP



Principe de DHCP Snooping

Grâce à la répartition des ports approuvés et non approuvés, DHCP snooping empêche l'exécution de l'attaque DHCP spoofing. En fait, si une réponse DHCP est reçue via un port non approuvé, le port sera automatiquement arrêté.



Réactions face à l'attaque DHCP spoofing

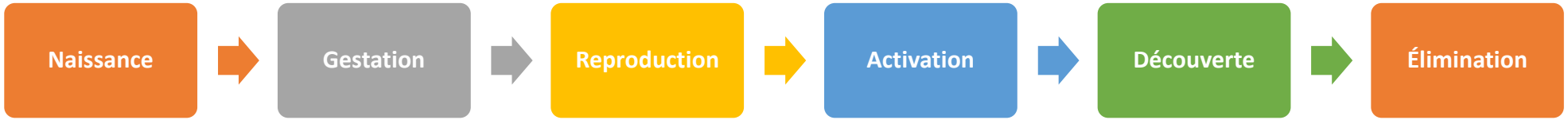
Copyright - Tout droit réservé - OFPPT

CHAPITRE 4

SÉCURISER LES ÉQUIPEMENTS INFORMATIQUES

Virus informatique

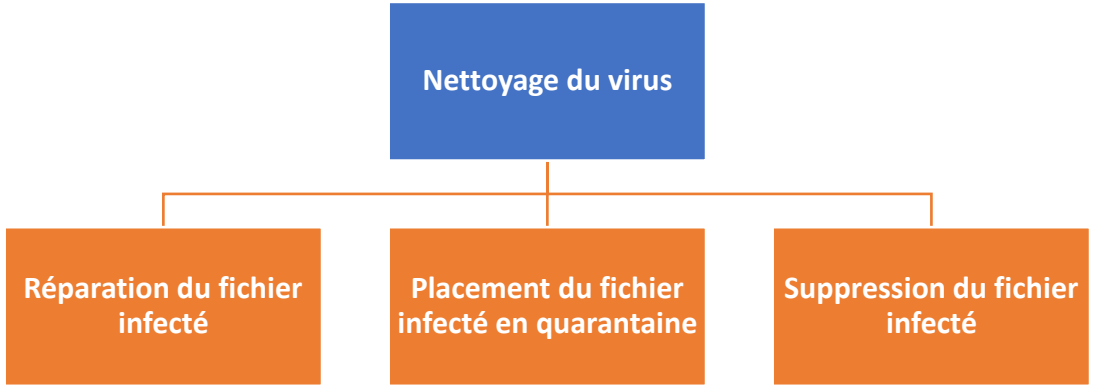
- Un virus informatique est un programme malveillant qui est capable de :
    - S'introduire dans un autre programme informatique afin d'entraîner diverses perturbations dans son fonctionnement.
    - Se reproduire et se propager dans d'autres programmes et fichiers afin de les infecter et nuire à leurs fonctionnement.
- Un virus informatique passe souvent par les étapes suivantes :
    - Naissance du virus : consiste au développement du code d'un nouveau virus par un pirate ;
    - Gestation : se réfère à l'introduction du virus dans le système visé ;
    - Reproduction : dès son introduction dans le système, un virus se reproduit plusieurs fois avant qu'il soit activé afin de garantir sa pérennité ;
    - Activation ; consiste à l'exécution des actions malveillantes afin de causer des dégâts au système infecté. L'activation peut être déclenchée soit :
        - En exécutant le programme infecté.
        - Suite à un événement particulier (date système, activation distante par le développeur du virus, etc.).
    - Découverte et élimination : se réfère à la détection de la présence d'un virus et la recherche des solutions visant à supprimer ce virus ainsi que les dégâts qu'il a causés. Souvent, la découverte et l'élimination des virus se réalise grâce à des logiciels spécifiques que sont les antivirus.



Copyright - Tout droit réservé - OFPPT

Anti-virus

- Un antivirus est un programme informatique permettant la détection de la présence de virus et le nettoyage d'un virus détecté dans la mesure du possible.
- Le nettoyage effectué par un antivirus peut se présenter essentiellement sous trois actions :
    - Réparation du fichier infecté en supprimant le virus. Parfois, ce type de nettoyage n'est pas possible ;
    - Emplacement du fichier infecté en quarantaine afin d'empêcher le virus d'agir ;
    - Suppression du fichier contaminé pour supprimer le virus.

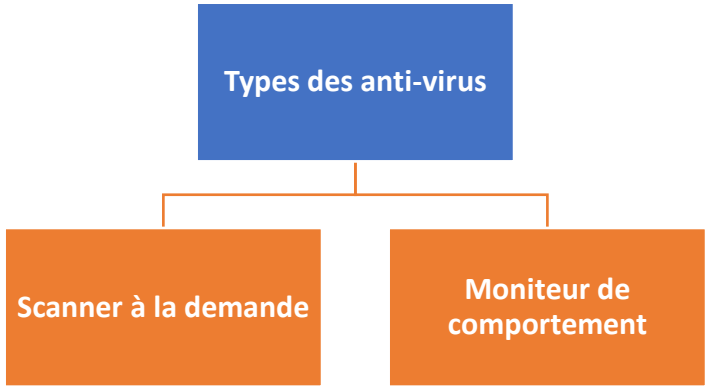


Actions possibles pour le nettoyage d'un virus informatique

Copyright - Tout droit réservé - OFPPT

Fonctionnalités offertes par les anti-virus

- Deux principales fonctionnalités peuvent être fournie conjointement par un anti-virus, grâce à :
    - **Un scanner** exécuté à la demande (On-Demand Scanner, en anglais) afin d'analyser un support de stockage (tel que les disques durs, clés USB, etc.) et y rechercher les logiciels malveillants.
    - **Un moniteur de comportement** toujours actifs en arrière-plan (On-Access Scanners, en anglais) pour assurer une protection résidente et détecter toute activité de type virale.



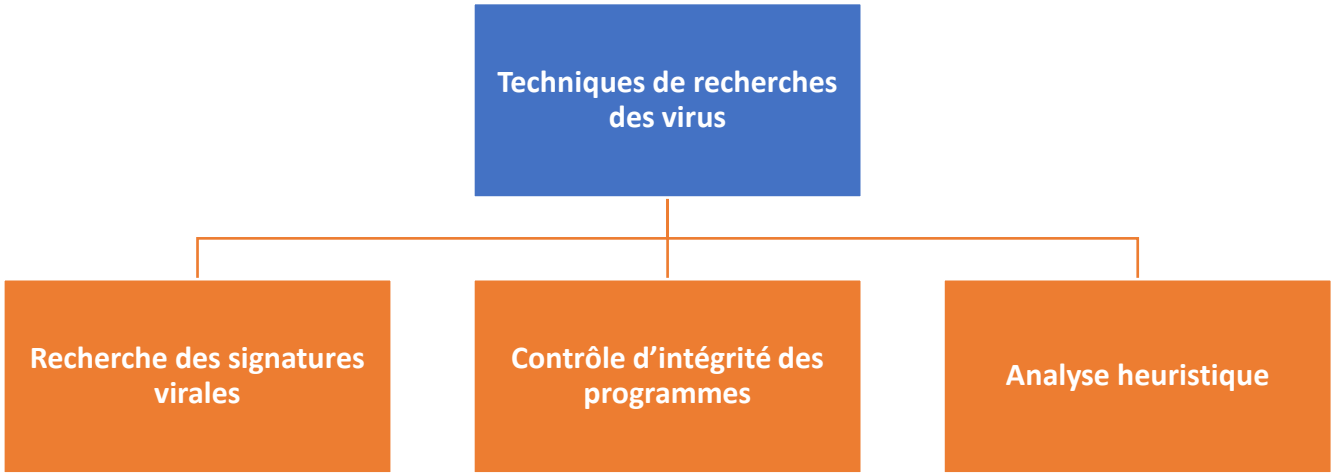
Les types d'anti-virus

- Il est extrêmement important d'activer un moniteur de comportement, en particulier sur les machines connectées à un réseau publiC (tel que Internet) pour qu'il veille à la protection de ces machines contre les virus. Toutefois, un moniteur de comportement peut affecter les performances de ces machines et les ralentir, notamment avec des machines présentant un nombre important d'événements.

Copyright - Tout droit réservé - OFPPT

Techniques de recherche des virus

Comme illustré dans la figure ci-dessous, trois techniques de recherche des virus peuvent être utilis2ES par un anti-virus pour qu'il puisse détecter la présence des virus. En ce qui suit, nous détaillerons le fonctionnement de chacune de ces techniques.



Les techniques de recherche des virus

Copyright - Tout droit réservé - OFPPT

Techniques de recherche des virus

- **Recherche des signatures virales** :
  - Une signature virale représente une suite d'octets significative qui est intégrée par un virus dans une application infectée pour qu'il puisse vérifier si une telle application est infectée. Par conséquent, un anti-virus peut détecter un virus via l'identification de sa signature virale;
  - C'est la méthode la plus utilisée par les antivirus. Cependant, elle n'est fiable que si la base virale de l'antivirus est à jour. En plus, certains virus peuvent crypter ou modifier leurs signatures pour les rendre indétectables.

- **Contrôle d'intégrité des programmes :**
  - Un virus modifie tout programme qu'il infecte. Un antivirus peut donc utiliser un contrôleur d'intégrité pour vérifier s'il y en a des fichiers exécutables infectés (c.à.d., modifiés par le virus).
  - Une base de données contenant des informations sur les fichiers exécutables du système (tel que la taille, date de modification, checksum) est nécessaire pour que l'antivirus puisse identifier les modifications effectuée et détecter la présence du virus.

Analyse heuristique :

- Elle consiste à la recherche et à l'analyse des codes correspondant à des fonctions virales dont l'action pourrait s'avérer suspecte (tel qu'un ensemble d'instruction causant la modification d'un fichier). Tout code viral détecté sera considéré comme une donnée qui n'est jamais autorisé à être exécuté.
- Cette méthode permet la détection des nouveaux virus dont la signature n'a pas été ajoutée à la base de données. Toutefois, elle peut produire des faux positives (génération de fausses alertes) et des faux négatives (présence des virus non détectés).

Copyright - Tout droit réservé - OFPPT

CHAPITRE 4

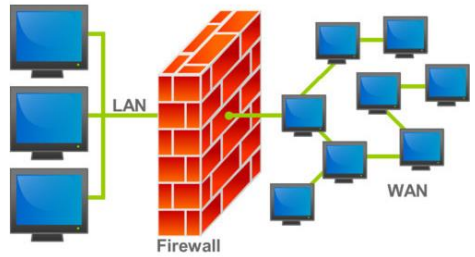
SÉCURISER LES ÉQUIPEMENTS INFORMATIQUES

Filtrage du trafic avec des Pares-feux logiciels

- Un pare-feu (firewall, en anglais) est un outil permettant la protection d'un ordinateur ou un réseau contre les attaques réseaux. En effet, il garantit la mise en place d'une politique de sécurité de filtrage du trafic entrant et sortant au réseau (ou à un ordinateur).
- Parmi les objectifs de la mise en place d'un pare-feu :
    - Tout trafic échangé entre réseaux de différents niveaux de confiance doit passer par un pare-feu pour qu'il soit filtré.
    - Uniquement un trafic autorisé peut passer un pare-feu, tel que défini par la politique de sécurité mise en œuvre.
- Deux classes de pare-feu peuvent être distinguées : pares-feux logiciels et pares-feux matériels. Dans ce chapitre, nous adressons uniquement les pares-feux logiciels.
- Les pares-feux logiciels, eux-mêmes, peuvent être classés en deux types : pare-feu hôte et pare-feu réseau.

Pare-feu hôte
Source : https://davescomputertips.com/wp-content/uploads/2014/09/firewall-image-1.jpg

Il s'installe sur la machine hôte (ordinateur) pour le protéger contre les attaques réseau.



Pare-feu réseau
Source : https://3.imimg.com/data3/DQ/WT/MY-3742189/firewell-xtm-utm-solutions-500x500.jpg

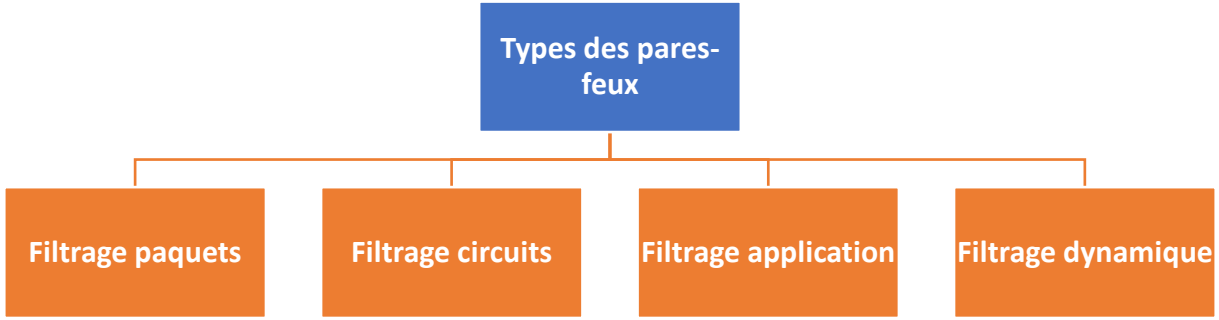
Il s'installe sur un serveur (généralement placé entre deux segments de réseau) pour protéger un segment réseau spécifique (réseau local LAN) contre d'autres segments (les segments faisant parti du réseau étendu WAN).

PARTIE 2

Copyright - Tout droit réservé - OFPPT

Types des pares-feux

- Les pares-feux peuvent être aussi classifié selon le un niveau de protocole contrôlé, nous pouvons donc distinguer :
    - Filtrage paquets : pare-feu agit au niveau de la couche réseau (niveau 3) du modèle OSI ;
    - Filtrage circuit : pare-feu agit au niveau de la couche transport (niveau 4) du modèle OSI ;
    - Filtrage application : pare-feu agit au niveau de la couche application (niveau 7) du modèle OSI ;
    - Filtrage dynamique : filtrage multi niveau (c.à.d., au niveau de la couche 3, 4 et 7 du modèle OSI).



Copyright - Tout droit réservé - OFPPT

Filtrage paquets

- Les pares-feux offrant le filtrage des paquets représentent la base des principaux systèmes de pare-feu.
- Ce type de pares-feux garantit le filtrage via l'examen de chaque paquet IP et l'application d'un ensemble de règles de filtrage :
    - Les règles de filtrage décrivent quels types de trafics sont autorisés, refusés ou doivent être redirigés ;
    - Les règles de filtrage sont implémentées sous forme des listes de contrôle d'accès ;
    - Les règles de filtrage sont définies sur la base des informations de la couche réseau, telles que :
        - Adresses IP source et destination ;
        - Numéros des ports source et destination TCP/UDP ;
        - Champs de protocole IP (TCP, UDP, ICMP, etc.) ;
        - Drapeaux (flags) TCP (SYN, ACK, FIN, RST, PSH, etc.) ;
        - Interfaces entrantes ou sortantes.
    - Exemple de règles de filtrage : Rejeter tous les paquets entrants sur le port 150 sauf ceux ayant des adresses IP sources de confiance connues (193.2.2.1/24).

Règle	Action	IP source	IP destination	Protocol	Port source	Port destination
1	Allow	193.2.2.1/24	any	tcp	150	any
2	Drop	any	any	tcp	150	any

Copyright - Tout droit réservé - OFPPT

Traitement des règles de filtrage de paquets

- Les règles de filtrage sont implémentées sous forme des listes de contrôle d'accès qui sont traitées dans **l'ordre descendant :**
    - S'il existe une correspondance avec l'une des règles de la liste, cette règle est invoquée pour identifier l'action à exécuter. Les règles suivantes sont ignorées.
    - S'il n'y a pas de correspondance avec l'une des règles de la liste, l'action par défaut est exécutée (c.à.d., l'action définie par la stratégie par défaut).

- Trois types de **stratégies par défaut** peuvent être souvent définies dans un pare-feu :
    - **Default = Allow** : tout type de trafic qui n'est pas expressément interdit, par une règle, est autorisé ;
    - **Default = Deny** : tout type de trafic qui n'est pas expressément autorisé, par une règle, est bloqué ;
    - **Default = Drop**: tout type de trafic qui n'est pas expressément autorisé, par une règle, est rejeté.

- Généralement, la méthodologie de configuration d'un pare-feu suit les étapes suivantes :
    1. Définir la politique de filtrage des paquets par défaut (Allow, Deny ou Drop) ;
    2. Valider soigneusement la politique ;
    3. Définir les règles de la liste du contrôle d'accès (ACL) à partir de la stratégie par défaut choisie, selon la syntaxe prise en charge par le pare-feu ;
    4. Valider et optimiser les règles .

Copyright - Tout droit réservé - OFPPT

PARTIE 3

DÉCOUVRIR LA CRYPTOGRAPHIE ET LES SOLUTIONS DE GESTION ET DE PARTAGE DE CLÉS

Dans ce module, vous allez :

- Découvrir la cryptographie
- Présenter l'architecture PKI (Public Key Infrastructure)

5 heures

CHAPITRE 1

DÉCOUVRIR LA CRYPTOGRAPHIE ET LES CERTIFICATS NUMÉRIQUES

Ce que vous allez apprendre dans ce chapitre :

- Définir les objectifs de la cryptographie
- Distinguer ente la cryptographie symétrique et la cryptographie asymétrique
- Présenter la fonction de hachage
- Découvrir les certificats X.509

3 heures

CHAPITRE 1

DÉCOUVRIR LA CRYPTOGRAPHIE ET LES CERTIFICATS NUMÉRIQUES

1. **Objectifs de la cryptographie**
2. Cryptographie symétrique et Cryptographie asymétrique
3. Fonction de hachage
4. Certificats X.509
5. Quiz sur la cryptographie et la gestion des clés

Objectifs de la cryptographie

- La **cryptologie** est la science qui regroupe la cryptographie et la cryptanalyse :
    - La **cryptographie** se réfère à la science du secret adressant la conception et le développement des systèmes de chiffrements permettant de transformer un message intelligible en non intelligible.
    - La **cryptanalyse** désigne la science de l'analyse des systèmes de chiffrements permettant d'étudier et identifier les attaques contre ces systèmes.
- Historiquement, la **cryptographie** permet de garantir la **confidentialité** des données (messages) en modifiant leurs natures intelligibles en non intelligibles à l'aide des codes secrets ou des clés de chiffrement.
- De nos jours, en plus de la confidentialité, la cryptographie permet également de garantir l'**authenticité** et l'**intégrité** des données.
- Pour offrir ces trois objectifs de sécurité (confidentialité, intégrité, et authenticité), la cryptographie regroupe trois techniques : le chiffrement, le hachage, et la signature numérique :
    - Le **chiffrement** permet d'assurer la **confidentialité ;**
    - Le **hachage** permet d 'assurer l'**intégrité ;**
    - La **signature numérique** permet d'assurer l'**authenticité.**
- En ce qui suit, nous détaillerons les différents techniques/mécanismes de la cryptographie.

Copyright - Tout droit réservé - OFPPT

CHAPITRE 1

DÉCOUVRIR LA CRYPTOGRAPHIE ET LES CERTIFICATS NUMÉRIQUES

1. Objectifs de la cryptographie
2. **Cryptographie symétrique et Cryptographie asymétrique**
3. Fonction de hachage
4. Certificats X.509
5. Quiz sur la cryptographie et la gestion des clés

Techniques de chiffrement classiques

- Avant de passer définir les schémas de chiffrement symétrique et de chiffrement asymétrique, nous allons présenter des exemples de techniques de chiffrement classiques.
- Les deux éléments de base de toutes les techniques de chiffrement sont la substitution et la transposition :
    - **Chiffrement par substitution** : une technique dans laquelle les lettres du texte en clair sont remplacées par d'autres lettres, chiffres ou symboles.
    - **Chiffrement par transposition** : une technique dans laquelle les lettres du texte en clair sont permutées (c.à.d., l'ordre des lettres est modifié).
- L'avantage majeur des techniques de chiffrement classiques est la simplicité des algorithmes de chiffrement et de déchiffrement. Cependant, elles sont vulnérables aux attaques de cryptanalyses.
- Plusieurs méthodes de chiffrement par substitution et par transposition ont été proposé dans la littérature. En ce qui suit, nous détaillerons les méthodes suivantes :
    - Chiffrement de César comme un exemple de chiffrement par substitution monoalphabétique ;
    - Chiffre de Vigenère comme un exemple de chiffrement par substitution polyalphabétique ;
    - Un exemple de chiffrement par transposition.

Copyright - Tout droit réservé - OFPPT

Chiffrement de César

- Le chiffrement de César est l'une des techniques les plus simples de substitution monoalphabétique.
- Un texte chiffré est obtenu en remplaçant chaque lettre appartenant au texte clair par une autre lettre qui est distante d'un décalage **d** de la lettre d'origine dans le texte claire.

Exemple 1 : d = 3

Lettres d'origines	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Lettres de remplacement correspondantes	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Texte en clair : **S E C U R I T Y**
- Texte chiffré : **V H F X U L W B**

Exemple 2 : d = 10

Lettres d'origines	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Lettres de remplacement correspondantes	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J

- Texte en clair : **B A N A N E**
- Texte chiffré : **L K X K X O**

Copyright - Tout droit réservé - OFPPT

Chiffre de Vigenère

- Le chiffre de Vigenère est l'un des plus simples méthodes de substitution polyalphabétique.
- Contrairement au chiffrement de César, dans le chiffre de Vigenère, le décalage **d** n'est pas fixe. C'est un décalage variable qui est désigné par la valeur de clé utilisée.
- **Principe du chiffre de Vigenère :**
    - Supposons avoir :
        - Un texte en clair P composé de n lettres ($P = p_0, p_1, \dots, p_{n-1}$) ;
        - Une clé K composée de m lettres ($\mathrm{K} = k_0, k_1, \dots, k_{m-1}$) ;
        - Un un texte chiffré C composé de n lettres : $\mathrm{C} = c_0, c_1, \dots, c_{n-1}$.

    Le processus du calcul d'un texte chiffré est le suivant :
        - La première lettre de la clé est ajoutée à la première lettre du texte en clair, mod 26 ;
        - Les deuxièmes lettres sont ajoutées, et ainsi de suite jusqu'aux **m** premières lettres du texte en clair ;
        - Pour les lettres suivantes du texte en clair, les lettres clés sont répétées. Ce processus se poursuit jusqu'à ce que toute la séquence de texte en clair soit cryptée ;
        - Une équation générale du processus de cryptage est tel que $c_i = (p_i + k_{i \bmod m}) \ mod \ 26$.

Copyright - Tout droit réservé - OFPPT

Chiffre de Vigenère : Exemple

Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Position	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Position des lettres dans l'alphabet

- Texte en clair : CIPHERTEXTE
- Clé : SECURE
- Texte Chiffré : UMRBVVLIZNV

CLAIR	C	I	P	H	E	R	T	E	X	T	E
P_{CLAIR}	2	8	15	7	4	17	19	4	23	19	4
CLÉ	S	E	C	U	R	E	S	E	C	U	R
$P_{CLÉ}$	18	4	2	20	17	4	18	4	2	20	17
$P_{CHIFFRÉ}$	20	12	17	1	21	21	11	8	25	13	21
CHIFFRÉ	U	M	R	B	V	V	L	I	Z	N	V

Calcul du texte chiffré

Copyright - Tout droit réservé - OFPPT

Chiffrement par transposition

- Les deux techniques examinées précédemment montrent la substitution d'un symbole de texte chiffré à un symbole de texte en clair. Un type de mappage différent est obtenu en effectuant une sorte de permutation sur les lettres en clair. Cette technique est appelée chiffrement par transposition.
- L'un des schémas de transposition les plus complexe consiste à **écrire** le message d'origine dans un **rectangle**, **ligne par ligne**, et à **lire** le message, **colonne par colonne**, **en permutant l'ordre des colonnes**. L'ordre des colonnes est définie par une clé.
- **Exemple 1 :**

  Texte en clair : C I P H E R T E X T E

  Clé : 24135

  Texte Chiffré : P E C R H X I T E T

Sens d'écriture →

Clé	2	4	1	3	5
Texte	C	I	P	H	E
	R	T	E	X	T

↓ Sens de lecture

- **Exemple 2 :**

  Texte en clair : C R Y P T O L O G I E E S T U N E S C I E N C E

  Clé : 436251

  Texte Chiffré : O E S E P I N N R O T I C L S C T E E C Y G U E

Clé	4	3	6	2	5	1
Texte	C	R	Y	P	T	O
	L	O	G	I	E	E
	S	T	U	N	E	S
	C	I	E	N	C	E

PARTIE 3

Copyright - Tout droit réservé - OFPPT

Chiffrement symétrique

Dans un schéma de chiffrement symétrique (souvent appelé aussi cryptographie symétrique), cinq concepts/termes peuvent être distingués :

- **Texte en clair (Plaintext, en anglais)** : un message ou un ensemble de données d'origine et intelligible. Il est introduit en entrée dans un algorithme de chiffrement afin de générer un texte chiffré. Il est également la sortie d'un algorithme de déchiffrement ;
- **Algorithme de chiffrement (Encryption algorithm, en anglais)** : un algorithme qui effectue diverses substitutions et transformations sur le texte en clair afin de fournir un texte chiffré ;
- **Clé secrète (Secret key, en anglais)** : c'est **une valeur secrète unique partagée entre deux interlocuteurs**. Un texte en clair est chiffré et déchiffré avec la **même clé secrète** qui est fournie comme entrée dans les deux algorithmes de chiffrement et déchiffrement. En fait, les substitutions et les transformations effectuées par l'algorithme de chiffrement (aussi de déchiffrement) dépendent de la clé secrète
- **Texte chiffré (Ciphertext, en anglais) :** un message brouillé et inintelligible qui est produit en sortie d'un algorithme de chiffrement à partir d'un texte en clair et une clé secrète. Notez que, pour un message donné, deux clés différentes produiront deux textes chiffrés différents
- **Algorithme de déchiffrement (Decryption algorithm, en anglais)** : un algorithme de cryptage exécuté à l'envers. Il prend le texte chiffré et la clé secrète et produit le texte en clair d'origine.

Principe de la cryptographie symétrique

Copyright - Tout droit réservé - OFPPT

Chiffrement symétrique

- L'**avantage** majeur de la cryptographie symétrique est **la simplicité** des algorithmes de chiffrement/déchiffrement symétrique. Par conséquent, ces algorithmes sont rapides et ne sont pas gourmand en termes de ressources systèmes
- Cependant, un système de chiffrement symétrique souffre de plusieurs **inconvénients** :
    - Il ne peut garantir que la confidentialité, mais pas les autres objectifs (authenticité et intégrité) ;
    - Gestion complexe des clés secrètes notamment lorsque le nombre des entités communicantes est important. En fait, une clé secrète ne peut être partagée qu'entre deux entités. Pour communiquer avec d'autres entités il faudra d'autres clés secrètes ;
    - Le partage d'une clé secrète entre deux interlocuteurs doit être réalisé d'une manière sécurisé pour qu'elle ne soit pas dévoilée. En effet, la robustesse du chiffrement symétrique, en terme de sécurité ,dépend essentiellement de la robustesse et la confidentialité de la clé secrète.
- Deux catégories de chiffrement symétrique peuvent être distingués :
    - **Chiffrement par flots (Stream ciphers, en anglais) :** le chiffrement d'un texte claire est réalisé bit par bit. Par conséquent, il n'y a aucun besoin de récupérer tout le texte pour commencer le chiffrement. Pour cette raison, le chiffrement par flots est considéré très rapide.
    - **Chiffrement par blocs (Block ciphers, en anglais) :** Le chiffrement d'un texte clair est réalisé par groupement de mots, souvent appelé bloc, de taille définie (e.g., 64 bits).

Copyright - Tout droit réservé - OFPPT

Chiffrement symétrique

- Plusieurs algorithmes de chiffrement symétrique ont été proposé dans la littérature, tel que :
    - **DES (Data Encryption Standard)** est un algorithme de chiffrement par bloc qui utilise **des clés de 56 bits ;**
    - **3DES (Triple DES)** consiste à appliquer successivement l'algorithme DES trois fois sur un même bloc de taille 64 bits avec **deux ou 3 clés**. Par conséquent, la **taille des clés** utilisées varie entre **112 à 168 bits ;**
    - **AES (Advanced Encryption Standard)** comprend trois algorithmes de chiffrements selon la longueur de la clé utilisée:
        - AES-128 utilise une longueur de clé de 128 bits pour chiffrer et déchiffrer un bloc de messages
        - AES-192 utilise une longueur de clé de 192 bits pour chiffrer et déchiffrer un bloc de messages
        - AES-256 utilise une longueur de clé de 256 bits pour chiffrer et déchiffrer un bloc de messages
    - **RC4 (Rivest Cipher 4**) est un algorithme de chiffrement par flots qui utilise **des clés de tailles variables.**
- Le tableau suivant fournit une comparaison entre les différents algorithmes de chiffrement symétriques cités précédemment

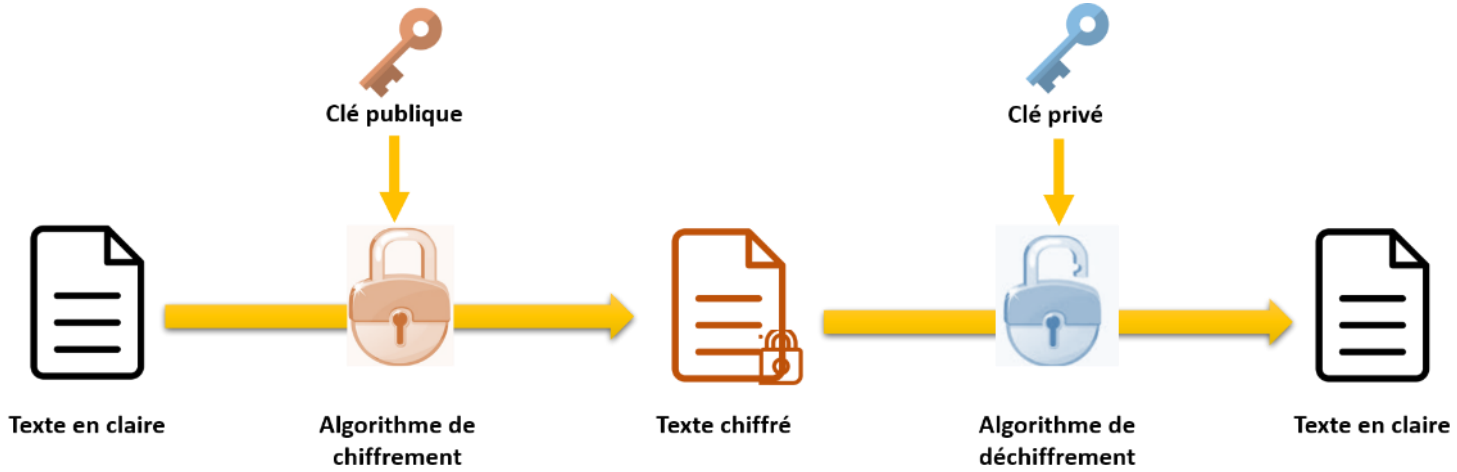
Algorithme de chiffrement symétrique	Longueur de la clé (bits)	Taille de bloc (bits)	Caractéristiques
DES	56	64	Non sécurisé (déjà cassé)
3DES	112, 168	64	Sécurité satisfaisante
AES	128, 192, 256	128	Sécurité excellente
RC4	Variable	Par flots	Rapide

Tableau comparatif des algorithmes de chiffrements symétrique

Copyright - Tout droit réservé - OFPPT

Chiffrement asymétrique

- Contrairement au chiffrement symétrique, un schéma de chiffrement asymétrique utilise une paire de clés distincte :
    - Une clé privée : une clé secrète (confidentielle) a une seule entité (un seul interlocuteur). Elle ne doit pas être partagée avec aucune autres entité.
    - Une clé publique : une clé connue part toutes les entités qui veulent désigner un destinataire spécifique.
- Une paire de clé (privé et publique) est sélectionnée de sorte que si l'une est utilisée pour le chiffrement, l'autre est utilisée pour le déchiffrement (et vice versa). Les transformations exactes effectuées par l'algorithme dépendent de la clé fournit comme entrée.
- Une clé publique peut être partagée librement sans aucun souci d'identification d'une clé privée à partir d'une clé publique.

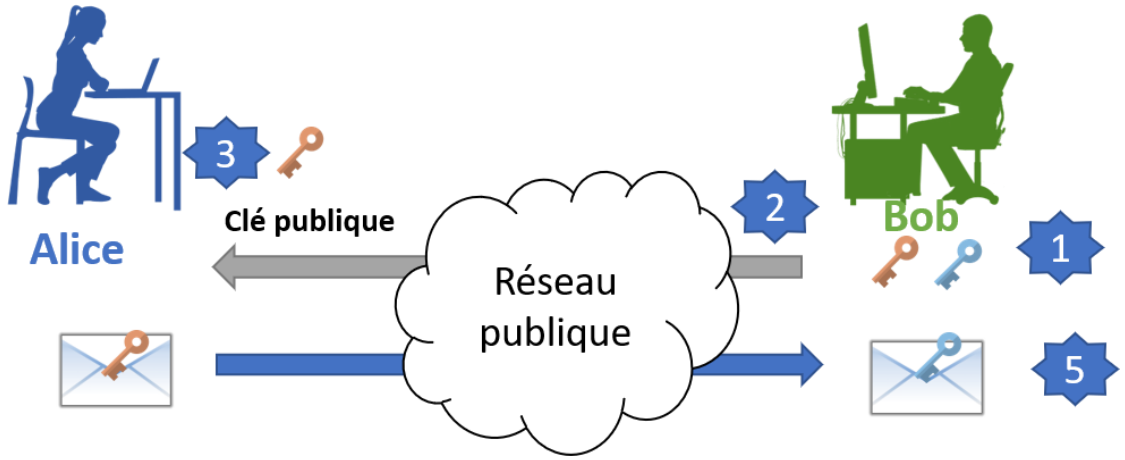


Principe de la cryptographie asymétrique

Copyright - Tout droit réservé - OFPPT

Chiffrement asymétrique

- Les étapes nécessaires de l'exécution d'un algorithme de chiffrement symétrique sont :
    1. Un utilisateur (Bob) génère une paire de clés (clé publique et clé privé) ;
    2. Bob publie sa clé publique, tandis que la clé associée reste privée. Comme illustré dans la figure ci-dessous, Bob envoie sa clé publique à Alice ;
    3. À la réception, Alice conserve la clé publique de Bob. En effet, chaque utilisateur doit conserver tous les clés publiques obtenues des autres ;
    4. Lorsque Alice souhaite envoyer un message confidentiel à Bob, elle crypte le message à l'aide de la clé publique de Bob ;
    5. Lorsque Bob reçoit le message, il le déchiffre à l'aide de sa clé privée. Par conséquent, aucun autre destinataire ne peut déchiffrer le message car seule Alice connaît la clé privée d'Alice.



Processus d'exécution de la cryptographie asymétrique

Copyright - Tout droit réservé - OFPPT

Chiffrement asymétrique

- Le tableau suivant résume certains des aspects importants du chiffrement symétrique et chiffrement asymétrique.

Chiffrement symétrique	Chiffrement asymétrique
Le chiffrement et le déchiffrement sont réalisés par le même algorithme et la même clé	Le chiffrement et le déchiffrement sont réalisés par le même algorithme avec une paire de clés, une pour le chiffrement et une pour le déchiffrement
L'expéditeur et le destinataire doivent partager l'algorithme et la clé.	L'expéditeur et le destinataire doivent chacun avoir l'une des paires de clés correspondantes (pas la même).
La clé doit rester secrète	Une des deux clés (la clé privée) doit être gardée secrète

Tableau comparatif du chiffrement symétrique et asymétrique

- Pour faire la distinction entre les deux classes de chiffrement, nous nous référons à la clé utilisée dans le chiffrement symétrique en tant que clé secrète. Les deux clés utilisées pour le chiffrement asymétrique sont appelées clé publique et clé privée.

Copyright - Tout droit réservé - OFPPT

Chiffrement asymétrique : Rivest-Shamir-Adleman (RSA)

- Le Rivest-Shamir-Adleman (RSA) est l'approche à usage général la plus utilisée et mise en œuvre pour le chiffrement asymétrique.
- **Principe de fonctionnement de RSA :**

1. **Génération des clés :**
   - Sélectionnez deux grands nombres premiers, p et q. Les nombres premiers doivent être grands pour qu'ils soient difficiles à deviner
   - Calculez $n = p \times q$
   - Calculez la fonction $\Phi(n) = (p-1) \times (q-1)$
   - Sélectionnez un entier e tel que : $PGCD(\Phi(n), e) = 1$ et $1 < e < \Phi(n)$
   - Calculez d tel que $e \times d = 1 mod \Phi(n)$
   - La clé publique : $PU = \{e, n\}$
   - La clé privée : $PR = \{d, n\}$
2. **Chiffrement :**

   Étant donné M un texte en clair, représenté par un nombre (tel que M<n), le texte chiffré C est calculé comme suit : $C = M^e mod\ n$
3. **Déchiffrement :**

   En utilisant la clé privé, le texte en clair pourra être retrouvé comme suit : $M = C^d mod\ n$

Copyright - Tout droit réservé - OFPPT

Chiffrement asymétrique : Rivest-Shamir-Adleman (RSA)

- **Exemple d'exécution du schéma RSA :**

1. **Génération des clés :**

P = 11, q=17

$$n = p \times q = 11 \times 17 = 187$$
$$\Phi(n) = (p-1) \times (q-1) = 16 \times 10 = 160$$

$PGCD(\Phi(n), e) = 1$ et $1 < e < \Phi(n)$ → $e = 7$

$e \times d = 1 mod \Phi(n)$, $d = 23$ tel que $7 \times 23 = 161$

- La clé publique : $PU = \{7,187\}$
- La clé privée : $PR = \{23,187\}$

2. **Chiffrement :**
   - Texte en clair : $M = 90$
   - Texte chiffré : $C = 90^7 mod\ 187 = 95$
3. **Déchiffrement :**
   - Texte chiffré : $C = 95$
   - Texte en clair : $M = 95^{23} mod\ 187 = 90$

PARTIE 3

Copyright - Tout droit réservé - OFPPT

Chiffrement asymétrique

- L'avantage principal du chiffrement asymétrique est l'absence du besoin de partage d'une clé secrète, tel que le cas du chiffrement symétrique. Ce qui élimine le besoin d'avoir un canal sécurisé pour la distribution des clés secrètes.
- L'inconvénient majeur du chiffrement asymétrique est la complexité. Les algorithmes de chiffrement asymétrique sont lourds et gourmand en termes de ressources systèmes.
- Comme le chiffrement symétrique, le chiffrement asymétrique n'offre que la confidentialité des données.

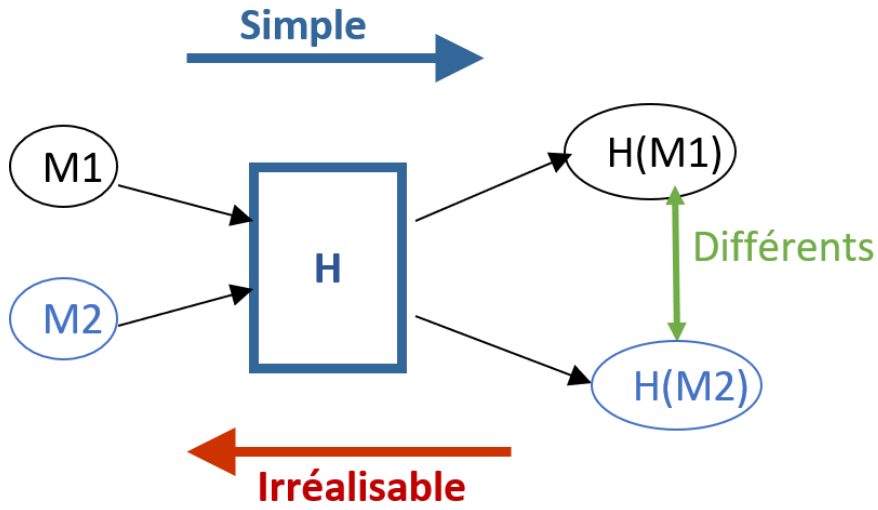
Copyright - Tout droit réservé - OFPPT

CHAPITRE 1

DÉCOUVRIR LA CRYPTOGRAPHIE ET LES CERTIFICATS NUMÉRIQUES

Fonction de Hachage

- Une fonction de hachage présente quatre propriétés principales :
    - **Sortie de longueur fixe** : l'entrée d'une fonction de hachage peut avoir une longueur variable, tandis que la sortie d'une fonction de hachage (hash) est de longueur fixe ;
    - **Simple** : Le calcul du hash d'un message est simple et rapide ;
    - **Unidirectionnelle (one-way)** : impossible de découvrir un message à partir de sa valeur hash ;
    - **Résistante aux collisions** : impossible d'avoir une même valeur hash pour deux messages différents.
- Les principales fonctions d'hachage sont :
    - **MD5 (Message Digest)** conçue par Ron Rivest. MD5 fonctionne sur des blocs de 512 bits et sa sortie (la valeur hach) possède une longueur égale à 128 bits ;
    - **SHA-1 (Secure Hash Algorithm 1)** conçue par National Security Agency. SHA-1 fonctionne aussi sur des blocs de 512 bits et sa valeur hast est de longueur égale à 160 bits en sortie ;
    - **SHA-2 (Secure Hash Algorithm 2)** version plus récente que SHA-1. Les valeurs de hash de SHA-2 peuvent fournir des valeurs hash de longueurs de 256, 384 ou 512 bits ;
    - **Whirlpool** conçue par Vincent Rijmen, Paulo S. L. M. Barreto dans le cadre d'un projet. Elle génère des valeurs hash de longueur égale à 512 bits.



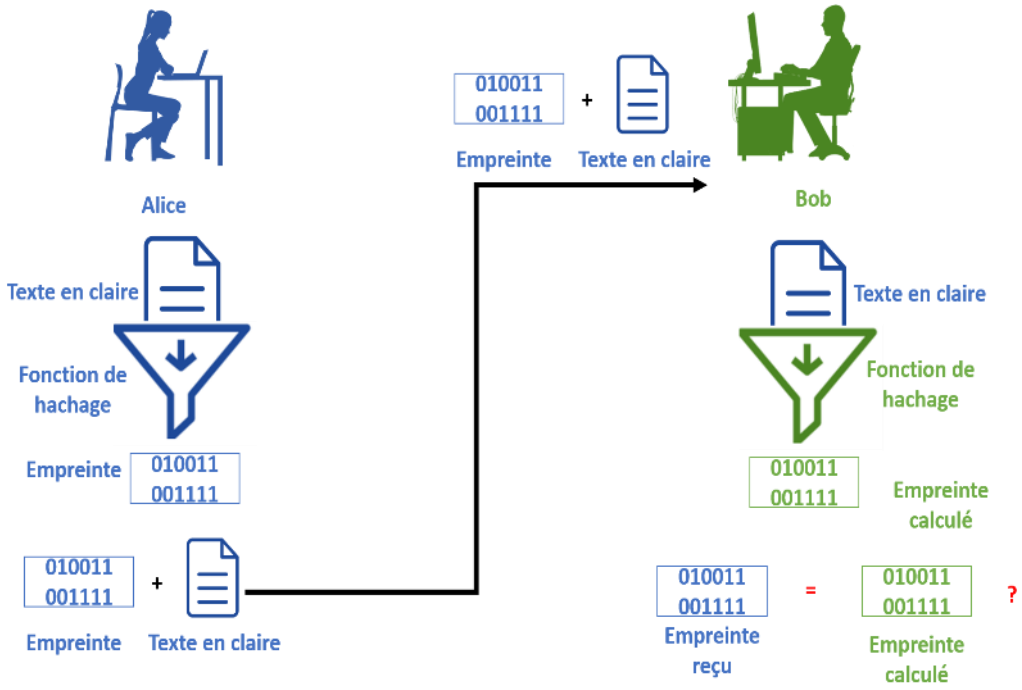
Caractéristiques d'une fonction de Hachage

PARTIE 3

Copyright - Tout droit réservé - OFPPT

Fonction de Hachage

- Puisqu'une fonction de hachage est **irréversible**, le processus de vérification d'une valeur hash (souvent appelée empreinte digitale) reçue est différent à celui utilisé dans le chiffrement (déchiffrer un message reçu pour découvrir le message d'origine)
- Comme illustré dans la figure ci-contre, le processus de vérification d'une empreinte générée par une fonction de hachage est le suivant :
    - Alice se met d'accord avec Bob sur une même fonction de hachage ;
    - Alice calcule l'empreinte digitale de son message et l'envoie avec le message d'origine à Bob ;
    - Lorsque Bob reçoit le message et l'empreinte, il calcule à son tour l'empreinte du message reçu (en utilisant la même fonction de hachage) et compare si l'empreinte reçue et celle calculée sont égales.
        - Si elles sont égales alors le message n'a pas été modifié
        - Si elles ne sont pas égales alors le message a été modifié
- D'où nous pourrons déduire que la fonction de hachage peut garantir l'**intégrité** des données. Néanmoins, pour une sécurité renforcée (confidentialité et intégrité), il faut utiliser conjointement un système de chiffrement et une fonction de hachage.
- Une fonction de hachage ne permet pas de garantir l'authenticité. En fait, il n'est pas possible de vérifier et prouver l'identité de l'expéditeur d'un message.



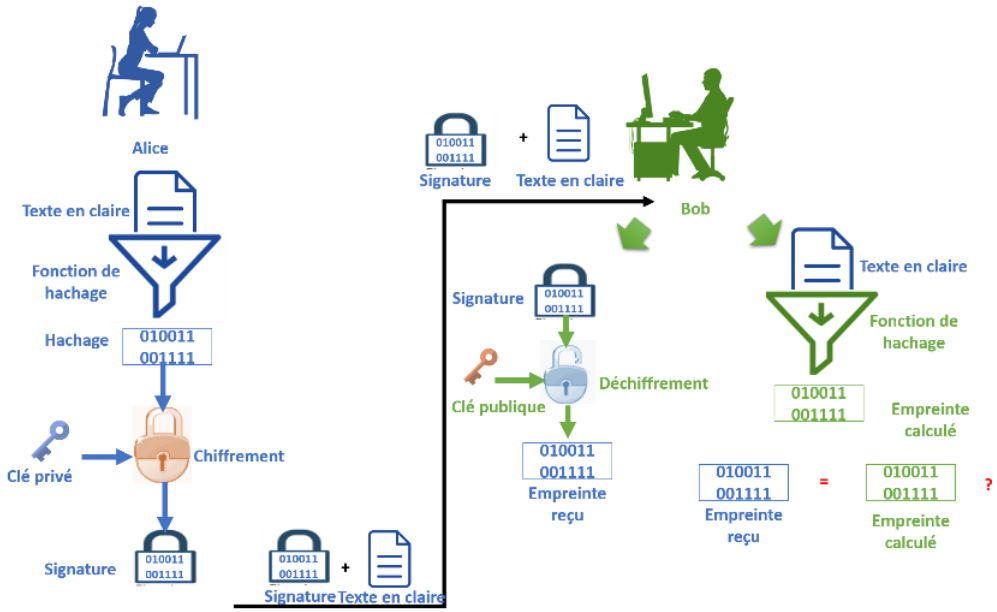
Processus de vérification d'une empreinte générée par une fonction de hachage

PARTIE 3

Copyright - Tout droit réservé - OFPPT

Signature Numérique

- La signature numérique est un schéma cryptographique utilisant les fonctions de hachage.
- Pour assurer l'authenticité, un message doit être signé par l'expéditeur avec sa clé privée.
- Comme illustré dans la figure ci-contre, le processus d'un schéma basé sur la signature numérique est le suivant :
    - Alice se met d'accord avec Bob sur une même fonction de hachage et partage avec lui sa clé publique ;
    - Alice calcule l'empreinte digitale de son message, puis elle signe l'empreinte (c.à.d., elle chiffre l'empreinte avec sa clé privé). Ensuite, Alice envoie le message en texte claire accompagné de la signature calculée à Bob ;
    - Lorsque Bob reçoit le message et la signature, il :
        - Déchiffre la signature avec la clé publique d'Alice pour récupérer l'empreinte reçu ;
        - Exécute la fonction de hachage sur le message reçu pour calculer son empreinte (empreinte calculé).
    - Bob vérifie ensuite si l'empreinte reçue est égale à celle calculée.
        - S'ils sont égaux, Bob peut prouver que c'est Alice qui a envoyé le message et que le message est intègre.
        - Sinon, Bob peut prouver que le message reçu a été modifié et que ce n'est pas Alice qui a signé le message.



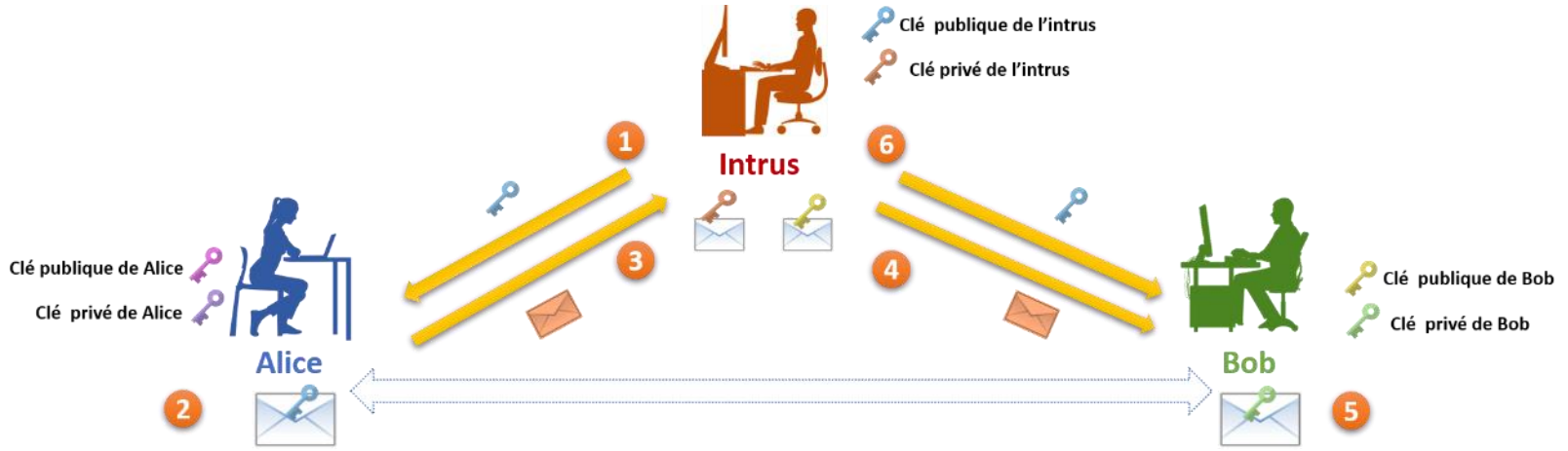
Processus de l'utilisation de la signature numérique

PARTIE 3

Copyright - Tout droit réservé - OFPPT

Attaque homme du milieu (Man in the Middle)

- Le problème majeur de la cryptographie asymétrique est la distribution des clés publiques. Notamment si un intrus partage sa clé publique en prétendant être un autre utilisateur. En ce qui suit, nous présentons une illustration de l'attaque homme du milieu qui exploite la faiblesse relative à la distribution des clés publiques.
- Processus de l'exécution de l'attaque homme du milieu :
    1. Un intrus envoie à Alice sa propre clé publique en prétendant être Bob ;
    2. Alice chiffre le message à envoyer à Bob en utilisant la clé publique de l'intrus ;
    3. L'intrus intercepte le message d'Alice, le déchiffre avec sa clé privée, et le modifie ;
    4. L'intrus chiffre le message modifié en utilisant la clé publique de Bob et l'envoie ;
    5. Bob déchiffre le message avec sa clé privée ;
    6. Si Bob envoie un message de réponse à Alice, l'intrus applique les mêmes étapes précédentes.



Processus de l'exécution de l'attaque homme du milieu

PARTIE 3

Copyright - Tout droit réservé - OFPPT

CHAPITRE 1

DÉCOUVRIR LA CRYPTOGRAPHIE ET LES CERTIFICATS NUMÉRIQUES

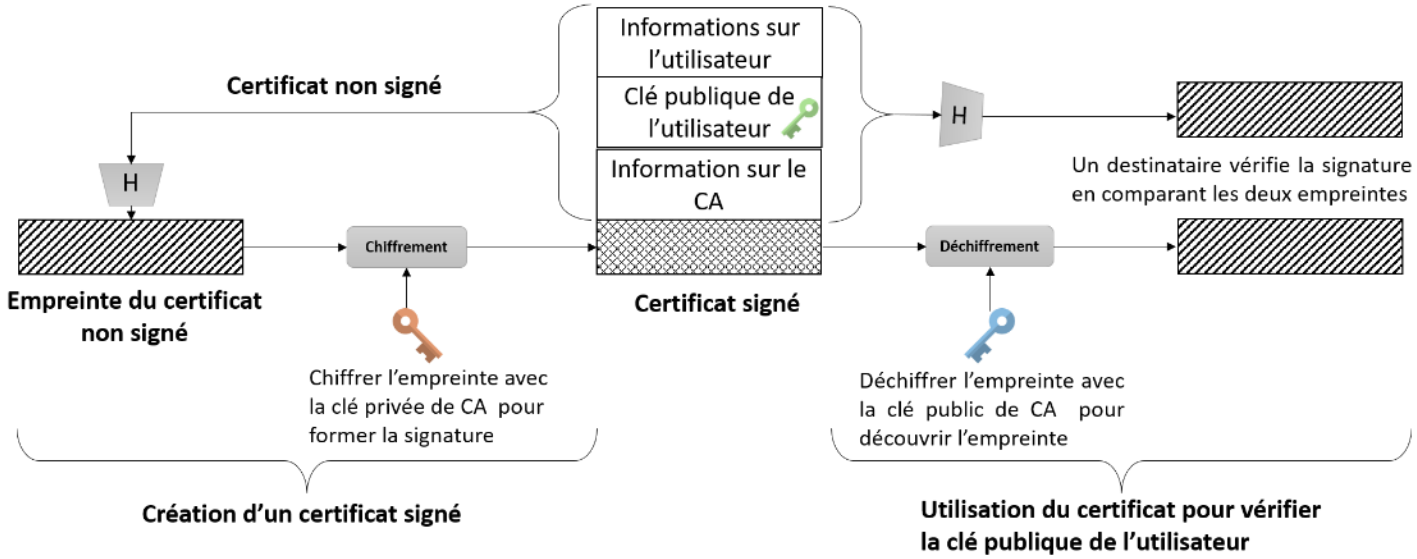
1. Objectifs de la cryptographie
2. Cryptographie symétrique et Cryptographie asymétrique
3. Fonction de hachage
4. **Certificats X.509**
5. Quiz sur la cryptographie et la gestion des clés

Certificats X.509

- Pour se protéger contre l'attaque homme du milieu et empêcher l'usurpation d'identité, il faut que chaque utilisateur confie sa clé publique à une autorité de certification (Certification Authority, CA).

  Chaque certificat contient la clé publique d'un utilisateur et il est signé avec la clé privée d'une autorité de certification (CA) de confiance.

- **La norme X.509** définit des protocoles d'authentification basés sur l'utilisation de certificats à clé publique. Elle définit également la structure d'un certificat
- **X.509** est basé sur l'utilisation de la cryptographie à clé publique et les signatures numériques.
  - Aucun algorithme de chiffrement n'est spécifié, cependant X.509 recommande RSA ;
  - Aucun algorithme de hachage n'est spécifié par X.509.



Processus de génération d'un certificat
Source :
https://media.cheggcdn.com/media/494/494442de-5b1e-49ab-83f0-d4d042acda85/php4Z3B9B[2]

PARTIE 3

Copyright - Tout droit réservé - OFPPT

Structure d'un certificat X509

- **Version** : spécifie la version du format de certificat. La valeur par défaut est la version 1.
  - Version 2 : l'identifiant unique de l'émetteur et/ou l'identifiant unique de l'utilisateur sont présents
  - Version 3 : les extensions sont présentes
- **Numéro de série** : valeur unique au sein de l'autorité de certification associée sans ambiguïté à ce certificat.
- **Algorithme de signature** : l'algorithme utilisé pour signer le certificat avec tous les paramètres associés.
- **Nom de l'émetteur** : le nom de l'autorité de certification qui a créé et signé ce certificat.
- **Validité** : se compose de deux dates : la première et la dernière à laquelle le certificat est valide.
- **Nom de l'utilisateur** : le nom de l'utilisateur auquel ce certificat fait référence
- **Informations sur la clé publique** : la clé publique de l'utilisateur, plus un identifiant de l'algorithme pour lequel cette clé doit être utilisée, ainsi que tous les paramètres associés.
- **Identificateur unique de l'émetteur** : chaîne de bits facultatif pour identifier de manière unique l'autorité de certification émettrice.
- **Identificateur unique de l'utilisateur** : chaîne de bits facultatif pour identifier de manière unique l'utilisateur
- **Extensions** : un ou plusieurs champs d'extension facultatifs.
- **Signature** : couvre tous les autres champs du certificat ; il contient le hash ode des autres champs chiffrés avec la clé privée du CA.

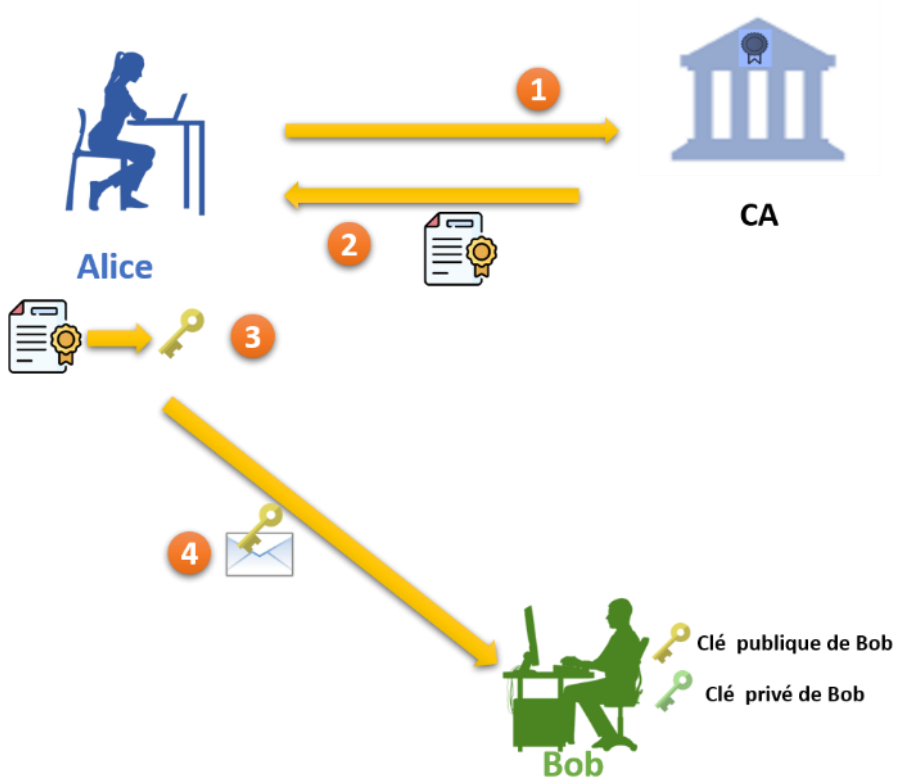
Structure d'un certificat X.509
Version
Numéro de série
Algorithme de signature
Nom de l'émetteur
Validité
Nom de l'utilisateur
Informations sur la clé publique
Identifiant unique de l'émetteur (Facultatif)
Identifiant unique de l'utilisateur (Facultatif)
Extensions (Facultatif)
Signature du certificat

Copyright - Tout droit réservé - OFPPT

Illustration de l'utilisation d'un certificat X.509

Comme illustré dans la figure ci-contre, lorsque Alice désire envoyer un message crypté à Bob en utilisant la cryptographie asymétrique, elle procède comme suit :

1. Pour récupérer la clé publique de Bob, Alice demande son certificat en envoyant une requête à l'autorité de certification (CA) ;
2. À la réception de la requête d'Alice, le CA lui envoie le certificat signé de Bob ;
3. Alice vérifie la signature du CA. Si c'est bien vérifié, alors elle extrait la clé publique de Bob ;
4. Alice utilisé la clé publique de Bob incluse dans le certificat pour chiffrer le message et l'envoie ensuite à Bob.



Exemple d'utilisation d'un certificat X.509

Copyright - Tout droit réservé - OFPPT

Révocation des certificats

- Comme vu dans la structure d'un certificat, chaque certificat possède une période de validité. Toutefois, un utilisateur peut avoir besoin de révoquer un certificat avant son expiration, pour l'une des raisons suivantes :
    - La clé privée de l'utilisateur a été compromise ;
    - L'utilisateur n'est plus certifié par cette autorité de certification ;
    - Le certificat de l'autorité de certification est compromis.
- Par conséquent, chaque autorité de certification maintient une liste des certificats révoqués, non expirés et qui ont été délivrés aux utilisateurs ou même aux autres autorités de certifications.
- Une liste de révocation de certificats (CRL) est publiée par une autorité de certification et inclut les champs suivant :
    - Le nom de l'émetteur (autorité de certification) ;
    - La date de création de la liste ;
    - La date à laquelle la prochaine CRL doit être émise ;
    - Une entrée pour chaque certificat révoqué, tel que chaque entrée inclut le numéro de série du certificat révoqué et la date de révocation de ce certificat.
- Un utilisateur doit alors vérifier si un certificat est révoqué avec la CRL de l'autorité de certification.

Copyright - Tout droit réservé - OFPPT

CHAPITRE 1

DÉCOUVRIR LA CRYPTOGRAPHIE ET LES CERTIFICATS NUMÉRIQUES

1. Objectifs de la cryptographie
2. Cryptographie symétrique et Cryptographie asymétrique
3. Fonction de hachage
4. Certificats X.509
5. **Quiz sur la cryptographie et la gestion des clés**

Énoncé

- **Question 1 : Parmi ces algorithmes de chiffrement, quels sont ceux utilisés pour le chiffrement symétrique ?**
  - ❑ RSA
  - ❑ DES
  - ❑ AES
- **Question 2 : Parmi les propriétés suivantes, quelles sont celles caractérisant une fonction de hachage ?**
  - ❑ Réversible
  - ❑ Irréversible
  - ❑ Son entrée doit être de longueur fixe
  - ❑ Résistante aux collisions

Question 3 : Que désigne X.509 ?

- ❑ Un algorithme de chiffrement
- ❑ Une norme définissant la cryptographie asymétrique basée sur l'utilisation des certification et signature numérique

Question 4 : Quels sont les objectifs de sécurité qui peuvent être offert grâce à l'utilisation de la cryptographie asymétrique basé sur l'utilisation des certificats et des signatures numériques ?

- ❑ Confidentialité
- ❑ Intégrité
- ❑ Non répudiation
- ❑ Authenticité

Copyright - Tout droit réservé - OFPPT

Correction

- **Question 1 : Parmi ces algorithmes de chiffrement, quels sont ceux utilisés pour le chiffrement symétrique ?**
  - ❑ RSA
  - ▣ DES
  - ▣ AES
- **Question 2 : Parmi les propriétés suivantes, quelles sont celles caractérisant une fonction de hachage ?**
  - ❑ Réversible
  - ▣ Irréversible
  - ❑ Son entrée doit être de longueur fixe
  - ▣ Résistante aux collisions

Question 3 : Que désigne X.509 ?

- ❑ Un algorithme de chiffrement
- ▣ Une norme définissant la cryptographie asymétrique basée sur l'utilisation des certification et signature numérique

Question 4 : Quels sont les objectifs de sécurité qui peuvent être offert grâce à l'utilisation de la cryptographie asymétrique basé sur l'utilisation des certificats et des signatures numériques ?

- ▣ Confidentialité
- ▣ Intégrité
- ▣ Non répudiation
- ▣ Authenticité

Copyright - Tout droit réservé - OFPPT

CHAPITRE 2

METTRE EN PLACE UNE PKI (PUBLIC KEY INFRASTRUCTURE)

Ce que vous allez apprendre dans ce chapitre :

- Découvrir les composants d'une architecture PKI
- Définir les différentes fonctions de gestion d'une PKI et les protocoles associés

2 heures

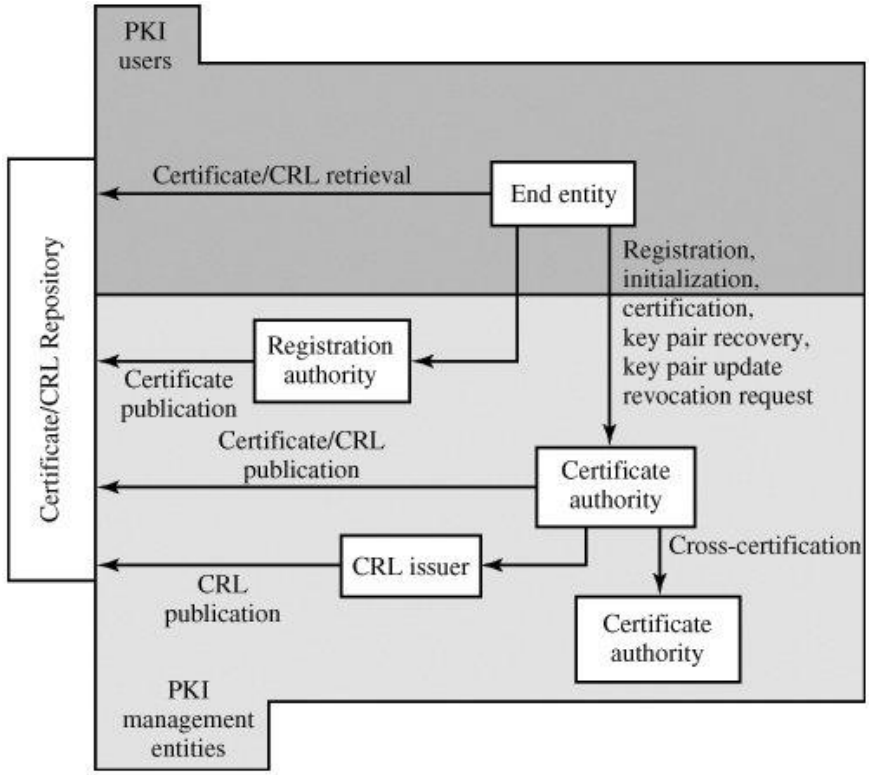
CHAPITRE 2

METTRE EN PLACE UNE PKI (PUBLIC KEY INFRASTRUCTURE)

1. **Architecture PKI**
2. Fonctions de gestion d'une PKI
3. Protocoles PKI : CMP et CMS

Architecture PKI

- Selon RFC 2822 (Internet Security Glossary), **une infrastructure à clé publique (Public Key Infrastructure, PKI, en anglais)** est l'ensemble du matériel, logiciels, personnes, politiques et procédures permettant de créer, gérer, stocker, distribuer et révoquer des certificats numériques basés sur la cryptographie asymétrique.
- L'infrastructure à clé publique conforme à la norme X.509 est connue sous le nom de PKIX.
- La figure ci contre illustre la relation entre les éléments clés du modèle PKIX, qui sont :
    - **Entité finale (End entity)**: désigne les utilisateurs finaux ou toute entité pouvant être identifiée dans le champ utilisateur d'un certificat de clé publique. Une entité finale consomme les services fournies par une infrastructure à clé publique.
    - **Autorité de certification (Certificate Autority)** : émetteur des certificats et des listes de révocation de certificats (Certificate Revocation Lists, CRL).
    - **Autorité d'enregistrement (Registration Autority)** : composant facultatif exécutant certaines fonctions administratives du CA. Elle est souvent associée au processus d'enregistrement de l'entité finale.
    - **Émetteur de CRL (CRL issuer)** : composant facultatif pour la publication des CRL .
    - **Référentiel (Repositiry)** : désigne toute méthode de stockage des certificats et des CRL afin qu'ils puissent être récupérés par les entités finales.
- PKIX définit également des fonctions de gestion qui doivent être prises en charge par des protocoles de gestion. Les fonctions de gestion et les protocoles seront détaillés en ce qui suit.



Modèle architectural PKIX

Source : https://flylib.com/books/3/190/1/html/2/images/14fig07.jpg

PARTIE 3

Copyright - Tout droit réservé - OFPPT

CHAPITRE 2

METTRE EN PLACE UNE PKI (PUBLIC KEY INFRASTRUCTURE)

1. Architecture PKI
2. **Fonctions de gestion d'une PKI**
3. Protocoles PKI : CMP et CMS

Fonctions de gestion d'une PKI

- **Enregistrement (Registration)** : Le processus par lequel un utilisateur s'enregistre auprès d'une autorité de certification (directement ou par l'intermédiaire d'une autorité d'enregistrement).
- **Initialisation (Initialization)** : Avant qu'un système client puisse fonctionner en toute sécurité, il est nécessaire d'installer les matériaux clés possédant une relation appropriée avec les clés stockées ailleurs dans l'infrastructure. Par exemple, un client doit être initialisé en toute sécurité avec les clés publiques et d'autres informations relatives aux autorités de certification approuvées, pour qu'il puisse valider les certificats en vérifiant la signature de l'autorité de certification.
- **Certification (Certification)** : Le processus par lequel une autorité de certification émet un certificat pour la clé publique d'un utilisateur, renvoie ce certificat au système client de l'utilisateur et/ou publie ce certificat dans un référentiel.
- **Récupération de pair de clés (Key pair recovery)** : permet aux entités finales de restaurer leur paire de clés de chiffrement/déchiffrement à partir d'une installation de sauvegarde des clés autorisées. En fait, il est important de prévoir un mécanisme permettant la récupération des clés de déchiffrement nécessaires lorsque l'accès normal au matériel de codage n'est plus possible, sinon il sera impossible de déchiffrer les données chiffrées
- **Mise à jour de pair de clés (Key pair update)** : toutes les paires de clés doivent être mises à jour régulièrement et par conséquent de nouveaux certificats sont émis. Une mise à jour est requise lorsque la durée de vie du certificat expire et/ou à la suite de la révocation du certificat.
- **Demande de révocation (Revocation request)** : une personne autorisée informe une autorité de certification d'une situation anormale nécessitant la révocation d'un certificat. Les raisons de la révocation incluent la compromission de la clé privée, le changement d'affiliation et le changement de nom.
- **Certification croisée (Cross-certification)** : deux autorités de certification échangent des informations utilisées pour établir une certification croisée. Une certification croisée est un certificat émis par une autorité de certification à une autre autorité de certification qui contient une clé de signature CA permettant l'émission des certificats aux autres autorités de certification

Copyright - Tout droit réservé - OFPPT

CHAPITRE 2

METTRE EN PLACE UNE PKI (PUBLIC KEY INFRASTRUCTURE)

1. Architecture PKI
2. Fonctions de gestion d'une PKI
3. **Protocoles PKI : CMP et CMS**

Protocoles PKI : CMP et CMS

- PKIX utilise deux protocoles de gestion alternatifs entre les entités PKIX qui prennent en charge les fonctions de gestion définies précédemment.
- Les deux protocoles de gestion sont :

Protocole de gestion des certificats (Certificate Management Protocols, en anglais) :

- Ce protocole est défini par RFC 2510 ;
- Il définit des échanges protocolaires spécifiques à chacune des fonctions de gestion de PKIX ;
- Il est conçu pour être un protocole flexible capable de s'adapter à une variété de modèles techniques, opérationnels et commerciaux.

Messages de gestion des certificats basé sur une syntaxe de messages cryptographiques définie (Certificate Management Messages over Cryptographic message syntax, en anglais, et abrégé en CMC)

- Ce protocole est par RFC 2797 ou CMS fait référence à la syntaxe de message cryptographique qui a été définie par RFC 2630;
- Ce protocole prend en charge tous les échanges nécessaires pour les fonctions de gestion de PKIX. Toutefois, les échanges protocolaires présentés dans CMC ne sont pas tous spécifiques, puisque ce protocole vise à tirer parti des implémentations existantes.

Copyright - Tout droit réservé - OFPPT

PARTIE 4

S’INITIER À L’AUDIT DE SÉCURITÉ DES SI

Dans ce module, vous allez :

- Découvrir les concepts de base relatifs aux audits de Sécurité SI
- Spécifier les phases d’audits de Sécurité
- Apprendre les exigences relatives à la prestation d’audits

11 heures

CHAPITRE 1

CONNAÎTRE LES CONCEPTS GÉNÉRAUX RELATIFS AUX AUDITS DE SÉCURITÉ SI

Ce que vous allez apprendre dans ce chapitre :

- Définir les objectifs des audits de sécurité SI
- Distinguer les différentes classes d'audits
- Présenter des référentiels d'audits

4 heures

CHAPITRE 1

CONNAÎTRE LES CONCEPTS GÉNÉRAUX RELATIFS AUX AUDITS DE SÉCURITÉ SI

1. **Objectifs des audits de sécurité SI**
2. Classification des audits
3. Les référentiels d'audit (COBIT, ISO 27002)
4. Quiz sur les objectifs et les référentiels d'audit

Objectifs des audits de sécurité SI

- Un audit de sécurité se réfère à une démarche permettant de :
    - Évaluer le niveau de sécurité d'une organisation et de son système d'information ;
    - Identifier les vulnérabilités du système d'information ;
    - Examiner la politique d'accès aux données et aux configurations réseau ;
    - Proposer des actions correctives et des recommandations .

- Un rapport est délivré à l'issue de la réalisation d'un audit de sécurité. Ce rapport décrit les écarts et les non-conformités découverts ainsi que le plan d'action à mettre en œuvre par l'organisation auditée.

- Généralement, un audit de sécurité est mené pour atteindre les objectifs suivants :
    - Évaluer les procédures et les mesures de sécurité en place déjà misent en place dans une organisation ;
    - Identifier les failles de sécurité du SI de l'organisation ;
    - S'assurer de la protection des données contre la perte et le vol ;
    - Vérifier la conformité des procédures d'une organisation par rapport aux exigences d'une norme (par exemple ISO 27001) ou un référentiel ;
    - Valider les configurations des systèmes et des réseaux en effectuant des tests d'intrusion et de vulnérabilités.

Copyright - Tout droit réservé - OFPPT

CHAPITRE 1

CONNAÎTRE LES CONCEPTS GÉNÉRAUX RELATIFS AUX AUDITS DE SÉCURITÉ SI

1. Objectifs des audits de sécurité SI
2. **Classification des audits**
3. Les référentiels d'audit (COBIT, ISO 27002)
4. Quiz sur les objectifs et les référentiels d'audit

PARTIE 4

Classification des audits

Trois différentes classes d'Audit

- peuvent être distingués, selon le guide d'audit de la sécurité des systèmes d'information (DGSSI) développé par la direction générale de la sécurité des systèmes d'information du Maroc en 2015.

Audit Interne

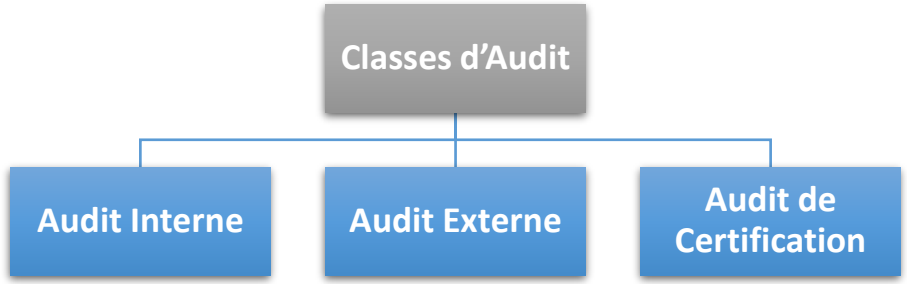
- Un audit mené suite à une décision prise par l'organisation auditée elle-même afin qu'elle puisse s'auto-évaluer en termes de sécurité en examinant le degré de sécurité de son système d'information.
- Ce type d'audit peut être mené par : des auditeurs internes (faisant parti de l'organisation) ou des auditeurs externes (faisant part de l'équipe d'un prestataire d'audit).

Audit Externe

- Un audit commandité par des tierces personnes qui ont un intérêt à l'égard de l'organisation auditée afin d'examiner le degré de sécurité de l'organisation ainsi que son système d'information.
- Ce type d'audit est mené par des auditeurs externes.

Audit de Certification

- Un audit mené suite à une décision prise par l'organisation auditée pour qu'elle puisse étudier le niveau de conformité de la sécurité de son système d'information par rapports aux exigences définies par des normes (par exemple ISO/CEI 27001)
- Ce type d'audit est mené par des auditeurs externes.



Les classes d'Audit

Copyright - Tout droit réservé - OFPPT

CHAPITRE 1

CONNAÎTRE LES CONCEPTS GÉNÉRAUX RELATIFS AUX AUDITS DE SÉCURITÉ SI

1. Objectifs des audits de sécurité SI
2. Classification des audits
3. **Les référentiels d'audit (COBIT, ISO 27002)**
4. Quiz sur les objectifs et les référentiels d'audit

Les référentiels d'audit (COBIT, ISO 27002)

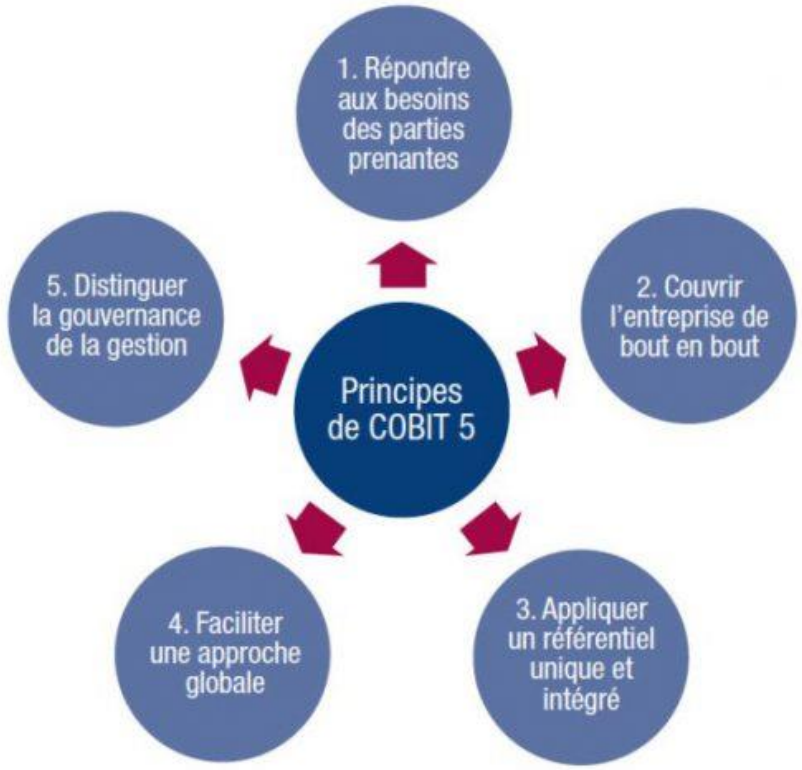
- Les référentiels se réfèrent à l'ensemble des normes, des méthodes et de bonnes pratiques.
- Différents référentiels d'audit ont été développés dans la littérature tel que :

  - **COBIT (Control Objectives for Information and Related Technology) :** C'est le principal référentiel de bonnes pratiques d'audit informatique et de gouvernance des systèmes d'information.
  - **CMMi (Capability Maturity Model integration) :** C'est un modèle d'évaluation **orienté processus** visant à mesurer la qualité de gestion des projets informatique en termes de délais, fonctionnalités, budget, etc. L'objectif de ce modèle est d'assurer une amélioration continue des processus de gestion des projets.
  - **ISO 27002 :** C'est le « Code de bonnes pratiques pour la gestion de la sécurité de l'information » qui a été publié en 2005 et révisé en 2013. Il définit un nombre de mesures de sécurités considérées comme des bonnes pratiques à appliquer lors de la mise en œuvre d'un SMSI (Système de Management de la Sécurité de l'Information).

Copyright - Tout droit réservé - OFPPT

COBIT

- Le référentiel COBIT a été développé en 1996, et depuis plusieurs versions de ce référentiel ont été proposé. Nous adressons dans cette partie la version 5 du référentiel, abrégé en COBIT 5.
- COBIT 5 est proposée depuis 2012 pour aborder la gouvernance et la gestion des systèmes d'Information des entreprises. Ce référentiel peut s'appliquer à des différents domaines, tel que la sécurité de l'information, la gestion des risques, les activités d'audit, etc.
- Comme illustré dans la figure ci-contre, les cinq principes du référentiel COBIT 5 sont :
    1. Répondre aux besoins des parties prenantes ;
    2. Couvrir l'entreprise de bout en bout en détaillant tous les processus requis depuis la gouvernance en passant par la gestion jusqu'aux opérations ;
    3. Appliquer un seul référentiel ;
    4. Simplifier l'approche globale ;
    5. Distinguer entre la gouvernance et la gestion.



Principes de fonctionnement du référentiel COBIT 5
Source : http://beeyou-partner.fr/wp-content/uploads/2019/10/COBIT-5-principes-BIS-e1570448107326.jpg

PARTIE 4

Copyright - Tout droit réservé - OFPPT

PARTIE 4

CMMI

- Le référentiel CMMI propose une démarche visant à assurer une efficacité organisationnelle. En effet, cette démarche permet d'évaluer la capacité d'une équipe (entreprise) à mener des projets informatiques, en termes de délais, de fonctionnalités et de budget.
- Une démarche CMMI est structurée en 25 processus adressant quatre domaines, qui sont : la gestion des processus, la gestion de projet, l'ingénierie, et le support.

- Comme illustré dans la figure ci-contre, CMMI définit également cinq niveaux de maturité :

Initial

- C'est le niveau par défaut ou les processus de gestion ne sont pas définis ;
- La réussite des projets repose sur les compétences et la motivation des individus et non pas sur des efforts collectifs de toute l'équipe ;
- Les facteurs de réussite ne sont pas identifiés, et le projet ne se construit pas sur les expériences passées.

Géré (Managed)

- C'est le deuxième niveau ou le déroulement d'un projet est planifié ;
- La gestion de projet est définie au niveau de l'organisation et appliquée par défaut sur tous les projets ;
- Ce niveau souffre du manque de la notion d'amélioration ;
- Les réussites sont répétables.

Les niveaux de maturité CMMI
Source : https://www.manager-go.com/assets/Uploads/CMMI-min.png

Copyright - Tout droit réservé - OFPPT

PARTIE 4

CMMI

Défini

- C'est le troisième niveau de maturité pour une organisation ;
- L'organisation dispose d'une discipline appliquée de manière cohérente pour guider les projets ;
- Les processus de pilotage des projets sont étendus à l'ensemble de l'organisation par l'intermédiaire de normes, standards, outils et méthodes ;
- L'organisation surveille et gère l'amélioration de ses processus.

Quantifié

- C'est le quatrième niveau de maturité ou les réussites des projets d'une organisation sont quantifiées.
- Les performances des processus sont prévisibles en quantité et en qualité.

Optimisé

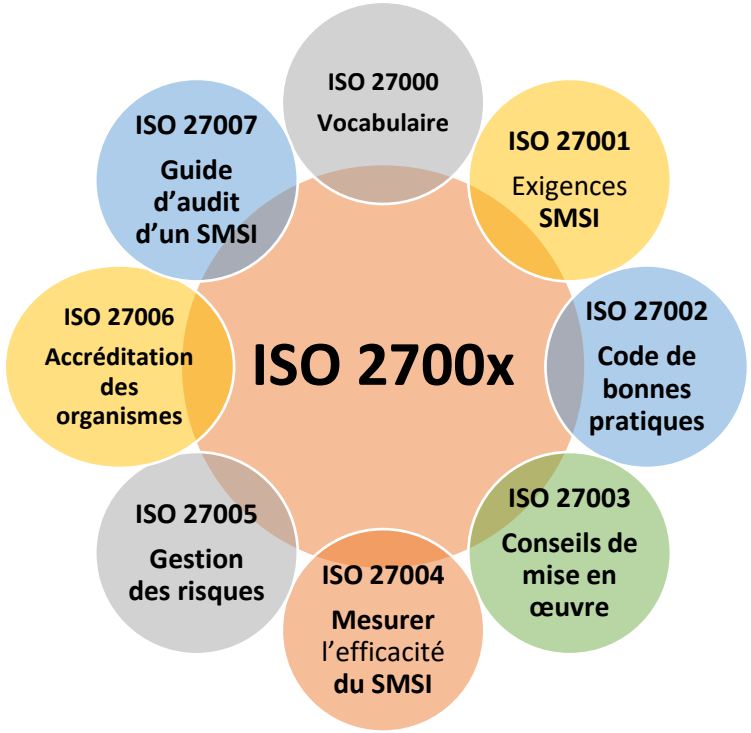
- Ce niveau de maturité définit le stade de l'adoption de l'amélioration continue des processus de manière incrémentale et innovante.

Les niveaux de maturité CMMI
Source : https://www.manager-go.com/assets/Uploads/CMMI-min.png

Copyright - Tout droit réservé - OFPPT

Normes ISO 2700x

- Outre les référentiels d'audit présentés précédemment, il y a les normes ISO 2700x qui traitent la sécurité d'information dans divers côtés
- Les normes ISO 2700x constituent une famille de normes qui traite la gestion de la sécurité de l'information
- ISO 27000 : définit le vocabulaire lié à la sécurité de l'information
- ISO 27001 : décrit les processus de la gestion et la mise en place d'un SMSI (Système de Management de la sécurité des informations)
- ISO 27002 : définit les bonnes pratiques de sécurité
- ISO 27003 : décrit les étapes à suivre pour la mise en place d'un SMSI conforme à la norme ISO 27001
- ISO 27004 : définit les indicateurs de pilotage d'un SMSI
- ISO 27005 : décrit les processus de la gestion des risques
- ISO 27006 : décrit les exigences relatives aux organisations qui auditent les SMSI
- ISO 27007 : définit les lignes directrices pour mener un audit SMSI



Normes ISO 2700x relatives à SMSI (Système de Management de la sécurité des informations)

PARTIE 4

Copyright - Tout droit réservé - OFPPT

CHAPITRE 1

CONNAÎTRE LES CONCEPTS GÉNÉRAUX RELATIFS AUX AUDITS DE SÉCURITÉ SI

1. Objectifs des audits de sécurité SI
2. Classification des audits
3. Les référentiels d'audit (COBIT, ISO 27002)
4. **Quiz sur les objectifs et les référentiels d'audit**

01 - Connaître les concepts généraux relatifs aux audits de sécurité si

Quiz sur les objectifs et les référentiels d'audit

Énoncé

- **Question 1 : Un audit de sécurité présente une démarche permettant :**
  - ❑ L'identification des éventuelles vulnérabilités
  - ❑ La mise place des mesures de sécurité afin de résoudre les failles de sécurité
  - ❑ La mise en place d'une politique de sécurité système d'information
  - ❑ Évaluer le niveau de sécurité d'un système d'information
- **Question 2 : Selon** DGSSI, un audit interne doit être réalisé par :
  - ❑ Des auditeurs internes uniquement
  - ❑ Des auditeurs externes uniquement
  - ❑ Des auditeurs interne ou des auditeurs externes
- **Question 3 : COBIT (Control Objectives for Information and Related Technology) représente :**
  - ❑ Une norme décrivant les principales directives d'un audit
  - ❑ Un référentiel décrivant une démarche qui inclut les bonnes pratiques d'audit informatique
  - ❑ Un modèle d'évaluation du niveau de maturité d'une organisation

Question 4 : La norme ISO qui décrit le vocabulaire de la sécurité de l'information est :

- ❑ ISO2700X
- ❑ ISO27000
- ❑ ISO27002

PARTIE 4

Copyright - Tout droit réservé - OFPPT

Correction

- **Question 1 : Un audit de sécurité présente une démarche permettant :**
  - ▣ L'identification des éventuelles vulnérabilités
  - ❑ La mise place des mesures de sécurité afin de résoudre les failles de sécurité
  - ❑ La mise en place d'une politique de sécurité système d'information
  - ▣ Évaluer le niveau de sécurité d'un système d'information
- **Question 2 : Selon** DGSSI, un audit interne doit être réalisé par :
  - ❑ Des auditeurs internes uniquement
  - ❑ Des auditeurs externes uniquement
  - ▣ Des auditeurs interne ou des auditeurs externes
- **Question 3 : COBIT (Control Objectives for Information and Related Technology) représente :**
  - ❑ Une norme décrivant les principales directives d'un audit
  - ▣ Un référentiel décrivant une démarche qui inclut les bonnes pratiques d'audit informatique
  - ❑ Un modèle d'évaluation du niveau de maturité d'une organisation

Question 4 : La norme ISO qui décrit le vocabulaire de la sécurité de l'information est :

- ❑ ISO2700X
- ▣ ISO27000
- ❑ ISO27002

Copyright - Tout droit réservé - OFPPT

CHAPITRE 2

DÉCRIRE LES PHASES D'AUDITS

Ce que vous allez apprendre dans ce chapitre :

- Spécifier les phases principales d'audits

5 heures

CHAPITRE 2

DÉCRIRE LES PHASES D'AUDITS

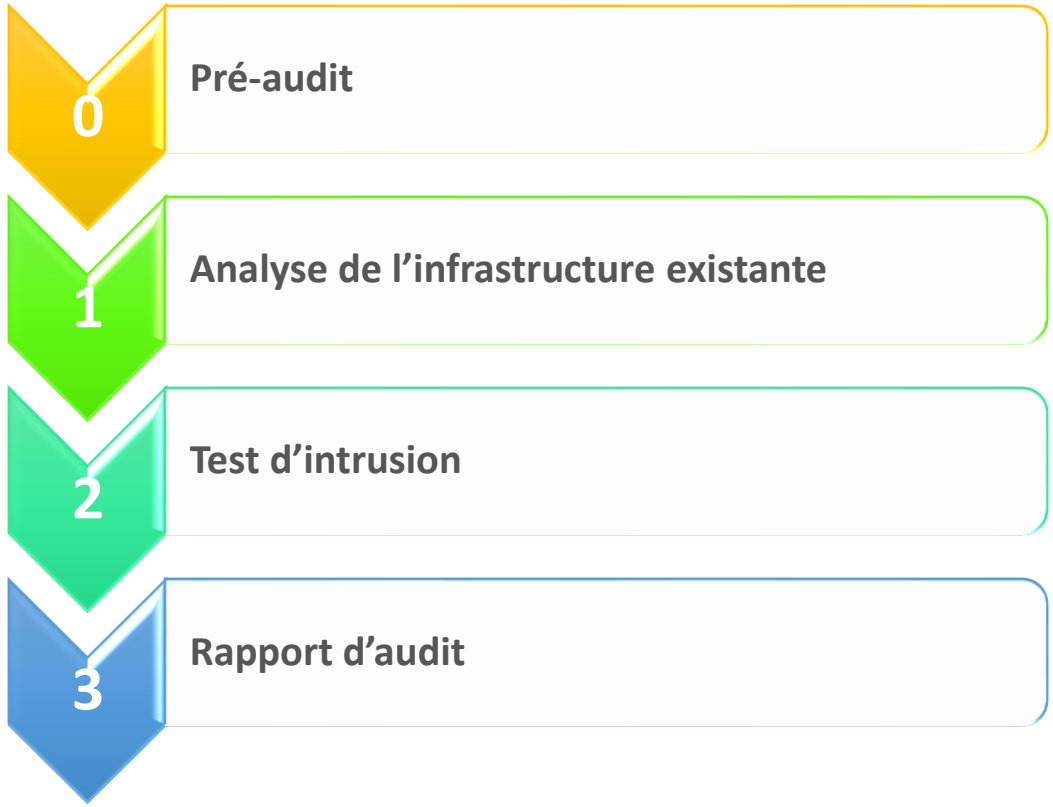
1. **Introduction**
2. Pré-audit
3. Analyse de l'infrastructure existante
4. Test d'intrusion
5. Rapport d'audit

Introduction

- Après avoir présenté les principaux référentiels d'audit de sécurité sur lesquelles les auditeurs peuvent être basés, ce chapitre détaille les principales étapes d'un audit de sécurité.

- Comme présenté dans la figure ci-contre, un audit de sécurité est organisé généralement en quatre phases :
    - Phase 0 : Pré-audit
    - Phase 1 : Analyse de l'infrastructure existante
    - Phase 2 : Test d'intrusion
    - Phase 3 : Rédaction du rapport d'audit

- En ce qui suit, nous détaillons les tâches à réaliser dans chacune des étapes citées précédemment.



Copyright - Tout droit réservé - OFPPT

CHAPITRE 2

DÉCRIRE LES PHASES D'AUDITS

1. **Pré-audit**
2. Analyse de l'infrastructure existante
3. Test d'intrusion
4. Rapport d'audit
5. Quiz sur la démarche d'audit

Pré-audit

- Cette phase est aussi appelée phase de préparation d'audit.

- C'est une phase importante pour la réalisation de l'audit de sécurité sur terrain, puisqu'elle permet de :

  définir le périmètre de l'audit et les sites de l'entreprise à analyser ;

  spécifier les objectifs à atteindre suite à la réalisation d'audit ;

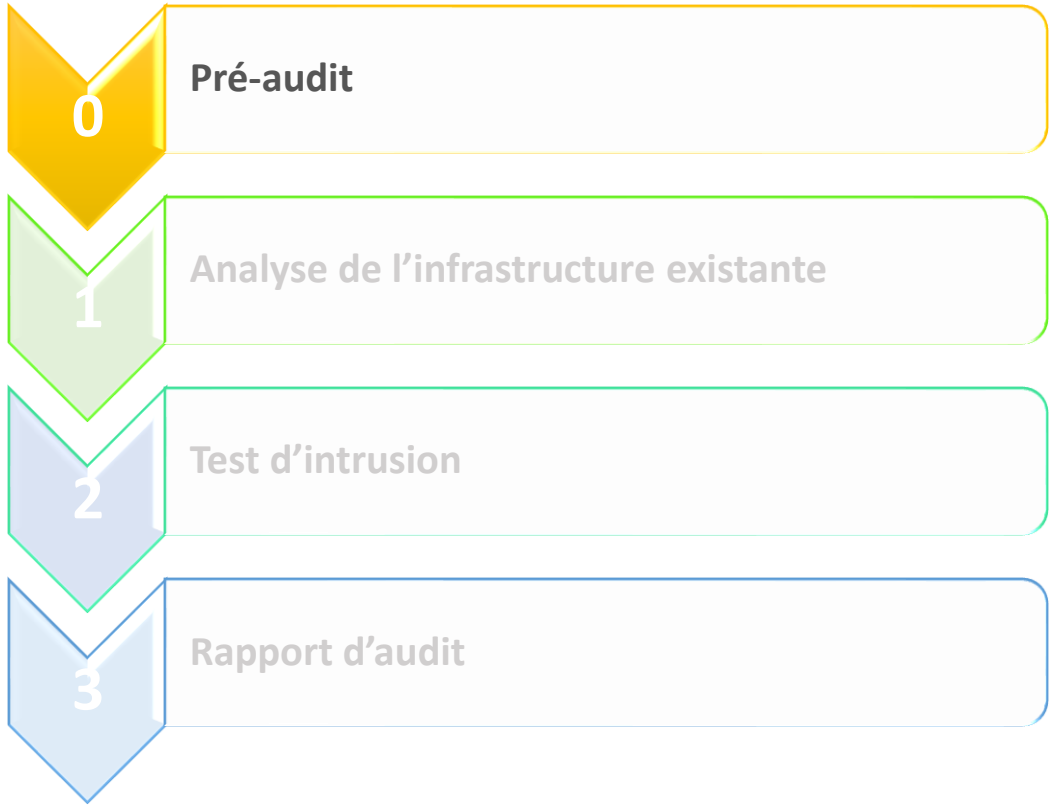
  construire une équipe d'audit en tenant en considération le périmètre de l'audit et les compétences requises pour atteindre les objectifs spécifiés ;

  fixer les grandes lignes à suivre lors de la réalisation de l'audit ;

  planifier la mission de l'audit en spécifiant les étapes à réaliser, les tests à exécuter et les ressources nécessaires pour mener à bien la mission d'audit ;

  spécifier les rôles et les responsabilités de tous les intervenants ;

  acquérir une bonne connaissance des réglementations.



Copyright - Tout droit réservé - OFPPT

CHAPITRE 2

DÉCRIRE LES PHASES D'AUDITS

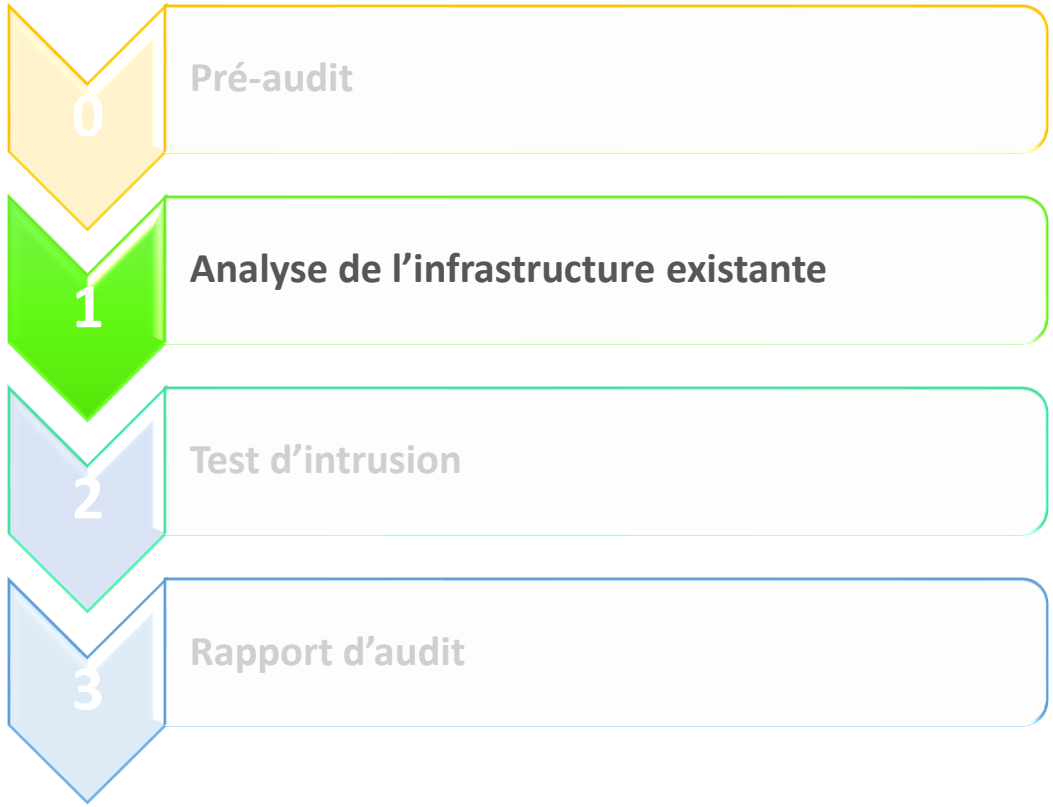
1. Introduction
2. Pré-audit
3. **Analyse de l'infrastructure existante**
4. Test d'intrusion
5. Rapport d'audit

Analyse de l'infrastructure existante

- L'analyse de l'infrastructure existante consiste essentiellement à diagnostiquer l'infrastructure matérielle et logicielle lié au système de l'information.

- L'objectif principal de cette étape est d'identifier les risques potentiels et d'évaluer l'efficacité des mesures de sécurité déjà mises en place et qui sont liées aux systèmes informatiques.

- Lors de cette phase, l'auditeur procède à :
    - Examiner les points d'entrées/sortie sur le réseau de l'entreprise ainsi que les services et les protocoles internes du réseau ;
    - Analyser les équipements de travail et de sécurité mises en place ;
    - Élaborer les scénarios possibles d'attaques de sécurité ;
    - Inspecter la qualité de l'architecture de sécurité du système audité en analysant la sécurité des flux des données sensibles et l'efficacité des outils de sécurité. Parmi les points essentiels à inspecter :
        - La politique des mots de passe
        - La configuration des pares-feux
        - Les listes de contrôle d'accès



Copyright - Tout droit réservé - OFPPT

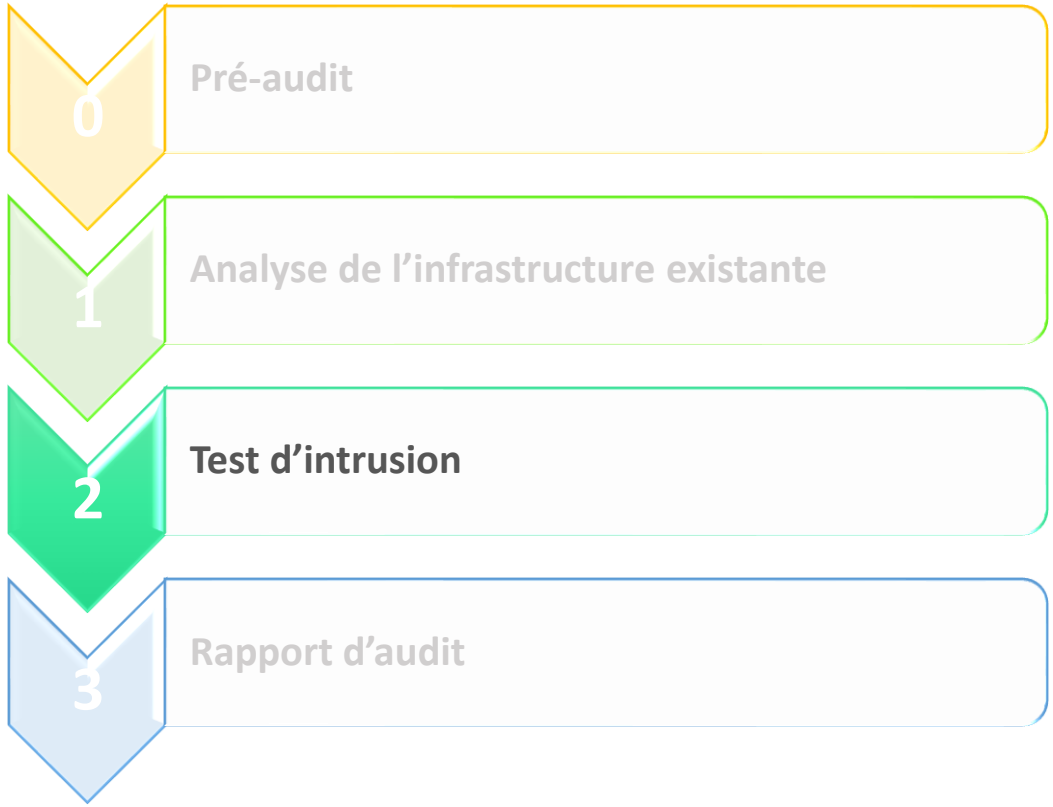
CHAPITRE 2

DÉCRIRE LES PHASES D'AUDITS

1. Introduction
2. Pré-audit
3. Analyse de l'infrastructure existante
4. **Test d'intrusion**
5. Rapport d'audit

Test d'intrusion

- Cette phase est souvent appelée phase de test de pénétration (Penetration Test, en anglais, abrégé en PenTest).
- Les principaux objectifs de test d'intrusion sont :
    - L'identification des vulnérabilités d'un système d'information ;
    - L'évaluation du degré de risque de chaque vulnérabilité identifiée ;
    - La proposition d'un ensemble de correctifs et de recommandations afin de réduire le degré de criticité des risques identifiés.
- Cette phase assure l'analyse d'une cible (système, application, réseau, etc.) en se mettant à la position d'un pirate. Elle permet d'évaluer :
    - Le degré de sévérité des failles de sécurité identifiées ;
    - Le niveau de complexité des correctifs à appliquer ;
    - La priorisation des correctifs à appliquer en fonction du degré de sévérité des failles et le niveau de complexité des correctifs.
- Noté qu'il ne faut pas confondre entre le test d'intrusion et le scan de vulnérabilité. En fait, le scan de vulnérabilité fait partie du test d'intrusion. Il permet uniquement à énumérer les vulnérabilités, sans les exploiter. Tandis que le test d'intrusion permet, en plus du scan, d'essayer d'exploiter les vulnérabilités et tester l'exécution des scénarios d'attaque.



Copyright - Tout droit réservé - OFPPT

Méthodes de test d'intrusion

- Pour réaliser des tests d'intrusion, il faut choisir entre les trois méthodes de tests qui sont des tests en boîte noire, blanche ou grise.
- **Test de la boîte noire (Black-Box Testing)**

- Consiste à tester un système sans accès aux informations sur le système testé.
- Le testeur (souvent appelé pentester) n'a aucune connaissance sur le système testé, son code source ou son architecture. La seule information détenue par le pentester est le nom de l'entreprise.
- Étant donné que le pentester ne connait aucune information, il adopte la méthode qu'un pirate utilise pour tenter de s'introduire dans le système.

- **Test de la boite blanche (White-Box Testing)**

- Permet de vérifier la structure interne d'une application.
- Le pentester connait toutes les informations sur le système d'information de l'entreprise, y compris l'architecture du système audité et son code source.
- Étant donné que le pentester connait toutes les informations, cette méthode permet une identification des vulnérabilités existantes plus simples par rapports aux deux autres méthodes de tests d'intrusion (boite noire et boite grise) .

- **Test de la boite grise (Gray-Box Testing)**

- Cette méthode combine des éléments de test de boîte noire et de boîte blanche.
- Le pentester a une certaine connaissance du système testé, qui se limite généralement aux documents de l'infrastructure réseau et de conception de l'architecture du système d'information.

Copyright - Tout droit réservé - OFPPT

Méthodes de test d'intrusion

- Le choix d'une méthode de test à adopter dépend des objectifs du test :
    - Le blanc pour découvrir les erreurs sémantiques des systèmes d'information ;
    - Le noir pour analyser le système d'information du point de vue d'un attaquant ;
    - Le gris fournit le programme d'assurance logicielle le plus complet.
- Quel que soit le type de test sélectionné, il est important que des testeurs (pentesters) qualifiés effectuent les tests et analysent les résultats afin de pouvoir spécifier les correctifs et les mesures de sécurité à mettre en place

Copyright - Tout droit réservé - OFPPT

CHAPITRE 2

DÉCRIRE LES PHASES D'AUDITS

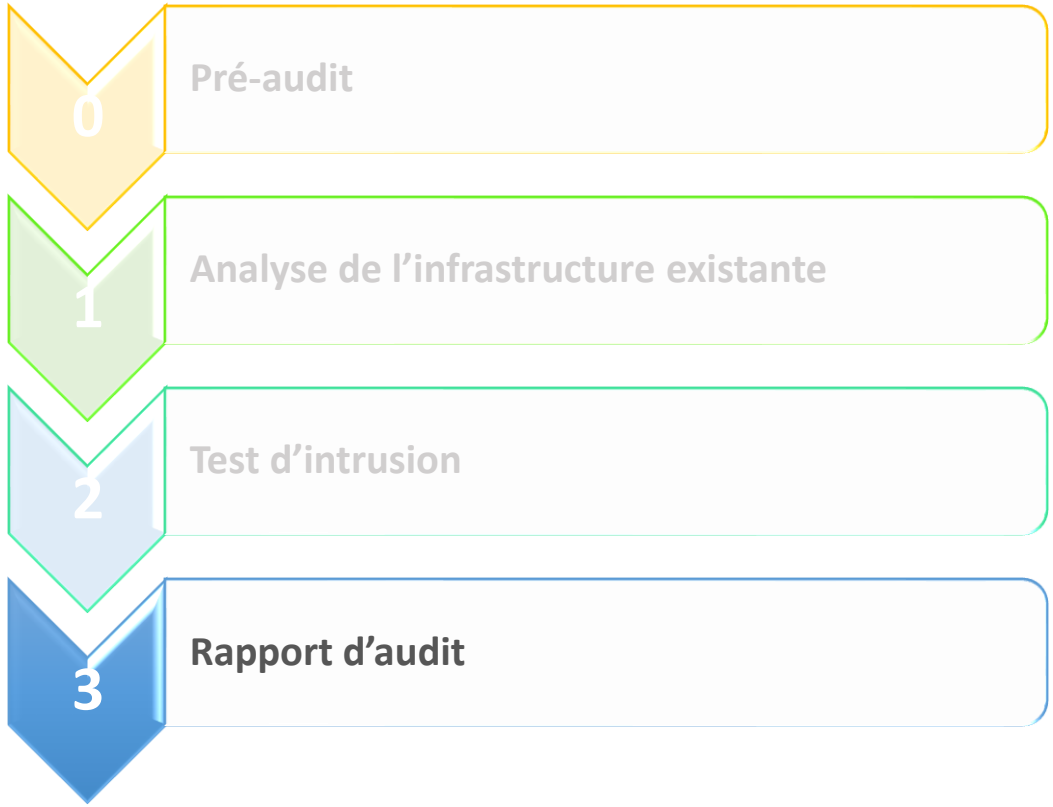
1. Introduction
2. Pré-audit
3. Analyse de l'infrastructure existante
4. Test d'intrusion
5. **Rapport d'audit**

Rapport d'audit

- La dernière phase du processus d'audit de sécurité système vise à rédiger un rapport d'audit

- Un rapport d'audit est rédigé sur la base des résultats obtenus dans les trois phases précédentes d'audit (Pré-audit, Analyse de l'infrastructure existante et test d'intrusion).

- Un rapport d'audit contient :
    - Un recueil des principales vulnérabilités et insuffisances identifiées ;
    - Un aperçu sur les outils de sécurité et les correctifs proposés ;
    - Une revue des recommandations à mettre en œuvre ;
    - Une proposition d'un plan d'action qui estime les budgets à allouer pour la mise en place des mesures et correctifs recommandés.



Copyright - Tout droit réservé - OFPPT

CHAPITRE 3

IDENTIFIER LES EXIGENCES RELATIVES À LA PRESTATION D'AUDITS

Ce que vous allez apprendre dans ce chapitre :

- Spécifier les exigences relatives au prestataire d'audit
- Spécifier les exigences relatives aux auditeurs

2 heures

CHAPITRE 3

IDENTIFIER LES EXIGENCES RELATIVES À LA PRESTATION D'AUDITS

Exigences relatives au prestataire d'audit

- Face à l'importance des prestations d'audit de sécurité des systèmes d'information, nous présentons les principaux exigences à remplir par les prestataires d'audit de sécurité des systèmes d'information.
- Un prestataire d'audit est chargé d'assister une organisation dans sa démarche d'amélioration continue de sécurité SI via l'évaluation de l'efficacité des méthodes et mesures de sécurité déjà mises en place. Par conséquent, un prestaire d'audit peut avoir accès à des informations sensibles de l'organisation auditée.
- Pour cette raison, il faut s'assurer de la présence de certains critères du prestataire d'audit tel que : l'objectivité, la responsabilité, le respect des lois, etc.
- Selon le guide d'audit de la sécurité des systèmes d'information (DGSSI) développé par la direction générale de la sécurité des systèmes d'information du Maroc en 2015, les exigences relatives à un prestataire d'audit peuvent être classés en sept classes :
    - **Exigences générales :** adressent la structure juridique du prestataire d'audit, son expérience et sa démarche d'audit ;
    - **Exigences relatives à la responsabilité du prestataire d'audit** : définissent la responsabilité d'un prestataire d'audit en vue des actions qu'il exécute ;
    - **Exigences relatives aux lois et réglementations en vigueur ;**
    - **Exigences relatives à la déontologie du prestataire d'audit** : présentent les règles relatives à l'éthique professionnelle que le prestataire d'audit doit respecter ;
    - **Exigences relatives à la protection des données de l'organisme audité** : adressent les exigences de confidentialités relatives aux données sensibles de l'organisation auditée que le prestataire d'audit doit respecter ;
    - **Exigences relatives à la gestion des ressources humaines du prestataire d'audit** : détailles les exigences relatives à la compétence de l'équipe d'audit chargée de la conduite d'audit ;
    - **Exigences relatives à la sous-traitance** : définissent les conditions dans lesquelles un prestataire peut sous-traiter une partie de l'audit.

Copyright - Tout droit réservé - OFPPT

CHAPITRE 3

IDENTIFIER LES EXIGENCES RELATIVES À LA PRESTATION D'AUDITS

1. Exigences relatives au prestataire d'audit
2. **Exigences relatives aux auditeurs**
3. Quiz sur les exigences relatives à l'audit

Exigences relatives aux auditeurs

- Comme présenté précédemment, un prestataire d'audit est responsable de former une équipe compétente pour qu'il puisse réussir sa mission d'audit
- En plus des compétences dans les domaines de la sécurité des systèmes d'information qu'ils doivent avoir, les auditeurs faisant partie dune équipe d'audit doivent présenter certaines **qualités personnelles** (qualités définies dans la norme ISO 19011 et recommandées par DGSSI) :


Intégrité : un auditeur doit être juste, sincère, honnête et discret.


Ouverture d'esprit : il doit également être capable d'envisager des idées ou des points de vue différents.


Diplomatie : il doit être capable de discuter des sujets sensibles.


Sens de l'observation : il doit être activement attentif.


Perspicacité : il doit être apte à résoudre facilement les différentes situations.


Polyvalence : il peut s'adapter aux différentes situations.


Ténacité : il peut se concentrer sur ses objectifs et les atteindre.


Sens de l'initiative et de prise de décisions.


Autonomie.

Copyright - Tout droit réservé - OFPPT

Exigences relatives aux auditeurs

- Outre les qualités personnelles, un auditeur doit :
    - Être apte à transmettre d'une manière simple et compréhensible ses idées et ses recommandations aux collègues faisant partie de l'équipe ou à l'équipe faisant partie de l'organisation auditée.
    - Être pédagogue pour qu'il puisse exposer ses recommandations d'une manière compréhensible aux différent intervenants (équipes techniques, équipes métier, dirigeants, etc.).
    - Être doté des qualités rédactionnelles pour qu'il puisse rédiger ses recommandations et son rapport d'audit.

Copyright - Tout droit réservé - OFPPT

CHAPITRE 3

IDENTIFIER LES EXIGENCES RELATIVES À LA PRESTATION D'AUDITS

03 - Identifier les exigences relatives à la prestation d'audits

Quiz sur les exigences relatives à l'audit

Énoncé

- **Question 1 : Les exigences générales d'un prestataire d'audit traitent**
  - ❑ Les exigences relatives à la compétence de l'équipe d'audit
  - ❑ Les règles relatives à l'éthique professionnelle
  - ❑ La structure juridique du prestataire d'audit
  - ❑ Les lois et les réglementations à respecter
- **Question 2 : Est-il possible à un prestataire de faire appel à des experts externes sous forme de sous-traitants dans le processus d'audit ?**
  - ❑ Oui
  - ❑ Oui à conditions qu'il faut respecter certaines exigences réglementaires précises
  - ❑ Non
- **Question 3 : Parmi ces qualités personnelles, quelles sont celles qu'un auditeur doit posséder ?**
  - ❑ Initiative
  - ❑ Autonomie
  - ❑ Monovalence
  - ❑ Dépendance

Copyright - Tout droit réservé - OFPPT

Correction

- **Question 1 : Les exigences générales d'un prestataire d'audit traitent**
  - ❑ Les exigences relatives à la compétence de l'équipe d'audit
  - ❑ Les règles relatives à l'éthique professionnelle
  - ▣ La structure juridique du prestataire d'audit
  - ❑ Les lois et les réglementations à respecter
- **Question 2 : Est-il possible à un prestataire de faire appel à des experts externes sous forme de sous-traitants dans le processus d'audit ?**
  - ❑ Oui
  - ▣ Oui à conditions qu'il faut respecter certaines exigences réglementaires précises
  - ❑ Non
- **Question 3 : Parmi ces qualités personnelles, quelles sont celles qu'un auditeur doit posséder ?**
  - ▣ Initiative
  - ▣ Autonomie
  - ❑ Monovalence
  - ❑ Dépendance

Copyright - Tout droit réservé - OFPPT