UNIVERSITÉ M'HAMED BOUGARA DE BOUMERDES
FACULTÉ DES SCIENCES
DÉPARTEMENT D'INFORMATIQUE

LICENCE 3

Module:
Sécurité informatique

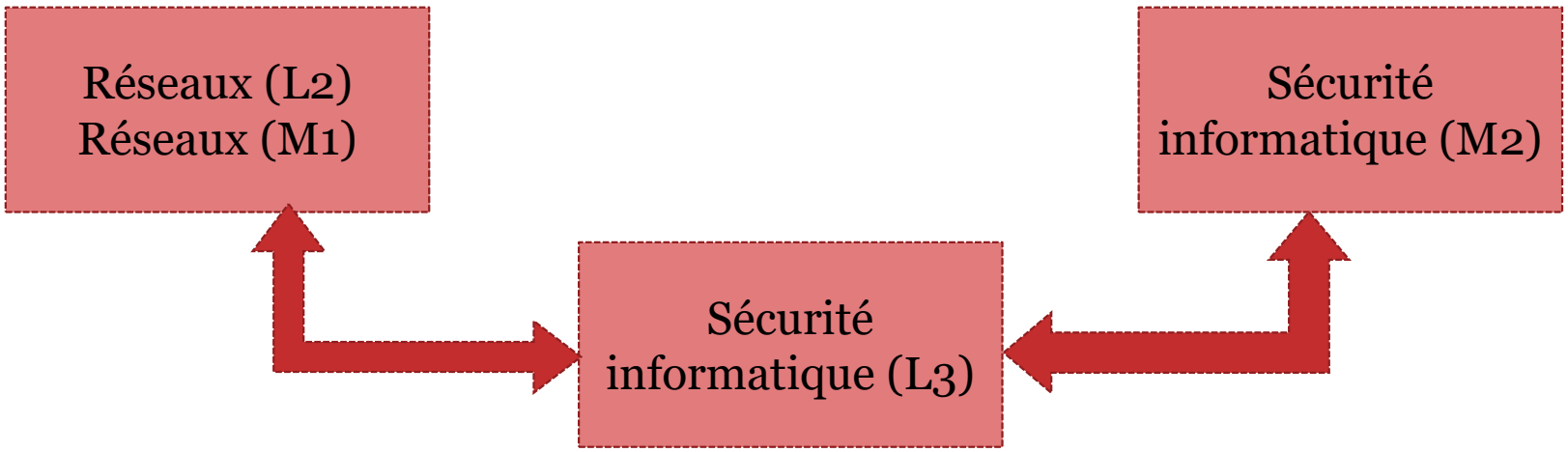
Principales parties du cours

- Introduction à la sécurité
- Introduction à la cryptographie
- Les attaques informatiques
- Les protections (mécanismes de défense)

Objectifs

- Se familiariser avec les concepts de la sécurité informatique.
- Connaître les différents services de sécurité.
- Savoir utiliser des mécanismes cryptographiques pour garantir différents services de sécurité.
- Se sensibiliser aux risques liés aux attaques sur les systèmes d'information.

Interaction avec les autres modules



- En pratique le module *sécurité informatique* s'intègre et interagit avec tous les autres modules (BDD, SE, Web, …)

Cours 1 :
Introduction à la sécurité informatique

Plan du cours

1. CONTEXTE GÉNÉRAL
2. LES ENJEUX DE LA SÉCURITÉ DES SI
3. OBJECTIFS/BESOINS DE LA SÉCURITÉ INFORMATIQUE
4. CONCEPTS DE SÉCURITÉ
5. DÉMARCHE GÉNÉRALE POUR SÉCURISER UN SI

Contexte général

- Information
  - L'avènement de l'informatique et des télécommunications à créer de grandes opportunités, pour les individus, les états, les industriels (économie, médias, etc.)
    - L'**information/donnée** -numérique-, sous ses différentes formes est devenue le "nerf de la guerre"
    - L'information numérique est omniprésente
      - *E-administration*
      - *E-commerce*
      - *E-Learning*
      - *E-Health*
      - Tranport
      - *etc.*
  - Les **systèmes d'information** sont devenus indispensables pour la gestion de ces données

Contexte général

- Système d'Information (S.I.)
  - C'est un ensemble constitué de: Données, logiciels, matériel, procédures, personnes, environnement physique
  - Cet ensemble de ressources est destiné **à collecter, classifier, stocker, gérer, diffuser** les informations au sein d'une organisation
- Système informatique
  - C'est l'ensemble d'équipements (matériels et logiciels) destiné au traitement automatique de l'information. **Il constitue la base sur laquelle repose un système d'information**

Contexte général

- Sécurité :
  - « état qui résulte de l'absence de risque » *Le Petit Robert*

- Sécurité informatique
  - Ensemble de méthodes, techniques et outils mis en œuvre pour la protection des systèmes, des données et des services contre des menaces accidentelles ou intentionnelles

Contexte général

- Évolution des Systèmes d'Information
  - Les SI aujourd'hui :
    - changent dynamiquement
    - intégration constante de nouveaux outils
    - mises à jour, réorganisations, …
    - se complexifient (hétérogénéité des systèmes),
    - s'interconnectent (en interne, mais aussi vers l'extérieur)
    - grande diversité de la nature des informations (financières, techniques, médicales, …)
  - Les technologies évoluent comme les menaces !
    - Le système d'information d'une organisation ou les données/PC d'un individu peuvent être la cible des individus/organisations voulant porter atteinte à leur sécurité (vol, destruction, manipulation, etc.)

Contexte général

- Pourquoi faut-il plus de sécurité informatique ?

Développement d'internet → **de plus en plus d'organismes ouvrent leur systèmes d'informations à leurs partenaires (fournisseurs , clients, …)**

↓

il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information

Les enjeux de la sécurité des SI

- La sécurité a pour objectif de réduire les risques pesant sur le système d'information, pour limiter leurs impacts sur le fonctionnement et les activités métiers des organisations

Les enjeux de la sécurité des SI

- **Exemples d'impacts:**
  - Impact Financiers
    - Supposant qu'une entreprise innovant ne sécurise pas son SI
    - Risque de vol des inventions en cours de réalisation et qui ne sont pas encore brevetées
    - → Une perte financière pour l'entreprise, car elle ne pourra pas prouver son antériorité, surtout si l'attaquant brevette/rend publique l'invention

Les enjeux de la sécurité des SI

- **Exemples d'impacts:**
  - Impact sur l'image et la réputation
    - Supposons que le système de passeport biométrique n'est pas sécurisé
      - Risque de délivrer un passeport falsifié → L'image du pays et sa réputation au niveau international seront fortement affectées
    - Supposons que le SI d'une banque est attaqué, et que les informations des clients sont divulguées
      - Risque de ne plus attirer de nouveaux client et de voir ses clients actuels partir

Les enjeux de la sécurité des SI

- **Exemples d'impacts:**
  - Impact Juridique/réglementaire
    - Supposons que le PC d'une personne n'est pas sécurisé et qu'un virus l'a infecté et par la suite une attaque a été lancée depuis ce PC à l'insu de son propriétaire
    - Cette personne est juridiquement responsable de l'attaque
  - Impact organisationnel
    - Si une attaque se produit, les personnes ayant été la cause devront être sanctionnées (dégradées, licenciées, etc.), ce qui pourra perturber l'organisation existante de l'entreprise

Objectifs/besoins de la sécurité informatique

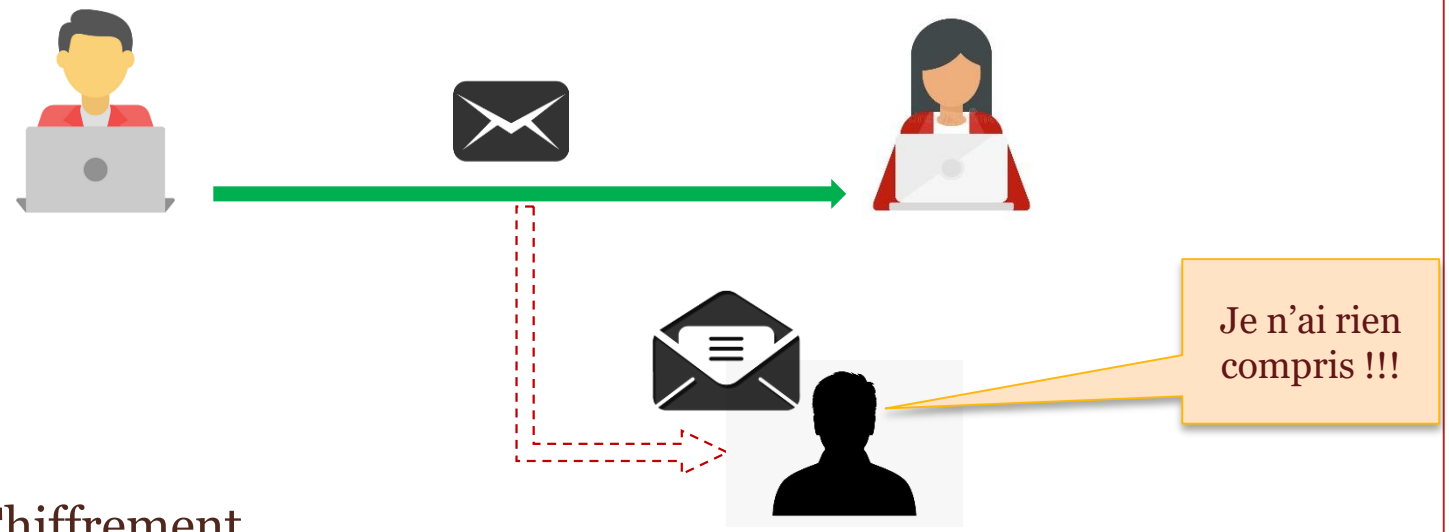
- Comment définir le niveau de sécurité des éléments d'un système ? Comment évaluer s'ils sont correctement sécurisés ?

- 3 critères sont retenus pour répondre à cette problématique, connus sous le nom de D.I.C.
  - Disponibilité
  - Intégrité
  - Confidentialité

- D'autres critères complémentaires
  - Non-répudiation
  - Authentification
  - …

Objectifs/besoins de la sécurité informatique

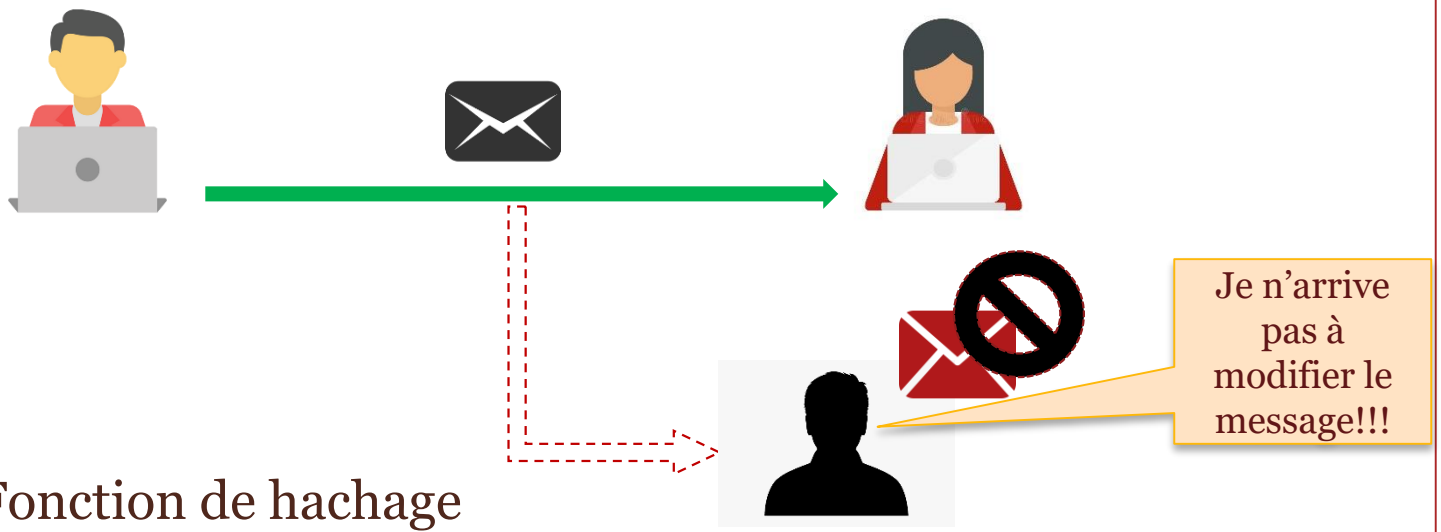
- Confidentialité
  - Elle vise à assurer que seules les entités autorisées aient accès aux ressources auxquelles elles ont droit.
  - La confidentialité a pour objectif d'empêcher que des informations secrètes soient divulguées à des entités non autorisés.



  - Solution: Chiffrement

Objectifs/besoins de la sécurité informatique

- Intégrité
  - Elle vise à assurer que les ressources ne soient pas corrompues (altération complète) ou modifiées (altération partielle) par des entités non autorisées à l'insu de leurs propriétaires
  - L'information reçue est bien celle qui a été envoyée → pas d'altération lors du traitement, conservation ou transmission



  - Solution: Fonction de hachage

Objectifs/besoins de la sécurité informatique

- Disponibilité
  - Assure que les ressources d'un système soient accessibles au moment voulu par les entités autorisées

AVAILABILITY

  - Solution: sauvegardes (redondance des données), gestion opérationnelle et maintenance efficaces

Objectifs/besoins de la sécurité informatique

- Non-répudiation
  - C'est le fait de ne pouvoir nier ou rejeter qu'un évènement (action, transaction) a eu lieu
  - La non répudiation de l'origine et de la réception des données empêche tant l'expéditeur que le receveur de nier avoir transmis ou reçu un message
  - Solution: Signature numérique

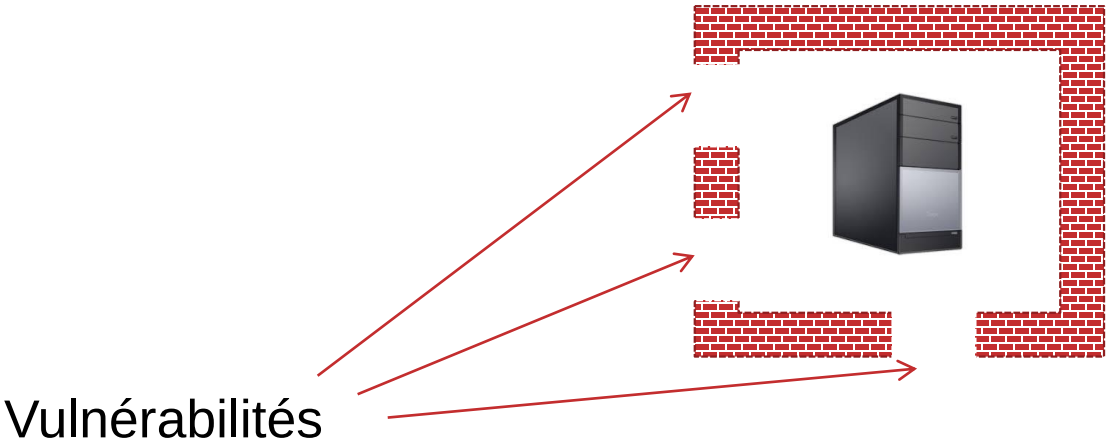
Objectifs/besoins de la sécurité informatique

- Authentification
  - Elle assure que seules les entités autorisées ont accès au système
  - Elle permet de vérifier l'identité d'une entité → protège contre l'usurpation d'identité

  - Il existe de nombreux mécanismes ou facteurs d'authentification:
    - **Ce que je sais:** un mot de passe;
    - **Ce que je sais faire:** une signature manuscrite sur écran tactile/digital;
    - **Ce que je suis:** une caractéristique physique comme une empreinte digitale;
    - **Ce que je possède:** une carte à puce.

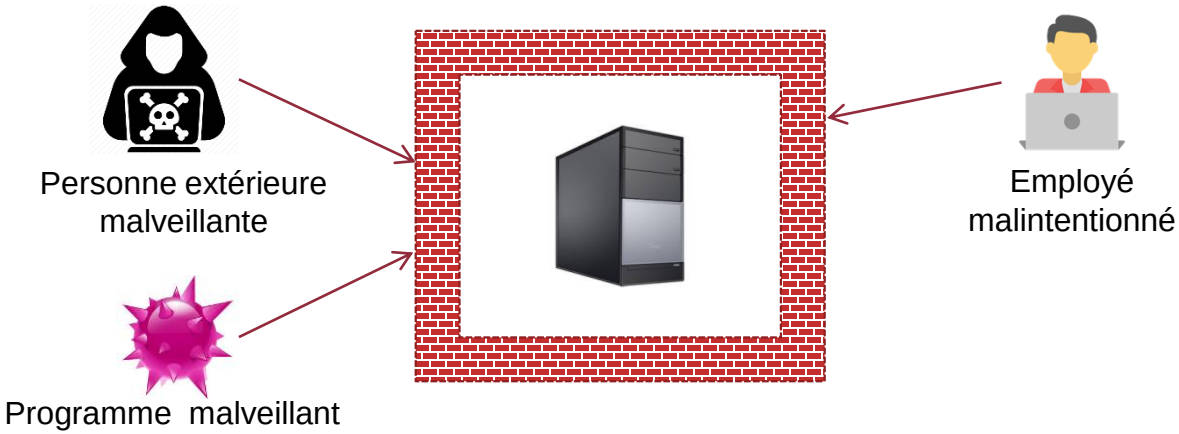
Concepts de sécurité

- Vulnérabilité
  - Faiblesse (faille/brèche) introduite intentionnellement ou accidentellement au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation d'un bien.
  - Un système sans vulnérabilités est un système fiable. Il n'existe pas un système fiable à 100% sauf s'il est complètement isolé!!



Concepts de sécurité

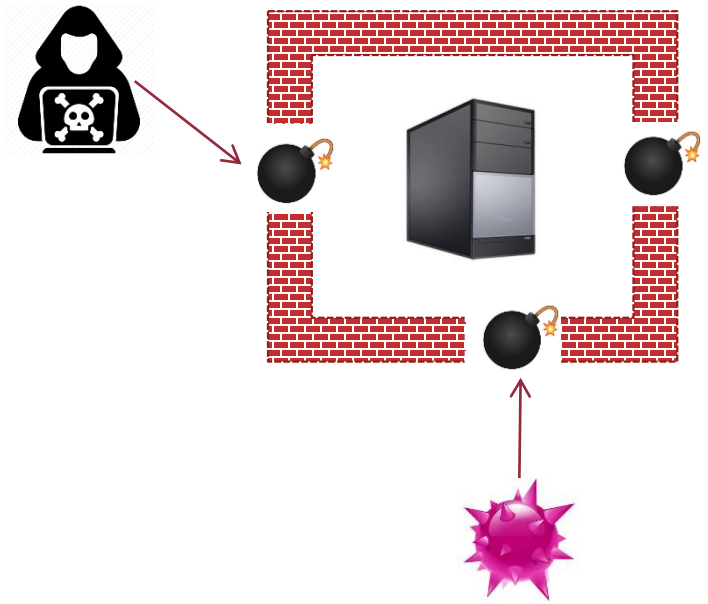
- Menace
  - Cause potentielle d'un incident, qui pourrait entrainer des dommages sur un bien si cette menace se concrétisait.
  - Une menace peut être une personne, un objet ou un événement pouvant potentiellement provoquer des dommages au réseau ou à ses équipements.
  - Les menaces peuvent être intentionnelles, comme la modification malveillante d'informations sensibles, ou accidentelles, suite à une erreur de calcul ou la suppression fortuite d'un fichier.



Concepts de sécurité

- Attaque

Action malveillante destinée à porter atteinte à la sécurité d'un bien. Une attaque représente la concrétisation d'une menace, et nécessite l'exploitation d'une vulnérabilité.



Concepts de sécurité

- Contre-mesures
  - Sont les actions mises en œuvre pour prévenir la menace, une fois qu'elle est mesurée

- Risque
  - C'est un scénario qui décrit comment des sources de risques (menaces) pourraient exploiter les vulnérabilités d'un système jusqu'à provoquer un incident sur les éléments à protéger et causer des préjudices.

Démarche générale pour sécuriser un SI

- Il est nécessaire d'entreprendre la sécurité informatique dans un cadre global. La sécurité doit être assurée:
  - **au niveau utilisateur**: les acteurs doivent comprendre l'importance de leur position.
  - **au niveau des technologies utilisées**: elles doivent être sûres et ne pas présenter de failles.
  - **au niveau des données en elles-mêmes**: avec une bonne gestion des droits d'accès (authentification et contrôle) l'utilisateur doit posséder uniquement les droits qui lui sont nécessaires.
  - **au niveau physique** (accès à l'infrastructure, au matériel): rien ne sert de sécuriser un système logiquement si matériellement l'accès à la salle des machines n'est pas sécurisé.

Démarche générale pour sécuriser un SI

- Un système de management de la sécurité de l'information, SMSI, est un dispositif qui gère et qui coordonne la manière dont la sécurité de l'information est mise en place

- Le SMSI est l'organisation en matière de sécurité définie par :
  - des processus
  - des politiques de sécurité
  - des structure de pilotage et de contrôle
  - une démarche d'amélioration continue

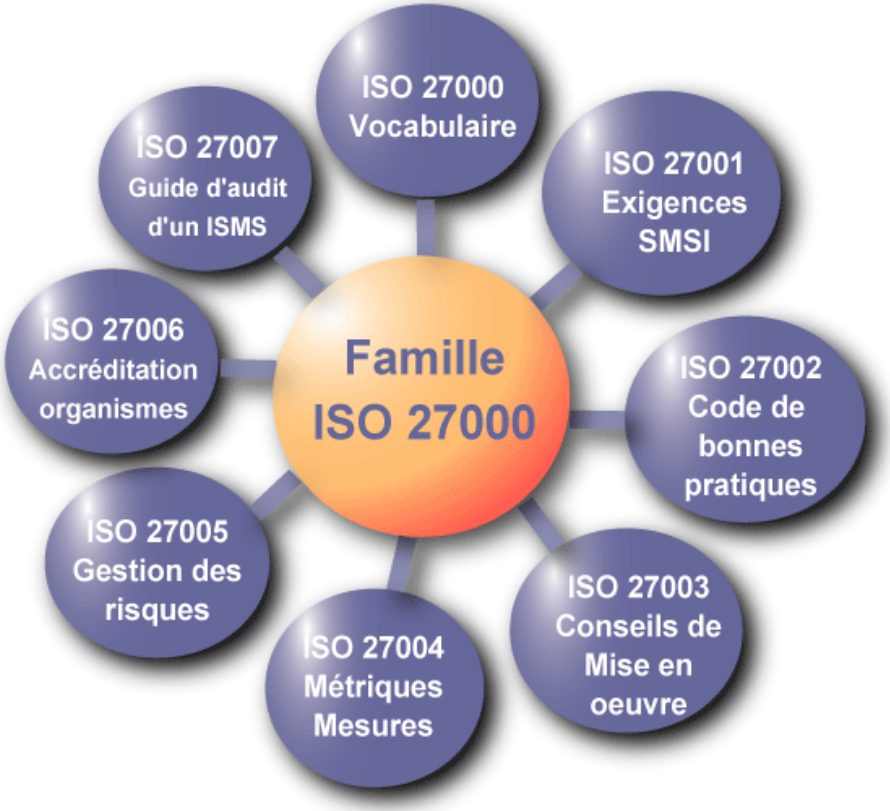
- Ce système prend en compte à la fois des facteurs techniques et humains.

- La mise en place d'un système de management de la sécurité de l'information (SMSI) offre une démarche pertinente pour améliorer l'efficacité de la sécurité de l'organisation et pour piloter la réduction des risques associés à ces informations.

Démarche générale pour sécuriser un SI

- Le Système de management de la sécurité de l'information (SMSI) est l'objet principal de la norme ISO 27001, qui en définit les caractéristiques.

- **Norme ISO 27001**
  - Publiée en octobre 2005 et révisée en 2013, elle succède à la norme BS 7799-2 de BSI (*British Standards Institution*)
  - Constitue le référentiel pour la mise en œuvre d'un SMSI
  - S'appuie sur une série de documents associés à ISO 27002/ISO 27004 / ISO 27005
  - Basée sur la **gestion des risques**
  - Met l'accent sur le **processus d'amélioration continue** du SMSI basé sur le modèle **PDCA** (Plan, Do, Check, Act).

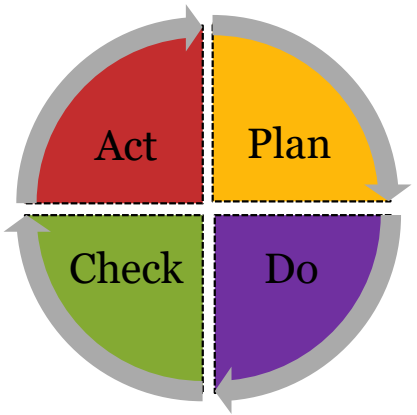


Démarche générale pour sécuriser un SI

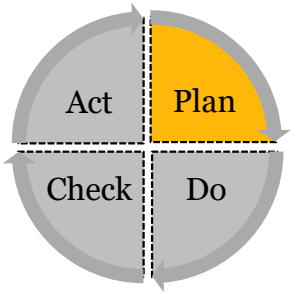
- Un SMSI doit être efficace à long terme, c'est-à-dire qu'il peut s'adapter aux changements qui ont lieu dans l'environnement interne et externe.

- L'ISO 27001 a adopté l'approche de la Roue de Deming (Deming Cycle ou Plan-Do-Check-Act : PDCA, en anglais)

- **Plan:** Je dois dire ce que je vais faire
  - Planifier, établir le SMSI
- **Do:** Je dois faire ce que j'ai dit
  - Implémenter et exploiter le SMSI
- **Check:** Je dois mesurer les écarts entre ce que j'aurais dû faire et ce que j'ai réellement fait
  - Contrôler, surveiller le SMSI
- **Act:** Je dois mettre en place des mesures correctives de ces écarts
  - Maintenir et améliorer le SMSI



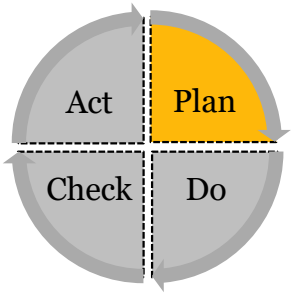
Démarche générale pour sécuriser un SI



- Phase 01: Plan
  - Étape 1: Identifier le périmètre de sécurité
  - Étape 2: Identifier et évaluer les risques liés à la sécurité
  - Étape 3: Elaborer la politique de sécurité

Démarche générale pour sécuriser un SI

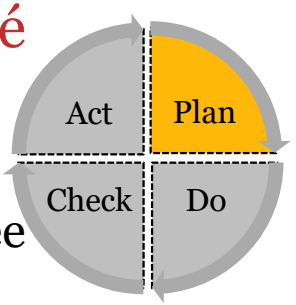
Étape 1: Identifier le périmètre de sécurité



- Le choix du périmètre revient de l'ordre de l'entreprise (il peut être restreint ou couvrir l'ensemble des activités de l'organisme)
- Déterminer le périmètre en termes d'activités de l'entreprise (périmètre fonctionnel, par métier, géographique, ...)
  - Périmètres de sécurité logiques ou physiques
- Déterminer les interfaces importantes entre ce périmètre et les domaines non couverts par le SMSI (qu'ils soient internes ou externes à l'entreprise)

Démarche générale pour sécuriser un SI

Étape 2: Identifier et évaluer les risques liés à la sécurité (Analyse des risques)



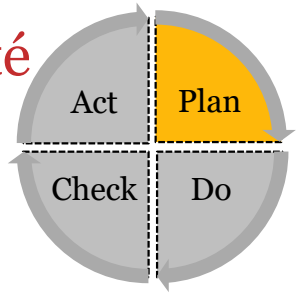
- Un risque est un danger éventuel qui se mesure par la probabilité qu'une menace particulière puisse exploiter une vulnérabilité donnée du système.
- Analyse de risque: consiste à répertorier les risques possibles, estimer leur probabilité et leur coût (impacts).

- Une analyse de risque peut être assez complexe et nécessite rigueur et méthode, il faut notamment trouver le bon niveau abstraction

- Plusieurs méthodes pour l'analyse et l'évaluation de risques (l'objectif est commun mais les termes et expressions employées varient d'une méthode à l'autre) :
  - MEHARI (MEthodologie Harmonisée d'Analyse de RIsques)
  - EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)
  - OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Évaluation*)

Démarche générale pour sécuriser un SI

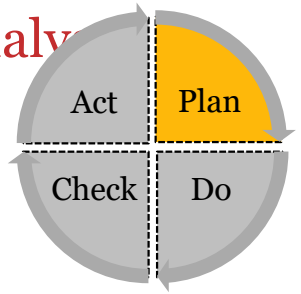
Étape 2: Identifier et évaluer les risques liés à la sécurité (Analyse des risques)



- Déterminer les éléments (biens/actifs) sensibles (ou ressources critiques) de l'entreprise
  - Matériels (ordinateurs, équipements réseaux, etc.)
  - Données (bases de données, sauvegardes, etc.)
  - Logiciels (sources des programmes, applications, etc.)
  - humains (tous les collaborateurs de l'entreprise)
  - Physique (bureaux, lieux de production, de livraisons)
- Identifier les vulnérabilités et les menaces possibles sur ces éléments
- Identifier l'impact (conséquences) des menaces sur les biens à protéger
- Estimation de la probabilité que ces menaces se réalisent
- Estimer les niveaux de risques
  - La norme n'impose aucune formule, on peut par exemple utiliser un code couleur

Démarche générale pour sécuriser un SI

Étape 2: Identifier et évaluer les risques liés à la sécurité (Analy des risques)



- Effectuer un classement rationnel des risques
  - Tous les risques n'ont pas la même probabilité de survenance
  - Tous les risques ne sont pas égaux en termes de gravité.

- **Niveau de Risque= Gravité * probabilité d'occurrence**

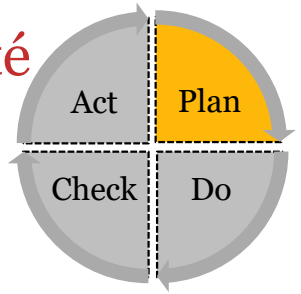
  - La gravité représente l'ampleur d'un risque. Elle dépend essentiellement du caractère préjudiciable des impacts potentiels.

  - La probabilité d'occurrence (vraisemblance) traduit la faisabilité d'un risque. Elle dépend essentiellement des vulnérabilités des supports face aux menaces et des capacités des sources de risques à les exploiter.

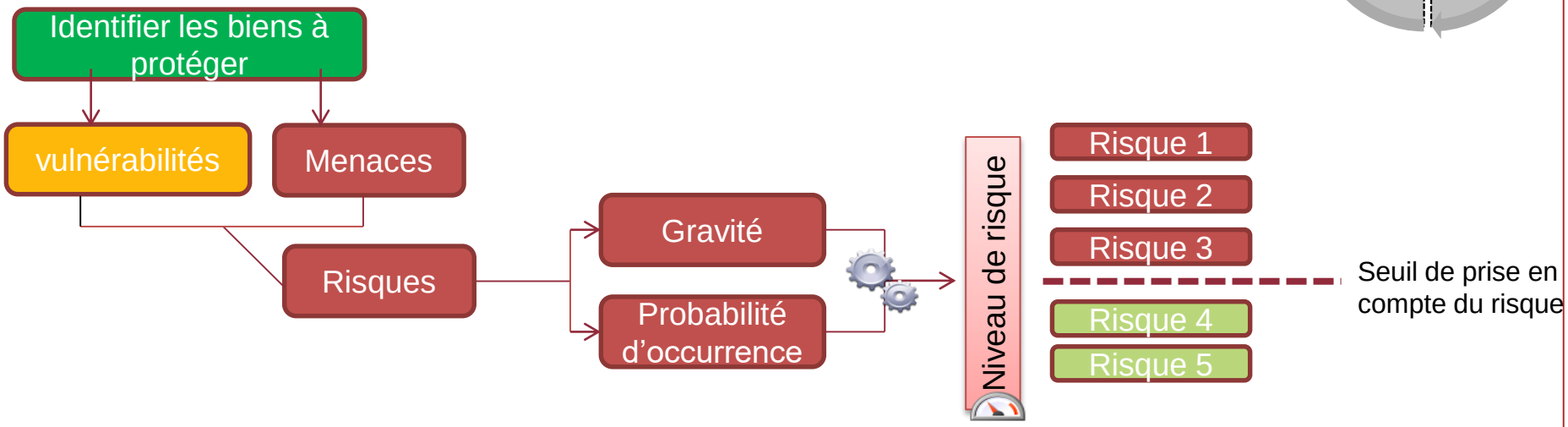
- Le risque « zéro » n'existe pas → l'entreprise détermine le niveau de risque qu'elle est prête à accepter sur ses ressources en comparaison avec le coût induit par les menaces qu'elle encourt → établir un seuil d'acceptabilité des risques

Démarche générale pour sécuriser un SI

Étape 2: Identifier et évaluer les risques liés à la sécurité (Analyse des risques)



Une démarche d'analyse de risque peut être schématisée ci-dessous :

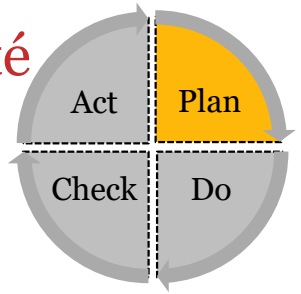


La hiérarchisation des risques permet de déterminer les risques qui :

- doivent absolument être traités et donc réduits par des mesures ;
- ceux qui sont acceptables et avec lesquels le système peut exister
  - un risque résiduel est le risque subsistant après le traitement de risque (car – par exemple – le coût pour compenser ce risque est trop élevé par rapport au risque encouru).

Démarche générale pour sécuriser un SI

Étape 2: Identifier et évaluer les risques liés à la sécurité (Analyse des risques)

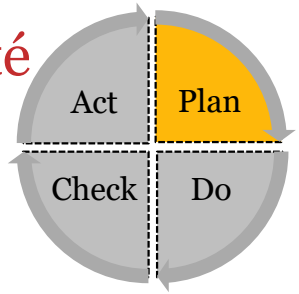


Matrice d'évaluation des risques

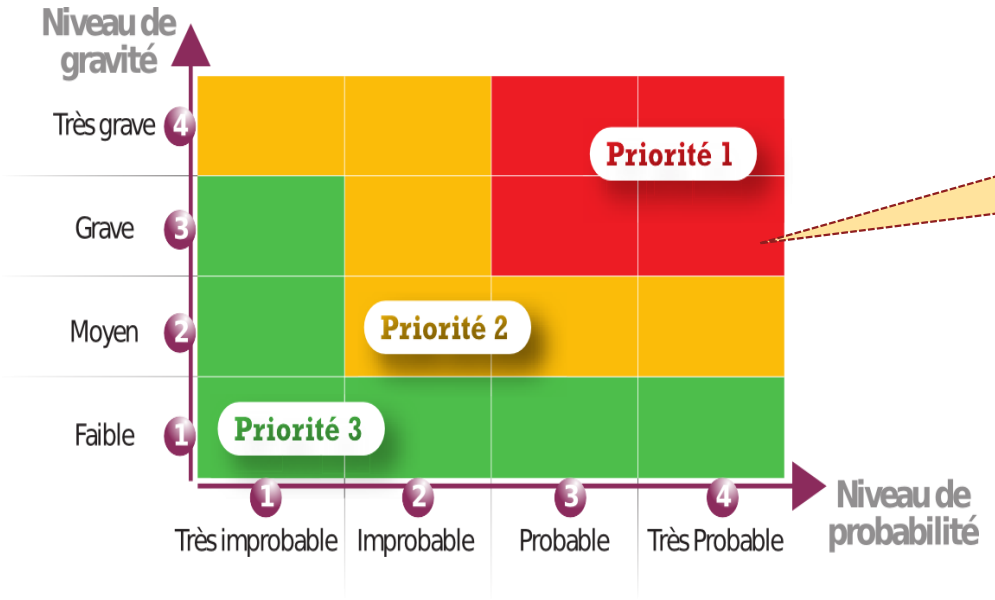
- C'est un outil qui permet de calculer le niveau d'un risque.
- Deux principaux paramètres:
  - La probabilité d'occurrence
  - La gravité
- On donne en général 3 à 5 niveaux à chaque paramètres
- Plutôt que de multiplier les deux valeurs, on construit une matrice et ce sont les zones de la matrice qui indiquent la criticité (niveau du risque)
- Les cases sont généralement colorées pour représenter les « niveaux d'acceptabilité »

Démarche générale pour sécuriser un SI

Étape 2: Identifier et évaluer les risques liés à la sécurité (Analyse des risques)



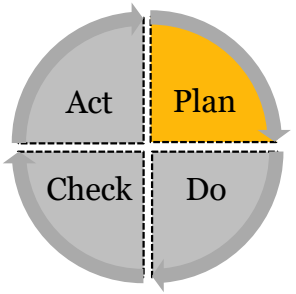
Matrice d'évaluation des risques (exemple)



Un code couleur (exemple):
Priorité 1: non acceptable
Priorité 2: acceptable
Priorité 3: négligeable

Démarche générale pour sécuriser un SI

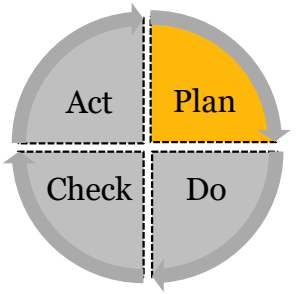
Étape 3: Elaborer la politique de sécurité



- **Définitions:**
  - La politique de sécurité des systèmes d'information (PSSI) est un plan d'actions définies pour maintenir un certain niveau de sécurité. Elle reflète la vision stratégique de la direction de l'organisme en matière de sécurité des systèmes d'information (SSI).
  - La politique de sécurité définit un certain nombre de règles, de procédures et de bonnes pratiques qui régissent la façon dont l'information sensible et les autres ressources sont gérées, protégées et distribuées à l'intérieur d'un système spécifique
  - Un document de référence permettant de décrire les mesures élémentaires de protection et d'utilisation du système d'information afin que tout le monde puisse les respecter

Démarche générale pour sécuriser un SI

Étape 3: Elaborer la politique de sécurité



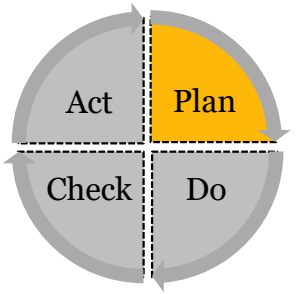
- **Etapes de mise en œuvre**

Après avoir identifier les besoins en terme de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences, il faudrait:

- Elaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés ;
- Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés ;
- Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace ;

Démarche générale pour sécuriser un SI

Étape 3: Elaborer la politique de sécurité



- **Exemple d'énoncé**

Une politique:

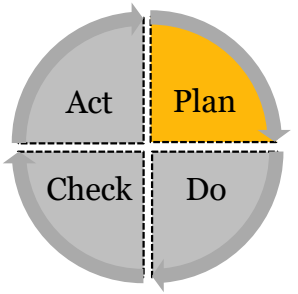
Cette politique vise à assurer que nos machines ne soient pas sujettes aux attaques de virus informatiques. Chaque machine doit utiliser un logiciel antivirus. Une seule personne doit être responsable de chaque machine. Elle doit vérifier que les logiciels antivirus sont mis à jour.

Une non-politique:

Cette compagnie prend la sécurité très au sérieux. Les attaques par virus informatiques sont très dangereuses. Nous ferons tout pour les éviter!

Démarche générale pour sécuriser un SI

Étape 3: Elaborer la politique de sécurité



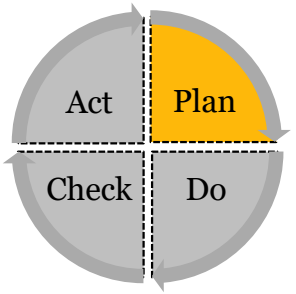
- Éléments d'une politique de sécurité

En plus de la formation et de la sensibilisation permanente des utilisateurs, la politique de sécurité peut être découpée en plusieurs parties:

- **Défaillance matérielle :**
  - L'achat d'équipements de qualité et standard accompagnés d'une bonne garantie avec support technique est essentiel pour minimiser les délais de remise en fonction.
  - Sauvegarde pour protéger les données.
- **Défaillance logicielle :**
  - Faire des copies de l'information à risque.
  - Une mise à jour régulière des logiciels.

Démarche générale pour sécuriser un SI

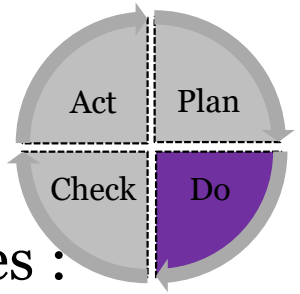
Étape 3: Elaborer la politique de sécurité



- Éléments d'une politique de sécurité
  - **Accidents (pannes, incendies, inondations…) :**
    - Une sauvegarde est indispensable pour protéger efficacement les données
    - La disposition et l'infrastructure des locaux peut aussi fournir une protection intéressante.
    - Prévoir la possibilité de basculer vers un site de secours
  - **Erreur humaine :** Outre les copies de sécurité, seule une formation adéquate du personnel peut limiter ce problème
  - **Vol via des dispositifs physique (clé usb):**
    - Contrôler l'accès à ces équipements.
    - Mettre en place des dispositifs de surveillance.

Démarche générale pour sécuriser un SI

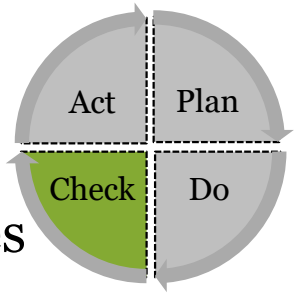
- Phase 02: Do



- Met en place les objectifs. Elle comporte plusieurs étapes :
  - Établir un plan de traitement des risques
    - Organiser les mesures, sélectionner les moyens nécessaires et définir les responsabilités
  - Déployer les mesures de sécurité
    - Techniques (contrôle d'accès, IDS, pare-feu, antivirus, contrôle des sauvegardes ….)
    - Organisationnelles (procédures de sauvegarde, définition des responsabilités, …)
  - Générer des indicateurs
    - De **performance** pour savoir si les mesures de sécurité sont efficaces
    - De **conformité** qui permettent de savoir si le SMSI est conforme à ses spécifications
  - Former et sensibiliser le personnel

Démarche générale pour sécuriser un SI

- Phase 03: Check

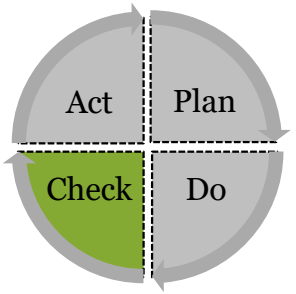


- Des contrôles sont mis en place pour vérifier l'efficacité des mesures appliquées.
- Vérifier que
  - il n'existe pas d'écarts majeurs entre ce que le SMSI définit et ce qui est mis en œuvre en pratique ;
  - les mesures de sécurité qui couvrent les risques les plus critiques sont adaptées, efficaces et suffisantes.

- Les indicateurs et les outils permettant ces contrôles sont multiples
  - **L'audit de sécurité**
  - **Les scans de vulnérabilité**
  - **Les tests d'intrusion**

Démarche générale pour sécuriser un SI

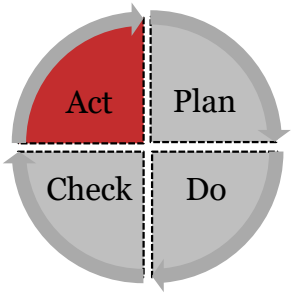
- Phase 03: Check



- **L'audit de sécurité:** Consiste à s'appuyer sur un tiers de confiance afin de:
  - Evaluer le niveau de sécurité d'un système face à un standard ou un référentiel externe
  - Vérifier que chaque règle de la politique de sécurité est correctement appliquée
- **Les scans de vulnérabilité**
  - C'est un **scan** du système qui permet **d'énumérer les vulnérabilités,** sans tenter de les qualifier ou de vérifier si elles sont exploitables.
- **Les tests d'intrusion**
  - Consiste à analyser le système en se mettant dans la peau d'un attaquant (identifier les vulnérabilités et tenter de les exploiter).

Démarche générale pour sécuriser un SI

- Phase 04: Act

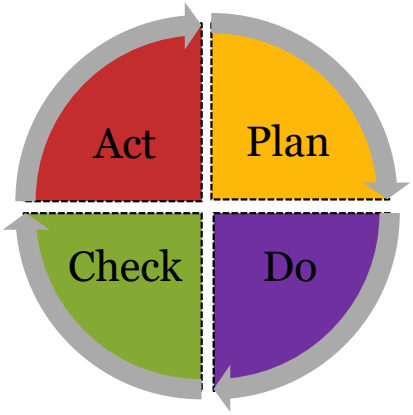


- Définir les actions qui permettront de réaliser les corrections et les améliorations du SMSI (mises en évidence par les indicateurs lors de l'étape Check)

- Prendre en compte tout changement éventuel intervenu entre temps dans le système d'information :
  - un changement de périmètre (technique, organisationnel ou fonctionnel) ayant un impact sur le périmètre du SMSI ;
  - de nouveaux risques (nouvelles menaces apparues, nouvelles vulnérabilités).

- Les actions résultantes sont:
  - **Actions correctives** : agir sur les effets pour corriger les écarts puis sur les causes pour éviter que les incidents ne se reproduisent
  - **Actions préventives** : agir sur les causes avant que l'incident ne se produise
  - **Actions d'amélioration** : améliorer la performance d'un processus du SMSI.

Démarche générale pour sécuriser un SI



- Pour résumer, la démarche consiste à:
  - Identifier le périmètre de sécurité (analyse du contexte)
  - Analyser les risques (identification et évaluation)
  - Établir une politique de sécurité
  - Définir et implémenter des mesures de sécurité (techniques / organisationnelles) permettant d'appliquer la politique de sécurité
  - Valider des mesures implémentées afin de vérifier qu'elles offrent la protection voulue

Conclusion

- La sécurité ne s'improvise pas et nécessite des professionnels
- Une politique de sécurité doit être adaptée à l'organisme et à ses évolutions
- La politique de sécurité d'une entreprise se fonde sur une analyse de risques décrivant les ressources critiques de l'entreprise, ses objectifs de sécurité, ses vulnérabilités, les probabilités d'occurrence de menaces sur ses ressources vitales, ainsi que leurs conséquences
- Les normes sont une aide pour mettre en œuvre une démarche d'amélioration continue de la sécurité