Sécurité des systèmes d'informations

Préparé par :Amal HADRI
E-mail: amal.hadri2009@gmail.com

Chapitre1: Introduction à la sécurité des systèmes informatiques

Plan du chapitre 1

1. Introduction :
2. Système informatique vs système d'information :
   a. Sécurité informatique :
   b. Sécurité des systèmes d'information :
3. Critères fondamentaux de la sécurité de l'information :
   a. Confidentialité:
   b. Intégrité ;
   c. Disponibilité ;
   d. Authenticité ;
   e. Non-répudiation ;
4. Niveau de sécurité:
   a. Utilisation;
   b. Fonctionnalités;
   c. Protection.

5. Domaines de la sécurité :
   a. Sécurité physique ;
   b. Sécurité de l'exploitation ;
   c. Sécurité logique ;
   d. Sécurité applicative ;
6. Taxonomies et définitions :
   a. Vulnérabilités ;
   b. Menaces ;
   c. Risques ;
   d. Attaques ;
   e. Service de sécurité ;
   f. Mécanismes de sécurité ;
7. Acteurs de sécurité :
   a. Les employés;
   b. La DG ;
   c. Le RSSI ;
8. Politique de sécurité:
   a. Catégories des attaquants :

Les défis du SI d'aujourd'hui
Concilier ouverture et sécurité

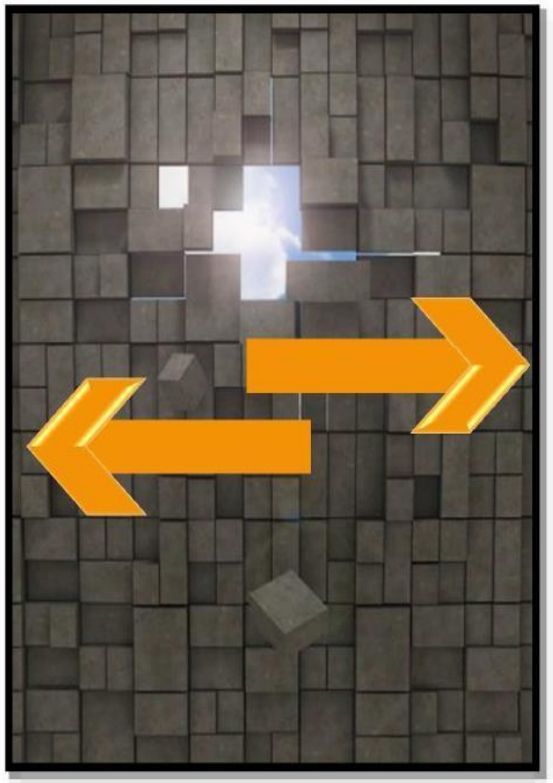
Globalisation

Mobilité

Collaboration

Salesforce.com

Logiciels en mode SaaS



Menaces

Politique d'utilisation

Chapitre 1: Démystifier la sécurité IP

Objectifs:

- Distinguer vulnérabilités, menaces, et risque dans le domaine IP;
- Identifier leurs relations; les classer, les prioriser afin de protéger le capital informationnel de l'entreprise;
- Faire le lien entre vulnérabilité, comportement des employés et procédures.

idées préconçues

J'ai installé un firewall, et c'est suffisant pour nous protéger?
D'accord ou pas d'accord

Notre site web ne risque rien car il est peu consulté et ne contient aucune Information Intéressante pour la concurrence.
D'accord ou pas d'accord

Je suis certain que nos administrateurs ont mis en place un systèmes de détection d'intrusion infaillible
D'accord ou pas d'accord

Notre réseau est protégé par ce que nous avons installé des anti spam et des anti virus sur chaque machine
D'accord ou pas d'accord

Système d'informations (SI) Vs système informatique (IT)

- **L'IT (Système informatique)** est l'ensemble des actifs matériels et logiciels de l'entreprise ayant pour vocation à automatiser le traitement de l'information. C'est la partie visible à laquelle tout le monde pense quand on parle de projets et d'infrastructures informatiques.

- **Le SI (Système d'information)** est l'ensemble des actifs de l'IT (matériels et logiciels, forcement référencé quelque part), qui comprend ainsi les actifs humains et immatériels, les procédés, procédures, et processus, d'industrialisation, sur lesquels on les affecte, les informations de niveau sémantique, organisationnelle et de structure.

SI= IT+ RH + environnement

Système d'informations (SI) Vs système informatique (IT)

Le SI:

- L'ensemble des moyens nécessaires à l'élaboration, au traitement, au stockage, à l'acheminement et à l'exploitation des informations;

- Le SI représente un patrimoine essentiel de l'entreprise;

Définitions (2/ 3)

La sécurité du système d'information :

- Ensemble de mesures de sécurité **physique**, **logique**, **administrative** et de mesures **d'urgence**, mises en place dans une organisation, en vue d'assurer:
  - La confidentialité des données de son système d'information;
  - La protection de ses biens informatiques;
  - la continuité de service.

Définitions (3/3)

- Les systèmes informatiques sont au cœur des systèmes d´information;
- Ils sont devenus la cible de ceux qui convoitent l'information;
- Assurer la sécurité de l'information implique l'assurance de la sécurité des systèmes informatiques.

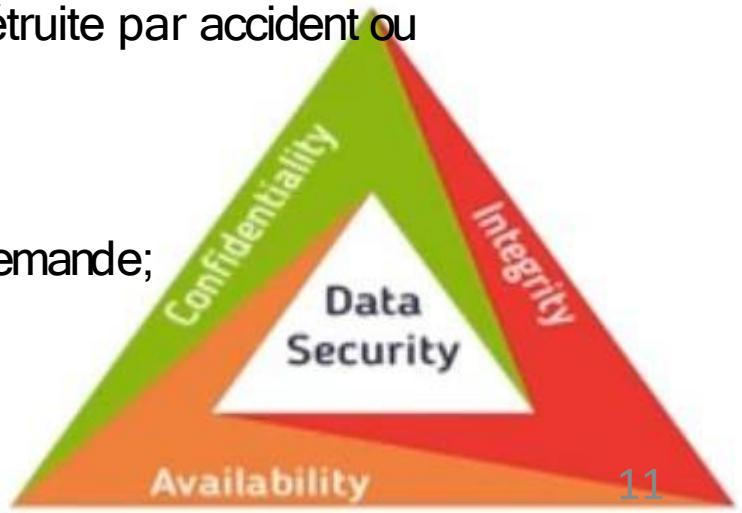
La sécurité IT est l'ensemble des moyens mis en œuvre pour **réduire la vulnérabilité** d'un système face aux **menaces** accidentelles ou intentionnelles.

Les critères fondamentaux de la sécurité de l'information

Les objectifs principaux de la sécurité:

Quelque soit la ressource présente dans un SI (matériel, information, logiciel, processus), on peut l'évaluer selon le plan de sécurité à travers 3 critères:

- **Confidentialité:** L'information ne peut être connue que par les personnes autorisées;
- **Intégrité:** L'information ne doit pas être altérée ou détruite par accident ou malveillance;
- **Disponibilité:** L'information doit être utilisable à la demande;



Triangle CIA de la sécurité SI

Les critères fondamentaux de la sécurité de l'information

Les objectifs principaux de la sécurité:

La confidentialité:

- Présente l'enjeu majeur de la sécurité, et l'objectif le plus étudié;
- La confidentialité est le maintien du secret des informations;
- Dans le cadre d'un système d'information, cela peut être vu comme une protection des données contre une divulgation non autorisée;
- Deux actions permettant d'assurer la confidentialité des données:
  - Limiter leur accès par un mécanisme de contrôle d'accès;
  - Transformer les données par des procédures de chiffrement.

« Seules les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être interdit »

Les critères fondamentaux de la sécurité de l'information

Les objectifs principaux de la sécurité:

L'intégrité:

- L'intégrité permet de certifier que les données, les traitements ou les services n'ont pas été modifiés, altérés ou détruits tant de façon intentionnelle qu'accidentelle.
- Se réfère à la confiance aux données et ressources (crédibilité);
- Ses mécanismes classés en deux catégories: prévention et détection;
- Mécanismes de prévention permettent d'empêcher la modification non autorisées;
- Mécanismes de détection permettent la détection des modifications engendrées accidentellement (erreur de transmission) ou intentionnellement (compromis de la sécurité).

« Les données doivent être celles que l'on s'attend à ce qu'elles soient, et ne doivent pas être altérées de façon fortuite ou volontaire »

Les critères fondamentaux de la sécurité de l'information

La disponibilité:

- Se réfère au principe qu'un utilisateur doit avoir le service demandé quand il a besoin immédiatement;
- Un système qui répond tardivement est un système indisponible;
- Une ressource doit être accessible au temps voulu;
- La disponibilité des services, systèmes et données est obtenue par un dimensionnement approprié;
- Un service doit être assuré avec le minimum d'interruptions possibles;
- Un système indisponible est beaucoup plus pire qu'un système inexistant.

« Le système doit fonctionner sans faille durant les plages d'utilisation prévues, garantir l'accès aux services et ressources installées avec le temps de réponse attendu »

Les critères fondamentaux de la sécurité de l'information

D'autres objectifs de la sécurité:

La sécurité de l'information repose sur la Confidentialité, la Disponibilité et l'intégrité, mais suis-je sur que la personne qui se connecte à l'application et celle qu'elle prétend?

- **Authenticité:** vérifier l'identité des personnes qui veulent manipuler l'information;
- **Non répudiation** : L'absence de possibilité de contestation d'une action une fois celle-ci est effectuée.

Les critères fondamentaux de la sécurité de l'information

La non-répudiation:

- La non répudiation, est le fait qu'une personne identifiée et authentifiée ne peut nier une action;
- C'est le fait qu'un utilisateur ne peut pas en aucun cas nier ce qu'il a fait;
- Ça revient à la confiance à la source de données et à la traçabilité des actions dans un système d'informations;

« Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur »

Les critères fondamentaux de la sécurité de l'information

L'authenticité (L'identification et l'authentification)

Q1: Qui êtes vous? L'identification

Q2: Êtes-vous réellement cette personne? Authentification

- L'identification de l'auteur d'un document peut être aisé par contre être en mesure d'assurer l'authenticité du document est chose plus délicate;
- Ces mesures doivent être mises en place afin d'assurer la confidentialité et l'intégrité des données d'une personne;
- L'identification peut être vu comme un simple login de connexion sur un système;
- L'authentification peut être un mot de passe connu seulement par l'utilisateur.

Critères de la sécurité de l'information: exercice

1. J'envoie ma déclaration de revenus, je déclare 3500 euros, le fisc reçoit 75000.

Critère non respecté:

2.Je transmets par internet mes données personnelles à une société de courtage en assurance, Afin qu'elle m'établisse un devis, le lendemain je reçois une dizaine de devis.

Critère non respecté:

3.Mon client m'a passé une commande sur internet et refuse de payer en prétextant qu'il ne m'a Jamais rien commandé.

Critère non respecté:0

4. Je reçois des photos par internet que je mets sur mon PC d'entreprise, 3h après les Serveurs de l'entreprise ne sont plus accessible.

Critère non respecté:

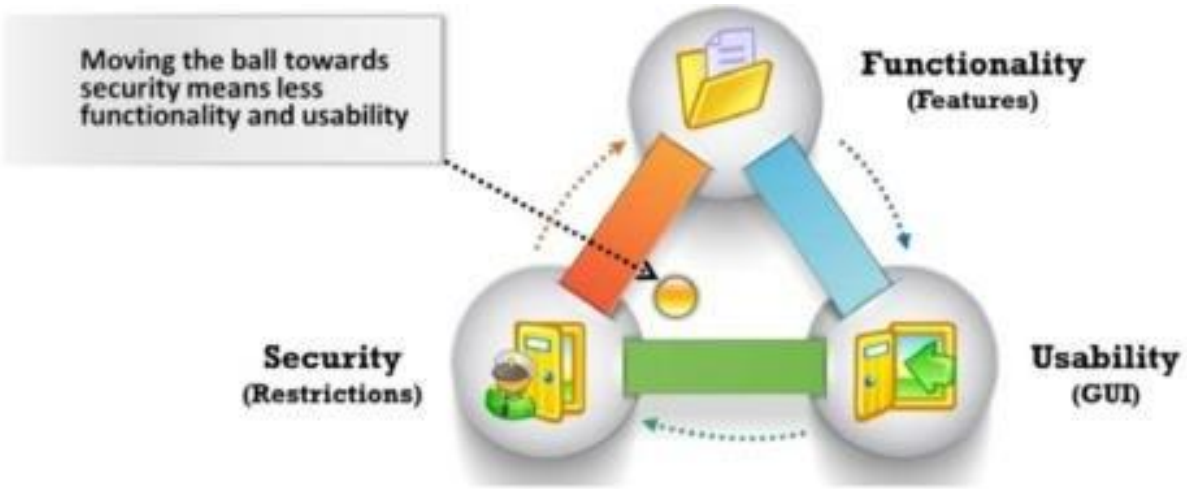
Niveau de sécurité

Triangle :Fonctionnalités, sécurité et accessibilité:

Fonctionnalités: L'ensemble des fonctionnalités fournies par le système.

Accessibilité (Facilité d'utilisation) : Les composants de l'interface utilisateur graphique utilisés pour concevoir le système en vue de sa facilité d'utilisation.

Sécurité : Restrictions imposées à l'accès aux composants du système.



Niveau de sécurité

Triangle :Fonctionnalités, sécurité et convivialité:

- l'augmentation ou la diminution de l'une des composantes affecte automatiquement les deux autres composants.
- Déplacer la balle vers l'un des trois composants signifie diminuer la l'intensité des deux autres composantes.
- Le diagramme représente la relation entre fonctionnalité, convivialité (facilité d'utilisation) et sécurité.
- Si la balle se déplace vers la sécurité, cela signifie qu'elle augmente sécurité et une diminution de la fonctionnalité et de l'utilisabilité.
- Si la balle se trouve au centre du triangle, alors les trois composantes sont équilibrées.
- Si la balle se dirige vers la facilité d'utilisation, cela signifie une augmentation de la facilité d'utilisation et la diminution des fonctionnalités ainsi que la sécurité.

Domaines de la sécurité

- Tous les domaines de l'informatique sont concernés par la sécurité d'un système d'information;
- En fonction de son domaine d'application, la sécurité informatique se décline en:
  1. Sécurité physique environnementale;
  2. Sécurité de l'exploitation;
  3. Sécurité logique;
  4. Sécurité applicative.

Domaines de la sécurité

1. Sécurité physique et environnementale:

Concerne la sécurité des aspects liés à l'environnement dans lequel les systèmes se trouvent et s'évoluent:

- **la protection de l'environnement (incendies, température, humidité,…)**
- **la protection des accès aux bâtiments,**
- **la redondance physique des composants (stockage, système, gérants),**
- **Plans de maintenances préventifs et correctifs.**

Pour assurer cette sécurité on fait recours aux normes :

- **ISO 27001: les exigences de la sécurité**
- **ISO 27002: les chapitres 9, 10 et 11 définissent les mesures à mettre en place.**
- **Mise en place d'un SMSI,**

Domaines de la sécurité

2. Sécurité de l'exploitation:

Se rapporte à tous ce qui touche au bon fonctionnement des systèmes, passant par:

la mise en œuvre **des outils** et **des procédures relatives aux méthodologies d'exploitation**, de **maintenance**, du **test**, de **diagnostic** et de **mise à jour**.

Pour assurer cette sécurité, nous devons penser à:

- **un plan de sauvegarde régulier et à jour;**
- **un inventaire géré et régulier ;**
- **une gestion du parc informatique, des configurations et des mises à jou**r.

Domaines de la sécurité

3. Sécurité logique :

Fait référence à la mise en place des mécanismes de sécurité par la voie logicielle, elle porte sur la mise en œuvre des systèmes de contrôle d'accès logique reposant sur les services **d'authentification, d'identification et d'autorisation**.

Elle se repose ainsi sur la mise en œuvre des dispositifs garantissant:

- **la confidentialité dont La cryptographie;**
- des **procédures d'authentification**;
- **des mesures antivirales et des sauvegardes** des informations stratégiques, critiques et sensibles.

Domaines de la sécurité

4. Sécurité applicative :

Faire un développement pertinent et l'intégrer harmonieusement dans les applications existantes.

Elle repose sur:

- Une méthodologie de développement,
- Audit du code (dépend du profil du programmeur);
- La robustesse des applications;
- Les tests.
- Les serveurs d'authentification et **SSO** (Single sign out): palier au problème de multiplication de mot de passe => contrôler tous les accès au SI en un point unique.

Taxonomies: Vulnérabilité, menace et risque

Vulnérabilité:

- C'est une faiblesse ou faille de sécurité au niveau du système informatique qui le rend sensible à une menace.
- Correspond à un ou plusieurs points faibles (défauts) dans le système (dans sa construction, configuration, ou conception:
- Au niveau du système d'exploitation, d'une application ou d'un protocole de communication;
- Une faille matérielle;
- Une faille humaine (comportement, manipulation).

- Exemple: Absence du contrôle d'accès, absence de traçabilité de l'information.

Taxonomies: Vulnérabilité, menace et risque

Vulnérabilité:

- **CVE** (Common Vulnerabilities and Exposures), désigne une liste publique de vulnérabilités de sécurité informatique.
- CVE est l'identifiant d'une faille de sécurité répertoriée dans cette liste.
- Les CVE aident les professionnels à coordonner leurs efforts visant à hiérarchiser et résoudre les vulnérabilités, et ainsi renforcer la sécurité des systèmes informatiques.
- Format de l'identifiant :
- **CVE-AAAA-NNNN** (AAAA est l'année de publication et NNNN un numéro d'identifiant unique).
  - Exemple: Wannacry : **CVE-2017-0144**
- **https://www.cvedetails.com/**
- **cve.mitre.org**

Vulnérabilité, menace et risque

Vulnérabilité:

Correspond à un ou plusieurs points faibles dans le système

- Absence du contrôle d'accès, absence de traçabilité de l'information.

Menace:

Une menace représente l'exploitation d'une vulnérabilité par une personne mal Intentionnée

- Vol d'information(menace associée à la vulnérabilité absence de contrôle d'accès)

Risque:

Est le résultat découlant d'une menace (est la probabilité qu'une menace particulière puisse Exploiter une vulnérabilité donnée du système.

- Plagiat industriel (risque associé à la menace vol d'information)

Vulnérabilité, menace et risque

Menace: Types

- **les menaces naturelles**: les inondations, incendie, ou une tempête…;
- **les menaces non intentionnelles**: un employé qui accède par erreur à une information erronée….;
- **les menaces intentionnelles**: logiciels espions, logiciels malveillants, des sociétés de logiciels publicitaires ou les actions d'un employé mécontent.

Vulnérabilité, menace et risque

Exercice: indiquez **pour chaque situation si c'est une vulnérabilité, menace ou risque ½)**

1. Utilisation frauduleuse d'une conversation
2. Intrusion volontaire sur un réseau WIFI;
3. Transport de la voix sur IP;
4. Se connecter en WIFI sur internet;
5. Ports ouverts sur un firewall;
6. Le protocole IP ne fait aucun contrôle d'intégrité;
7. Circulation de fausses informations.

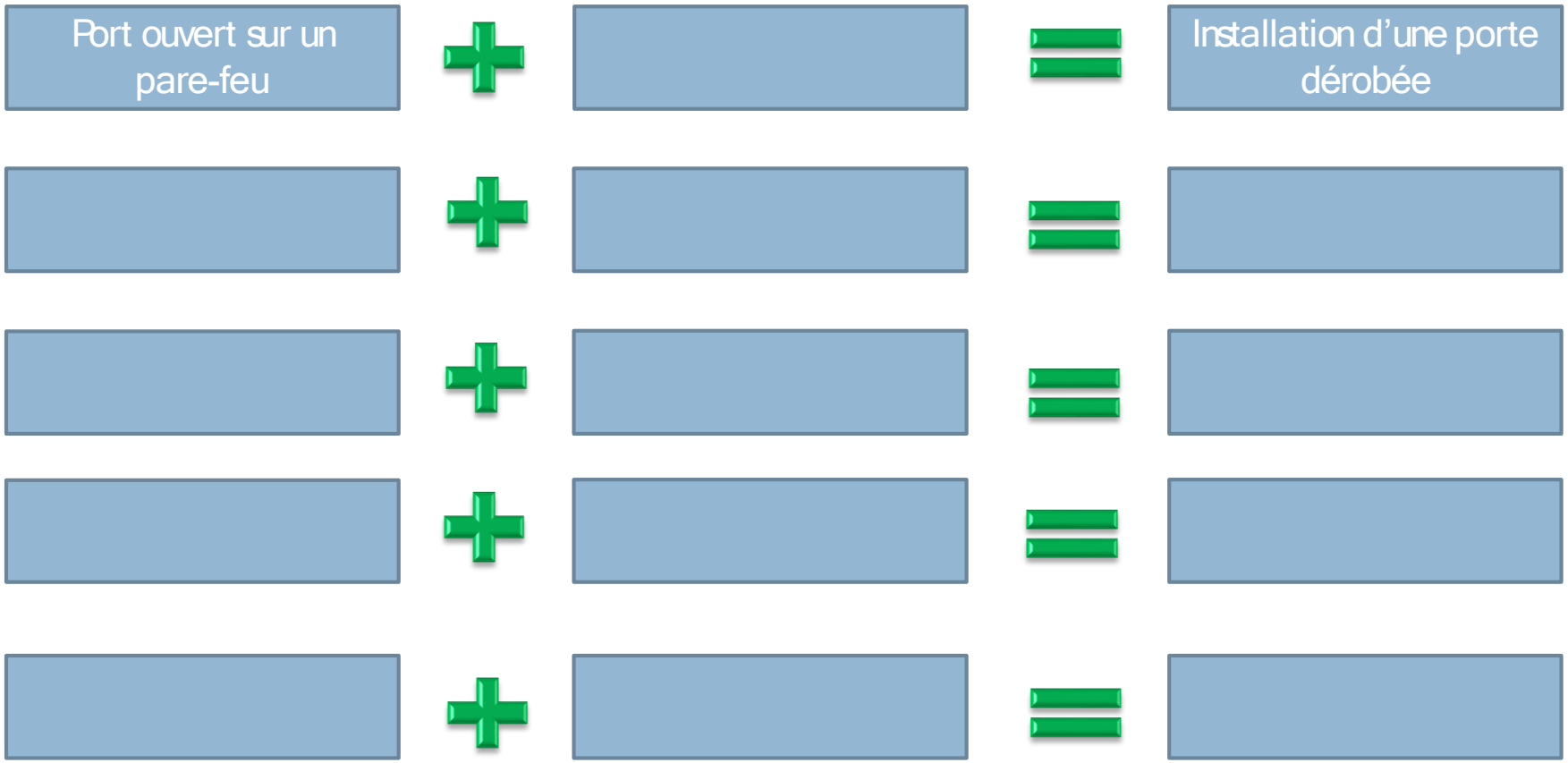
Vulnérabilité, menace et risque

Exercice: indiquez **pour chaque situation si c'est une vulnérabilité, menace ou risque 2/2)**

8. Espionnage du réseau
9. Intrusion volontaire dans le réseau
10. Installation d'une porte dérobée
11. Modification des messages échangés
12. Plainte juridique suite à une intrusion volontaire

Relations entre vulnérabilité, menace et risque

Exercice: reprendre les situations de l'exercice précèdent et faire correspondre une vulnérabilité à une menace, et une menace à un risque



Relation entre vulnérabilité, menace et risque

Exercice: Associer chacun des risques proposés à un ou plusieurs critères de sécurité(mettez une croix quand l'association est vraie)

Risque	Disponibilité	Intégrité	Non-répudiation	Confidentialité
Refus de service				
Circulation de fausses informations				
Utilisation frauduleuse d'une conversation				
Lancement de faux programmes (chevaux de Troie)				

Attaques, Mécanismes et Services

Attaque (intrusion):

Toute action qui compromet la sécurité des informations.

Exploit:

La procédure d'exploitation d'une vulnérabilité logicielle.

Mécanisme:

Est une méthode conçue pour **détecter**, **prévenir** et **lutter** contre une attaque de sécurité.

Service:

est un mécanisme qui augmente la sécurité des traitements et des échanges de données d'un système. Un service de sécurité utilise un ou plusieurs mécanismes de sécurité.

Acteurs de la sécurité

Intranet: employés de l'entreprise;

- Administrateur systèmes et réseaux;
- Responsable de sécurité;
- Direction générale.

Extranet: Partenaire, fournisseurs, autres site de l'entreprise.

Internet: Clients, prospects, utilisateurs itinérants.

Acteurs de la sécurité

- Une politique de sécurité s'appuie sur des acteurs;
- Les aspects humains représentent 80% des menaces dans la sécurité des Systèmes d'Information;
- Réduire le risque lié au facteur humain c'est :
  - ✓ **Employés**: respect de la charte informatique;
  - ✓ **Administrateur systèmes et réseaux**: Mise en place et suivi des parades contre les attaques;
  - ✓ **Responsable de sécurité (RSSI):** pilotage de la politique de sécurité;
  - ✓ **Direction générale**: sensibilisation des employés.

Politique de sécurité et critères

- Vouloir tout sécuriser est une **UTOPIE**!
- Vis-à-vis des critères de sécurité, selon leur activités, les entreprises n'ont pas les mêmes besoins.

Analysons les deux secteurs d'activités ci après:

Banque: ?

Opérateur téléphonique: ?

Politique de sécurité et critères

Banque: Confidentialité/intégrité/non répudiation/disponibilité

Avant tout garantir la confidentialité de leurs clients et l'intégrité des transactions.

La non répudiation permet de garantir le fait que le client a fait telle ou telle opération la disponibilité est moins sensible

Opérateur téléphonique: ? Disponibilité/l'intégrité/ non répudiation/ confidentialité

Avant tout le réseau opérateur doit être accessible et garantir que les informations transportées ne sont pas manipulable.

Il est très difficile pour un client de nier sa consommation car les systèmes de facturation mis en place sont très performants.

La confidentialité est presque déjà garantie par le fait que les points d'accès au réseau opérateur sont très surveillés.

Politique de sécurité et critères

- Vouloir tout sécuriser est une UTOPIE!
- Vis-à-vis des critères de sécurité, selon leur activités les entreprises n'ont pas les mêmes besoins.

Banque: Confidentialité/intégrité/non répudiation/disponibilité.
Opérateur téléphonique: Disponibilité/l'intégrité/ non répudiation/ confidentialité

Quel niveau de risque peut on prendre pour un actif vis-à-vis de tel ou tel critère?
Risk management !!

Politique de sécurité (1/3)

1. **Identifier ce qu'il faut protéger:**
    1. Les actifs;
    2. Classifications des documents informatiques et les postes;

2. **Analyser les risques :**
        3. Audit de survol;
        4. Scénarios d'intrusion;

3. **Pondérer les risques:**
    3. Risque = Impact*probabilité

Politique de sécurité (2/3)

4. **Evaluer les contraintes:**
    4. L'existent;
    5. Le budget;
    6. Le temps;
    7. L'humain.

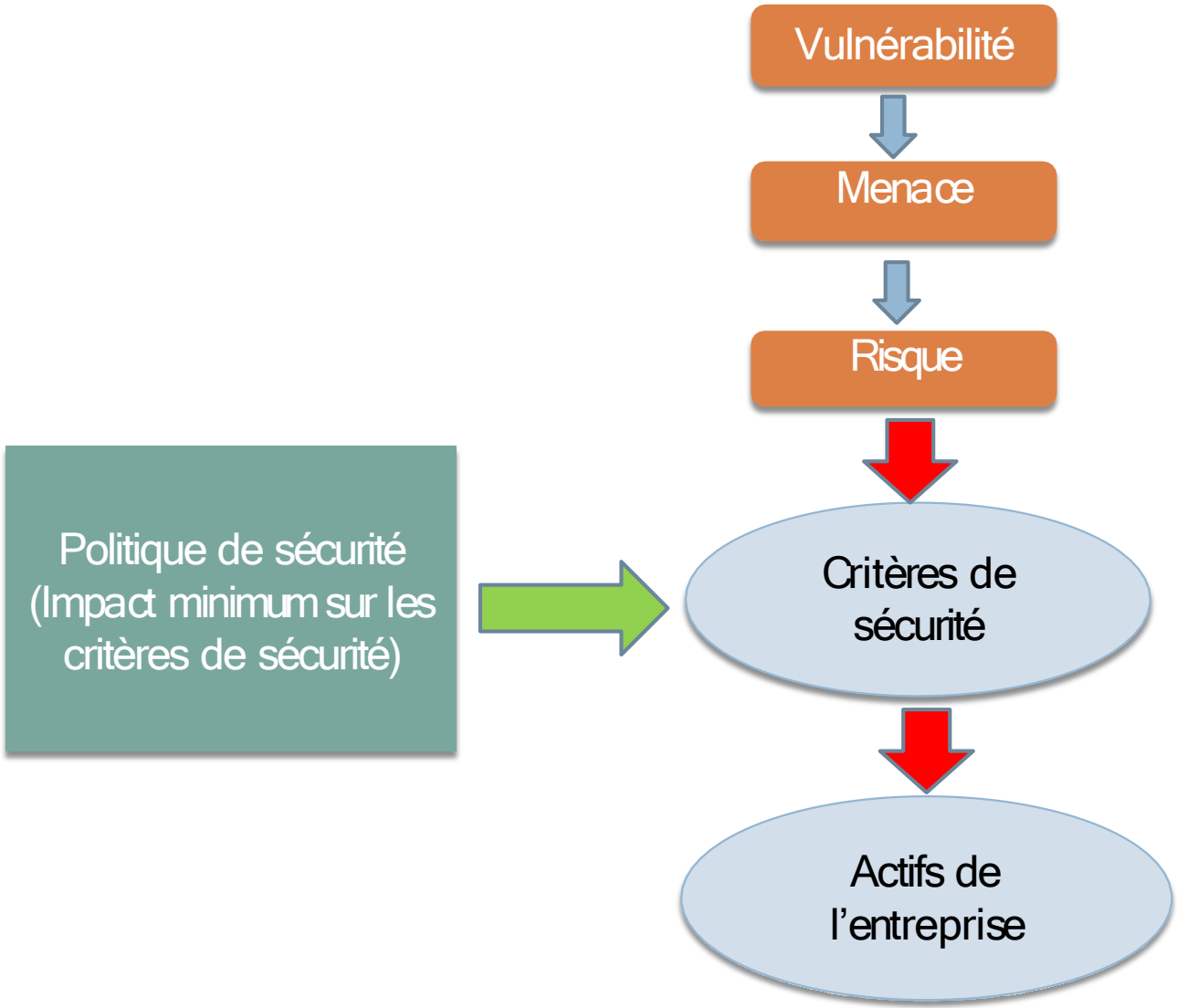
5. **Choisir les moyens:**
    5. Les moyens de sécurisation: techniques de crypto, sécurisation des serveurs, Authentification des applications et des users, pare feu, VPN, Les antiX..
    6. Les moyens de détections d'intrusion: IDS/IPS, Honeypot..
    7. Etablir la conduite à tenir en cas d'incident.

Politique de sécurité (3/3)

6. **Adopter la politique:**
    6. Désigner un responsable.
    7. Mettre en œuvre et Faire vivre la PSSI;
    8. Choisir une conduite d'incidents de sécurité;

7. **Tester:**
    8. Audit externe;
    9. Intrusion;
    10. Degré de résistance.

En définitif !!!



Pourquoi les systèmes sont-ils vulnérables ?

- La sécurité est cher et difficile: Les organisations n'ont pas de budget pour ça;
- La sécurité ne peut être sûr à 100%, elle est même souvent inefficace;
- La politique de sécurité est complexe et basée sur des jugements humains;
- Les organisations acceptent de courir le risque, la sécurité n'est pas une priorité;
- De nouvelles technologies (et donc vulnérabilités) émergent en permanence;
- Les systèmes de sécurité sont faits, gérés et configurés par des hommes.
- ...

Démystifier la sécurité IP: Synthèse

- Toutes les organisations utilisent le réseau IP aujourd'hui, **la mobilité** se généralise et rend incontournable l'interconnectivité via internet.

- Mais ils s'exposent ainsi à des **vulnérabilités** et des **menaces** qui sont autant de risques pouvant compromettre les critères de sécurité (CDI).

- La DG, les acteurs de la sécurité, les employés doivent tous contribuer à minimiser les risques en mettant en œuvre **une politique globale de sécurité**, afin de protéger efficacement **le patrimoine informationnel** de l'entreprise et de lui permettre de **continuer ses activités**.

Synthèse

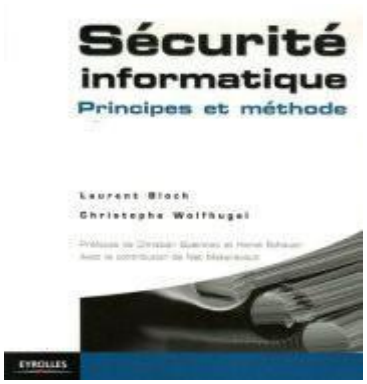
- Aucune sécurité n'est parfaite;
- Des outils sont nécessaires, mais le travail quotidien est indispensable;
- La sécurité n'apporte qu'un gain indirect. Par conséquent, il n'est pas facile de convaincre les décideurs de l'entreprise;
- **Le seul système informatique qui est vraiment sûr est un système éteint et débranché, enfermé dans un blockhaus sous terre, entouré par des gaz mortels et des gardiens hautement payés et armés.**

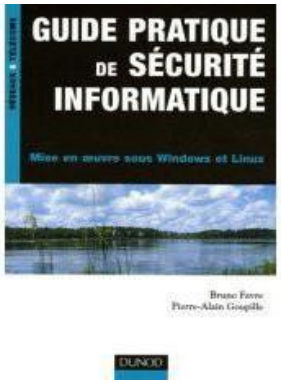
A méditer

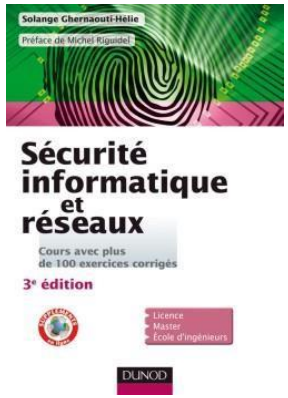
« Ce ne sont pas les murs qui protègent la citadelle, mais l'esprit de ses habitants »

Thudycite

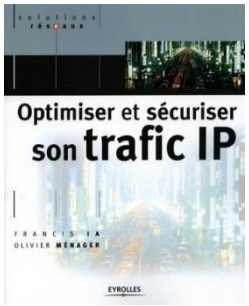
Références

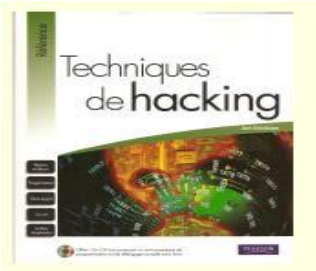

Sécurité
informatique
Principes et méthode
Laurent Bloch
Christophe Wolfhugel
EYROLLES


GUIDE PRATIQUE
DE SÉCURITÉ
INFORMATIQUE
Mise en œuvre sous Windows et Linux
Bruno Favre
Pierre-Alain Goupille
DUNOD


Solange Ghernaouti-Hélie
Préface de Michel Riguidel
Sécurité
informatique
et
réseaux
Cours avec plus
de 100 exercices corrigés
3e édition
Licence
Master
École d'ingénieurs
DUNOD


Tout sur la
Sécurité
informatique
2e édition
DUNOD


Optimiser et sécuriser
son trafic IP
FRANCIS LA
OLIVIER MÉNAGER
EYROLLES


Techniques
de hacking