LSI3 – Sécurité informatique

Chapitre 1
Introduction à la sécurité informatique

École Nationale Supérieure Polytechnique
Serge Mani
serge.mani@polytechnique.cm

1

1

2

2

Sommaire

- Définitions et objectifs
- Principes fondamentaux
- Risque
- Méthodologie
- Notion de risque
- Acteurs et intervenants
- Stratégie et politique de sécurité
- Cadre légal et déontologique
- Standards applicables
- Organismes

3

3

Définitions et objectifs

- Sécurité informatique
  - Sécurité des systèmes d'information et des réseaux
  - **Techniques**, **méthodes** et **outils** de protection des systèmes, de l'information et des services contre les menaces accidentelles et délibérées.
  - Exemples d'**apport de la sécurité informatique** :
    - Éviter l'utilisation d'un serveur de production pour servir de serveur de fichiers sur Internet
    - Éviter la divulgation des informations financières confidentielles
    - Éviter une interruption de service causée par un désastre/sinistre
    - Éviter la modification non autorisée d'une entrée dans une base de données
    - Éviter une destruction accidentelle de fichiers

4

4

Définitions et objectifs

- Sécurité informatique
  - Objectifs principaux :
    - Assurer la **Confidentialité**
    - Assurer l'**Intégrité**
    - Assurer la **Disponibilité**
  - Principe de CIA
    - **C**onfidentiality, **I**ntegrity, **A**vailability

5

5

Définitions et objectifs

- Confidentialité de l'information
  - L'information n'est accessible qu'à ceux qui en ont le droit

  - Peut changer avec le temps
  - Jeu des intérêts : publics et privés, vie privée

6

6

Définitions et objectifs

- Intégrité des services et de l'information
  - Les services et l'information ne peuvent être modifiés que par les individus autorisés (administrateurs, propriétaires, etc.).

  - Objectifs : exactitude, précision, autorisation de modification, cohérence

7

7

Définitions et objectifs

- Disponibilité des services et de l'information
  - Les services et l'information ne sont accessibles qu'aux personnes autorisées **et** quand elles en ont besoin.

  - Doit tenir compte
    - des besoins et spécifications
    - des contraintes (temps, qualité, performance)

8

8

Définitions et objectifs

- Sécurité informatique
  - Autres objectifs :
    - L'**authentification** : entité, l'origine de l'information, opération sur l'information
    - L'**autorisation** : à faire quoi, à accéder à quoi…
    - La **non-répudiation** : ne pas être en mesure de nier ses actes
    - La **journalisation** : répertorier tout accès, toute modification, etc.

9

9

Définitions et objectifs

- Sécurité informatique
  - Du concret dans une organisation
    - Protéger sa réputation
    - Assurer la continuité de ses activités
    - Protéger ses données stratégiques et ses propriétés intellectuelles
    - Protéger les données privées de ses employés et de sa clientèle
    - Se prémunir de la fraude
    - Satisfaire aux exigences légales
    - Éviter des pertes financières

10

10

Principes fondamentaux

- Principe du point le plus faible
  - Une personne qui cherche à pénétrer un système utilisera tous les moyens possibles pour le faire, mais pas nécessairement le moyen le plus évident ou celui bénéficiant de la défense la plus solide

11

11

Principes fondamentaux

- Principe de la protection adéquate (gestion du risque)
  - Le niveau et le coût de la protection doivent correspondre à l'importance et à la valeur de ce qu'on veut protéger
  - La durée de la protection doit correspondre à la période pendant laquelle l'importance et la valeur sont présentes, et pas plus

12

12

Risque

- Définition
  - C'est la prise en compte de l'exposition à un danger, un préjudice ou tout autre évènement dommageable.
  - Le risque est inhérent à une situation ou à une activité : il est donc impossible de l'éliminer
  - Traitement du risque :
    - Réduction
    - Transfert
    - Acceptation
    - Arrêt de l'activité

13

13

Risque

- Terminologie autour du risque (1/2)
  - **Actif** : Objet ayant de la valeur (y compris, l'humain)
    - Serveur de production
  - **Menace** : Entité physique ou morale qui met un actif à risque
    - Virus
  - **Vulnérabilité** : Faille qui donne l'opportunité de porter atteinte à un actif et donc de concrétiser une menace
    - Absence d'antivirus sur le serveur

14

14

Risque

- Terminologie autour du risque (2/2)
  - **Impact :** Perte ou dommage causé à un actif
    - Perte de la base de données
  - **Scénario (de risque)** : Exploitation d'une vulnérabilité par une menace pour causer un impact.
    - Le virus est introduit dans le serveur pour détruire le contenu de la base de données.
  - **Contre-mesure** : Protection d'un actif contre une menace
    - Antivirus

15

15

Risque

- Quand y'a-t-il risque ?
  - Si un scénario a la chance de réaliser
  - Il faut que les **deux conditions** suivantes soient toutes les deux réunies :
    - Présence d'une vulnérabilité
    - Présence d'une menace

16

16

Risque

- Menaces (1/2)
  - Actes accidentels
    - Internes ou externes
    - Exemples :
      - Évènements hors contrôle : incendies, coupures de courant, inondation, etc.
      - Actes humains involontaires : divulgations accidentelles, mauvaise saisie de données, erreur de frappe, difficultés techniques
      - Performance imprévue du système : erreur de conception dans les logiciels ou matériels, erreur de fonctionnement du matériel

17

17

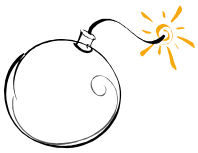
Risque

- Menaces (2/2)
  - Actes malicieux ou délibérés
    - Internes ou externes
    - Exemples :
      - Vols de systèmes, intrusions, utilisation de codes cachés, déni de services, ingénierie sociale, espionnage, bombardements électroniques, sabotage, piratage, détournements de courriels, répudiation, obtention de données, modification non autorisée de données, contrefaçon, usurpation et vol d'identité, habillage de sites Web, etc.

18

18

Risque



- Origine de la menace
  - Catastrophes naturelles
  - Compagnie de marketing
  - Hackers
  - Compétiteurs
  - États étrangers
  - Crime organisé
  - Terrorisme
  - Ceux à qui on fait confiance…

19

19

Risque

- Formulation du risque
  - Le risque est similaire à un jeu de loterie dans lequel vous partez perdant !
  - Le calcul s'apparente donc à celui de l'espérance de perte :
    - P : Probabilité de survenue d'un incident
    - I : Impact de l'incident sur l'actif
    - R : Risque

$$R = P \times I$$

20

20

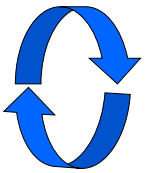
Risque

- Évaluation du risque
  - L'impact est plus ou moins facile à évaluer car il est sous notre contrôle
  - Risques liés aux actes accidentels
    - Valeurs connues pour le calcul de la Probabilité : statistiques, actuariat, historique de catastrophes, etc.
  - Risques liés aux actés malicieux ou délibérés
    - Difficile d'évaluer le Risque (la Probabilité) car il ne s'agit pas d'évènements aléatoires.
    - Solution : **Analyse des risques**

21

21

Méthodologie



- Sécurité informatique en somme
  1. **Identifier la menace**
     - Recensement des actifs (informationnels)
     - Qui, quoi, comment (vulnérabilités) ?
  2. **Évaluer les risques**
     - Probabilité, impact
  3. Considérer les mesures de protection par rapport au risque
     - Efficacité (risque résiduel), coût, difficulté d'utilisation
  4. Mettre en place et opérer les mesures de protection
     - Modification et/ou installation, changement des politiques, éducation des utilisateurs, etc.
  5. Retourner à l'étape 1 !

22

22

Analyse de risque

- Évaluation de l'impact
  - Faire le recensement et la classification des actifs informationnels
    - S'appuyer sur les propriétaires des actifs
    - Exemples :
      - Le directeur informatique est le propriétaire du système VPN, des composantes Firewall
      - Le directeur de la paie est le propriétaire du système (informatique) qui gère la paie

23

23

Analyse de risque

- Évaluation de l'impact
  - Définir une échelle d'appréciation de l'impact
    - Exemple : Échelle « semi-objective »

Cote	Impact
1	**Faible:** perte d'argent ou de données négligeable, courte indisponibilité, effet minime sur la réputation, etc.
2	**Moyen :** perte d'argent significative, perte de données peu dommageable, indisponibilité de plusieurs heures, etc.
3	**Élevé :** Importante perte d'argent, perte d'un grand volume de données, indisponibilité de plusieurs jours, etc.
4	**Très élevé :** perte de plusieurs centaines de milliers (millions) de dollars, divulgation de secrets d'affaires, indisponibilité indéfinie, etc.

24

24

Analyse de risque

- Évaluation de l'impact
  - Chiffrer des impacts en fonction
    - de la classification des impacts
    - de l'échelle choisie
    - des processus et objectifs d'affaires
    - Exemples :
      - Le vol d'une base de données de clients pourrait coûter la réputation à la compagnie
      - L'incendie d'une salle de serveurs de petite taille (un dizaine de serveurs) pourrait coûter plus de 100k$ à la compagnie

25

25

Analyse de risque

- Évaluation de la probabilité
  - Il est question de déterminer une valeur de la probabilité d'observer un impact dans un scénario de risque donné
    - Pour les risques accidentels
      - Utilisation d'une échelle « exacte » : données actuarielles
    - Pour les risques délibérés
      - Utilisation d'une échelle semi-objective

Cote	Probabilité
1	**Faible :** Probabilité presque nulle
2	**Moyen :** Peu probable
3	**Élevé :** Probable
4	**Très élevé :** Très probable

26

26

Analyse de risque

- Évaluation de la probabilité
  - Dépend de l'intervenant
    - Experts en sécurité, experts en systèmes, propriétaires de systèmes, etc.
  - Trois grandes composantes pour la probabilité
    - Capacité
      - Savoir et connaissances
      - Outils et argent
      - Accès au savoir et ressources humaines
    - Opportunité
      - Espace : avoir un accès physique
      - Connectivité : existence d'un lien physique et logique
      - Temps : être « là » au bon moment

27

27

Analyse de risque

- Évaluation de la probabilité
  - Motivation
    - Qui : à qui profite le crime ?
    - Quoi : que va gagner le malfaiteur ?
    - Combien : combien va gagner le malfaiteur ?
  - Combinaison des trois composantes
    - Produit des trois ?
    - Médiane des trois ?
    - Min ou Max des trois ?
    - Moyenne des trois ?

28

28

Analyse de risque

- Tableau d'analyse de risque

Scénario	C	O	M	P	I	R
Scénario 1	1	4	3	4	3	12
Scénario 2	3	2	1	3	2	6
Scénario 3	2	2	3	3	4	12
…						
Scénario *n*	3	1	4	4	2	8

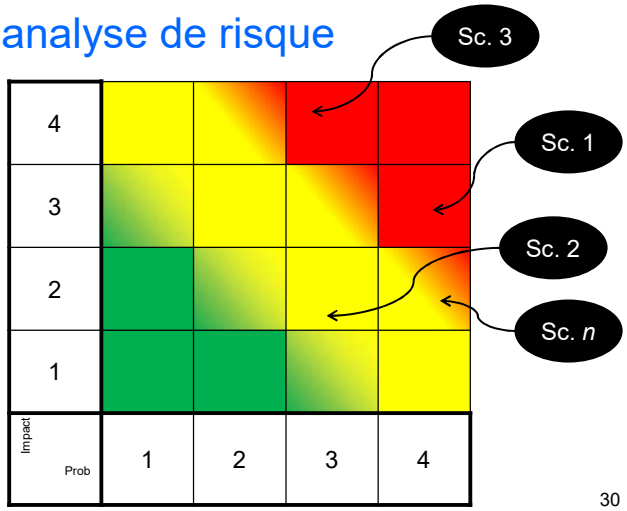
  - Considérations dans cet exemple :
    - Probabilité : maximum des trois composantes
    - Attention à la consistance !
    - Rappel : Calcul du risque : **R = P x I**

29

29

Analyse de risque

- Tableau d'analyse de risque
  - Échelle LOG



30

30

Analyse de risque

- Tableau d'analyse de risque
  - Interprétation de l'échelle LOG
    - Prioritairement, on doit s'occuper de la zone rouge
      - Scénarios 1 et 3
    - Selon le niveau de tolérance au risque, on peut aussi s'occuper de la zone jaune
      - Scénarios *n* et 2
      - Si on est très tolérant, on accepte tout ce qui se trouve dans la zone jaune
      - Si peu tolérant, on **contrôle** même ce qui se trouve dans la zone jaune
    - Le contrôle se fait à travers la mise en place de **contre-mesures**

31

31

Analyse de risque

- Évaluation de la probabilité
  - Exercice
    - La compagnie ABC dispose d'un serveur Web à travers lequel des revendeurs se connectent, à partir de leurs propres serveurs, pour vendre des produits aux clients. Les profits sont distribués au prorata des ventes faites pendant une période de temps. ABC est préoccupée par l'intégrité de ses résultats
      - Quels sont les agents de menace ?
      - Définir quelques scénarios de risques
      - Dresser un tableau d'analyse de risques

32

32

Analyse de risque

- Évaluation de la probabilité
  - Solution
    - Agents de menace
      - Pirates informatiques
      - Revendeur malicieux
    - Scénarios de risques
      - Le pirate exploite une vulnérabilité du serveur Web
      - Le pirate exploite une vulnérabilité chez le revendeur
      - Le revendeur exploite une vulnérabilité du serveur Web
    - Tableau d'analyse de risque
      - *Cette partie du cours est faite au tableau*

33

33

Acteurs et intervenants

- Haute direction
  - VP
  - Responsable de la sécurité informatique
- CISO (*Chief Information System Officer*) ou ISO
  - Information Security Officer
  - Moitié/moitié ou plutôt technique
  - Responsable de la sécurité informatique
- Équipe de sécurité informatique
  - Externe ou interne
  - Responsable technique

34

34

Acteurs et intervenants

- Responsable de la sécurité physique
  - Aspects non-techniques de la sécurité des SI
    - Personnel : mesures physiques, etc.
  - Fonction d'investigation
- Administrateur de systèmes
  - Admin BD, Développeur d'applications, Admin réseau/LAN
  - ISP et autres fournisseurs
- Utilisateurs
  - Éducation
  - Déterrent : Poursuite criminelle; Poursuite civile ;Terminaison d'emploi

35

35

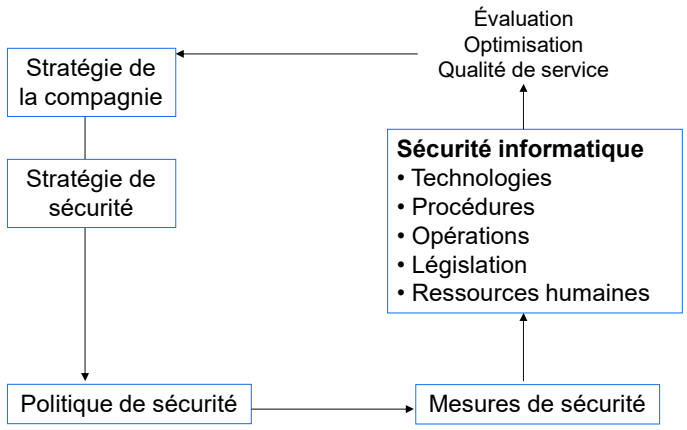
Stratégie de sécurité

- Définition et objectifs
  - Conception d'une conduite générale de protection, d'organisation de la défense (mesures proactives) et d'élaboration des plans de réaction (mesures réactives)
  - Avoir une vision stratégique de la sécurité
    - Définir clairement les objectifs de sécurité
  - Implantation de la culture de la sécurité informatique au sein de l'organisation pour garantir sa pérennité
  - La stratégie de sécurité est fonction d'une analyse préalable des risques

36

36

Stratégie de sécurité



37

37

Stratégie de sécurité

- Éléments d'une stratégie (Questions)
  - Quelles sont les actifs de la compagnie ?
  - Quel est leur niveau de sensibilité et de criticité ?
  - De qui, de quoi doit-on se protéger ?
  - Quels sont les risques réellement encourus ?
  - Ces risques sont-ils supportables ?
  - Quel est le niveau actuel de sécurité ?
  - Quel est niveau de sécurité que l'on désire atteindre ?
  - Comment passer du niveau actuel au niveau désiré ?
  - Quelles sont les contraintes effectives ?
  - Quels sont les moyens disponibles ?

38

38

Politique de sécurité

- Élaborer par : CISO, équipe de sécurité
- Promulguer sous l'autorité du CISO et de la Haute direction
- Signature de contrat…
- Éléments
  - Analyse de risque
  - Responsabilités de chacun des intervenants
  - Utilisateurs
    - Politique d'utilisation : Contrat entre utilisateurs et organisme, Règles d'utilisation, Consignes techniques
  - Équipe de sécurité et administrateurs de système
    - Modes d'interventions en sécurité
    - Règles d'opérations des systèmes

39

39

Politique de sécurité

- Éléments de politiques de sécurité
  - **Introduction**
    - Engagement de la Direction Générale
    - Revue et évaluation de la politique de sécurité
  - **Organisation de la sécurité**
    - Attribution des rôles et responsabilités
    - Autorisation pour l'ajout de systèmes/outils informatiques
    - Conseils d'un spécialiste/expert en sécurité de l'information
    - Revue indépendante de la sécurité de l'information
    - Accès par des tiers et sous-traitants

40

40

Politique de sécurité

- Éléments de politiques de sécurité
  - **Classification des actifs informationnels**
    - Recensement des actifs informationnels
    - Responsabilités des détenteurs des actifs informationnels
  - **Sécurité liée aux ressources humaines**
    - Respect de la sécurité informatique
    - Formation et sensibilisation

41

41

Politique de sécurité

- Éléments de politiques de sécurité
  - **Sécurité physique et environnementale**
    - Périmètre de sécurité physique
    - Règles dans le périmètre de sécurité
    - Sécurité électrique des équipements
    - Maintenance du matériel
    - Sécurité des équipements hors des locaux
    - Mise au rebut et réutilisation des équipements
    - Sécurité des supports d'information

42

42

Politique de sécurité

- Éléments de politiques de sécurité
  - **Sécurité opérationnelle**
    - Documentation des procédures
    - Séparation des environnements de développement et de production
    - Gestion de ressources informationnelles par des tiers
    - Protection contre les logiciels malveillants
    - Copie de sécurité des données
    - Sécurité des médias pendant les transports
    - Site Web et Courriel

43

43

Politique de sécurité

- Éléments de politiques de sécurité
  - **Contrôle d'accès**
    - Politique de contrôle d'accès
    - Gestion des droits d'accès
    - Gestion des mots de passe
    - Gestion des clés de chiffrement/déchiffrement
    - Utilisation de réseaux externes
    - Connexion de l'extérieur
    - Segmentation des réseaux
    - Procédure de connexion

44

44

Politique de sécurité

- Éléments de politiques de sécurité
  - **Protection des données électroniques**
    - Chiffrement
    - Signature électronique
  - **Gestion des incidents de sécurité**
    - Réponse aux incidents de sécurité
    - Plan de continuité des activités

45

45

Politique de sécurité

- Éléments de politiques de sécurité
  - **Conformité**
    - Législation applicable
    - Propriété intellectuelle
    - Protection des données opérationnelles
    - Protection de la vie privée
  - **Annexes**
    - Lettre d'engagement : respect de la sécurité pour les employés de la Compagnie X
    - Lettre d'engagement : respect de la sécurité pour les tiers et sous traitants de la Compagnie X

46

46

Stratégie vs. Politique

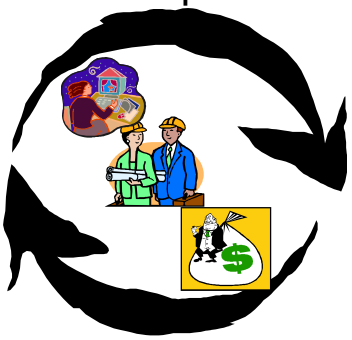
- Stratégie
  - équivalente à la **Constitution** dans un pays
- Politique
  - équivalente à la **Loi** dans un pays

47

47

Méthodologie de la sécurité informatique

1. Identifier la menace
   - Recensement des actifs
   - Qui ou quoi ?
   - Comment (vulnérabilités) ?
2. Évaluer les risques
   - Probabilité
   - Impact
3. Considérer les mesures de protection par rapport au risque
   - Efficacité (risque résiduel)
   - Coût
   - Difficulté d'utilisation
4. Mettre en place et opérer les mesures protections
   - Modification et/ou installation
   - Changer les politiques
   - Éduquer les utilisateurs
5. Retourner à 1…



48

48

Cadre légal et déontologique

- Protection de la vie privée
  - Renseignements désignés
  - Commissariat à la protection de la vie privée au Canada (privcomm.gc.ca)
    - Agence qui relève directement du Parlement et du Sénat
    - Cadre légal
      - Loi sur la Protection des renseignements personnels (1980)
      - Loi sur la Protection des renseignements personnels et les documents électroniques (2000)
- Protection des renseignements classifiés
  - Loi des secrets officiels
  - Politique de sécurité du Gouvernement du Canada

49

49

Cadre légal et déontologique

- Protection des droits des actionnaires
  - Loi Sarbanes/Oxley (US)
    - politique stricte de contrôles internes destinée à encadrer la publication des comptes annuels.
  - Auditeurs financiers externes
- Répartition et gestion du risque
  - Compagnie d'assurances
- Protection du consommateur et du public
  - Médical : Health Insurance Portability and Accountability Act (HIPAA)

50

50

Standards applicables

- Gestion de la sécurité
  - ISO/IEC
    - 27002 : Information technology - Code of practice for information security management (www.iso.org, pour la modique somme de 179$ US)
    - 27001 : Standard to manage information security
    - 27005 : Standard on systematically identifying, assessing, evaluating and treating information security risks
  - HIPAA (US)
    - Health Insurance Portability and Accountability Act
    - Standard de sécurité pour tous les systèmes traitant des informations médicales
    - Date limite d'application : avril 2004
    - Le prix à payer pour une violation du règlement va de 100$ d'amende à 25 000$ + 10 ans de prison

51

51

Organismes

- ISC2
  - www.isc2.org
  - La doyenne de ces organisations plus ancienne
  - Maintenant accrédité ISO/ANSI (standard des accréditations)
  - Certifications SSCP (Systems Security Certified Practitioner) et CISSP (Certified Information Systems Security Professional)
- SANS Institute
  - www.sans.org
  - Nature essentiellement technique
  - Offre formation par cours intensifs
  - Programme de certifications GIAC (très technique et spécialisé)
  - Organisme privé (à but lucratif…)
  - Opère de façon "volontaire" le Internet Storm Center (isc.sans.org)

52

52

Organismes

- ISACA - Information Systems Audit Control Association (www.isaca.org)
  - Certifications
    - CISA (Certified Information Systems Auditor)
    - CISM (Certified Information Systems Security Manager)
    - CGEIT (Certified in the Governance of Enterprise IT)
    - CDPSE (Certified Data Privacy Solutions Engineer
- CIS - Center for Internet Security (www.cisecurity.org)
  - Organisme sans but lucratif pour aider les organisations à réduire le risques d'affaires résultant de l'insuffisance des contrôles techniques de sécurité.
  - Normes consensuelles :
    - Meilleures pratiques pour les configurations de sécurité
    - Métriques pour mesurer l'état de sécurité de l'information
    - Décisions rationnelles au sujet des investissements en sécurité

53

53