Introduction à la sécurité et à la gestion des risques

Yves LALOUM
Conseil Audit de Systèmes d 'information CISA
ylaloum@advisehr.com
Professeur Associé au Conservatoire National des Arts et Métiers - Paris

1.Objectifs du cours

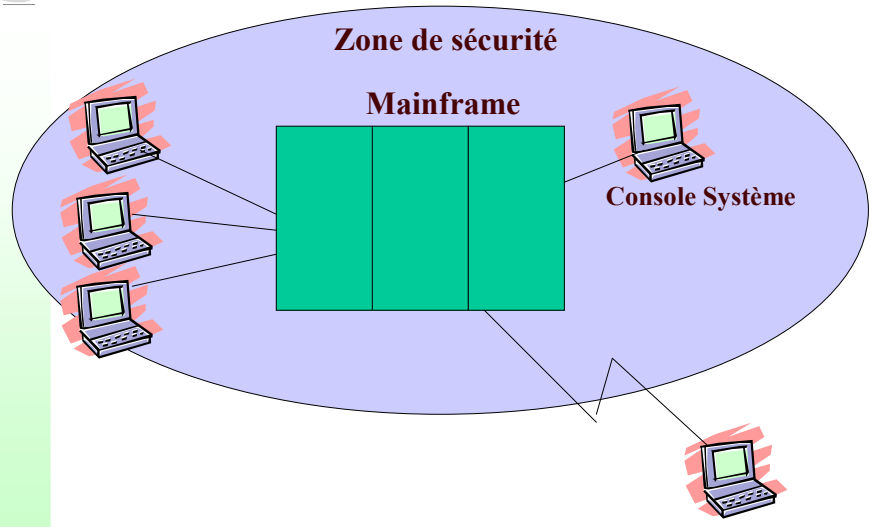
- Appréhender la sécurité informatique dans toutes ses dimensions :
  - Organisationnelle
  - Economique
  - Réglementaire
  - Technique et opérationnelle

2. Le terrain

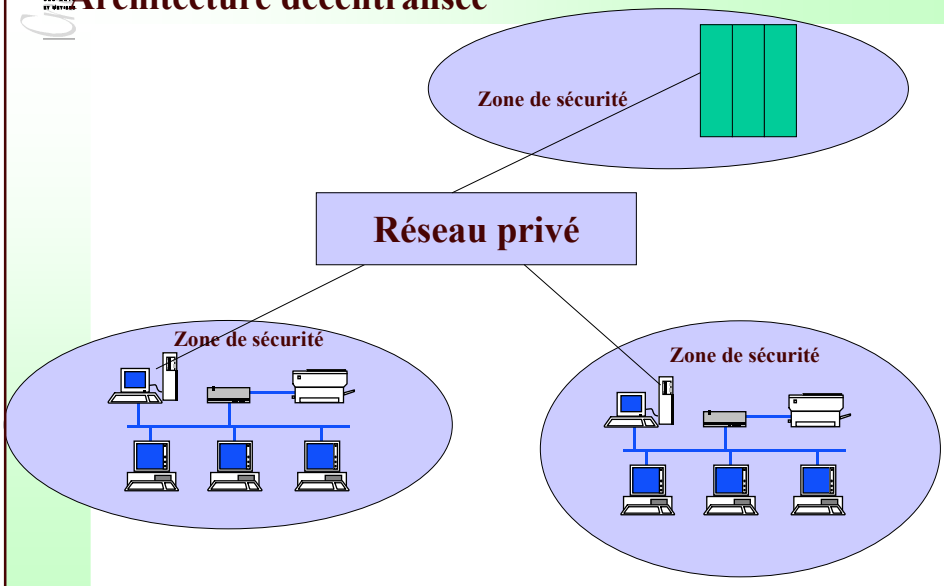
- L'évolution des systèmes d'information dans les 40 dernières années a entraîné :
  - Une décentralisation de l'infrastructure
  - Une décentralisation des ressources
  - Une décentralisation des applications
  - Une diversification et une augmentation des utilisateurs
  - Une complexité et une ouverture accrue des systèmes . On est passé des systèmes propriétaires aux systèmes ouverts
  - Hétérogénéité et interactivité des éléments constitutifs des SI

- Face à cette évolution les menaces se sont diversifiées :
  - Agression physique (effraction, destruction...)
  - Malveillance
  - Espionnage économique
  - Manque de maîtrise de la complexité des systèmes entraînant des dysfonctionnements
  - Perte de confidentialité
  - Mise à profit de l'ouverture des systèmes pour nuire
  - Perte d'intégrité des données
  - Détournement de fond

- Architecture Centralisée

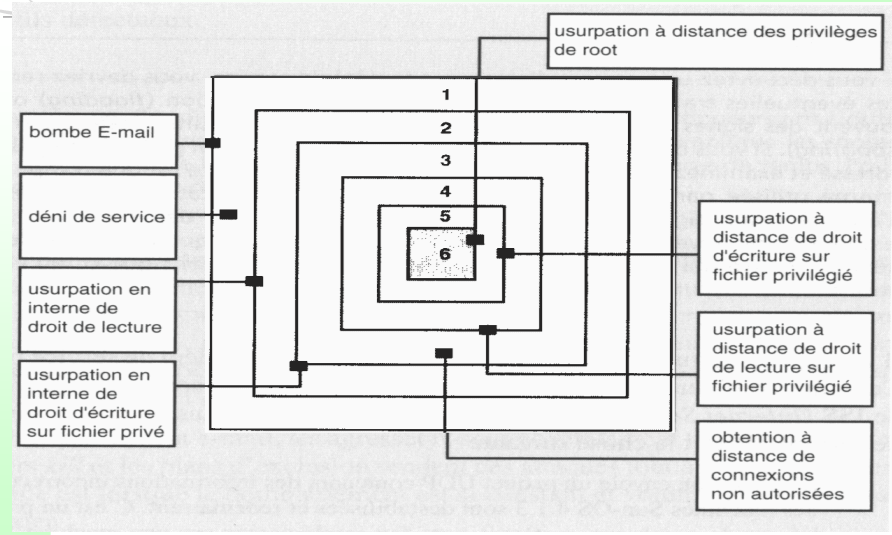


Architecture décentralisée



- Internet bouleverse le problème de la sécurité :
  - Interaction de différents acteurs
  - Ouverture sur l'extérieur
  - Réseau public et partagé à faible contrôle
  - Banalisation des accès (utilisation du réseau téléphonique)
  - Nécessité d'authentification et de reconnaissance
  - Augmentation de la menace externe et anonyme
  - La sécurité ne peut être assurée à tous les nœuds du réseau

Niveaux d'attaques



3. Classification et Gestion des Risques

- Les risques doivent être appréhendés dans le cadre global de l 'entreprise et de son modèle économique :
- Les risques peuvent être classés selon des critères d ' importance en fonction des conséquences pour l'entreprise :
  - Vital : La nature du risque peut mettre en cause la survie de l'entreprise
  - Critique : La nature du risque peut affecter durablement les performances économiques de l'entreprise
  - Sensible : La nature du risque peut affecter l'entreprise de manière non négligeable même si limitée dans le temps.
  - Non critique : coût lié au risque existant mais limité

- Nature des risques à prendre en compte :
  - Risques d ’environnement (exposition aux catastrophes naturelles)
  - Risques dus aux erreurs humaines : erreurs de manipulation, négligence
  - Risques dus à la qualité des sources d ’énergie (surtension)
  - Risques d ’incendie, d’inondation, de pollution
  - Malveillance interne (sabotage, abus de droit)
  - Malveillance externe (attaques logiques, vols, attentats)

Evolution des risques

- Le processus d ’évaluation des risques doit être un processus continu car :
  - La technologie évolue
  - La stratégie et le périmètre d ’activité de l’entreprise évolue
  - L’environnement évolue
  - Le système d ’information évolue

4. Périmètre de la sécurité

- Evolution des risques
  - Extension du commerce électronique
    - B2B
    - B2C
  - Le SI de l'entreprise n'a plus de frontière précise
    - Nomadisme
    - Interconnexions
  - Mondialisation des échanges
- Evolution des législations
  - Copyright
  - Contre le piratage
  - Sur la protection intellectuelle
  - Sur les données personnelles nominatives

- Dépendance des organisations vis-à-vis des SI
  - Problèmes de sécurité sont dommageables au business
    - Coût direct : perte matérielle, reconstruction
    - Coût indirect : perte d'exploitation, perte d'image de marque
  - Nouvelle organisation du travail liée aux nouvelles technologies de l 'information

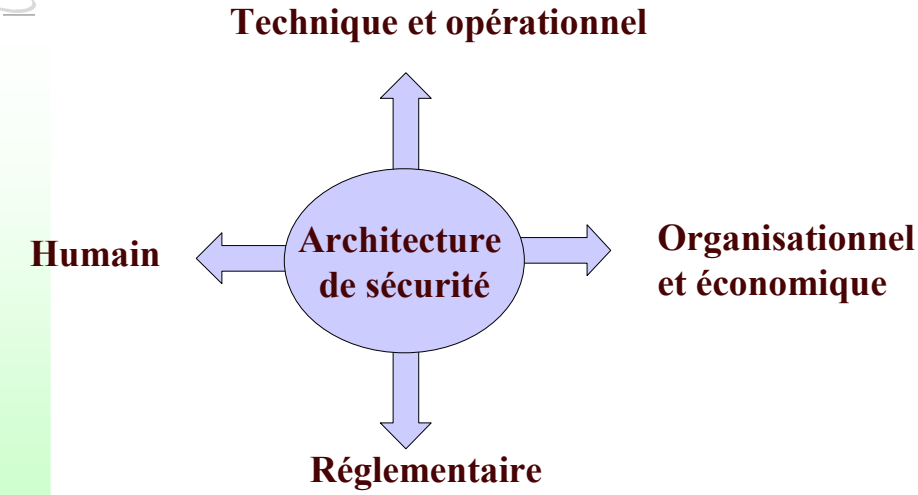
⇒Pour rester compétitive l'entreprise doit :

- Garantir l'intégrité des informations
- Préserver la confidentialité des données sensibles
- Garantir la disponibilité des SI
- S'assurer de la conformité aux législations

Rôle du SI

- Qu'attend-on du Système d'Information?
  - Capacité à pouvoir être utilisé : Disponibilité
  - Capacités à effectuer des actions de manière fiable et sans interruption : Fiabilité, Continuité de service
  - Capacité à ne permettre l'accès qu'aux entités autorisées : Confidentialité, Intégrité
  - Prouver des actions : Non-Répudiation

Toutes les dimensions de la sécurité



Aspects Organisationnels et économiques

- Définition des responsabilités
- Méthodologie
- Stratégie et politique de sécurité
- Mise en place des contrôles
- Aspects budgétaires (la sécurité a un coût)
- Les assurances

Aspects Humains

- Ethique
- Formation des hommes
- Compétences
- Sensibilisation
- Dissuasion
- Surveillance

Aspects techniques et opérationnels

- Sécurité physique
- Sécurité logique
- Sécurité environnementale
- Sécurité de l'exploitation
- Outils
- Sécurité applicative
- Sécurité des télécommunications

Aspects réglementaires

- Normes de sécurité (Orange BOOK, ITSEC)
- Procédures
- Autorisation de chiffrement
- Législation en vigueur
- Contractuels : utilisation de logiciels sous licence

5. Domaines d ’application de la sécurité

- La sécurité physique.
  - Concerne tous les aspects liés à la maîtrise des infrastructures et de l ’environnement. Elle repose sur :
    - Des normes de sécurité (température, rayonnement, dispositifs anti incendie…..)
    - La protection des sources énergétiques
    - La protection des accès aux équipements
    - La traçabilité et la surveillance des accès
    - Une gestion rigoureuse et à jour des autorisations
    - La redondance physique des équipements sensibles
    - La gestion de l ’inventaire et le marquage des équipements
    - Le plan de maintenance préventive et corrective

La sécurité de l'exploitation

Tout ce qui touche au bon fonctionnement des systèmes :

- **Plan de sauvegarde**
- **Plan de secours**
- **Plan de continuité**
- **Plan de tests**
- **Gestion du parc des équipements**
- **Gestion des configurations et des mise à jour (contrôle du changement)**
- **Gestion des incidents**
- **Contrôle et suivi d 'exploitation**
- **Analyse des fichiers de journalisation et des traces**
- **Gestion des contrats de maintenance**
- **Séparation des environnements de développement, de tests et de production**

La sécurité logique

- concerne la réalisation de mécanismes de sécurité par logiciel :
  - Contrôle des accès logiques aux systèmes par :
    - Identification
    - Authentification
    - Autorisation
  - Ensemble de mécanises logiciels permettant d 'assurer :
    - La confidentialité des données
    - L 'intégrité des données
    - Mesures de protection contre les virus
  - Classification des données selon leurs sensibilité
- La sécurité logique fait largement appel à la Cryptographie

- La sécurité applicative :

Elle repose sur :

  - Une méthodologie de développement
  - La robustesse des applications
  - Des contrôles programmés sur les entrées
  - Des jeux de tests
  - Des procédures de recette
  - L 'intégration des mécanismes de sécurité et d 'audit
  - La sécurité des progiciels (choix des fournisseurs, interface sécurité etc…)
  - Un plan de migration des applications critiques
  - Un plan d 'assurance qualité

– L 'application ne doit pas être une « porte dérobée » pour s'attaquer au système.

- La sécurité des télécommunications :

– Objectifs :

  - Offrir aux applications une connectivité :
    - Fiable
    - de qualité (performance, régulation de trafic)
    - de bout en bout (end to end)
  - Sécurisation de tous les maillons de la chaîne :
    - Systèmes
    - Equipements de réseaux (concentrateurs, routeurs, lignes….)
    - Câbles
  - Assurer la confidentialité des échanges par des mécanismes appropriés (lignes spécialisées, VPN, firewall, proxy…..)

6. Point sur la législation

- La législation nationale française doit s'adapter aux développements de la cybercrimalité ==> évolution du code pénal :
  - Crimes et délits contre les personnes
  - Crimes et délits contre les biens
  - Infraction de Presse
  - Infraction au code de la propriété intellectuelle
  - Infraction aux règles de cryptologie
  - Infraction sur les jeux de hasard

Crimes et délits contre les personnes

- Atteinte à la vie privée
- Atteinte à la représentation de la personne
- Dénonciations calomnieuses
- Atteinte au secret professionnel
- Atteinte aux droits de la personne résultant de traitements informatiques
- Diffusion d'images pornographiques susceptibles d'être vues par des mineurs

Crimes et délits contre les biens

- Escroquerie, détournement de fond
- Atteinte aux systèmes informatiques (article 323- à 323-7 du 5 janvier 1988 sur la fraude informatique)

Infraction de presse

- Loi du 29 Juillet 1981 modifiée :
  - Provocation aux crimes et délits
  - Apologie des crimes contre l'humanité
  - Apologie et provocation au terrorisme
  - Provocation à la haine raciale
  - Négationisme : contestation des crimes contre l 'humanité
  - Diffamation

Code de la propriété intellectuelle

- On ne peut pas faire n'importe quoi
  - textes, images, sont protégés par défaut et soumis au droit d'auteurs
  - accès et copie faciles ne signifie pas autorisation de duplication ou d'altération.
- détournement / alteration
  - page de liens, frame, meta index

Cryptologie

- En France, la cryptologie est autorisée sous réserve de l'utilisation de clés de 128 bits maximum (40 bits jusqu'en 1996). Bientôt plus de limites sur les clés mais :
- L'utilisation de la cryptologie reste soumise à déclaration.
- La loi évolue sans cesse notamment sur la reconnaissance légale de la signature électronique

7. Les normes de sécurité des Systèmes d'information

- 2 référentiels :
  - Orange Book : origine DoD (Department of Defense américain) en 1985 +
    Red Book : Complément pour les réseaux en 1987
  - Le référentiel Européen ITSEC (Information Technology Security Evaluation Criteria) équivalent européen de l'orange book

L'Orange Book

- **7 classes de sécurité définies itérativement par degré croissant de précision :**
  - **D** (minimal protection) : produit ou système qui ne rencontre aucun des critères de l'Orange Book
  - **C1** (discretionary security protection) : un utilisateur peut décider ce qui doit être contrôlé. Les utilisateurs doivent être identifiés par le système, les utilisateurs sont séparés en terme de données
  - **C2** (controlled access protection) : comme en C1, les utilisateurs sont responsables de leurs actions avec une granularité de contrôle plus fine. Mise en place d'audit des actions des utilisateurs sur chacun des objets du système.

- **B1** (labelled security protection) : contrôle d'accès non à discretion des utilisateurs. Tous les objets contrôlés et tous les sujets sont assignés à un niveau de sécurité. Tous les objets ne doivent pas être contrôlés en B1. Chaque objet contrôlé et sujet possède un label indiquant ce niveau de sécurité. Ce label sera utilisé lors du contrôle d'accès.

- **B2** (structured protection) : un design de haut niveau (conceptuel) vérifiable doit être présenté, ainsi qu'un test confirmant que le système ou produit implémente ce design. Le système ou produit doit être conçu en modules indépendants.

- **B3** (security domain) : le management du système ou produit doit permettre l'audit et la récupération des données (« recovery »). Chaque fonctionnalité de sécurité doit pouvoir être complètement testée. En plus des tests, une argumentation formelle montrant que le système ou produit respecte le design doit être présentée.

- **A1** (verified design) : le design est entièrement vérifié formellement. Il faut :
  - un modèle formel du système de protection et la preuve de sa consistance
  - une spécification formelle des fonctionnalités de haut niveau du système de protection
  - une preuve de la correspondance du modèle et de la spécification
  - montrer que l'implantation du système de protection est consistant avec la spécification

Référentiel européen ITSEC

- **F1 à F5** : correspond respectivement aux fonctionnalités décrites dans les classes D à A1 de l'Orange Book
- **F6** : haute intégrité
- **F7** : haute disponibilité
- **F8** : intégrité des données au cours de communications
- **F9** : haute confidentialité
- **F10** : réseau avec hautes confidentialité et intégrité

- **E0** : assigné aux systèmes qui échouent à l'évaluation
- **E1** : description informelle du système et tests de la correspondance du système avec son but sécuritaire.
- **E2** : E1 + une description informelle du design doit être fourni
- **E3** : un design détaillé et les codes sources des fonctions sécuritaires doivent être fournis. C'est le niveau le plus habituel
- **E4** : un modèle formel de la police de sécurité ainsi qu'une analyse rigoureuse des vulnérabilités doivent être fournis
- **E5** : établissement des correspondances entre le design détaillé et le code source. L'analyse des vulnérabilités se base dés lors sur le code source.
- **E6** : description formelle de l'architecture sécuritaire et la vérification de la consistance vis à vis du modèle formel de la police de sécurité doivent être fournis

Correspondance Orange Book ITSEC

Orange Book		ITSEC	
D	⟺	E0	**Protection minimale**
C1	⟺	F1 + E2	**Protection discrétionnaire**
C2	⟺	F2 + E2	**Protection des accès**
B1	⟺	F3 + E3	**Protection labelisée**
B2	⟺	F4 + E4	**Protection structurée**
B3	⟺	F5 + E5	**Domaines de la sécurité**
A1	⟺	F5 + E6	**Conception vérifiée**

Pour en savoir plus

- Orange book
  http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html
- ITSEC
  http://www.cesg.gov.uk/assurance/iacs/itsec/index.htm
- A titre d'exemple : Windows NT 4 est certifié C2 (orange book) et E3 (ITSEC)

8. Les organismes

- Les organismes Internationaux :
  - ISO (International Organization for Standardization)
  - UIT (Union Internationale des Télécommunications)
  - ISACA : Information System Audit and Control Association (http://www.isaca.org)

- Les organismes américains :
  - NCSC (National Computer Security Center) centre de sécurité informatique de la NSA (National Security Agency)
  - CERT (Computer Emergency Response Team) : Organisation créé en 1988 publiant des bulletins d 'informations et des statistiques sur les failles de sécurité http://www.cert.org
  - CIAC (Computer Incident Advisory Capability) Agence créée en 1989 par le Département à l'énergie américain http://ciac.llnl.gov
  - PCCIP (President 's Commission on Critical Infrastructure) créé par Clinton en 1996 http://www.pccip.gov.

- Les organismes Européens :
  - Pas d'organismes importants au niveau européen
- Les organismes Français :
  - Direction centrale de la sécurité des systèmes d'information (DCSSI ex SCSSI) http://www.scssi.gouv.fr
  - CLUSIF : Club de la Sécurité des Systèmes d 'Information Français
  - AFAI (Association Française d 'Audit et de conseil en Informatique) affiliée à l 'ISACA http://www.afai.asso.fr
  - CNIL Commission Nationale Informatique et Liberté

9. Stratégie et politique de sécurité

- Objectifs de la politique de sécurité :
  - Présenter une démarche globale de maîtrise des risques
  - Garantir qu'aucun préjudice ne puisse mettre en péril la pérennité de l'entreprise
  - Déterminer la stratégie de protection et de détection des intrusions et un plan de réaction en cas d'attaques

Démarche Globale

- Comprendre les enjeux liés aux systèmes d 'information
- La sécurité ne doit pas être envisagée uniquement comme un centre de coût
- Politiques de prévention, de dissuasion et de récupération
- A défaut d'éliminer les risques, il faut les minimiser
- Identifier les risques (processus continu)
- Couvrir les risques (assurances, plan de secours)
- Mesurer l'efficacité et l 'efficience de la politique de sécurité.

Mise en place de la sécurité

- **Le choix des mesures à mettre en place résulte d'un compromis entre le coût lié au risque et celui de sa réduction.**
- Mettre en place un vocabulaire commun sur la sécurité
- Cohérence des mécanismes sécuritaires utilisés
- Mettre en place des procédures de suivi de la sécurité
- Mise en place du plan de secours en cas de sinistre
- Mettre en place un « tableau de bord » de la sécurité

Les clés du succès

- Une volonté et une implication forte au niveau de la Direction Générale
- Une politique de sécurité simple, compréhensible, et applicable
- La publication en interne de la politique de sécurité
- Une gestion centralisée de la sécurité et une certaine automatisation des processus de sécurité
- Un niveau de confiance déterminé des personnes, des systèmes et des outils
- Des procédures de surveillance, d'enregistrement et d'audit
- L'expression des besoins sécuritaires au niveau des contrats
- Ethique du management et le respect des contraintes légales (déclaration des fichiers nominatifs auprès de la CNIL)

Quelques principes à retenir

- Un système parfaitement sûr n'existe pas
- Plus l'entreprise a de notoriété et plus elle peut être attaquée
- Le maillon faible de la sécurité c'est l'homme
- Pas de sécurité par l'obscurité
- La technologie ne résous pas à elle seule le problème de la sécurité
- La sécurité est l'affaire de tous
- La sécurité a un coût, ce coût doit être mis en balance par rapport aux coûts liés aux risques
- La sécurité n'est jamais acquise définitivement, elle doit être ré - évaluée périodiquement
- La qualité des outils utilisés dépend de la politique qu'ils servent
- Donner à chaque utilisateur les privilèges juste nécessaires à l'accomplissement d'une opération autorisée, ni plus, ni moins
- Minimiser le nombre, l'importance et la complexité de composants du système dans lesquels il faut être « aveuglément » confiants

BIBLIOGRAPHIE non exhaustive

- Sécurité Optimale 3eme édition Campus Press (ouvrage collectif)
- Sécurité Internet stratégies et technologies Solange Ghernaouti Hélie Dunod
- CISA Review Technical Information Manual ISACA
- Protection des Systèmes d ’Information, qualité et sécurité informatiques Référentiels Dunod