Résumé du cours Introduction à la Sécurité des Systèmes d'Information (IntroSSI)

Objectifs du cours

Ce cours est une introduction générale à la sécurité des systèmes d'information (SSI), couvrant des aspects techniques, managériaux, physiques et psychologiques. Les principaux objectifs sont:

- Développer un état d'esprit de sécurité (penser comme un attaquant)
- Acquérir des connaissances pratiques sur les méthodes de protection des données
- Apprendre les méthodes d'attaque et de défense
- Comprendre les disciplines nécessaires à la sécurité de l'information
- Savoir communiquer efficacement sur les risques et les réponses

Importance de la cybersécurité

- La cybersécurité est un aspect fondamental de la vie moderne
- Elle concerne chaque personne, entreprise et nation
- Les adversaires sont de plus en plus puissants et sophistiqués
- La cybercriminalité est une industrie de plusieurs millions de dollars
- Les nations utilisent l'Internet comme champ de bataille

Définition de la sécurité de l'information

La sécurité de l'information est définie comme "la protection des informations et des systèmes d'information contre tout accès, utilisation, divulgation, perturbation, modification ou destruction non autorisés".

Modèles conceptuels de sécurité

La triade CIA

Modèle fondamental comprenant trois principes:

1. **Confidentialité**: Protection des données contre les accès non autorisés
2. **Intégrité**: Empêcher la modification non autorisée des données
3. **Disponibilité**: Assurer l'accès aux données quand nécessaire

L'hexade de Parker

Extension du modèle CIA comprenant six principes:

1. **Confidentialité**
2. **Intégrité**
3. **Disponibilité**
4. **Possession ou contrôle**: Disposition physique du support de données
5. **Authenticité**: Attribution correcte des données au bon propriétaire/créateur
6. **Utilité**: Utilité pratique des données

Types d'attaques

1. **Interception**: Accès non autorisé (attaque contre la confidentialité)
2. **Interruption**: Rendre les actifs inutilisables (attaque contre la disponibilité)
3. **Modification**: Altération d'un bien (attaque contre l'intégrité)
4. **Fabrication**: Générer de fausses données/processus (attaque contre l'intégrité)

Concepts clés en gestion des risques

Menace

- Quelque chose ayant le potentiel de causer des dommages
- Peut être spécifique à certains environnements
- Les types de menaces incluent les attaques intentionnelles, les erreurs humaines, les défaillances structurelles et les perturbations environnementales

Vulnérabilité

- Faiblesse ou faille que les menaces peuvent exploiter

- Aspect non intentionnel d'un système (conception, mise en œuvre, configuration)

Risque

- Probabilité qu'un "malheur" se produise
- Nécessite à la fois une menace et une vulnérabilité que la menace pourrait exploiter

Principes de sécurité

Approches de sécurité

1. **Prévention**: Concevoir des systèmes sans vulnérabilités
2. **Gestion des risques**: Investir dans des contre-mesures
3. **Dissuasion par la responsabilité**: Attribuer les attaques et poursuivre en justice

Principes de prévention

1. **Responsabilité**: Tenir les utilisateurs responsables de leurs actes
2. **Médiation complète**: Intercepter et évaluer chaque opération
3. **Moindre privilège**: Accorder uniquement les privilèges nécessaires
4. **Failsafe par défaut**: Refuser par défaut, permettre sur justification
5. **Séparation des privilèges**: Différentes opérations requièrent différents privilèges
6. **Défense en profondeur**: Utiliser plusieurs mécanismes complémentaires
7. **Économie de mécanisme**: Préférer des mécanismes simples et petits
8. **Conception ouverte (Open Design)**: La sécurité ne doit pas dépendre du secret
9. **Acceptabilité psychologique**: Minimiser le fardeau des mécanismes de sécurité

Processus de gestion du risque

1. **Identification des actifs**: Identifier ce qui doit être protégé
2. **Identification des menaces**: Déterminer les menaces potentielles
3. **Évaluation des vulnérabilités**: Identifier les faiblesses
4. **Évaluation des risques**: Évaluer la probabilité et l'impact
5. **Atténuation des risques**: Mettre en place des contrôles

Types de contrôles pour l'atténuation des risques

1. **Contrôles physiques**: Protègent l'environnement physique (clôtures, serrures, gardes, etc.)
2. **Contrôles logiques/techniques**: Protègent les systèmes et réseaux (mots de passe, cryptage, pare-feu, etc.)
3. **Contrôles administratifs**: Basés sur des règles, politiques et procédures

Contre-mesures

Stratégies de défense:

- **Prévenir**: Bloquer l'attaque ou neutraliser la vulnérabilité
- **Dissuader**: Rendre l'attaque plus difficile
- **Dévier**: Rendre d'autres cibles plus attrayantes
- **Atténuer**: Réduire la gravité des dommages
- **Détecter**: Identifier les attaques en temps réel ou après coup
- **Récupérer**: Réparer les dommages

Réponse aux incidents

Processus de réponse aux incidents:

1. **Préparation**: Se préparer en amont
2. **Détection et analyse**: Identifier et analyser l'incident
3. **Confinement**: Limiter les dégâts
4. **Éradication**: Éliminer la menace
5. **Recouvrement**: Restaurer les systèmes
6. **Activité post-incident**: Analyser et tirer des leçons

Défense en profondeur

Stratégie de défense multicouche:

1. **Réseau externe**: DMZ, VPN, journalisation, audit, tests de pénétration

2. **Périmètre du réseau**: Pare-feu, proxy, inspection des paquets
3. **Réseau interne**: IDS, IPS, journalisation, audit
4. **Hôte**: Authentification, antivirus, pare-feu, mots de passe
5. **Applications**: Single Sign-On, filtrage du contenu, validation des données
6. **Données**: Cryptage, contrôles d'accès, sauvegardes

Cette approche multicouche rend difficile la pénétration du réseau et l'attaque des actifs, offrant du temps pour détecter et contrer les intrusions.