Cours INF 6420: Sécurité Informatique

Chapitre 10: Gestion de la sécurité

ÉCOLE POLYTECHNIQUE MONTRÉAL
Le génie sans frontières

Bernard Lanctôt

A-306.11
340-4711 poste 4233

Plan de ce chapitre

- **Gestion de la sécurité des ordinateurs personnels**
- **Sécurité dans un environnement UNIX**
- **Analyse du risque**
- **Plans et politiques de sécurité**
- **Récupération post-désastre**

Sécurité des ordinateurs personnels

- **C'est une gestion décentralisée**
  - **manque de connaissance des risques**
  - **manque d'outils de sécurité**
- **Vulnérabilités**
  - **peu de sécurité bâtie dans le matériel**
  - **faible usage de ce qu'il y a**
  - **insensibilité aux risques et aux problèmes**
  - **pas de journal de bord**
  - **dangers venant de l'environnement**
    - fumée et autres particules
    - nourriture et breuvages
    - surtensions et sous-tensions
  - **manque de contrôle de l'accès physique**
  - **vulnérabilité des média et des composants**

- **absence de système de prise de copies de sécurité**
- **documentation absente, incomplète ou inadéquate**
- **logiciels de qualité "amateur"**
- **portabilité élevée de certains matériels**
- **rétension de l'information sous forme magnétique**
- **cumul de tâches ou de responsabilités**

- **Mesures de sécurité**
  - **protéger l'accès physique aux machines**
  - **contrôler l'accès aux imprimantes lors de la sortie d'information sensible**
  - **mêmes contrôles sur les média magnétique que sur les média papier**
  - **prise périodique de copies de sécurité**
  - **séparation des tâches et des responsabilités**

Mécanismes de protection

- **Matériel**
  - fixer ou attacher l'équipement
  - dispositifs matériel de sécurité ("security board")
- **Logiciel**
  - bien comprendre le potentiel de risque du logiciel
  - bien connaître l'origine des logiciels utilisés
  - utiliser un processus bien défini et contrôlé pour le développement de logiciel
  - valider les résultats: ne pas prendre pour acquis que l'ordinateur fournira des résultats corrects
  - prise de copies de sécurité périodiquement
  - contrôle des fenêtres temporelles d'accès
  - minuterie d'inactivité
  - auto identification de chaque machine

Points particuliers de la sécurité sous UNIX

- Il y existe encore des failles de sécurité
- Manque de cohérence dans les divers fichiers de configuration
- Garder son système d'exploitation à jour
  - utiiser la version la plus récente
  - s'assurer que toutes les rustines ont été appliquées
- Bien gérer les comptes d'usager
  - détecter les comptes inutilisés pendant assez longtemps
  - déactiver/supprimer les comptes dormants
  - supprimer les comptes des personnes qui ne sont plus à l'emploi de l'entreprise
- Restreindre les comptes "anonymes" ou "invités"
  - ne pas en avoir
  - limiter les permissions
  - assigner à une machine distincte

Gestion de la sécurité du réseau

- Problèmes de distance et de taille dans les WAN
- Définition et contrôle du périmètre protégé
- Contrôle des privilèges et des permissions sur la base du "besoin de connaître"("need to know")
- Définition des propriétaires et des responsables
- Nécessité de bien connaître la structure du réseau
- Contrôle de la connectivité
- Contrôle des permissions et des privilèges de réseau
- Contrôle des versions de logiciel
- Éducation des usagers relativement aux comportements questionnables
  - qui contacter
  - prédéfinition des actions à prendre
  - moyen d'avertir tous les usagers
  - se servir du CERT ("Computer Emergency Response Team")
- Outils: CRACK, COPS, SATAN, etc..

Analyse de risque

- **Définition**
  - étude formelle des vulnérabilités et des probabilités qu'elles soient exploitées, des contrôles possibles pour s'en protéger, et de l'équilibre des coûts entre les deux
- **Motivation**
  - stimuler la prise de conscience de l'importance de la sécurité
  - identifier les actifs, les vulnérabilités et les contrôles
  - améliorer les bases de décision
  - justifier les dépenses de sécurité
- **Étapes**
  - identifier les actifs à protéger
  - déterminer les vulnérabilités
  - estimer les probabilités qu'une menace se matérialise
  - calculer les coûts annuels probables
  - déterminer les contrôles disponibles et leurs coûts
  - projeter les épargnes ou les coûts nets

Identifier les actifs

Actifs	Confidentialité	Intégrité	Disponibilité
Matériel		Surchargé Détruit Altéré	Défectueux Volé Détruit
Logiciels	Volé Copié Piraté	Cheval de troie Bombe ou oeuf Modifié	Détruit Perdu Licence périmée
Données	Dévoilées Accédées Déduites	Endommagées -défaut logiciel -défaut matériel -erreur de l'usager	Détruites Perdues Effacées
Personnes			Démission Retraite Remerciement
Documentation			Perdue Volée Détruite
Fournitures			Perdues Volées Endommagées

Catégoriser les probabilités d'occurrence

Fréquence	Code
Plus qu'une fois par jour	10
Une fois par jour	9
Une fois par trois jours	8
Une fois par semaine	7
Une fois par quinzaine	6
Une fois par mois	5
Trois fois par année	4
Une fois par année	3
Une fois par trois ans	2
Moins qu'une fois par trois ans	1

Prédire les probabilités d'occurrence

- Probabilité selon les statistiques observées en général et dans notre secteur
- Probabilité observées pour un système en particulier
- Estimé du nombre d'évènements au cours d'une période spécifique
- Estimé à partir de l'expérience des évaluateurs
- Utiliser une approche "Delphi"
  - plusieurs évaluateurs
  - évaluations indépendantes et confidentielles
  - diffusion des résultats
  - ronde de révision
  - atteinte d'un consensus

Déterminer les coûts reliés à chaque type d'incident

- Coût de remplacement
  - matériel et/ou logiciel
  - inclure les côuts résultant du temps perdu
  - inclure tous les autres coûts indirects
- Coûts découlant d'aspects légaux
  - pénalités et amendes
  - recours en justice
  - frais légaux
- Effets sur la poursuite des affaires
  - difficulté/impossibilité de poursuivre la gestion de l'entreprise
  - avantages indus à des compétiteurs
  - pertes de ventes ou de contrats
- Effets sur "l'image" de l'entreprise
  - confiance des clients
  - confiance du personnel
  - confiance des investisseurs et des actionnaires

Faire une liste des contrôles possibles

- Contrôles cryptographiques
- Protocoles sécuritaires
- Contrôle sur le développement des logiciels
- Contrôle sur l'environnement d'exploitation
- Caractéristiques des systèmes d'exploitation
- Identification et authentification
- Contrôles sur les bases de données: accès, fiabilité, inférence
- Sécurité à niveau multiple et catégorisation du personnel
- Sécurité des postes de travail: physique, procédural, etc…
- Contrôles d'accès aux réseaux: coupe feux et autres
- Contrôles physiques: sécurité des lieux

Comparer les coûts de faire et de ne pas faire

- **Exemple 1**

Risques: dévoilement d'informations confidentielles
calculs effectués utilisant des données falsifiées

Coûts pour reconstruire les données correctes: $1,000,000
@ probabilité sur base annuelle = 10% **$100,000**

Efficacité du logiciel de contrôles d'accès: 60% **-$60,000**

Coût du logiciel de contrôle d'accès: **$25,000**

Coût annuel net: **$65,000**

Économie: **$100,000 -$65,000 => $35,000 (=60,000 – 25,000)**

Exemple 2

Risques: Accès non autorisé à des données et des programmes	
$100,000 @ probabilité de 2% par année	**$2,000**
Usage non autorisé des ressources informatiques	
$10,000 @ probabilité de 40% par année	**$4,000**
Total	**$6,000**
Efficacité des contrôles proposés: 100% économie	**$6,000**
Coût de matériel: $50,000 amorti sur 5 ans	**$10,000**
Coût du logiciel: $20,000 amorti sur 5 ans	**$ 4,000**
Coût de personnel	**$40,000**
Coût total	**$54,000**
Économie: $6,000 - $54,000	**- $48,000**

Analyse du risque: le pour et le contre

Contre

- pas très précis; beaucoup d'estimés et de prévisions
- fausse impresion de précision et de sécurité
- tendance à la finalité; nécessité de mises à jour régulières
- pas de fondements scientifiques ou théoriques

Pour

- mieux que de ne rien faire
- meilleure identification des problèmes possibles
- prise de conscience des conséquences de failles de sécurité
- approche plus formelle à la prise de décision
- meilleure justification des investissements et des dépenses de fonctionnement

Planification de la sécurité

- **Nécessité d'un plan**
  - **préparation initiale et révision périodique**
- **Participants à la préparation**
  - groupe matériel
  - programmeurs de système et d'applications
  - personnel de la sécurité physique
  - personnel "entrée des données" et autres usagers typiques
- **Doit couvrir**
  - **définition de politiques et d'objectifs**
  - **description de la situation au moment de la préparation du plan**
  - **recommandation, plan d'investissement et d'effectifs**
  - **imputabilités**
    - liste des personnes responsables et de leurs secteurs particuliers
  - **formation des personnels en cause**
  - **échéancier**
  - **structure de mise à jour**
    - date d'évaluation et de revue et critères d'évaluation

Survivre à un désastre

- **Variété de désastres**
  - **désastres naturels: inondation, refoulement d'égouts, incendie, panne électrique majeure,**
  - **vol et vandalisme**
  - **accès et usage non autorisé**
- **Protection en cas de désastre**
  - **copies de sécurité**
  - **site alternatif**
    - "cold site"
    - dédoublement complet
- **Vol et intrusion**
  - **prévention**
  - **détection**
- **Mise au rebut d'information sensible**

Conclusions

- Les moyens techniques de contrôle sont disponibles
- Il faut déterminer qu'est ce qu'on veut protéger, et comment
- Il faut planifier et non pas seulement réagir
- Intégrer la sécurité informatique avec le plan général de sécurité de l'entreprise
- Conscientiser et former les usagers
- Savoir à l'avance les gestes à poser s'il y a une brèche de sécurité