3TI
Sécurité des réseaux informatiques
2015-2016

La sécurité des réseaux

V. Van den Schrieck

Références

Le contenu et les figures de ce slideshow sont principalement tirés de Stallings et Brown, « Computer Security, Principles and Pratice », 3rd edition, Ed. Pearson

Gestion de la sécurité

Trois questions fondamentales :

- Quels sont les avoirs à protéger?
- En quoi sont-ils menacés?
- Que pouvons-nous faire pour contrer ces menaces?

Gestion de la sécurité

Gestion de la sécurité : Processus utilisé pour réaliser et maintenir un certain niveau de confidentialité, d'intégrité, de disponibilité, d'authentification, de traçabilité et de fiabilité

Gestion de la sécurité

- Déterminer les objectifs, les stratégies et les politiques de sécurité de l'organisation
- Déterminer les requirements de sécurité
- Identifier et analyser les menaces sur les avoirs
- Identifier et analyser les risques
- Spécifier des mesures de protection appropriées
- Surveiller l'implémentation et le fonctionnement de ces mesures
- Détecter et réagir aux incidents

Gestion de la sécurité

Standards de sécurité : Représentent un consensus sur les bonnes pratiques dans le domaine de la sécurité

- Standards ISO
- Standards NIST (US)
- …

Gestion de la sécurité

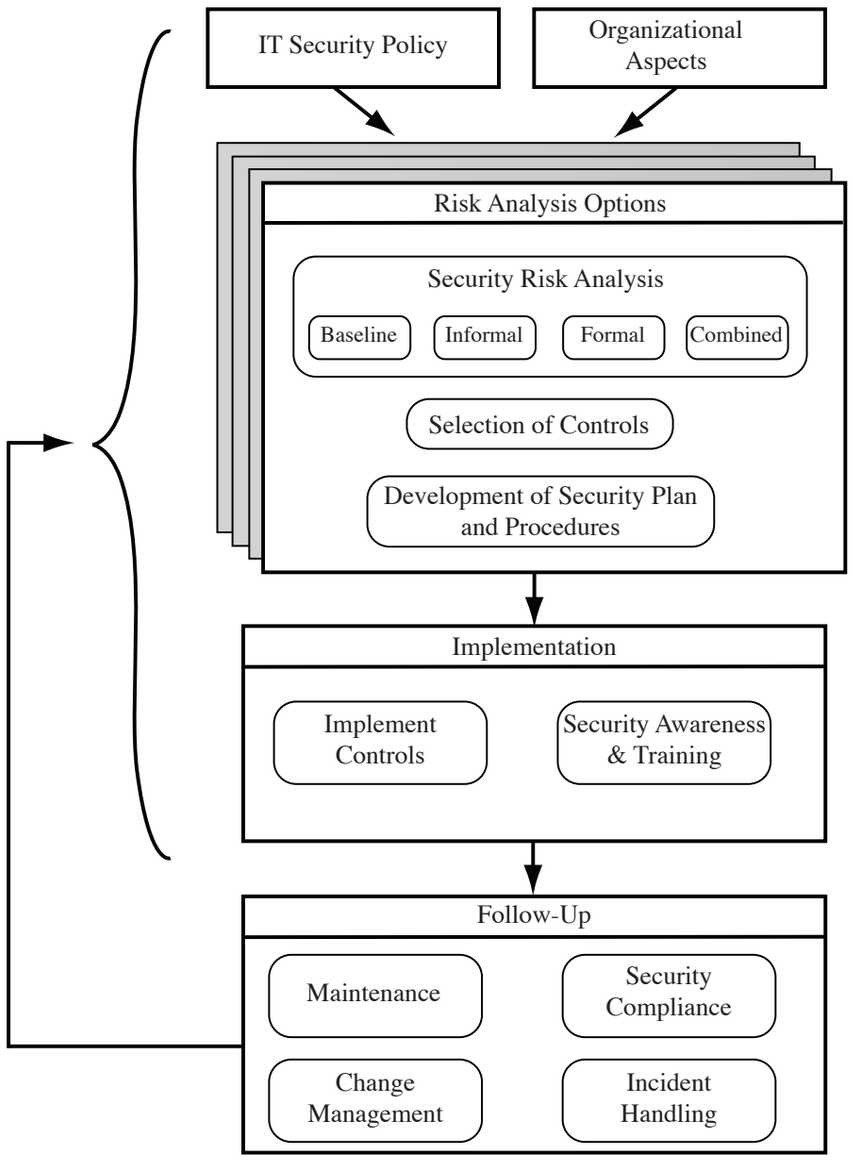

Figure 14.1 Overview of IT Security Management

Gestion de la sécurité : Procédure

1. **Analyse des risques** : Définir ce que le mécanisme doit faire, et ce qu'il doit protéger
   1. Valeurs des avoirs
   2. Vulnérabilités
   3. Probabilité et impact => Calcul du risque
2. Mettre en place des **contre-mesures/contrôles**
   1. Prévention, Détection, Réaction, Récupération
   2. Choix stratégique : Budget limité! => sélection des contre-mesures sur base de l'analyse des risques
   3. Ne pas oublier les risques résiduels!
3. **Validation** : Comment s'assurer que la contre-mesure fonctionne?

Analyse des risques : Exemple

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Internet router	Outside hacker attack	Admin password only	Possible	Moderate	High	1
Destruction of data center	Accidental fire or flood	None (no disaster recovery plan)	Unlikely	Major	High	2

Contrôles

Contrôle : Action, appareil, procédure ou tout autre mesure qui réduit le risque en éliminant ou en empêchant une violation de la sécurité, en minimisant le danger qu'elle peut causer ou en découvrant et signalant son apparition pour permettre une action corrective

Types de contrôle (1)

- Les contrôles peuvent être de différents types :
  - Contrôles de gestion : Procédures, politiques et processus guidant la stratégie de sécurité
  - Contrôles opérationnels : S'occupent de l'implémentation et de application des politiques et des standards de sécurité
  - Contrôles techniques

Types de contrôles (2)

- Les contrôles peuvent agir à différents niveaux/moments :
  - Contrôles de soutien : « mesures de base » utilisées par les autres contrôles
  - Contrôles préventifs : Empêche les tentatives de violation
  - Contrôles de détection et de recovery : En réponse aux attaques

Plan de sécurité IT

Une fois identifiés les contrôles susceptibles de diminuer les risques de sécurité identifiés, un plan de sécurité IT doit être créé, contenant :

- Les risques
- Les contrôles recommandés
- La priorité d'action pour chaque risque
- Les contrôles sélectionnés sur base d'une analyse coût/bénéfices
- Les ressources nécessaires pour l'implémentation de ces contrôles
- Le personnel responsable
- Les dates de début et de fin d'implémentation
- Les requirements pour la maintenance, et tout autre commentaire

Plan d'implémentation : Ex

Risk (Asset/Threat)	Hacker attack on Internet router
Level of Risk	High
Recommended Controls	•Disable external telnet access •Use detailed auditing of privileged command use •Set policy for strong admin passwords •Set backup strategy for router configuration file •Set change control policy for the router configuration
Priority	High
Selected Controls	•Strengthen access authentication •Install intrusion detection software
Required Resources	•1 day of training for network administration staff
Responsible Persons	John Doe, Lead Network System Administrator, Corporate IT Support Team
Start – End Date	1-Feb-2011 to 4-Feb-2011
Other Comments	•Need periodic test and review of configuration and policy use

Implémentation des contrôles

Deux étapes :

1. Implémentation du plan lui-même + validation :
   - Suivi des dépenses
   - Mise en place correcte des contrôles
   - Surveillance et administration des contrôles
2. Formation et conscientisation à la sécurité
   - Le personnel impacté par les contrôles doit être formé à l'utiliser correctement

Validation et monitoring

Les contrôles doivent être constamment surveillés pour s'assurer de leur bon fonctionnement

- Maintenance
- Adéquation par rapport au plan de sécurité (Audit)
- Gestion des changements
- Gestion des configurations
- Réaction aux incidents

Business Continuity Plan

Plan permettant à une organisation de fonctionner même en cas de désastre (vol, incendie, innondation,…), éventuellement en mode dégradé, ou en situation de crise majeure

« Si nous perdons ce bâtiment, comment pourrions-nous recommencer notre activité? »

Business Continuity Plan

- A prévoir dans un BCP :
  - Personnel critique?
  - Processus métiers?
  - Listing des fournisseurs/clients/contacts importants?
  - Infrastructure IT? (=> DRP)
- Les procédures doivent être testées régulièrement (exercices)

Disaster Recovery Plan

- DRP : permet d'assurer, en cas de crise majeure ou importante d'un **centre informatique**, la reconstruction de l' infrastructure et la remise en route des applications supportant l'activité d'une organisation.

- Le plan de reprise d'activité doit permettre, en cas de sinistre, de basculer sur un système de relève capable de prendre en charge les **besoins informatiques** nécessaires à la survie de l'entreprise.

« Si nous perdons nos services IT, comment pouvons-nous les récupérer? »

Disaster Recovery Plan

- Deux concepts importants à préciser :

  - **Recovery Time Objective (RTO)** : le délai de rétablissement d'un processus, suite à un incident majeur, pour éviter des conséquences importantes associées à une rupture de la continuité d'activité. Il définit le temps alloué pour faire le basculement vers le nouveau système.

  - **Recovery Point Objective (RPO)** : Le RPO commence à s'exprimer à l'instant où l'incident majeur arrive et peut être exprimé en secondes, minutes, heures ou jours. Il s'agit donc de la quantité maximale acceptable de perte de données. C'est la durée des fichiers ou des données dans le stockage de secours exigé par l'organisation pour reprendre des opérations normales après l'incident. Ce critère définit l'état dans lequel doit se trouver le nouveau système après basculement.

Sécurité physique et des infrastructures

- Objectifs :
  - Empêcher les dommages à l'infrastructure physique qui sous-temps le système d'information
    - HW, réseau, bâtiments, systèmes de contrôle de l'environnement, personnel, …
  - Empêcher les mauvaises utilisations (accidentelles ou non) de l'infrastructure qui pourraient nuire à l'information
    - Vol, copie, accès non autorisé

Menaces à la sécurité physique

Menaces environnementales :

- Cause : Désastres naturels (tornade, tremblement de terre, orage, inondations)
- Menace :
  - Température ou taux d'humidité inadéquats
  - Feu et fumée
  - Dégats des eaux
  - Nuisances chimiques, radiologiques, biologiques
  - Poussière
  - Infestation

Menaces à la sécurité physique

Menaces techniques :

- Alimentation électrique :
  - Sous-voltage
  - Sur-voltage (ex : foudre)
  - Bruit
- Interférences électromagnétiques
  - Ex : Causés par du bruit sur une ligne d'alimentation électrique

Menaces à la sécurité physique

Menaces liées aux personnes :

- Accès non autorisé
- Vol
- Vandalisme
- Mauvaise utilisation des ressources

Sécurité et ressources humaines

Formation, conscientisation et éducation du personnel :

- Objectif :
  - Améliorer le comportement des employés
  - Accroître la capacité à tracer les actions des employés
  - Diminuer la dépendance de l'organisation au comportement d'un employé
  - Se conformer aux obligations contractuelles et de régulation

Sécurité et ressources humaines

- Niveau 1 : Conscientisation
  - Les employés sont conscients de leur responsabilité au niveau de la sécurité et des restrictions sur leurs actions, et agissent en fonction
  - Les utilisateurs comprennent l'importance de la sécurité pour le bien-être de l'organisation

Sécurité et ressources humaines

- Niveau 2 : Entrainement

  - **Donner au personnel les compétences pour pouvoir mener à bien leurs tâches IT de manière plus sécurisée (Quoi et Comment)**

  - **Utilisateurs généraux** : Fermer les portes, utiliser les mécanismes d'authentification, signaler les anomalies de sécurité

  - **Développeurs et spécialistes systèmes** : Intégrer la sécurité dans les cycles de vie des produits, apprendre comment limiter les vulnérabilités et comment surveiller les systèmes

  - **Gestionnaires** : Doivent pouvoir faire des compromis entre risques, coûts et bénéfices impliquant la sécurité

  - …

Sécurité et ressources humaines

- Niveau 3 : Education
  - Formation des spécialités en sécurité
  - Formations généralement en dehors des organisations (certifications, formations universitaires, …)

Pratiques et politiques d'emploi

- Les employés peuvent être impliqués dans des violations de sécurité de deux manières :
  - Aide involontaire
  - Violation volontaire de la politique de sécurité
- Menaces : Accès non autorisé, altération de données, suppression de backups, destruction de systèmes, …

Pratiques et politiques d'emploi

- Sécurité au moment de l'embauche
  - Vérification des CVs
  - Engagement écrit vis-à-vis des procédures de sécurité
- Sécurité pendant l'emploi
  - Principe du moindre privilège
  - Séparation des responsabilités de sécurité
  - Ne pas dépendre d'employés-clé (départ, maladie, …)

Pratiques et politiques d'emploi

- Fin de contrat
  - Supprimer les accès de la personne (codes/liste)
  - Informer les gardes du départ de la personne
  - Changer les codes des serrures, les cartes d'accès au système, voire les serrures physiques
  - Récupérer tous les avoirs à disposition de la personne (disques, ID, documents, équipement, …)
  - Informer tous les départements du départ

Politiques eMail et Internet

- Définir les règles d'accès et d'utilisation des emails et du web :
  - Business Use Only?
  - Accès au mail en extérieur?
  - Accès au mail privé?
  - Standards de conduite dans l'utilisation des ressources
  - Propriété des contenus?
  - Actions disciplinaires?
  - …