CHAPITRE 2 :
La Politique de sécurité Informatique

Mohammed SABER

Département Électronique, Informatique et Télécommunications
École Nationale des Sciences Appliquées "ENSA"
Université Mohammed Premier OUJDA

Année Universitaire : 2017-2018

Plan de chapitre

1. Introduction
2. Mise en place d'une politique de sécurité
3. Phases de définition d'une politique de sécurité
4. Les méthodologies de sécurité
5. Statistiques

Plan de chapitre

1. Introduction
2. Mise en place d'une politique de sécurité
3. Phases de définition d'une politique de sécurité
4. Les méthodologies de sécurité
5. Statistiques

Introduction

- L'information s'impose comme un capital des plus précieux pour l'organisation.
- Le système d'information, constituer de moyens informatiques, est essentiel à l'activité de l'organisation.
- L'utilisation inappropriée du SI, ou son mal fonctionnement peuvent menacer l'existence de l'organisation.
- En analysant et définissant les risques, l'on peut construire une politique de sécurité du SI, définissant le cadre d'utilisation des moyens informatiques.
- Toute utilisation d'une information doit respecter la confidentialité de cette dernière, en se conférant aux lois, règlement ou directives internes en vigueur.

Introduction

- La politique de sécurité informatique fixe les principes visant à garantir la protection des ressources informatiques et de télécommunications en tenant compte des intérêts de l'organisation et de la protection des utilisateurs.
- Les ressources informatiques et de télécommunications doivent être protégées afin de garantir confidentialité, intégrité et disponibilité des informations qu'elles traitent, dans le respect de la législation en vigueur.
- La sécurité des systèmes informatiques se cantonne généralement à garantir les droits d'accès aux données et ressources d'un système en mettant en place des mécanismes d'authentification et de contrôle.
- Les mécanismes de sécurité mis en place peuvent néanmoins provoquer une gêne au niveau des utilisateurs et les consignes et règles deviennent de plus en plus compliquées au fur et à mesure que le réseau s'étend.
- La sécurité informatique doit être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance.

Plan de chapitre

1 Introduction
2 Mise en place d'une politique de sécurité
3 Phases de définition d'une politique de sécurité
4 Les méthodologies de sécurité
5 Statistiques

Introduction

La raison pour laquelle il est nécessaire de définir dans un premier temps une **politique de sécurité**, dont la mise en œuvre se fait selon les quatre étapes suivantes :

- **Identifier les besoins** en terme de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences ;
- **Élaborer des règles et des procédures** à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés ;
- **Surveiller et détecter les vulnérabilités** du système d'information et se tenir informé des failles sur les applications et matériels utilisés ;
- **Définir les actions** à entreprendre et les personnes à contacter en cas de détection d'une menace.

La politique de sécurité

- La politique de sécurité est donc l'ensemble des orientations suivies par une organisation (à prendre au sens large) en terme de sécurité. A ce titre elle se doit d'être élaborée au niveau de la direction de l'organisation concernée, car elle concerne tous les utilisateurs du système.
- L'organe compétent édicte les règles et procédures relatives à l'utilisation des différentes ressources informatiques et de télécommunications nécessaires à la concrétisation de la présente politique de sécurité informatique.
- Les responsables de chaque service sont responsables du bon respect, par les utilisateurs, de la politique de sécurité informatique, ainsi que des règles et procédures de sécurité.
- L'organe compétent en la matière vérifie la bonne application des règles et procédures.
- Les utilisateurs doivent assurer la confidentialité, intégrité et disponibilité des ressources informatiques qu'ils utilisent.

Définition des rôles

- Existence ou non d'un Responsable Sécurité des Systèmes d'Informations (RSSI) ;
- Externalisation ou non de la sécurité (si oui : totale ou partielle) ;
- Hiérarchie de la sécurité (Exemple) :
  - RSSI à DSI à DG ;
  - RSSI à DG ;
  - RSSI à Direction métier ;
- Chaînage des responsabilités au sein de l'équipe Sécurité ;
- Rôle (en termes de sécurité) de l'utilisateur final (salarié, client ou fournisseur).

Mise en place d'une politique de sécurité

- L'objectif consiste à déterminer les besoins de l'organisation en faisant un véritable état des lieux du système d'information, puis d'étudier les différents risques et la menace qu'ils représentent afin de mettre en œuvre une politique de sécurité adaptée.
- La phase de définition comporte ainsi trois étapes :
  - L'identification des besoins ;
  - L'analyse des risques ;
  - La définition de la politique de sécurité.

Plan de chapitre

1 Introduction

2 Mise en place d'une politique de sécurité

3 Phases de définition d'une politique de sécurité

4 Les méthodologies de sécurité

5 Statistiques

Identification des besoins

Identification des besoins

- La phase de définition des besoins en terme de sécurité est la première étape vers la mise en œuvre d'une politique de sécurité.
- Les Besoins en termes de sécurité se situent à plusieurs niveaux :
  - Sécurité des équipements (physique) ;
  - Sécurité des réseaux ;
  - Sécurité des applications et des systèmes d'exploitation (logiciels) ;
  - Sécurité des données (BD).
- Il faut donc utiliser des outils et des éléments de sécurité distincts pour assurer la sécurité à chaque niveau, en vue de sécuriser globalement tout le SI.

Analyse des risques

- L'étape d'analyse des risques consiste à répertorier les différents risques encourus, d'estimer leur probabilité et enfin d'étudier leur impact.
- La détermination des éléments critiques d'une entreprise est une tâche délicate.
- Nécessité de mener avec les responsables de l'entreprise une analyse de risque.
- Cette analyse consiste à identifier les ressources et biens vitaux de l'entreprise : matériel, données, logiciels, personnes.
- Il convient pour chacune de ces ressources d'associer les trois éléments suivants : conséquence, menace, vulnérabilité
- Mener des actions ciblées en fonction du risque :
  - **Prévention** : Faire en sorte que les menaces ne soient pas mises à exécution
  - **Réaction** : Réagir lors de l'apparition des menaces
  - **Correction** : Reconstituer le système après élimination du risque
- Évolution des risques
  - Croissance de l'Internet ;
  - Croissance des attaques ;
  - Failles des technologies ;
  - Failles des configurations ;
  - Failles des politiques de sécurité ;
  - Changement de profil des pirates.

Définition de la politique de sécurité

Définition de la politique de sécurité

- La politique de sécurité est le document de référence définissant les objectifs poursuivis en matière de sécurité et les moyens mis en œuvre pour les assurer.
- La politique de sécurité définit un certain nombre de règles, de procédures et de bonnes pratiques permettant d'assurer un niveau de sécurité conforme aux besoins de l'organisation.

Plan de chapitre

1 Introduction

2 Mise en place d'une politique de sécurité

3 Phases de définition d'une politique de sécurité

4 Les méthodologies de sécurité

5 Statistiques

Les méthodologies de sécurité

Pour mesurer le niveau de sécurité (analyser les niveaux des risques). Il existe de nombreuses méthodes permettant de mettre au point une politique de sécurité. Voici une liste non exhaustive des principales méthodes :

- MARION (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux) `https://www.clusif.asso.fr/fr/production/mehari/` ;
- MEHARI (MEthode Harmonisée d'Analyse de RIsques) ; `https://www.clusif.asso.fr/fr/production/mehari/` ;
- EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), mise au point par la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) ; `http://www.ssi.gouv.fr/fr/confiance/ebios.html` ;
- Les normes ISO 17799, ISO 27001 et ISO 27002 ;
- CRAMM ;
- OCTAVE ;
- Melisa, INCAS ;
- ...

Application d'une méthode de sécurité

Méthode

Mét

Plan de chapitre

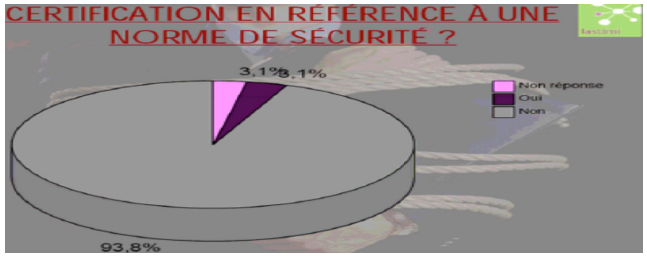
1 Introduction
2 Mise en place d'une politique de sécurité
3 Phases de définition d'une politique de sécurité
4 Les méthodologies de sécurité
5 Statistiques

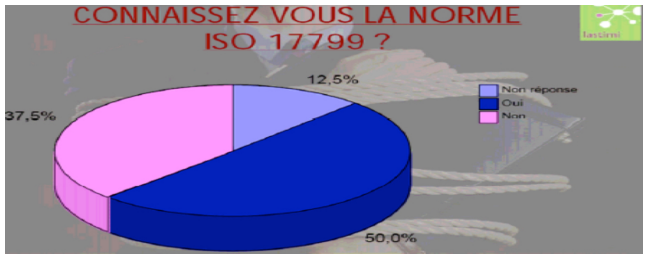
Statistiques

Obstacles à l'obtention d'un niveau de sécurité adapté :

- Manque de ressources : 35 % ;
- Sensibilisation insuffisante des utilisateurs : 34 % ;
- Manque de budget : 32 % ;
- Implication insuffisante du management : 26 % ;
- Manque d'outils/solutions : 22 % ;
- 41 % des entreprises n'ont pas de budget pour la sécurité du Système d'Information.

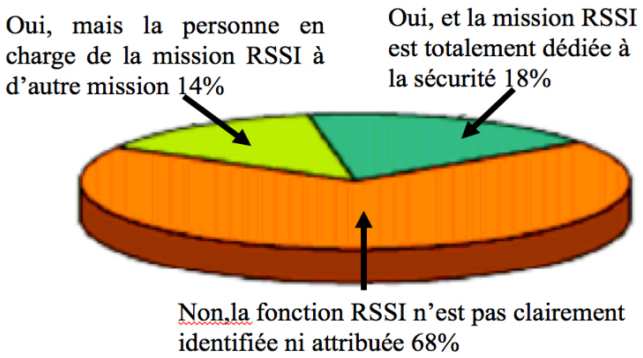
Statistiques





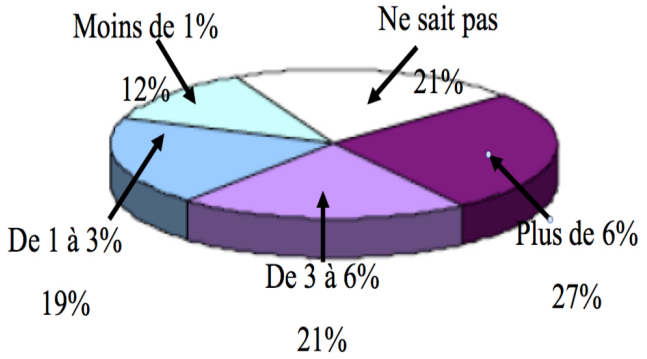
Statistiques

La fonction RSSI est-elle clairement identifiée ? Si oui la personne en charge de la mission RSSI est-elle dédiée à cette mission ?



Statistiques

Part du budget sécurité dans le budget informatique des entreprises :



QUESTIONS ?