Chapitre 3

Politique de sécurité informatique

I. Aspects généraux de la politique de sécurité de système d'information

I.1. Définition :

Une **politique de sécurité informatique** est une stratégie visant à maximiser la sécurité informatique d'une entreprise. Elle est matérialisée dans un document qui regroupe l'ensemble des règles de sécurité à adopter ainsi que le plan d'actions ayant pour objectif de maintenir le niveau de sécurité de l'information dans l'organisme.

La politique de sécurité du système d'information, élaborée « sur-mesure » pour chaque établissement, décrit l'ensemble des enjeux, des besoins, des contraintes, ainsi que des règles à adopter propres à chaque structure. Elle doit être validée par la direction et prise en compte par chaque collaborateur.

Elle définit les objectifs de sécurité des systèmes informatiques d'une organisation. La définition peut être formelle ou informelle. Les politiques de sécurité sont mises en vigueur par des procédures techniques ou organisationnelles. Une mise en œuvre technique définit si un système informatique est sûr ou non sûr.

I.2. Objectif principal

La politique de sécurité informatique sert à empêcher les violations de sécurité telles que: accès non autorisé, perte de données, interruption de services, etc.

I.3. Principes

Les principes de la politique de la sécurité de l'information dans une entreprise sont :

• Protéger la réputation, l'intégrité, l'éthique, et l'image publique de l'entreprise.
• Maintenir la confiance des clients, fournisseurs ainsi que les partenaires de l'entreprise.
• Protéger le caractère confidentiel de l'information sensible.
• Protéger les données opérationnelles sensibles des divulgations inappropriées.
• Prévenir les tiers contre les actes illégaux ou malveillants à l'encontre des systèmes de l'organisation.
• Assurer la non-répudiation : Permet de garantir qu'une transaction ne peut être niée.
• Vérifier l'authentification : Consiste à s'assurer de l'identité d'un utilisateur et garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. L'authentification est nécessaire pour la non-répudiation.
• Assurer la traçabilité : Consiste à conserver une trace probante : originale, horodatée, explicite et intègre, d'un évènement technique (ex : Traces techniques de sécurité ou logs) ou d'un acte métier (ex: piste d'audit). Pour être probante une trace doit pouvoir être rattachée à un acteur et une référence au temps fiable.
• Optimiser l'utilisation des ressources de l'entreprise en s'assurant qu'elles ne sont pas mal utilisées ou sont gaspillées.

• Prévenir contre les fraudes.
• Prévenir contre les incidents importants et qui peuvent occasionner des ruptures de l'activité.
• Se conformer avec les exigences réglementaires et légales.
• Supporter les objectifs métiers de l'entreprise.
• Réduire le risque de perte de Confidentialité, d'Intégrité et de Disponibilité de l'information, en définissant les principes pour l'usage et le traitement de l'information.

I.4. Etendu

La politique de sécurité informatique peut être organisationnel, ou individuel.
Les Politiques de sécurité de système d'information s'appliquent à:

- L'information dans toutes ses formes, résidente sur des serveurs, des PCs, des équipements réseaux ou autres, les bases de données, les documents personnels, dossiers et documents de travail.
- Toutes les applications, systèmes d'exploitation, progiciels et logiciels.
- Tous le matériel, serveurs, postes de travail, Laptops, composants du réseau, équipements de communication et périphériques possédés.
- Tous les sites hébergeant des informations et ses systèmes supports.
- Tous les employés permanents, contractuels et temporaires, consultants, fournisseurs et prestataire tiers.

I.5. Domaines d'application

Il est nécessaire de clairement identifier le cadre de la mise en œuvre de la politique de sécurité de système d'information. Est-elle applicable à l'ensemble du système d'information de l'organisme ? Est-elle applicable à l'extérieur de l'entreprise ?
Les champs d'application de la sécurité informatique:

- La sécurité physique (la sécurité au niveau des infrastructures matérielles)
- La sécurité personnelle
- La sécurité procédurale (audit de sécurité., procédures informatiques...)
- La sécurité des émissions physiques (écrans, câbles d'alimentation, courbes de consommation de courant...)
- La sécurité des systèmes d'exploitation
- La sécurité des communications

I.6. Quelques normes et standards utilisés

- Les principes directeurs qui sous-tendent la politique de sécurité peuvent être tirés des bonnes pratiques des normes internationales telles que :

- Norme internationale ISO 27002: Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information.
- Norme internationale ISO 27001: Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Exigences.
- Norme internationale ISO 27005: Techniques de sécurité – Gestion du risque en sécurité de l'information.

- L'utilisation d'une méthode ou une norme pour définir une politique de sécurité peut avoir des avantages et des inconvénients.

Les avantages :

- Gain en terme d'efficacité en réutilisant le savoir-faire transmis par la méthode. Capitalisation des expériences.
- Langage commun, référentiel d'actions structuration de la démarche, approche exhaustive.
- Etre associé à des groupes d'intérêts. Partage d'expériences, de documentation, formation possibles.

Les inconvénients :

- Bien qu'elles peuvent faire l'objet de révision (nouvelles versions), les normes ou méthode se n'évoluent pas au même rythme que les besoins ou les technologies.
- Une norme ou une méthode est générale. Il faut s'avoir la spécifier en fonction de besoins particuliers de l'organisation.
- Prolifération des méthodes : difficulté de choix.
- Disposer des compétences nécessaires. Efforts financiers, durée, coûts, difficultés à maitriser la démarche qui peut s'avérer lourde et nécessité des compétences externes. Recourt à des consultants spécialisés.

I.7. Types de politiques de sécurité

- Politique de sécurité du réseau informatique
- Politique de sécurité système d'exploitation
- Politique des mots de passe

I.8. Composantes d'une politique de sécurité

Les composantes d'une politique de sécurité sont :

Politique de sécurité	
Politique de contrôle d'accès	Gestion des identités, des profils utilisateurs, des permissions, des droits, etc.
Politique de protection	Prévention des intrusions et malveillances, gestion des vulnérabilités, dissuasion, etc.
Politique de réaction	Gestion des crises, des sinistres, des plans, de continuité, de reprise, de modification, d'intervention, de poursuite, etc.
Politique de suivi	Audit, évaluation, optimisation, contrôle, surveillance, etc.
Politique d'assurance	Politique de sensibilisation

II. mise en place une politique de sécurité informatique

1. Identifier les besoins en terme de sécurité, les risques informatiques et leurs éventuelles conséquences sur l'entreprise.

2. Elaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés.

3. Surveiller et détecter les vulnérabilités su système d'information et se tenir en compte des failles sur les applications et les matériels utilisés.

4. Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace.

II.1. Phase de définition 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. Elle comporte ainsi trois étapes : l'identification des besoins, l'analyse des risques, le choix de la méthode.

a) Identification des besoins :

La phase d'identification des besoins consiste dans un premier temps à faire l'inventaire du système d'information notamment pour les éléments suivants :

- Personnes et fonctions
- Matériels, serveurs et les services qu'il délivrent
- Cartographie du réseau (plan d'adressage, topologie physique, topologie logique, …)
- Liste des noms de domaines de l'entreprise
- Infrastructure de communication (routeurs, commutateurs, etc.)
- Données sensibles

b) Analyse des risques :

Le risque en terme de sécurité est généralement caractérisé par l'équation suivante :

$$Risque = \frac{Menace \times Vulnérabilité}{Contre - mesure}$$

Le menace « threat » représente le type d'action susceptible de nuire dans l'absolu. Tandis que la vulnérabilité « vulnerability » (faille) représente le niveau d'exposition face à la menace dans un contexte particulier. Enfin, la contre-mesure est l'ensemble des actions mises en œuvre en prévention de la menace.

L'étape d'analyse des risques consiste à représenter les différents risques encourus, d'estimer leur probabilité et enfin d'étudier leur impact.

La meilleure approche pour analyser l'impact d'une menace consiste à estimer le cout des dommages qu'elle causerait (par exemple attaque sur un serveur ou détérioration de données vitales pour l'entreprise).

Sur cette base, il peut être intéressant de dresser un tableau des risques et de leurs potentialités 'c.à.d. leurs probabilités de se produire) en leur affectant des niveaux échelonnés selon un barème à définir, par exemple :

Improbable : la menace n'a pas lieu d'être

Faible : la menace a peu de chance de se produire

Moyenne : la menace est réelle

Haute : la menace a de grande chance de se produire

c) Choix de la méthode :

Les méthodes sont réalisées par des grands utilisateurs de techniques de sécurité ou des groupes de travail, elles sont applicables par des prestataires de service sous forme d'audit de sécurité.

N.B : Un audit de sécurité (en anglais : Security Audit) consiste à s'appuyer sur un tiers de confiance (généralement une société spécialisée en sécurité informatique) afin de valider les moyens de protection mis en œuvre, au regard de la politique de sécurité.

Il existe de nombreuses méthodes permettant de mettre au point une politique de sécurité. Voici une liste exhaustive des principales méthodes :

- **MARION** (Méthodologie d'Analyse de Risque Informatique Orientée par Niveau)
- **MEHARI** (Méthode Harmonisée d'Analyse de Risque)
- **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)
- La **norme ISO-17799**

II.2. Phase d'élaboration des règles et des procédures

La phase de mise en œuvre : cette phase consiste à déployer des moyens et des dispositifs visant à sécuriser le système d'information ainsi et de faire les règles définies dans la politique de sécurité. Les principaux dispositifs permettant de sécuriser un réseau contre les intrusions sont les systèmes pare-feu.

Cependant ce type de dispositif ne protège pas la confidentialité de données circulant sur le réseau. Ainsi, la plupart de temps il est nécessaire de recouvrir à des applications complémentant les algorithmes de décryptage permettant de garantir la confidentialité des échanges.

On peut aussi mettre en place des tunnels sécurisés VPN qui permet d'obtenir un niveau de sécurité supplémentaire dont la mesure ou l'ensemble de communication est chiffré.

II.3. Phase de détection des incidents

Afin d'être complétement fiable, un système d'information sécurisé doit disposer les mesures permettant de détecter les incidents. Il existe ainsi les systèmes de détection d'intrusion IDS chargés de surveiller le réseau et capable de déclencher une alerte lorsqu'une requête est suspect ou non-conforme à la politique de sécurité.

La disposition de ces sondes et leur paramétrage doivent être soigneusement étudiés car ce type de dispositif est susceptible de générer des nombreuses fausses alertes.

II.3. Phase de réaction

Généralement c'est la phase la plus négligée dans un projet de sécurité informatique. Elle consiste à anticiper les évènements et à prévoir les mesures à prendre en cas de pépin. En effet, dans le cas d'une intrusion par exemple il est possible que l'admin de système réagisse selon des scénarios:

- Obtention de l'adresse de pirate et reposter.
- Distinction de l'alimentation de la machine.
- Débranchement de la machine de réseau.
- Réinstallation du système.