Politique de sécurité et conduite à tenir en cas d'attaque

Équipe Pédagogique Réseau Informatique @
UVCI 2018

Mai 2018
Version 1.0

Table des matières

Objectifs

A la fin de cette leçon, vous serez capable de :

- *Décrire* les étapes d'établissement d'une politique de sécurité
- *Énumérer* les bonnes pratiques en cas d'attaque et *Identifier* les erreurs à ne pas commettre.

Politique de sécurité

Objectifs

Décrire les étapes d'établissement d'une politique de sécurité

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 permettant d'assurer que les utilisateurs des dites ressources possèdent uniquement les droits qui leur ont été octroyés.

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. Ainsi, 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.

C'est la raison pour laquelle il est nécessaire de définir dans un premier temps une politique de sécurité.

1. Établir une politique de sécurité

Définition : 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.

Un tel document doit nécessairement être conduit comme un véritable projet associant des représentants des utilisateurs et conduit au plus haut niveau de la hiérarchie, afin qu'il soit accepté par tous. Lorsque la rédaction de la politique de sécurité est terminée, les clauses concernant le personnel doivent leur être communiquées, afin de donner à la politique de sécurité le maximum d'impact.

1.1. Principaux points de politique de sécurité

La procédure de sécurité tourne autour de 4 points principaux :

- Évaluation (de ce qu'on veut sécuriser)
- Protection
- Détection
- Réponse (ou reprise d'activité)

1.2. Étapes d'établissement d'une politique de sécurité

L'établissement d'une politique de sécurité se fait selon différentes étapes.

1.2.1. Étape 1 : Identifier ce qu'il faut protéger

La première étape est de bien identifier ce qu'il faut protéger : réseaux, ordinateurs, matériels, données.

Ensuite, il faudrait classifier les documents informatiques. Par exemple, on peut les classer avec les

termes « très secret », « Secret », « Confidentiel » et « Public ». Cette classification permet d'attribué un certain niveau de sécurité aux documents.

Certaines données classées Public doivent être éventuellement protégées soit de leur destruction, soit de leur altération.

Les postes seront classés en utilisant les termes suivants : Bastions (serveurs devant être hyper protégés), postes sensibles ou ordinateurs à accès libre.

1.2.2. Étape 2 : Analyser les risques

On analyse l'existant et on met en évidence les risques. Il faut pour cela évaluer l'impact de chaque événement sur le système et l'occurrence de celui.

1.2.3. Étape 3 : Évaluer les contraintes

Pour assurer la sécurité, on ne peut pas se permettre de faire n'importe quoi. Il faut tenir compte de plusieurs contraintes. Les principales sont l'existant (matériels, logiciels, personnel, locaux...), le budget et le temps. Par exemple, il n'est pas possible de se débarrasser de la plupart des logiciels sous prétexte qu'ils ne sont pas sur sans tenir compte du budget, du temps pour le changement...

Il est aussi important d'établir un budget de la sécurité en fonction des pertes qu'elle évite.

1.2.4. Étape 4 : Choisir les moyens

Il existe plusieurs techniques de base pour assurer la sécurité. Il faut faire un choix cohérent de ces techniques. Ces techniques se subdivisent en deux catégories :

1. *Les moyens de sécurisation*
   Ces moyens constituent l'élément clé de la sécurité. On peut citer :
   - Les techniques cryptographiques
   - La sécurisation des serveurs et des postes de travail
   - L'authentification des utilisateurs et des applications
   - Les raccordements aux réseaux locaux ou distants
   - Les routeurs
   - Les pare-feux
   - Les VPN
   - Les antivirus
   - Les politiques d'acquisition de matériels et de logiciels
   - Les politiques d'embauche et de classification...
2. *Les moyens de détection d'intrusion*
   Tous les moyens logiciels et matériels permettant de détecter toute intrusion dans le système.

1.2.5. Étape 5 : Adopter la politique de sécurité

Il faut enfin adopter une politique. Une mauvaise politique sera toujours préférable à pas du tout de politique. Il faut évidemment nommer un responsable.

1.2.6. Étape 6 : Tester

Après avoir adopté et mis en place une politique de sécurité, il faut s'assurer par un audit externe si celle-ci répond au cahier des charges.

Cela peut consister par exemple à réaliser des intrusions et de démontrer la résistance du système face à des scénarios de risque.

2. Niveaux de contrôle de la sécurité

Il existe différents niveaux de contrôle de la sécurité :

2.1. Niveau de la direction

Plus critique (documentation, rôles des responsabilités, gestion des configurations)

2.2. Niveau opérationnel

Concerne le contrôle des médias et les dispositions à prendre, la sécurité physique et des personnes, éducation et formation

2.3. Niveau technique

Concerne la gestion des sessions, des authentifications, identifications

3. Acteurs et avantages d'une politique de sécurité

3.1. Acteurs

Une politique de sécurité doit être mise en œuvre avec la participation du personnel clé de l'entreprise concerné, à savoir :

- Les membres de la direction générale
- Le personnel technique
- Le personnel juridique, éventuellement

La sécurité informatique de l'entreprise repose sur une bonne connaissance des règles par les employés, grâce à des actions de formation et de sensibilisation auprès des utilisateurs, mais elle doit aller au-delà et notamment couvrir les champs suivants :

- Un dispositif de sécurité physique et logique, adapté aux besoins de l'entreprise et aux usages des utilisateurs ;
- Une procédure de management des mises à jour ;
- Une stratégie de sauvegarde correctement planifiée ;
- Un plan de reprise après incident ;
- Un système documenté à jour

3.2. Avantages

Une politique de sécurité d'entreprise apporte les avantages suivants:

- Un cadre fonctionnel (« un cadre fonctionnel (« le voir comme un CPS ou ou un Texte de Loi») permettant d'implémenter des Procédures de sécurité dans l'infrastructure de réseau
- Un processus permettant l'audit de la sécurité
- une sécurité globale
- Une base pour toute action juridique éventuelle
- un processus permettant l'audit de la sécurité actuelle du réseau

4. Exercice

[Solution n°1 p 10]

Exercice : Question 1

Définir une politique de sécurité informatique consiste à :

- ◯ A) définir un algorithme cryptographique
- ◯ B) Renouveler tous les logiciels présentant des problème de sécurité
- ◯ C) Installer des anti-virus, des pare-feux et de nouveaux logiciels
- ◯ D) Concevoir un document de référence définissant les objectifs poursuivis en matière de sécurité et les moyens mis en œuvre pour les assurer.

Exercice : Question 2

Quelles sont les réponses qui resument dancs leur ensemble une procédure de sécurité informatique?

- ☐ A) Détection
- ☐ B) Vigilance
- ☐ C) Évaluation
- ☐ D) Protection
- ☐ E) Formation
- ☐ F) Reprise

Exercice : Question 3

A quel niveau de contrôle appartient le contrôle des règles d'utilisation de clés USB dans l'entreprise ?

- ◯ A) Niveau de la direction
- ◯ B) Niveau opérationnel
- ◯ C) Niveau technique
- ◯ D) Niveau informatique
- ◯ E) Niveau physique

Bonnes pratiques en cas d'attaque

Objectifs

- *Énumérer* les bonnes pratiques en cas d'attaque
- *Identifier* les erreurs à ne pas commettre

1. Conduite à tenir en cas d'incident

Exemple de problème

Problème : Votre entreprise est victime d'une intrusion. Que faire ?

1. Évaluer l'importance de l'incident et sa nature. Rassembler l'équipe anti-intrusion. Évaluer la solution de débrancher l'ordinateur du réseau concerné.

2. Constituer un dossier d'analyse (pouvant servir plus tard de preuves) et diagnostiquer le problème principalement en étudiant les journaux de bord.

Faire si possible une copie ou une sauvegarde du système infecté

3. Avertir les autorités, les utilisateurs, la direction

4. Réparer les systèmes et reprendre les activités

5. Évaluer les dommages et les coûts de l'incident. Documenter l'incident

6. Vérifier s'il n'est pas nécessaire de modifier les stratégies et les moyens de sécurité.

2. Les erreurs à ne pas commettre et prévoyance

2.1. Erreurs à ne pas commettre

1. Paniquer
2. Ne pas avoir de plan de réponse aux attaques
3. Résoudre le problème sans essayer de le comprendre.

2.2. Prévoyance

1. Constituer une équipe de réponse aux incidents
2. rassembler les informations nécessaires (par exemple les coordonnées du FAI)
3. Prévoir des check-lists pour diagnostiquer les problèmes
4. Prévoir un plan de reprise d'activité (sauvegarde...)

3. Exercice

[Solution n°2 p 10]

Citez trois mesures à exécuter si vous constatez que les comptes de plusieurs utilisateurs de votre entreprise ont été piratés :

- [ ] A) Limiter l'attaque (stopper l'attaque)
- [ ] B) Évaluer le coût de l'attaque
- [ ] C) Supprimer tous les comptes piratés
- [ ] D) Limiter la portée du dommage crée par l'attaque
- [ ] E) Informer les dirigeants
- [ ] F) Informer les clients affectés pour Changer les mots de passe et login sur tous les sites qu'ils utilisent.

4. Exercice

[Solution n°3 p 11]

En cas d'attaque d'un système, il faut immédiatement modifier la politique de sécurité et les moyens utilisés. Vrai ou Faux ?

- ◯ A) Vrai
- ◯ B) Faux

Solutions des exercices

> Solution n°1

Exercice p. 7

Question 1

- ○ A) définir un algorithme cryptographique
- ○ B) Renouveler tous les logiciels présentant des problème de sécurité
- ○ C) Installer des anti-virus, des pare-feux et de nouveaux logiciels
- ◉ D) Concevoir un document de référence définissant les objectifs poursuivis en matière de sécurité et les moyens mis en œuvre pour les assurer.

Question 2

- ☑ A) Détection
- ☐ B) Vigilance
- ☑ C) Évaluation
- ☑ D) Protection
- ☐ E) Formation
- ☑ F) Reprise

Question 3

- ○ A) Niveau de la direction
- ◉ B) Niveau opérationnel
- ○ C) Niveau technique
- ○ D) Niveau informatique
- ○ E) Niveau physique

> Solution n°2

Exercice p. 9

- ☑ A) Limiter l'attaque (stopper l'attaque)
- ☐ B) Évaluer le coût de l'attaque
- ☐ C) Supprimer tous les comptes piratés

☑ D) Limiter la portée du dommage crée par l'attaque

☐ E) Informer les dirigeants

☑ F) Informer les clients affectés pour Changer les mots de passe et login sur tous les sites qu'ils utilisent.

> Solution n°3

Exercice p. 9

○ A) Vrai

◉ B) Faux

Chercher à comprendre d'abord le problème avant de penser à changer de politique.