**Etude de cas 29/03/2017 - Réseaux, Systèmes et Menaces - EL IDRISSI Rahali**

ORINEL Gwendal

MINARET Alexandre

BERNARD Gary

## CAS N°3 : Politique de sécurité, analyse des risques et des menaces :

**Missions :**

### Partie I

#### Quels sont les avantages et les inconvénients relatifs à la création d’une politique de sécurité pour l’entreprise X. SA ?

**Avantage** :

* Analyser le problème de la sécurité info via une méthode connue ou reconnu (EBIOS)

**Inconvénients** :

* Conséquence de la sécurité. Le fait de lister les caractéristiques présupposé, la connaissance de toutes les attaques connus ou non. Cette politique sera donc cloisonnée à la connaissance actuelle du système d’information

**La définition de la politique de sécurité** permet de se concentrer sur le pourquoi de la sécurité avant de mettre en place les outils et permet de connaitre les enjeux et les aboutissements de sa mise en place et d’appréhender tous les domaines de la sécu informatique, organisationnel, humaine, juridique.

#### Votre Responsable de la sécurité de système d’information RSSI ne croit pas trop en une politique de sécurité. Comment justifiez-vous la mise en place de cette politique pour le bien de l’entreprise ainsi qu’à sa rentabilité ?

Une politique de sécurité est un outil de management permet de prendre des décisions ou non lors d’un processus de gestion, surtout en cas de crise, lorsque la PSSI sera en place celui-ci reflètera la criticité des risques et l’appréciation encouru. Les différents plan d’action permettront de se relevé plus rapidement d’un sinistre pour répondre à la demande des clients et fournisseurs. Tant qu’un sinistre n’est pas arrivé il est dur de quantifié le cout de cette sécurité Par conséquent il est très difficile de mesurer la rentabilité surtout au début. Mais la pérennisation de l’entreprise et donc la compétitivité sont deux caractéristiques tout aussi dures à chiffrer.

**Le cout de la valeur à protéger ne doit pas être supérieur à la perte de celui-ci**

#### Quelles sont les étapes primordiales d’un PSSI ?

1. Analyse de l’existant, évaluer la valeur à sécuriser, des besoins, des menaces et des vulnérabilités.
2. Appréciation et connaissances des risques
3. Lister les contraintes budgétaire, technique, managérial et juridique
4. Identifier les objectifs de la PSSI
5. Sensibilisation du personnel et responsabilisation, (social ingeenering)
6. Mise en place et maintenance des mesures la PSSI (matériel, logiciels, procédure)
7. Gestion de la PSSI (surveillance, exploitation, mise à jour)
8. Evaluation, audit et optimisation des mesures de sécurité mise en place (risque résiduel)
9. Veille technologique pour connaitre les nouvelles attaques et les nouveaux outils de défense

Des questions simples peuvent nous aider :

1. Que protéger de qui de quoi, pourquoi ?
2. Quelles sont les risques encourus ?
3. Criticité ?
4. Contraintes ?
5. Quelles sont les moyens en ma possession ou ceux que je dois investir ?
6. Comment les mettre en œuvre et les surveiller ?
7. Existe –il une faille résiduelle ?

### Partie II

#### Quels sont pour la filiale en question, les avantages et les inconvénients de l’externalisation de leur sécurité par rapport à une gestion interne

L’avantage de **l’outsourcing** réside dans le fait que les services sont gérés par des professionnels de la sécurité répondant à des certaines connaissances dans les domaines, de plus ces entreprises ont souvent des assurances permettant de rembourser de une entreprise lorsque les données sont perdues suite à une attaques. En revanche de nombreux inconvénients sont présents :

- La dépendance de l’entreprise qui fournit le service

- Des solutions pas forcément, processus et valeur de l’entreprise

- Employé interne moins sensibilisé

- Un SI moins maitrisé par les acteurs internes

#### Dans la PSSI proposé par l’entreprise externe, celle-ci a présenté un plan de secours et un plan de reprise. Définir ces termes et expliquer leur existence.

Les principaux critères de la sécurité sont :

Disponibilité, Intégrité, Confidentialité (DIC) Preuve (DICP)

Ces exigences sont aussi exprimées en haute disponibilité à savoir en combien de temps le système sera rétablie en cas de désastre. Les dispositifs de secours doivent être décidés lors de la mise en place de la PSSI afin de répondre à la disponibilité des ressources de l’entreprise pour garantir les ressources mêmes en cas de sinistre. Les critères les plus courants sont :

1. Mobilisation des ressources
2. Secours des équipements informatique et téléphonique
3. Les reprises de la production, traitement et logistique
4. La reprise des activités utilisateur, clients et fournisseurs
5. Dispositif post crise (attentat)

Un plan de reprise liste les différents processus mettre ne œuvre lors d’un sinistre pour priorisé les tâches et le niveau de criticité de chacun des évènements. Elle porte aussi bien sur l’infrastructure physique, matériel et logiciels de SI. De plus il permet d’avoir un tableau de bord sur les évènements identique et le choix de la meilleure solution pour la reprise de post-sinistre

#### Quelles sont les principales caractéristiques permettant de mesurer l’efficacité d’une politique de sécurité ?

La métrique de sécurité facilite la prise de décision et améliore les performances du SI, ces métrique sont des paramètres de référence dont les valeurs est un critère d’efficacité. Plusieurs contraintes sont associées, comme les lois, les règlementations ou encore des contraintes techniques. Voici les objectifs à atteindre avec les métriques :

1. Etablir un niveau de surveillance et une amélioration perpétuelle d’un PSSI
2. Justifier le budget lié à la mise en place d’une PSSI
3. Minimiser les problèmes techniques, par exemple avec une sensibilisation accrue
4. Contribué à la définition de niveaux de sécurité (critique, alerte, information, négligeable)

Ces métriques permettront d’avoir une base solide de notre SI, Que peut-on avoir avec ces objectifs :

1. Avoir des politiques de sécurité
2. Des procédures détaillées de sécurité
3. Implémenter ces procédures
4. Tester la conformité de ses procédures et les risques résiduels
5. Intégrer et mettre à jour ces procédures

### Partie III

#### Donner les définitions des 3 attaques citées et leurs traductions françaises

Les trois attaques sont :

Trojan Horse : Cheval de Troie d’apparence légitime conçu pour exécuter des actions à l’insu de l’utilisateur. En général il utilise les droit appartenant à son environnement pour détourner, diffuser, détruire des informations ou encore pour ouvrir une Backdoor. Les Trojans sont programmé pour être installé de manière invisible, notamment pour corrompre l’ordinateur hôte. La principale différence entre les virus, les vers, par rapport aux chevaux de trois, ce dernier ne se réplique pas.

Backdoor : Une porte dérobée est une fonctionnalité inconnue de l’utilisateur qui donne un accès secret au logiciel qui permet au pirate de prendre à distance le contrôle de l’ordinateur.

Keylogger : Enregistreur de frappes qui est un logiciel espion, ou un périphérique qui espionne électroniquement l’utilisateur. Le but de cet outil est varié il peut se présenter sous des aires de légitimité mais il ne peut être assuré qu’en espionnant l’intimité informatique de l’utilisateur.

#### Expliquer en quoi la prise à distance via Telnet n’est pas sécurisée. Proposer une autre solution à mettre en œuvre.

Le problème avec le protocole Telnet est la sécurisation, les données transit en clair, plus particulièrement l’authentification. Pour sécuriser le réseau il faudrait utiliser une solution de chiffrement donnée, connection par protocole ssh, vpn.

CAS N°4 : Norme en matière de sécurtié

Missions :

Partie I

1.

2.

3.

4.

Partie II

1.

2.

CAS N°6 : Faille et vulnerabilité au niveau des reseaux

Missions :

Partie I

1.

2.

Partie II

1.

2.

Partie III

1.

2.

Partie IV

1.

2.