Risque

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

Résumé

Une bonne compréhension du risque et l'application d'une méthodologie d'évaluation des risques sont les éléments indispensables à la mise en place d'une solution informatique sûre. Des analyses récentes ont montré qu'une majorité des responsables informatiques ne sont pas capables d'évaluer le degré d'exposition aux risques de leur solution informatique et encore moins d'évaluer financièrement le risque encouru. Le but de cette fiche est de donner une réponse aux questions suivantes :

> Qu'est ce qu'un risque en matière informatique ?
> Pourquoi la compréhension des risques est-elle si importante ?
> Quelles sont les méthodes communes d'évaluation des risques ?

Table des matières

1 La notion de risque en informatique

Le risque peut se résumer par l'équation suivante : **Risque = Vulnérabilité x Menace x Impact**, qui en détermine les composantes de base (ces composantes font l'objet d'une analyse détaillée au travers d'autres fiches).

- **Les « menaces »** désignent l'ensemble des éléments (généralement externes) pouvant atteindre les ressources informatiques d'une organisation.
- **Les « vulnérabilités »** expriment toutes les faiblesses des ressources informatiques qui pourraient être exploitées par des menaces, dans le but de les compromettre.
- **L'« impact »** est le résultat de l'exploitation d'une vulnérabilité par une menace et peut prendre différentes formes : perte financière, affectation de l'image de marque, perte de crédibilité...etc.

> La combinaison des ces trois facteurs fonde le «risque», qui permet notamment de mesurer l'impact financier et/ou la probabilité de survenance d'un évènement indésirable.
Le fait de calculer un risque doit permettre d'évaluer des évènements connus ou inconnus qui pourraient affecter l'intégrité des ressources informatiques d'une organisation, et en conséquence de trouver des contre-mesures.

2 L'importance de mesurer les risques

En ce qui concerne les systèmes informatiques, la mesure des risques et leur pondération sont importantes parce que ceci permet :

- **D'identifier des failles.**

Les failles sont identifiables au niveau des ressources informatiques (infrastructure, applications...) mais aussi au niveau organisationnel (politique de sécurité, processus, etc.). Parfois, l'évaluation des risques liés à un élément de l'architecture informatique permet de révéler des failles au niveau du traitement informatique global de l'organisation.

suite au verso

Risque

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

suite

D'evaluer la valeur des éléments informatiques.

Pour réaliser une évaluation des risques, il est nécessaire de procéder à la détermination de la valeur des différentes ressources informatiques. Les ressources informatiques présentant le plus d'intérêt devront être évaluées.

De donner des priorités de correction.

Afin de pouvoir gérer des priorités au niveau des mesures préventives, il est nécessaire d'avoir procédé à l'identification, à l'évaluation et à la comparaison des risques encourus au coeur de l'organisation.

D'élaborer des expertises.

L'application des méthodologies «standards» d'évaluation des risques permet de profiter de l'expérience d'experts informatiques et d'obtenir des conclusions à haute valeur ajoutée, surtout si l'on n'est pas un expert en ce domaine.

De définir une politique de sécurité adaptée.

Seule une évaluation détaillée des risques permet de donner une idée de l'exposition financière de la société et donc de mettre en place une solution de sécurité des systèmes d'information et de communication permettant d'afficher un retour sur investissement raisonnable.

3 Les «Ecoles»

En préliminaire il est nécessaire de définir clairement la différence entre un audit et une évaluation en matière de sécurité informatique :

L'évaluation ou «assessment» est une mesure de l'état de la sécurité informatique qui n'inclut pas nécessairement de comparaison par rapport aux standards ou aux obligations légales.

L'audit a pour but de positionner le niveau de la sécurité informatique par rapport à un standard ou par des exigences légales. Une des phases de l'audit pourra être un «assessment».

3.1 La vue des auditeurs

Les méthodes utilisées par les plus grands cabinets d'audit fournissent une multitude de «checklists» permettant de contrôler les systèmes d'information mais aussi la gestion globale de l'entreprise. Ces méthodes sont souvent orientées vers une comparaison avec les meilleures pratiques du métier (Best Business Practice). Les méthodes les plus répandues sont : COBIT (Control Objectifs for Information and related Technology), FISCAM (Federal Information System Controls Audit Manual), CISA (Computer Information Systems and Analyses).

3.2 La vue des informaticiens

La méthode utilisée en informatique est TBS (Time Based Security). Contrairement aux méthodes traditionnelles d'audit, cette méthode ne cherche pas à répondre à la question «Comment savoir où je me situe par rapport aux standards de mon métier ?», TBS vise à mesurer la résistance de la solution face aux attaques. Elle permet d'exprimer sous forme de «durée» la viabilité d'une solution mais aussi d'évaluer financièrement les pertes potentielles ou réelles.

4 La métrique des risques

4.1 Evaluation quantitative des risques :

Cette méthodologie vise à exprimer le risque en termes financiers et de fréquence.

Lorsque l'on mesure le risque de cette manière, il est possible de comparer l'évaluation financière des risques encourus avec le coût d'implémentation des méthodes de protection. On peut donc parler de l'évaluation du retour sur investissement (ROI = Return On Investment).

Cette méthodologie est basée sur la formule suivante :
Perte potentielle annuelle =
Valeur de l'élément exposé x Facteur d'exposition x Estimation de la fréquence annuelle de l'incident.

«La valeur de l'élément exposé» représente l'estimation financière de l'élément qui pourrait être touché par l'incident.

«Le facteur d'exposition» représente la partie de l'élément qui est exposée en cas de sinistre.

«La fréquence annuelle» est une estimation du nombre de fois où l'incident pourrait se produire sur base annuelle.

Cette méthode est surtout utilisée par les compagnies d'assurance et n'est pas vraiment adaptée à l'évaluation de risques informatiques. En effet cette évaluation est confrontée à la difficulté d'attribuer une valeur financière aux éléments de la solution informatique et l'absence de statistiques fiables quant à la fréquence des évènements.

Risque

suite

4.2 Evaluation qualitative des risques :

Cette méthode vise à identifier et évaluer les risques entre eux.

Cette méthodologie est basée sur la formule suivante :
Risque = Valeur de l'élément exposé x Indice de vulnérabilité x Menace.

« La valeur de l'élément exposé » en matière de risque informatique, il s'agit de la valeur souhaitée à protéger.

« L'indice de vulnérabilité » représente le niveau de vulnérabilité auquel l'élément est exposé. Dans le cas où des éléments de sécurité sont déjà en place cet indice sera donc le reflet de la vulnérabilité native pondéré par les mesures de protection déjà en place.

« La menace » est une estimation de nombre d'attaques auxquelles l'élément est exposé.

Dès le départ de cette évaluation il est défini une matrice reprenant les différentes combinaisons (Haut, Moyen, Bas) des composantes et exprimant leur résultat.

Exemple de matrice :

- Valeur HAUTE x Vulnérabilité HAUT x Menace HAUT = HAUT RISQUE
- Valeur HAUTE x Vulnérabilité MOYEN x Menace HAUT = HAUT RISQUE
- Valeur HAUTE x Vulnérabilité BAS x Menace HAUT = MOYEN RISQUE

4.3 Exemple d'évaluation :

Imaginons l'estimation du risque relatif de cet état de fait « Laisser de l'argent sur le sol dans un parc public ». La valeur de l'élément exposé est estimable puisqu'il s'agit de la somme abandonnée sur le sol dans un parc. La vulnérabilité est haute puisque l'endroit est visible et accessible à tous et toutes. La menace est grande puisque toute personne passant dans le parc pourrait s'en saisir.

Résultat :

- Valeur HAUTE x Vulnérabilité HAUT x Menace HAUT = HAUT RISQUE

5 La règle de Pareto

La règle des 80/20 est également applicable à la gestion des risques informatiques, elle revient alors à dire que 80% des risques peuvent être couverts par 20% des investissements nécessaires. Sachant que la sécurité des systèmes d'information et de communication sans failles n'existe pas, il est élémentaire d'appliquer ce principe qui pourrait être considéré comme une gestion « en bon père de famille ».

CASES,
pour plus de sécurité dans l'utilisation des systèmes d'information électroniques. Une initiative européenne soutenue par l'Etat luxembourgeois

OFFICE LUXEMBOURGEOIS D'ACCREDITATION ET DE SURVEILLANCE

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Economie et du Commerce extérieur