CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Gestion normalisée du risque de sécurité

Comment une méthode d'analyse de risque ou une norme internationale contribue effectivement à la mesure du préjudice (anticipé)

Pierre Dewez
Devoteam

SI – Le point de vue de la norme

« La Sécurité de l'Information » vise à protéger l'information contre une large gamme de menaces, de manière à garantir la continuité des transactions, à réduire le plus possible le risque et à optimiser le retour sur investissement ainsi que les opportunités en termes d'activité pour l'organisme. »

ISO/CEI 27002:2005, clause 0.1

Quelques référentiels

Tableau des différents référentiels utilisés en SI		
Orientation de l'approche	Meilleures pratiques / Méthodes	Normes (ex.)
Gestion des risques	**MEHARI** **EBIOS** **OCTAVE**	**ISO/CEI 27005:2008** ISO/FDIS 31000 IEC/FDIS 31010
Processus	ITIL	ISO/CEI 9001:2008 **ISO/CEI 27001:2005** ISO/CEI 13335-1:2004 ISO/CEI 20000-1:2005 **ISO/CEI 18044 :2004**
Contrôles / Mesures de protection	COBIT	**ISO/CEI 27002:2005** ISO/CEI 20000-2:2005
Produits		ISO/CEI 15408-1:2005

Historique du mot « Risque »

Risque provient du terme italien (Moyen âge) « risico » signifiant « rocher escarpé, écueil », utilisé pour désigner le péril couru en mer par les premières compagnies d'assurance.

Beucher, S., Reghezza, M., (2004)
Les risques (CAPES Agrégation), Éditions Bréal, Paris

Définition du risque SI

"La probabilité qu'une menace donnée tire parti des vulnérabilités d'un actif ou d'un groupe d'actifs et cause dès lors du tort à l'organisation."

NB: Il est mesuré en termes de combinaison de la probabilité d'un événement et de sa conséquence.

Source: ISO/CEI 27005:2008

Scientifiquement parlant …

« Le risque est l'espérance mathématique d'une fonction de probabilité d'événements. »

- En prédisant si une pièce de monnaie va tomber sur pile ou face en la lançant, on a un risque de 50% des chances de se tromper
- Par contre, en prédisant qu'en lançant la pièce un million de fois, 500 000 vont tomber sur face à +/- 1%, les risques d'erreurs sont presque zéro

Calcul de risque

Une question de statistiques …

Si l'on possède des données suffisantes sur les incidents de sécurité, on pourra :

- Prévoir les tendances
- Calculer les pertes et les risques résiduels
- Attribuer les ressources de sécurité à un ROI optimal

Par exemple, une enquête statistique nous apprend que 2% des employés fournissent un faux diplôme lors de l'embauche:

- L'entreprise de 10 000 employés déduit qu'elle a 200 cas à l'interne
- Mais ne peut pas dire qui…

Estimer le risque avec méthode

« L'analyse des risques est envisageable à différents degrés de détails, en fonction de la criticité des actifs, de la portée des vulnérabilités connues et des incidents précédemment survenus dans l'organisation. (…)

La méthode d'estimation peut être qualitative ou quantitative, ou une combinaison des celles-ci, en fonction des circonstances. »

ISO/IEC27005:2008, clause 8.2.2.1

L'approche qualitative

L'estimation qualitative utilise une échelle d'attributs qualificatifs pour décrire l'amplitude des conséquences possibles (par ex. faible, moyenne ou haute) et la probabilité que ces conséquences surviennent.

L'avantage majeur de l'estimation qualitative réside dans sa compréhension aisée par tous les membres du personnel d'une organisation alors que son inconvénient principal reste la dépendance au choix initial subjectif de l'échelle de qualification.

L'approche quantitative

L'estimation quantitative utilise une échelle de valeurs numériques (plutôt que des échelles descriptives) pour évaluer à les conséquences ainsi que la probabilité de leur survenance à l'aide de diverses sources de données.

La qualité de l'analyse dépend fortement de l'exactitude et de l'adéquation des valeurs numériques utilisées ainsi que de la validité des modèles utilisés.

La norme fournit-elle une réponse?

Selon, ISO/CEI 27005:2008 :

- Identifier les actifs
  - Leur attribuer une **valeur**
    - ✓ Sur base d'une analyse d'impact

ISO 27005 n'est cependant pas une méthode. Le standard précise les grandes étapes d'une gestion des risques dans décrire le « comment ».

Et du côté des méthodes ?

Les 3 principales méthodes d'analyse de risques des TI qui peuvent s'articuler avec le standard ISO 27005:

- MEHARI
- EBIOS
- OCTAVE

Ces méthodes proposent toutes de mesurer le risque sur base d'une évaluation des actifs à protéger qui peuvent présenter des vulnérabilités exploitables par des menaces … mais …

Les limites

Si ces méthodes diffèrent dans leur approche, elles sont toutes 3 plutôt orientées sur l'évaluation qualitative des actifs et des conséquences possibles sur ceux-ci plutôt que sur la mesure quantitative de ces éléments.

En ce sens, elles ne répondent pas aisément à la question:

« Combien dois-je dépenser pour me protéger efficacement? »

Alors, que faire ?

Construire un cadre référentiel général (ex. ISO 27005)

Utiliser une méthode de support pour l'analyse (ex. MEHARI, EBIOS, OCTAVE, …) et l'évaluation qualitative.

Utiliser une ou plusieurs méthodes d'évaluation quantitative basée(s) sur les données de l'organisation (méthodes de modélisation comme T-Map, ALE, ROSI, ISRAM, …)