ITIL et la sécurité

Compte rendu d'une rencontre autour d'un verre

rapporté par Roger Kirschwing

Le 17 septembre dernier, Eric Glace, Consultant et chargé d'affaires chez Telindus France, nous a fait un retour d'expérience dans ce domaine, lors d'une rencontre Adeli « Autour d'un verre ».

Présentations

M. Eric Glace cumule une expérience de 16 ans dans le monde de l'informatique, soit 14 ans chez un Grand Compte où il a été Directeur de la Production et Directeur des Infrastructures et de la Sécurité. Depuis 2 ans chez Telindus, spécialiste du marché des services réseaux et sécurité, il développe au sein de la Direction Conseil France une offre autour des problématiques liées au Datacenter[1] et au management de la continuité d'activités.

Aujourd'hui, Telindus regroupe près de 3 000 collaborateurs en Europe dont 600 en France pour un chiffre d'affaires de 700 millions d'Euros.

Préambule

En préambule, il faut prendre en compte la nouvelle vision de la direction générale des entreprises quant à la Direction des Systèmes d'Information (DSI). La DSI, vue auparavant comme un centre de coûts, est reconnue aujourd'hui comme un contributeur à la performance globale de l'entreprise.

Dans le cadre de cette nouvelle approche, la DSI se positionne comme fournisseur de services au profit de l'entreprise. Si l'entreprise maîtrise ses processus et si la DSI s'appuie sur ITIL, alors on peut d'autant plus dire que la DSI apporte de la valeur à l'entreprise.

En plus d'être un fournisseur interne de services, la DSI se positionne de plus en plus comme un fournisseur externe de services. Ce qui permet à l'entreprise de faire partager son système d'information à ses clients. Le fait d'ouvrir le système d'information à l'extérieur implique encore d'avantage la DSI dans la problématique du risque.

En conclusion, la nouvelle gouvernance porte sur l'entreprise, sur le système d'information et sur les risques. Le management des risques est donc au cœur de la stratégie de l'entreprise.

Les principaux acteurs impliqués dans ce changement sont la Direction Générale qui est en charge de la stratégie de l'entreprise, la DSI qui assure le maintien opérationnel du système d'information et le RSSI (Responsable de la Sécurité des Systèmes d'Information) qui est un peu le « gardien du temple ». Tous ces acteurs utilisent des approches et des méthodes différentes, qui peuvent être CobIT pour la DG, ITIL pour la DSI et la série des normes ISO 27000 pour le RSSI.

Positionnement d'ITIL par rapport à la sécurité

En rapport avec le thème développé ce soir, se pose la question du positionnement d'ITIL par rapport à la Sécurité.

Le challenge du DSI est de concilier les pressions de réduction de ses coûts opérationnels, d'exploitation, d'évolution, de maintenance avec les pressions du métier qui demande que le système d'information soit encore plus performant, disponible et sécurisé.

Bien que les coûts matériels soient en baisse constante, la DSI se doit de porter l'effort sur les processus pour atteindre son objectif de réduction des coûts. Ces derniers doivent être définis, implémentés, supportés et contrôlés. La DSI se doit d'engager une dynamique d'amélioration des processus.
ITIL permet à la DSI d'optimiser sa production donc de réduire ses coûts, de réduire le taux de pannes et de rendre le système d'information plus performant.

À ce stade, quels sont les principaux risques qui pèsent sur une DSI ?

Il est possible d'évoquer 7 risques majeurs qui sont le respect de la CNIL, l'atteinte à la vie privée du collaborateur, les atteintes en provenance de l'intérieur comme de l'extérieur (virus, attaques, …), la continuité du service (disponibilité, performance et continuité d'activité) et enfin la perte, le vol et la divulgation des données.

En conclusion, lorsque la DSI formalise ses processus, notamment ceux pris en compte par ITIL, elle minimise ses risques opérationnels. D'autre part, l'utilisation d'ITIL permet à tous les acteurs d'avoir le même vocabulaire pour communiquer mieux et plus.

[1] *Datacenter : salle d'hébergement spécialisée*

L''enjeu de la sécurité selon ITIL, c'est de placer la sécurité au niveau de chaque processus, la « sécurité est partout ».

Exemples d'intervention

M. Eric Glace présente un premier exemple personnel d'intervention au sein d'une entreprise pour un besoin de sécurisation de la messagerie :

- société du CAC 40, 3 000 utilisateurs, messagerie en architecture redondante, hautement sécurisée, systèmes de sauvegarde exemplaires, maintenance fournisseurs 24/24, maintenance préventive, meilleures solutions en termes d'antivirus, d'antispam, etc.
- 4 incidents bloquants dont 3 dus à des interventions planifiées (nettoyage de la base de données suite à une attaque de virus, intervention suite à une défaillance du système de sauvegarde, réorganisation des droits d'accès) et un incident du à une règle de redirection de message (de la messagerie d'entreprise vers une messagerie personnelle qui s'est avérée être pleine d'où des messages d'erreur en retour créant un déni de service).

La cartographie des risques se décompose en :
- risques majeurs pour 5% : destruction de l'immeuble, incendie salle machine etc.
- défaillance technique pour 35% : d'un élément technique comme un disque dur, un routeur, un composant de stockage etc.
- autre type de défaillance pour 60%, défaillance logicielle, erreur d'exploitation, erreur d'un collaborateur, virus, attaque etc.

Constat sur l'exemple précédent : l'ensemble des incidents bloquants survenus fait partie des défaillances à 60% alors que les moyens (organisation, processus, procédures, instructions…) mis en œuvre ne sont pas calibrés par rapport aux risques potentiels.

M. Eric Glace présente un deuxième exemple personnel d'intervention au sein d'une entreprise pour un besoin de continuité d'activité :
- PME de 200 utilisateurs,
- toutes les meilleures solutions en termes de sécurité du système d'information sont mises en place,
- le RSSI a défini les enjeux de besoins de continuité avec les différents métiers de l'entreprise (aval DG, aval Directions métier etc.),
- cependant, le plan de continuité d'activités (PCA) est dans une impasse, impossible à mettre en œuvre.

Il n'existe pas de processus d'industrialisation et de simplification du SI :
- pas de cartographie matérielle et logicielle,
- pas de gestion du parc existant,
- en conséquence la gestion évolutive du parc est inexistante,
- pas de stratégie de simplification, parc étonnement hétérogène,
- pas de pilotage, pas de tableaux de bord,
- aucun contrôle opérationnel,
- donc pas de retour opérationnel,
- etc.

Constat sur cet exemple : le système d'information existant n'est pas « PCA enable » c'est à dire n'est pas en état de faire partie ou de supporter une solution de continuité.

La **conclusion** suite à ces deux exemples, est qu'il faut :
- adapter les moyens face aux risques,
- ne pas oublier que la technologie ne répond qu'à une partie du problème,
- ne pas négliger le triptyque technologie, organisation, juridique,
- mettre en place les bonnes pratiques et les normes, en particulier ITIL,
- que chaque acteur de l'entreprise doit être moteur dans l'application de ces bonnes pratiques,
- et enfin, se mettre dans une dynamique de progression et d'amélioration, par exemple sur une trajectoire à 3 ans.

Questions-réponses

M. Eric Glace répond aux questions de l'auditoire.

Quelle est la place du RSSI dans l'entreprise, dans la DSI ?

Cela dépend avant tout de la maturité de l'entreprise : selon le cas, il peut ne pas y avoir de RSSI, le RSSI peut être intégré dans la DSI, ou être en dehors de la DSI.
S'il est positionné en dehors de la DSI, hiérarchiquement proche de la DG, alors il participe au management global des risques de l'entreprise.
Et dans certaines entreprises, il faut aussi tenir compte du positionnement du RSSI par rapport au Risk Manager (Gestionnaire des Risques).

Quelle est l'évolution de la prise en compte des risques ?

Cette évolution est constatée par la presse : l'actualité aide les entreprises à réfléchir. Au minimum se pose la question de sauvegarder les bases clients et comptables, ainsi que la question des données sensibles etc.

Quel est l'apport d'ITIL à la sécurité ?

ITIL doit être envisagé comme étant au service de la Sécurité. L'apport minimal est que le vocabulaire

commun permet de décloisonner les métiers. Et les deux acteurs principaux, que sont le DSI et le RSSI se comprendront mieux.

Y a-t-il des particularités dans la gestion des incidents de sécurité ?

Il faut au préalable un accord entre la DSI et le RSSI. D'autre part, il faut gérer la difficulté de qualification de l'incident : relève-t-il de la sécurité ou non ? Tous les critères habituels sont utiles pour effectuer cette classification. Cependant, le focus sécurité ou le niveau de granularité doit avoir été défini entre la DSI et le RSSI. Il ne faut pas oublier qu'à la base, c'est un incident qui a perturbé le bon fonctionnement du SI.

Quel est l'apport de la nouvelle version d'ITIL ?

Les apports de la version 3 par rapport à la version 2 sont limités. La version 3 apporte des conseils sur la stratégie dans l'amélioration constante ce qui est un plus pour la communauté des RSSI. Ainsi, elle adopte une dynamique d'amélioration des processus ce qui est nouveau par rapport à la version précédente. De ce fait, elle est plus souple pour prendre en compte la stratégie de sécurité. ITIL renforce la qualité dans l'entreprise.
Le RSSI doit s'approprier la sécurité de l'entreprise. Au cœur de l'entreprise, il doit avoir une démarche de terrain, voir les techniciens, parler avec tout le monde.
Il a un rôle de sensibilisation du personnel quant aux risques.
Pourquoi ne pas instaurer un « permis de conduire » pour toute personne qui pilote son poste de travail ?

Quels sont les enjeux de la sécurité ou comment définir une politique ?

Dans ce cas, nous sommes en amont d'ITIL qui n'a que des préoccupations opérationnelles. ITIL ne peut donner que des recommandations sur la sécurité. Pour définir une politique d'entreprise, il faut s'appuyer sur une analyse de risques selon des démarches et méthodes disponibles sur le marché (Mehari, ISO 17799 etc.). Ensuite seulement, la politique élaborée pourra être déclinée selon ITIL.

Quels critères pour un Système d'Information « PCA enable » ?

Tout d'abord, il faut que le système primaire soit maîtrisé avant de s'attaquer à un système secondaire. Le niveau de maturité d'ITIL doit être pris en compte. Les tableaux de bord donnent également une bonne idée du niveau de maîtrise.

Autres remarques.

En tant que support, sécurité & gestion d'infrastructure, c'est à dire Sécurité et ITIL, doivent répondre aux exigences du métier, c'est leur point commun. La différence porte sur la disponibilié. ITIL parle de disponibilité du service, alors qu'en termes de sécurité la disponibilité est celle des informations.
À cela, ajoutons le fait que les exigences de disponibilité, de confidentialité et d'intégrité des données (optique sécurité) peuvent conditionner la gestion de la disponibilité du service (Processus ITIL). Il y a donc un point de jonction majeur entre Sécurité et ITIL.
La sécurité est mise en place par rapport aux besoins d'information, la disponibilité du service par rapport aux informations. La Sécurité répond par rapport au métier alors qu'ITIL le fait par rapport au service.

ITIL permet de rapprocher les hommes des études de ceux de la production. Grâce à ITIL, la production reprend le pas sur les études et redevient le « Nerf de la guerre ».

La sécurité doit être intégrée à la Qualité.▲

eric.glace@telindus.fr
roger.kirschwing@adeli.org