

EDITO

AGENDA

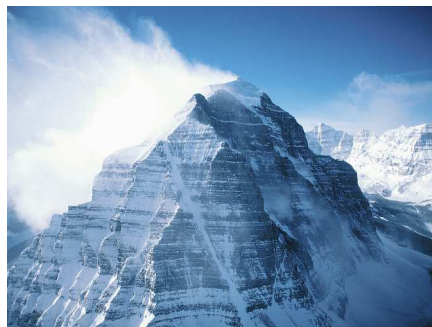
ACTUALITES P2

L'ESSENTIEL P3

Comment choisir un bon mot de passe ?

ZOOM P5

ITIL et la sécurité



EDITORIAL

Noël est à peine là qu'il s'éloigne, et déjà 2006 n'est plus... Au milieu des bulles de champagne, voici qu'arrive 2007 et ses bonnes résolutions : « C'est promis, je verrouillerai mon PC quand j'irai prendre mon café ! » ou « j'arrête de fumer, c'est décidé ! ».

Vous les avez déjà toutes entendues (et peut-être même suivies ?), alors prenez le temps de lire cette newsletter qui vous permettra peut être de choisir les bonnes. Nous commencerons par nous intéresser à la clé de voûte de tout système de sécurité : le mot de passe. En effet, sous ce nom commun et banal se cache la plupart du temps la vulnérabilité de tous nos systèmes d'information. Malgré l'utilisation de systèmes de chiffrement de plus en plus perfectionnés, les fonctions de sécurité s'effondrent si les clés qui les protègent ne sont pas suffisamment robustes. Nous vous proposons donc ici un petit rappel utile sur les mots de passe, notamment comment les générer. Mais rappelez-vous, rien ne sert d'avoir un mot de passe complexe si c'est pour l'écrire sur un post-it collé sur l'écran de son ordinateur !

Nous aborderons ensuite ITIL (Information Technology Infrastructure Library), le guide des bonnes pratiques pour la gestion des Systèmes d'Information, en nous attardant plus particulièrement sur la partie sécurité. Cela vous donnera un aperçu des points clés de cette méthodologie sans vous obliger à lire les 44 volumes la composant.

Bonne lecture et bonnes fêtes de fin d'année à tous.

AGENDA - Sélection début d'année 2007

⇒ Le CLUSIF présente MEHARI 2007 - Paris - 10 janvier 2007

Le CLUSIF présentera la nouvelle version de MEHARI, la Méthode Harmonisée d'Analyse de Risque.

Plus d'infos : <http://www.clusif.asso.fr/>

⇒ Mobile World Congress TV2007 - Paris - Hôtel Saint Jacques - Du mardi 23 janvier 2007 au vendredi 26 janvier 2007

Tutoriels techniques consacrés aux services et contenus de la télévision sur téléphone mobile. Des experts présenteront les tendances, les enjeux et les promesses de cette nouvelle technologie. Au programme : les processus de standardisation, les modèles économiques existants et les contenus.

Plus d'infos : <http://www.upperside.fr/>

⇒ Business Online Expo - CNIT de la Défense - Paris La Défense - 30-31 janvier 2007

Toutes les solutions de communication et de commerce en ligne.

Plus d'infos : <http://www.businessonline.fr/>

⇒ Networkers 2007 - Palais des Festivals de Cannes (06) - France - 30 janvier au 2 février 2007

C'est l'événement annuel Cisco, la plus importante des conférences dans l'industrie des réseaux. Le thème de cette année est : « The Network as the Platform »

Plus d'infos : <http://www.cisco.com/web/FR/events/networkers/index.html>



Directeur de la publication :
Edouard Jeanson

Agence ESEC
Sogeti Infrastructures Services
6-8 rue Duret
75016 Paris - France
Tél : 33 (0)1 58 44 55 66

Société par Actions Simplifiée au
capital de 15 999 790 euros
RCS Paris 479 942 583

Edition du 26 décembre 2006



ACTUALITES

Vos pas sont comptés par... vos chaussures de sport !

L'idée est originale : fournir les données qu'un coureur a besoin de connaître pour chacune de ses excursions. Un fournisseur international d'articles de sport et le créateur du baladeur numérique se sont associés dans un produit 'high-tech' permettant au sportif équipé de connaître principalement les informations météorologiques, les calories brûlées, la distance parcourue et à quelle vitesse.

Comment ? Un système ingénieux constitué d'un capteur sans fil installé dans les chaussures de course est connecté à un baladeur numérique.

Et à toute idée louable, il y a les limites qui alertent immédiatement tout défenseur des libertés personnelles.

Commercialiser outre-Atlantique, ce produit reçoit de vives critiques concernant la traçabilité des personnes. Equipées d'une puce RFID d'une portée de 20 mètres, ces chaussures peuvent en dire davantage que leur fonction initiale. Une démonstration de l'université de Washington a mis en évidence les dérives inopportunes par la conception d'un système d'interception relié à Google Maps avec un budget de 250 dollars [1].

De l'autre côté de l'atlantique, et notamment en France, la question de la libre circulation des personnes sera très certainement un 'droit de douane' à clarifier pour la vente de ce type d'article.

Pour en savoir plus :

http://www2.canoe.com/techno/nouvelles/arc_hives/2006/12/20061214-121323.html

[1] http://www.cs.washington.edu/research/sy_stems/nikeipod/tracker-paper.pdf



Un ver dans les contacts MySpace ?

Un ver baptisé JS.Qspace s'est propagé sur le site de MySpace.com depuis décembre, exploitant ainsi une vulnérabilité du service communautaire.

Ce ver s'en prend aux contacts des internautes en reproduisant leur espace personnel et a pour objectif de récupérer leur email et leur mot de passe.

Considéré comme non dangereux par les experts, ce code malicieux s'exécute sur le poste client et se propage en utilisant les contacts de l'internaute. C'est sous la forme d'une vidéo corrompue que le ver installe des liens vers de faux sites dans l'espace et tente de se propager.

Après la contamination du webmail de

Yahoo un peu plus tôt, et maintenant avec celle de MySpace, ce sont donc les applications web qui sont la cible des pirates. Le Web 2.0 n'a décidément pas fini de faire parler de lui...

Pour en savoir plus :

<http://www.01net.com/editorial/335676/secure/ite-des-pirates-s-en-prennent-a-la-communaute-myspace/>



Les achats en ligne

Avec les fêtes de fin d'année, c'est l'éternel problème des cadeaux, auquel s'ajoute le stress de ne pas trouver le produit de son choix, l'attente dans les magasins surchauffés... Mais depuis la démocratisation d'Internet, fini la queue dans les grands magasins, place aux achats en ligne depuis son canapé !

Qui n'a jamais acheté en ligne ? Aujourd'hui plus d'un français sur quatre achète ses billets de théâtre ou de cinéma en quelques clicks sur Internet.

Quelques règles de base sont toutefois à respecter face à certaines indécidités de nos fournisseurs.

L'une d'elle consiste à bien vérifier le contenu de son panier avant de régler ses achats car certains sites n'hésitent pas à inclure des assurances ou autres produits à votre commande. Dans la majorité des situations, c'est à vous de ne pas les inclure, tout simplement en décochant les articles.

Attention à vos achats en dehors de nos

frontières, pensez à vérifier si les montants indiqués incluent les divers taxes et droits de douane.

Une brochure mise en place par le Forum des Droits sur Internet (FDI) récapitule vos droits et les recours dont vous disposez. N'hésitez pas à la consulter.

Pour en savoir plus :

<http://www.01net.com/editorial/335793/e-commerce/rappels-utiles-pour-les-achats-de-noel-sur-internet/>
http://www.foruminternet.org/telechargement/documents/guide_cyberconso_2007.pdf



L'ESSENTIEL

➔ COMMENT CHOISIR UN BON MOT DE PASSE ?

Choisir un code secret n'est pas toujours chose aisée : il faut choisir un mémo qui soit facile à retenir et qui soit suffisamment complexe pour qu'il ne puisse pas être trouvé ou déduit par un individu malveillant. Alors comment estimer qu'un mot de passe est efficace ?

Pour répondre à cette interrogation, nous allons présenter, en nous aidant des mathématiques, les erreurs les plus courantes commises lors du choix de mot de passe, puis proposer plusieurs méthodes permettant de générer des codes robustes.

📁 Le stockage des mots de passe

Dans un premier temps, il est nécessaire de présenter rapidement comment sont stockés les mots de passe dans les systèmes informatiques.

Un principe élémentaire : une fois le mot de passe défini par l'utilisateur, l'application ne doit pas le stocker en clair. Celle-ci en calcule une empreinte (aussi appelée « hash ») qu'elle stocke dans un fichier ou en base de données.

De cette façon, les personnes pouvant accéder à la version hachée du mot de passe, notamment l'administrateur, ne peuvent savoir quelle est sa valeur en claire, choisie par l'utilisateur.

Pour cela, le recours à une fonction de hachage est requis ; celle-ci génère une empreinte unique à partir de la chaîne de caractères (mot de passe) qui lui est fournie. Pour être efficace, cette fonction doit avoir les propriétés suivantes :

- 'Mixing-transformation' : quelque soit la chaîne en entrée, l'empreinte n'est pas différenciable d'une chaîne aléatoire.
- 'Collision resistance' : il est impossible de trouver deux chaînes différentes fournissant la même empreinte.
- 'Pre-image resistance' : étant donné une empreinte, il est impossible de trouver une chaîne donnant cette empreinte (dans un temps humainement raisonnable).

On utilisera typiquement des fonctions telles que MD5 ou SHA1, parfois assorties d'un complément aléatoire (appelé « sel »).

Lorsqu'une personne essaie de s'authentifier, l'application calcule l'empreinte du mot de passe proposé et la compare à la version stockée. Les deux empreintes identiques signifient : accès autorisé.

Supposons qu'une personne mal intentionnée entre en possession de ces empreintes et cherche à trouver le mot de passe d'un utilisateur.

En raison des propriétés des fonctions de hachage, la seule possibilité est d'essayer tous les mots de passe possibles, jusqu'à l'obtention du 'hash identique'. Afin de diminuer le temps de recherche, l'attaquant commencera par tester les cas les plus probables.

Pour faire face à une telle attaque, un test préalable de la résistance logique du mot de passe est nécessaire.

Le postulat de base est le suivant : l'attaquant a recours à un système lui permettant de calculer et de tester 10^5 empreintes par seconde ; cette valeur est raisonnable dans le cas de l'utilisation d'un ordinateur personnel avec un outil de « cassage de mot de passe » courant, calculant des empreintes SHA1.

📁 Les erreurs à ne pas commettre dans le choix de mot de passe

Rappel de base : ne pas utiliser d'informations personnelles comme le nom, le prénom, l'adresse, etc. Ces éléments sont simples à trouver, et ne constituent pas un mot de passe fiable.

La première erreur classique est l'utilisation d'un code d'accès dérivé de l'identifiant.

Les modifications effectuées peuvent être simples (voire même pas de modification du tout), ou plus complexes par l'ajout d'un ou deux chiffres (ou de caractères spéciaux) avant ou après l'identifiant, ajout d'une majuscule dans le login, etc.

Ces mots de passe semblent généralement forts grâce à l'utilisation de minuscules, de majuscules, de chiffres et de caractères spéciaux.

Pourtant les transformations utilisées sont généralement identifiées ; il est donc facile de toutes les tester.

A partir d'un identifiant, ces transformations classiques vont permettre de générer au plus quelques milliers de mots de passe possibles.

Sur notre système, l'attaquant testera ces combinaisons en $10^3/10^5$ sec = 0.01 seconde. Un mot de passe basé sur le login, même s'il semble fort, sera donc trouvé en un temps négligeable.

Une autre erreur classique est d'utiliser une courte suite de lettres aléatoires et de la dupliquer pour constituer le mot de passe.

Par exemple, pour obtenir un mot de passe de 10 lettres, on utilisera la chaîne 'adfth', ce qui donnera le mot de passe 'adfthadfth'. Ce mot de passe peut sembler aléatoire et donc fort ; en fait, il n'existe que 26^5 mots de passe de ce type, ce qui permet de tester l'ensemble de ce type de chaîne en 2 minutes environ. Le constat est d'ailleurs identique en utilisant une chaîne alphanumérique.

Une troisième erreur classique est un code d'accès composé uniquement de chiffres. Par exemple, on utilisera un code, une date de naissance comme valeur secrète.

Or même relativement long, ce type de mot de passe n'est pas robuste : il existe 10^N mots de passe de ce type de longueur N ; pour tester l'intégralité des mots de passe de longueur inférieure ou égale à N, il faut donc tester $10^N + 10^{(N-1)} + \dots + 10$ mots de passe. Pour une longueur de 8 caractères, il faudra compter environ 18 minutes. Il est donc possible de tester rapidement l'ensemble de ces mots de passe.

De la même manière, on pourrait étendre ces tests afin de vérifier si les valeurs correspondent à un numéro de téléphone. Si l'on considère qu'un mot de passe est un code à 8 chiffres avec un préfixe (01, 02, 03, 04, 05 ou 06), il faudra tester au maximum 6×10^8 possibilités, soit un temps de 100 minutes pour parcourir l'ensemble. Il est donc facile de tester l'ensemble de ces mots de passe potentiels.

Une méthode utilisée également pour générer un mot de passe consiste à créer une variation sur un mot du dictionnaire, à savoir des termes usuels pratiqués aussi bien en français qu'en anglais, les prénoms, les noms de marque, les noms des dieux dans les différentes mythologies, etc.

On applique alors sur ce mot choisi comme base, une ou plusieurs variations telles que :

- ajout d'un ou deux chiffres (ou de caractères spéciaux) avant le mot ;
- ajout d'un ou deux chiffres (ou de caractères spéciaux) après le mot ;
- ajout d'un chiffre (ou d'un caractère spécial) avant et d'un autre après le mot ;

- ajout d'une majuscule au début du mot ;
- miroir d'un mot ;
- doublement d'un mot ;
- conversion d'une ou plusieurs lettres en chiffres (o -> 0, l -> 1, e -> 3, e -> €, etc) ;
- suppression des voyelles ;
- etc.

Cette méthode est très souvent utilisée, consciemment ou non, afin de générer des mots de passe complexes, qui seront considérés comme forts par la politique de sécurité de l'entreprise.

Pour autant, il est relativement simple de trouver des dictionnaires contenant les mots les plus couramment utilisés, et de les tester, ainsi que leurs déclinaisons.

Même avec un dictionnaire de grande taille et de nombreuses variations, l'ensemble des possibilités sera testé en quelques heures.

Malgré leur apparence, ces mots de passe ne sont donc pas forts.

Les méthodes de génération de mots de passe

Revenons à notre attaquant : si aucune des méthodes ci-dessus n'a abouti, il ne reste plus qu'à tester tous les mots de passe possibles. Il s'agit en quelque sorte de la dernière chance, et seuls les plus courts pourront être trouvés de cette manière.

Mais en dessous de quelle taille minimale un code secret est-il considéré comme court ?

Si l'on considère un code de longueur inférieur ou égal à n, composé de caractères pris dans un alphabet de cardinal N, le nombre de possibilités à tester est de $N^n + N^{(n-1)} + \dots + N = N \times (1 - N^n) / (1 - N)$ (suite géométrique de raison N et de premier terme N).

L'alphabet sera de cardinal 26 dans le cas de mots de passe alphabétiques, de cardinal 36 pour les mots de passe alphanumériques, de cardinal 75 si l'on inclut les caractères spéciaux, et enfin, de cardinal 101 en ajoutant les majuscules.

On obtient les temps suivants pour tester l'ensemble des mots de passe, en considérant un système unique capable de calculer 10^5 empreintes par seconde (cf tableau ci-après).

Ainsi établi, le cardinal de l'alphabet est un facteur très important : son efficacité est comparable à celle d'un code composé d'un ou de plusieurs caractères supplémentaires.

Ce tableau permet de définir des limites pour un mot de passe suffisamment

		Cardinal de l'alphabet			
		26	36	75	101
Longueur du mot de passe	3	<1 s	<1 s	4 s	10 s
	4	5 s	17 s	5 min	18 min
	5	2 min	10 min	7 h	30 h
	6	54 min	6 h	21 jours	124 jours
	7	23 h	9 jours	4 ans	34 ans
	8	25 jours	336 jours	322 ans	35 siècles
	9	654 jours	33 ans	241 siècles	3 500 siècles
	10	47 ans	12 siècles	1 808 millénaires	35 353 millénaires

résistant : il faudra au moins 9 caractères dans le cas d'un mot de passe alphabétique (minuscules), et seulement 6 caractères si l'on utilise minuscules, majuscules, chiffres et caractères spéciaux.

Un bon mot de passe doit donc à la fois ne pas appartenir aux catégories précédemment évoquées, et être de longueur suffisante (cases vertes dans le tableau). Même si ces calculs ont été effectués en se basant sur une méthode particulière d'attaque, les résultats concernant la solidité restent valables de manière générale.

Quant à la mémorisation par l'individu de ce code, ceci est une autre composante à ne pas négliger côté utilisateur.

Nous avons mentionné que la plupart des méthodes mnémotechniques utilisées aboutissent à des mots de passe faibles. Se souvenir d'une valeur purement aléatoire n'est pas toujours aisé (surtout si son usage n'est pas quotidien). Et il est tout aussi déconseillé d'utiliser un mot de passe faible que d'en utiliser un fort et de le noter (post-it, PDA, etc) par crainte de l'oublier.

Donc, voici quelques méthodes permettant de créer et mémoriser facilement un mot de passe fort :

- Utilisation des premières lettres : à partir d'une phrase facile à retenir (vers connu, réplique d'un film, publicité, etc), on gardera la première lettre de chaque mot (en évitant de n'utiliser que des minuscules). Le vers « Je suis belle, ô mortels ! comme un rêve de pierre » donnera le mot de passe : Js b,Om!c1r2p
- Utilisation des sons : une variation de la méthode précédente consiste à utiliser les sons : Js8bl,omt!

Il faut, de plus, respecter un certain nombre de règles concernant la gestion des mots de passe :

- Côté administrateur: pensez à vos utilisateurs.
Une politique de sécurité trop forte nuit à la sécurité : forcer un mot de passe de 12 caractères devant être changé tous les mois et interdisant la réutilisation des 20 derniers mots de passe incitera beaucoup d'utilisateurs à simplement inscrire celui-ci sur un post-it ...
- Encore pour les administrateurs : lors de la création d'un compte sur un service quelconque, créez le compte avec un mot de passe fort, et si possible forcez les utilisateurs à changer de mot de passe à la première connexion.
Sans cela, beaucoup gardent le mot de passe initial, parfois identique au login ...
- Côté utilisateurs: utilisez des mots de passe différents pour les différents services. Le nombre de services accessibles à un attaquant sera plus restreint si par hasard il découvre l'un de vos mots de passe.
- Pour les administrateurs et les utilisateurs : changez de mot de passe régulièrement, car aucun n'a une durée infinie. Selon le matériel et les méthodes utilisées, les durées de vie d'un code secret peuvent être notablement différentes.
- Enfin, nul n'est à l'abri d'une divulgation : qui n'a jamais entré son mot de passe à la place de son login par erreur ?

Conclusion

La qualité d'un mot de passe doit résulter d'un subtil équilibre entre l'obligation de solidité (cassable en un temps très long), et la lisibilité (mémorisation possible sans devoir le noter sur papier). Le facteur humain est donc déterminant.

Pour cela, une sensibilisation des utilisateurs (et même des administrateurs !) s'avère souvent payante, si on l'associe à une politique de sécurité rigoureuse mais compréhensible de tous.

ZOOM

⇒ ITIL (Information Technology Infrastructure Library) et la sécurité

Dans le monde du management des systèmes d'information, ITIL est souvent cité en référence pour la gestion de l'informatique orientée services. Moins connue, la gestion de la sécurité fait partie des 44 volumes de recommandations. En voici un aperçu.

📁 Rappel sur ITIL

ITIL est un référentiel de recommandations et de bonnes pratiques, dont le nom signifie "Information Technology Infrastructure Library".

Appliqué dans de nombreuses organisations, il met en phase le système d'information (SI) avec les besoins métier, par une approche fonctionnelle orientée services.

Le référentiel est constitué de huit blocs comme la fourniture des services, la gestion de l'infrastructure ou la gestion des applications. Ils définissent les objectifs, les fonctions, les entrées et les sorties de nombreux processus que l'on trouve dans la gestion d'un SI, en décrivant les principes, et non la méthodologie.

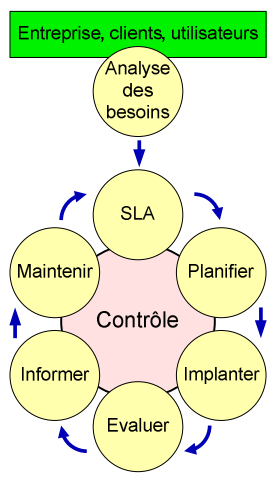
La gestion de la sécurité est l'un de ces blocs, dont nous présentons ici un aperçu.

📁 La sécurité dans ITIL

ITIL traite de la sécurité d'un point de vue "fournisseur de services" (**le département informatique**) par rapport à un client (**l'entreprise, le client, l'utilisateur**). Il aborde l'organisation de la sécurité nécessaire à la fourniture du service à l'entreprise. En particulier, ITIL décrit la façon de mettre en place des critères de sécurité, qui seront définis dans un Contrat de Service Informatique.

La sécurité y est définie comme un cycle de gestion (et d'amélioration) de la Politique de Sécurité. **Il s'applique à tous les secteurs de la gestion de service**, dont la gestion de la disponibilité et la continuité de service.

La première phase du cycle traite de l'expression des besoins des clients du SI au travers d'une analyse de risques. Puis on détermine la faisabilité des demandes des clients en les comparant aux critères de sécurité en place.



Cycle de gestion et d'amélioration de la politique de sécurité

Le client et le département informatique définissent ensuite un accord de niveau de service (SLA - Service Level Agreement), qui inclut les critères de sécurité mesurables, définit leurs seuils acceptables et la façon de vérifier s'ils sont atteints.

Puis ils définissent les niveaux de service opérationnels (OLA - Operational Level Agreement) qui spécifient comment les services de sécurité seront fournis par le département informatique.

Viennent alors les phases de mise en place et d'évaluation des niveaux de service. Les clients reçoivent ainsi des rapports réguliers sur l'état et l'efficacité des services de sécurité fournis.

Par la suite, des décisions sont prises pour faire évoluer les SLA en fonction des retours d'information obtenus.

Et le cycle redémarre.

Les Accords de Niveaux de Service "SLA"

La bonne définition des SLA est un facteur clé pour la réussite du processus Sécurité dans ITIL.

Un SLA est un document écrit, détaillant les critères de performance, les indicateurs à mesurer et les niveaux de service attendus.

En termes de sécurité, on peut y trouver:

- Les moyens d'accès autorisés au SI,
- Les accords sur les audits et les traces,
- Les mesures de sécurité physique,
- La formation des utilisateurs à la sécurité et la vigilance,
- Les procédures d'autorisation pour les droits d'accès,
- Les accords sur le reporting et les enquêtes sur les incidents de sécurité,
- Les rapports et audits attendus.

Exemples de SLAs :

- Insertion de la gestion des patches de sécurité dans le cadre existant de la gestion des changements.
- Gestion spécifique des incidents de sécurité, et des seuils d'escalade, dans le cadre de la gestion globale des incidents. Et plus particulièrement, la gestion des incidents de sécurité majeurs.
- Définition des données d'audits et rapports, en particulier dans le cas d'une sécurité externalisée. Définition de leurs fréquences (réguliers / ponctuels sur incident) et leur profondeur. Accords sur les logs et les incidents communiqués.
- Gestion des relations avec les CERT (incidents, déclarations, ... etc). Définition d'un responsable CERT identifié, surveillant les alertes et déclenchant des alertes internes sur les avis CERT concernant le client.

Autres documents de sécurité

Outre les accords de niveaux de service et de niveaux opérationnels, d'autres documents sont définis dans ITIL:

- *La politique de sécurité informatique:*
Elle doit provenir des instances de direction de la sécurité, et doit contenir:
 - o Les objectifs et le périmètre de la sécurité de l'information pour le client ;



o Les buts et les principes de management de la sécurité de l'information ;

o La définition des rôles et des responsabilités.

• *Le plan de sécurité informatique:*

Il décrit comment la Politique de Sécurité est déclinée pour le SI de chaque entité.

• *La documentation sécurité sur le terrain:*

Ce sont les procédures nécessaires aux actions de sécurité quotidiennes, donnant des détails sur le contenu des tâches de sécurité.

 **Points positifs**

• Trop souvent la sécurité est perçue comme un centre de coûts et une contrainte. La mise en place de SLAs sécurité clairs permet de sortir la sécurité d'une situation de centre de coût vers une situation en phase avec les besoins métiers.

• Déployer ITIL pousse à documenter ses processus et méthodes d'une façon standardisée (comme les SLAs et OLAs), ce qui facilite les audits à venir. Ceci peut aider une entreprise à mesurer l'efficacité de son organisation sécurité, et à mieux se

conformer aux contraintes réglementaires, par exemple SOX.

• ITIL permet de structurer plus clairement les tâches de sécurité, sur la base de "bonnes pratiques". Ceci permet d'organiser le travail des équipes sécurité, et de passer d'un mode de travail "pompiers" à une approche plus structurée et mieux planifiée.

• De par son organisation cyclique, la gestion ITIL de la sécurité permet le maintien à niveau des mesures de sécurité face à l'évolution des demandes, des environnements et des menaces.

• ITIL développe un langage compris par les entités management et métier, et sort les équipes sécurité du jargon technique. Ce langage commun permet au management de mieux comprendre en quoi la sécurité est un composant clé dans le bon fonctionnement du SI.

 **Limites**

• ITIL ne donne pas de détails sur les niveaux de service (SLA) et les indicateurs clés (KPIs) à mettre en place. Il définit un cadre, et laisse chaque entreprise adapter ses processus pour les intégrer à ITIL.

En cela, ITIL peut être assez déroutant, car les recommandations n'indiquent pas de détails de mise en place. Il décrit "quoi" faire, mais pas "comment".

• ITIL ne prétend pas décrire tous les processus nécessaires au fonctionnement de l'informatique de l'entreprise. Il s'occupe principalement du management des services courants. La gestion de la sécurité peut donc sembler moins développée que la gestion des changements, incidents, ... etc.

• De nombreux utilisateurs d'ITIL le considèrent comme une norme, un cadre cohérent, alors que ce n'est qu'un référentiel de bonnes pratiques. En cela, ce point est le reflet du besoin des utilisateurs d'être guidés par une norme ... qu'il faudra trouver ailleurs.

• Pour mettre en œuvre la gestion de la sécurité, il faut avoir mis en place une bonne partie des modules ITIL: gestion des configurations, des changements, des incidents, ... car la sécurité est transversale à plusieurs de ces domaines.

Conclusion

ITIL peut avantageusement remplacer les processus "maison" par des processus standardisés, basés sur des bonnes pratiques éprouvées. Bien que cela nécessite du temps et des efforts, ITIL peut améliorer la façon dont une organisation gère la sécurité de son information.

Pour beaucoup d'entreprises, la mise en place réussie d'ITIL nécessitera des changements en matière d'organisation, et de culture, et également, l'implication et l'engagement de ses intervenants.

Les facteurs de succès sont, entre autres:

- Un engagement poussé du management et une implication dans la mise en place d'ITIL,
- Une approche par phases,
- La formation approfondie des équipes et leur management,
- La possibilité de rendre suffisamment visibles les gains en qualité et la réduction des coûts,
- L'utilisation d'outils logiciels d'organisation ITIL.

Il faut cependant garder à l'esprit qu'ITIL est un cadre dont le contenu doit être fourni par les processus de l'entreprise.

Pour vous inscrire à la newsletter, veuillez envoyer un mail à newsletter-subscribe@esec.fr et pour vous désabonner, veuillez envoyer un email à newsletter-unsubscribe@esec.fr

Conformément à la loi « Informatique et libertés » du 6 janvier 1978, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent. Si vous souhaitez exercer ce droit et obtenir communication des informations vous concernant, veuillez vous adresser au directeur de l'agence ESEC