PUBLIC RESEARCH CENTRE HENRI TUDOR

« La protection des données personnelles : défis, enjeux et limites »

La responsabilité des entreprises face aux nouvelles technologies de communication électronique.

Mercredi 25 mai 2011

PUBLIC RESEARCH CENTRE HENRI TUDOR

Workshop N°2 : "La sécurisation des données : exemples de bonnes pratiques"

Responsabilité des dirigeants d'entreprises en matière de sécurité de l'information et de protection du patrimoine informationnel et intellectuel

M. Frédéric Girard,

Information Security Project Leader, CRP Henri Tudor

Sécurité de l'information et responsabilité des Dirigeants

La responsabilité de la sécurité de l'information sous l'angle :

- La responsabilité à l'intérieur de l'entreprise (versus externe, légale, etc.)
- La responsabilité dans les projets de sécurité
- La responsabilité dans l'approche et l'ouverture culturelle

But : participer au succès de la mise en place des protections

- De son information
- De son patrimoine informationnel
- De sa propriété intellectuelle

Conséquence : performance + confiance = business

Ce sont des prérogatives de Dirigeant.

- Le dirigeant est un acteur à part entière de la sécurité de l'information !

Le dirigeant et ses responsabilités

- **Une fonction clé : donner le GO**
- **Une fonction de guidance : désigner la CIBLE**

- **Développer les affaires : gardien du patrimoine**
- **Responsabilité : en interne comme à l'externe**
- **Sponsors**

→ **Vrai dans l'entreprise**

→ **Particulièrement vrai pour la sécurité de l'information de l'entreprise**

La réalité du dirigeant face à la sécurité de l'information

- Quelques évidences pour les Dirigeants ?
  - L'outil informatique est critique : sans lui je ne travaille pas
  - L'information est critique : mal gérée elle empêche mon développement
  - L'organisation est critique : mal organisé, certaines solutions deviennent hors de portée

- Réflexes ….spontanés ou réfléchis …
  - J'achète un outil, On externalise, Pas Prioritaire , Jusque là tout va bien !….

=> Il y a besoin d'adéquation entre le Dirigeant et la sécurité de l'information

Adéquation Dirigeants et sécurité de l'information

Intégrer "le profil du dirigeant" dans le design des solutions, permet de faire émerger des méthodes et des pratiques nouvelles, avec des concepts ou des outils pas forcément récents.

Intégrer les critères directeurs qui apparaissent en filigrane dans la suite de la présentation permet d'améliorer la communication entre l'exécutif et les projets de sécurité de l'information ainsi que leur performance

Solutions de sécurité : 1 - CONTEXTE

Des dirigeants peu convaincus, qui doutent, qui cherchent.

Des besoins, mais ils font peur.

Par où commencer ?

L'utile et l'inutile ?

Des entreprises qui fonctionnent :

- **Des entreprises déjà actives**
- **Avec des mesures en place**
- **Du personnel compétent**

Solutions de sécurité : 2 - APPROCHE

Le travail se fait AVEC l'entreprise

- Entretiens ciblés, débriefing sur le fond, analyses croisées, étapes suivantes

On VISUALISE des éléments factuels CONNEXES à la sécurité

- Organisation, Stratégie, gestion de projets, accompagnement, systèmes de gestion

La SENSIBILISATION apporte

- La prise de conscience (lien biens/enjeux)
- Un recadrage par rapport aux besoins (utile/inutile)

On pousse l'analyse au-delà des simples constatations

- Aide à la DECISION
- Viser des résultats rapides, ajustés, pertinents

Solutions de sécurité : 3 - RESULTATS

L'entreprise réactive qui s'initie à la pro-activité

- Un apport organisationnel pour préparer le futur

L'entreprise tient une position mais elle doit évoluer

- Elle doit trouver son BON chemin
- Elle doit se développer à la BONNE vitesse pour absorber le changement et préparer le futur

La sécurité de l'information

- Intégrée au contexte
- Inscrite dans le temps (durable)
- Mise au service des métiers

→ une opportunité pour la PME ?

Illustration de "bonnes pratiques" à travers deux Services-exemples

1. Une évaluation flash de la sécurité de l'information et de son organisation au sein d'un organisme

2. La Politique de Sécurité de l'Information de l'organisme

D'une évaluation flash à la mise en place d’une politique de sécurité

Une posture de départ

- Rester centré sur le besoin : "*Nous avons besoin de…*"
- Pas de concession aux fondamentaux
- Pas de concession à la qualité
- "*Seulement*", s'appuyer sur les outils
- Utiliser LEURS ressources pour s'adapter

Dès lors, la sécurité peut évoluer vers une approche nouvelle

- Agilité vs blocs
- En suivant "*les besoins*" et non "*parce qu'il faut*"
- Raisonner en terme de combinaison d'ingrédients plus qu'en terme de produits ou services COTS (Commercial Off-The-Shelf)

Une évaluation, une Politique : Deux outils, un but

But pour l'entreprise : Rendre l'activité plus sûre

- L'information est l'Actif N°1
- Criticité et effet de seuil

L' Evaluation de la maturité : "Le repère pour bien commencer"

- Sensibiliser le dirigeant et son responsable IT à l'importance de la sécurité
- En peu de temps, Identifier les axes de progrès
- Recommander la démarche adaptée au contexte

La Politique de sécurité : "Affirmer son engagement"

- Accompagner les dirigeants à formaliser le "Que dois-je faire ? Comment le faire ?"
- Adresser les bonnes cibles, le strict nécessaire
- Communiquer un plan de travail
- Diffuser un document de référence

EVALUATION DE LA MATURITÉ DE LA SÉCURITÉ DE L'INFORMATION:
L'outil et sa contribution dans l'entreprise

Approche par les PROCESSUS METIER

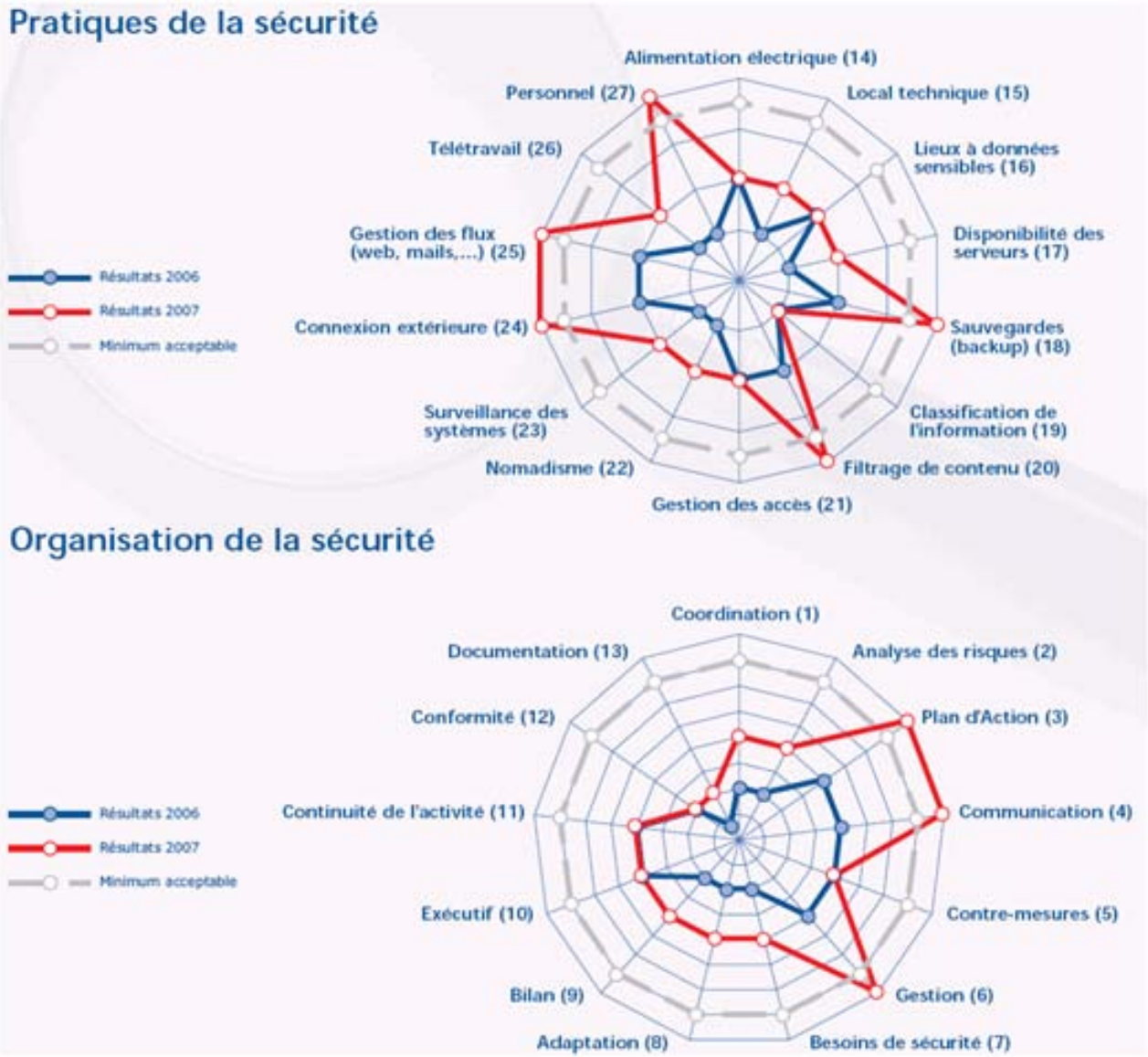
Outil basé sur les normes en vigueur

Deux sessions de travail qui permettent de :

- ***Sensibiliser*** **du DIRIGEANT et de son responsable informatique à l'importance de sécuriser son patrimoine informationnel**
- ***Visualiser*** **l'état courant de la sécurité de l'information: *Comment mon entreprise fonctionne ?"Quel est mon niveau ?"***
- ***Disposer*** **d'une analyse pragmatique pondérée sur le contexte de l'entreprise**
- ***Recommander*** **la démarche la plus adaptée pour lancer la démarche d'entreprise.**
  "dois-je faire ? Comment prendre une décision ?"

Démarrer et obtenir des résultats concrets utiles et rapidement

Résultats visuels



ACCOMPAGNEMENT A LA DEFINITION DE LA POLITIQUE DE SECURITE :
L'outil et sa contribution dans l'entreprise

Approche par les REGLES DE SECURITE (et les normes en vigueur)

Sessions de travail pour définir la première PSI de l'entreprise, c'est :

- **Sensibiliser et impliquer le DIRIGEANT et son responsable associé**
- **Analyser et construire le "Comment mon entreprise doit fonctionner !"**
- **Décider "A quel niveau ?"**
- **Adresser des acteurs précisément : "Pour Qui ? Comment ?"**
- **Elaborer un plan d'actions à**
  - **Court terme en vue de résultats rapides**
  - **Long terme en vue d'un dispositif d'amélioration continue**

Organiser les règles de sécurité

Communiquer, affirmer et gagner en maturité

Des éléments, outils, services complémentaires

D'autres outils

- Systèmes de management
- Analyses de risque

les nouvelles approches

- Partir sur un aspect précis, puis progresser en tâche d'huile
- Ouvrir l'approche technologique en intégrant d'autres aspects :
  - Organisationnel,
  - Communication,
  - Écrit
  - Humain
  - Culturel,
  - etc

La sécurité de l'information permet à une organisation :

1. **Assumer la responsabilité finale** de protection de l'information du périmètre de l'organisation

2. **Demander aux équipes** de permettre d'assumer cette responsabilité

3. **Affecter des moyens** pour obtenir une sécurité effective

4. **Favoriser un management et un contrôle** efficace et mature de ses systèmes

5. **S'engager** et le faire savoir (courage, volonté, vision)

La sécurité de l'information est un vecteur pour favoriser dans l'entreprise :

- **Vision :** elle comprend que les affaires professionnelles, aujourd'hui, intègrent de fait la sécurité de l'information, à fortiori demain !

- **Entreprenariat :** elle utilise les nouveaux moyens et approches innovants offerts par le domaine de la sécurité de l'information pour développer son organisation et donc ses affaires !

- **Tranquillité :** le niveau de maîtrise et de réflexion apporté par le domaine de la sécurité de l'information, aide le Dirigeant, son organisation et leurs affaires, à entrer dans le futur.