

# Utilisation de MEHARI chez ORSID

**Contexte ORSID**

**Organisation sécurité**

**Manager la sécurité**

**Caractéristiques MEHARI**

**Utilisation et perspectives**

**Conclusions**

Olivier Corbier

10 janvier 2007

# Contexte ORSID (1) - L'entreprise

- **Entreprise**
  - 450 personnes, 42 M€ de CA
  - 6 sites : 4 sur Paris/RP, 2 en province
  - staff technique de 70 personnes (dév., sys., rés.)
- **Activité éditique et archivage**
  - documents de gestion (factures, payes, états comptables, relevés, ...)
  - 650 millions de pages imprimées
  - 300 millions de pages archivées
  - clientèle grands comptes

## Contexte ORSID (2) - Contraintes

- Internes
  - existant (hommes, matériel, processus)
  - faible disponibilité
  - organisation décentralisée (= une certaine hétérogénéité)
- Externes
  - typologie des applications
  - contraintes réglementaires (Bâle II, SoX, LSF, PCI, CCLRF ...), et contractuelles (risque opérationnel)
- Structurelles
  - politique sécurité « groupe »
  - s'appuyer sur un (des) référentiel connu (et reconnu), partagé avec nos clients

## Contexte ORSID (3) – Les fondations

- Très forte implication de la Direction
  - Très forte culture service (+turn-over très faible du personnel cadre)
  - Certification ISO9001
  - Maîtrise de notre SI
    - développements internes
    - pas d'infogérance
    - s'appuyer sur des standards
  - Structure de coordination technique
  - 1 site de délestage et de backup
- Fondements sains

# Organisation de la sécurité

- Historique

- 2000 : éveil lié à l'utilisation d'internet
- 2002 : cellule d'expertise et de support (rôle consultatif, administration des outils de sécurité)
- 2004 : formalisation et promotion de la politique sécurité (organisation, charte, comités, ...)
- 2005 : Premiers tests PCA
- 2006 : mise en place d'un management de la sécurité (objectifs : contrôles, plans d'action, mesurer, ...)

Décisionnel	comité sécurité (DG+RSSI+DAF+DT+DQ)
Pilotage	RSSI + comité technique + RLS
Opérationnel	comité adminres + cellule expertise/supervision

# Manager la sécurité (1)

- S'améliorer
  - définir et constater les points d'amélioration
  - ne pas refaire les mêmes choses (capitaliser)
  - efficacité : réactivité (outils) et délégation (cadre)
- Etablir des plans d'action
  - justifier, organiser, prioriser
  - intégrer dans des projets (charge, budget, exploitation)
- Gestion du changement
  - architecture / application
  - veille (vulnérabilités, réglementaire)
  - évolutions des besoins de sécurité

# Manager la sécurité

- Sensibiliser / Former
  - garantie de la sécurité dans les **processus**
  - informer, responsabiliser
  - induire un comportement (déductif, inductif, et ... intuitif !)
- Auditer (« consulter » )
  - support de **sensibilisation** : contrôle **ET vecteur**
  - plans d'action concertés (**appropriation** de la sécurité par les opérationnels)
  - ne pas se limiter aux contre-mesures, mais intégrer les enjeux (besoins de sécurité -> ressources critiques)
  - **périmètre**
    - la bonne personne
    - le bon format (durée, fréquence, ...)
    - les bonnes questions (et les bonnes réponses !)

## Pourquoi MEHARI – « a priori »

- Analyse de risques
  - notions de besoins de sécurité/menaces/contre-mesures en cohérence, connectées, **harmonisées**
- Contexte institutionnel
  - CLUSIF
  - français
- La base de connaissance
  - diagnostic intégrant :
    - des notions de robustesse et de mise sous contrôle
    - cotation avec effet de « seuil »
  - couverture fonctionnelle (et complétude)
  - automatismes (calculs)
  - intégration dans outil « maison »

## MEHARI – « a fortiori »

- Modèle (dans toute son acception)
  - représentation schématisée d'un système complexe
  - référence (à imiter)
  - système de référence (pour se situer)
- Conduite d'audit
  - définition du périmètre (empirique si sans ... **analyse**)
  - schéma d'audit
- Analyse des enjeux
  - lutter contre la subjectivité
  - « expliquer » la classification
  - intégrer à la sensibilisation
- Pertinence des plans d'action
  - en intégrant (obligatoirement) les impacts intrinsèques

# Utilisation de MEHARI

- Base de connaissance... étendue
  - liens avec la documentation interne
  - affectation des responsabilités PSSI
  - liens avec référentiels spécifiques client
- Enregistrement des audits dans une BdD
  - daté : historique, péremption
  - schéma d'audit « dynamiques » dans le cadre de nouveaux projets client (utilisation de plusieurs sites de production par exemple, ou utilisation de « briques » particulières)
  - analyse de risques « systématisée »
- Outil intranet
  - appropriation (du modèle) par les opérationnels

# Perspectives

- Liaison avec gestion de projets (pour les projets spécifiques sécurité)
- Simulation et PA « proactifs »
- Auto-diagnostic
- Utilisation du scoring ISO17799 dans un cadre commercial (questionnaires de pré-audit)
- Intégration dans l'offre commerciale (strictement sur un périmètre ORSID)
- Base d'une future démarche ISO27001

# Conclusions (1)

- Ne pas se limiter au diagnostic
  - PA peu « efficaces »
  - PA incomplets car « confus »
  - travail de titan !
- L'analyse des enjeux est
  - la garanti de PA optimisés et motivés
  - un des piliers de la sensibilisation (et donc de la prévention)
- Bâtir la sécurité = démarche dans la durée
  - différents niveaux d'appropriation
  - outil vivant

## Conclusions (2)

- Enorme pouvoir pédagogique de la méthode
- Outil fondamental d'aide à la décision

→ **Complicquée** ?

**Complexe**, reflet du sujet qu'elle entend traiter

→ **Exhaustive** ?

Ou plutôt **complète**, ce qui est gage de qualité

→ **Rigide** ?

Diversité des **démarches** proposées

→ **Inadaptée** ?

Oui, si pas de **management** de la sécurité

→ **Théorique** ?

**Rationnelle**, indispensable par exemple pour résoudre les nombreuses contradictions (apparentes)

« Il faut créer l'action, parce que l'action crée le mouvement, et que le mouvement entraîne les individus. » (*Christian le Guillochet*)

## **MAIS ATTENTION**

« Ne jamais confondre mouvement et action »  
(*Ernest Hemingway*)

## **CAR**

« Celui qui n'a pas d'objectifs ne risque pas de les atteindre » (*Sun Tzu*)