



GROUPE HISI

LES ENJEUX DE LA SECURITE DE VOTRE SYSTEME IBM i et DES DONNEES



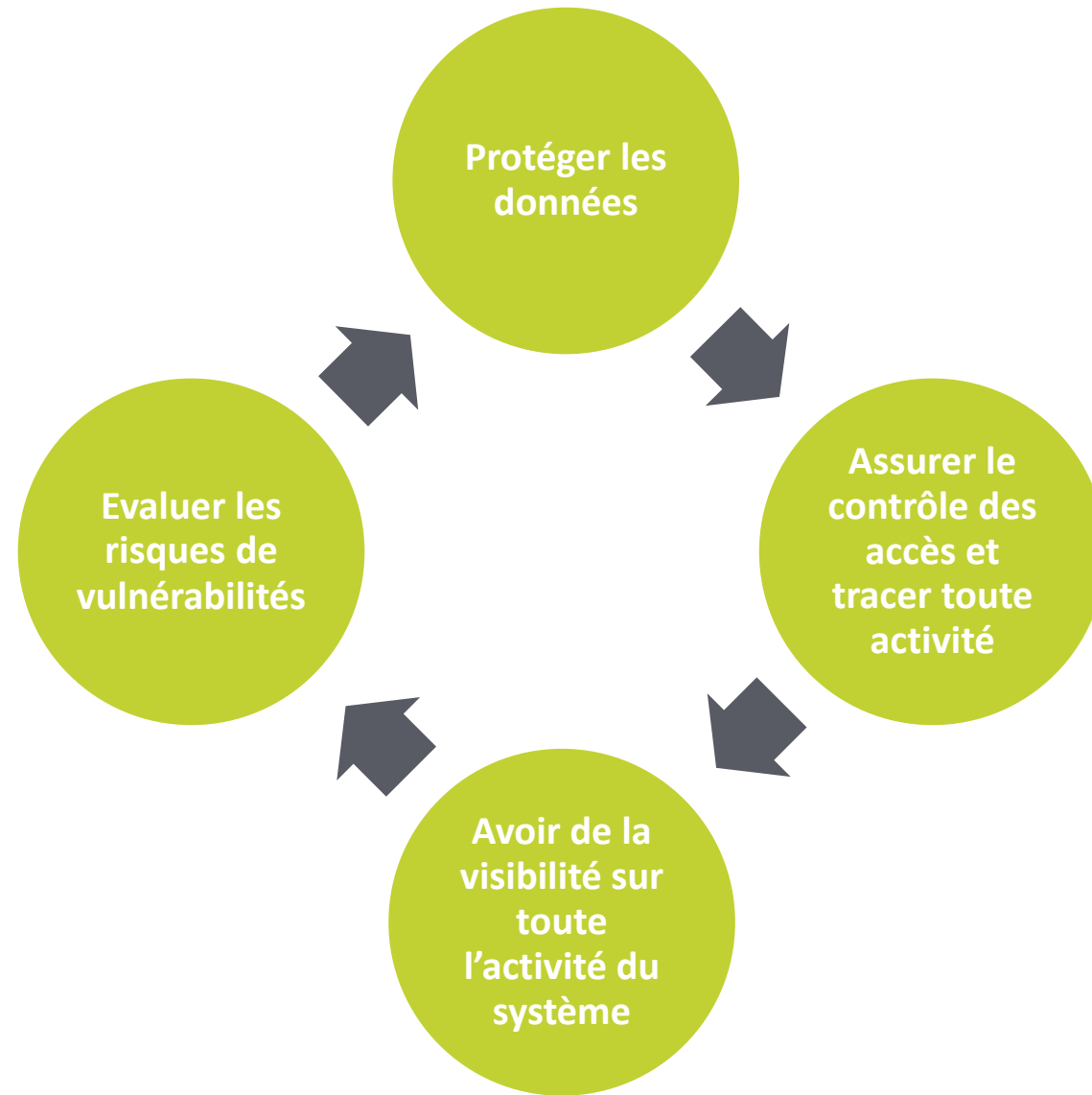
Sécurité IBM i Pourquoi plus de sécurité ?

- ❑ Les contraintes réglementaires exigent une protection accrue des données
 - Normes PCI DSS, RGPD, SOX etc
 - Données personnelles soient protégées
 - Les atteintes à la protection des données ont un impact très négatif sur l'image de l'entreprise

- ❑ Les entreprises sont devenues plus exigeantes quant à la maîtrise de l'accès aux données
 - Les utilisateurs ne devraient voir que les données dont ils ont besoin dans le cadre de leur fonction
 - Les prestataires intervenant sur les systèmes d'informations devraient avoir un accès limité aux données

- ❑ La croissance des projets Cloud & Infogérance a un impact sur les projets Sécurité
 - L'externalisation des systèmes impliquent une meilleure gestion de la sécurité

Sécurité IBM i – Vos attentes



Sécurité IBM i – Les domaines concernés

- ❑ Authentification, login
- ❑ Contrôle d'accès aux applications et fonctions systèmes
- ❑ Sécurité des données quelque soit leur localisation (disques, bandes, flux)
- ❑ Cryptage (Disques, Sauvegarde, Fichiers, Flux)
- ❑ Anonymisation, Pseudonymisation
- ❑ Gestion et contrôle des changements liés à la sécurité du système et des données

Encryption sur IBM i – 3 niveaux possibles



Disques

Option de l'OS IBM i
Clés gérées par l'OS



Sauvegardes

Option de l'OS IBM i
+ Option de la bibliothèque
Gestionnaire de clé TKLM (Tivoli)



Base données

L'OS fournit l'API qui permet
de chiffrer le fichier au niveau
de la colonne (FIELDPROC)
Solution Tierce pour faciliter la
mise en œuvre

Solution IBM i – Encryption des disques

- ❑ Option de l'OS IBM i
- ❑ Option facturable
- ❑ Cryptage des ASP (SS1 Option 45 – Encrypted ASP Enablement)
- ❑ L'IBM i (microcode) gère les clés de cryptage à partir de la clé principale « ASP »

Solution IBM i – Encryption des sauvegardes

- ❑ C'est l'unité de sauvegarde qui effectue le cryptage
 - Depuis LTO4 et ultérieures
 - Librairies TS3100/3200/3310/3400/3500/TS4300 etc...
 - Possibilité de crypter une copie (la sauvegarde d'origine reste en clair)
- ❑ Les clés sont fournies par la solution TKLM (Tivoli Lifecycle Key Manager) qui s'installe sur un serveur Linux/Windows/AIX/ZOS

- ❑ Sur l'IBM i les options suivantes (facturables) sont nécessaires
 - Sur le logiciel de sauvegarde BRMS : BRMS Advanced Feature (BR1 Option 2)
 - Sur l'OS SS1 Option 44 – IBM i Encrypted Backup Enablement

Solution IBM i – Encryption de la base de données

- ❑ Disponible dans l'IBM i depuis la V7R1
- ❑ Field Procedure (FIELDPROC)
- ❑ IBM fournit une API qui s'applique aux colonnes de fichiers,
- ❑ Il faut développer des procédures de chiffrement/déchiffrement
 - L'éditeur spécialiste de la sécurité SYNCSORT fournit une solution qui permet de simplifier la gestion des USER EXIT/API (solution AES/400)

- ❑ Si la base de données est SQL, il existe aussi une fonction de cryptage/décryptage SQL

Solution IBM i – Encryption des flux

- ❑ Basé sur SSL
- ❑ Fonctions intégrées à l'OS
- ❑ Outils de gestion des certifications intégré à l'OS
- ❑ Protection des transferts FTP et Telnet
- ❑ Solutions assez répandues dans le monde IBM i

Encryption – Être méthodique et prudent !

Si vous voulez mettre en œuvre l'encryption :

- Analysez les performances du système avant l'encryption
- Qualifiez précisément les besoins pour choisir le périmètre d'encryption adapté
- Ne négligez pas le processus de gestion des clés

Si vous cryptez les sauvegardes ou les données :

- Assurez vous de pouvoir restaurer
- Où sont les clés ?
- Le serveur de gestion des clés est-il sauvegardé ?
- L'architecture est elle redondante ?
- Faites des tests !

Le groupe Hisi vous accompagne pour assurer la sécurité du système IBM i et des données :

- Prestations d'audit, conseil
- Accompagnement pour la réalisation des POCs
- Revente des solutions SYNCSORT
- Mise en œuvre de projets
- Gestion de projet
- Offres Cloud & Infogérance



www.groupehisi.fr
contact@groupehisi.fr

