Modernisation IBM i – Nouveautés 2014-2015

19 et 20 mai 2015 – IBM Client Center, Bois-Colombes

S3 – Le top 10 des erreurs de configuration de sécurité

Mardi 19 mai – 14h00-15h30

Dominique GAYTE – NoToS
dgayte@notos.fr – www.notos.fr

NoToS

- Expertise autour de l'IBM i
  - Sécurité
  - Regard moderne (DB2 Web Query)
- Service
  - Formation, audit, développement…
- PHP sur IBM i avec Zend
- Développement de progiciels
  - PHP

zend

php.Spool
Valorisation des spools des IBM i (AS/400)
Transformation en PDF, archivage, indexation
http://www.notos.fr/phpSpool.aspx

LoReNa
Gestion de Contenu (ECM)
GED, graphiques, alertes, workflow, GANTT...
http://www.lorena.pro

Introduction

- Evènements qui défraient la chronique
  - Piratage de TV5 Monde
  - Espionnage massif des états
    - Maison Blanche (10/2014) par les russes ?
    - Réseau de l'Elysée (05/2012) par les USA ?
- La stratégie de protection doit changer
  - L'ère de l'écran 5250 en twinax est terminée. Les réseaux sont omniprésents
  - Il est illusoire de vouloir se protéger derrière un mur infranchissable
    - Les pare-feu sont indispensables mais pas infranchissables !
    - Notamment car les attaques s'appuient sur des relais internes (souvent involontaires)
  - Il faut donc
    - S'assurer que le niveau de sécurité de chaque composant du réseau est optimal (IBM i !)
    - Être capable d'assurer la reprise d'activité dans des délais acceptables
    - Comprendre ce qui s'est passé

Introduction (2)

- Mais tout le monde ne se sent pas concerné. Arguments classiques :
  - On n’est pas sur Internet
  - On n’est pas une cible potentielle
  - On ne gère pas des données critiques
  - …
- La Sécurité c’est aussi prévenir
  - La consultation de données confidentielles
  - La modification, la suppression de données vitales
    - Pas forcément intentionnelle
    - Souvent origine interne (80 % des cas de malversations selon certaines sources…)
  - L’impossibilité de redémarrer après un incident
  - …

Introduction (2)

- Je ne parlerai pas de tous les aspects de la Sécurité des IBM i !
- Nous ne détaillerons pas
  - Toutes les valeurs système
  - Tous les mécanismes de protection
- Nous allons essayer de définir des grandes lignes

1- Ignorer la Sécurité

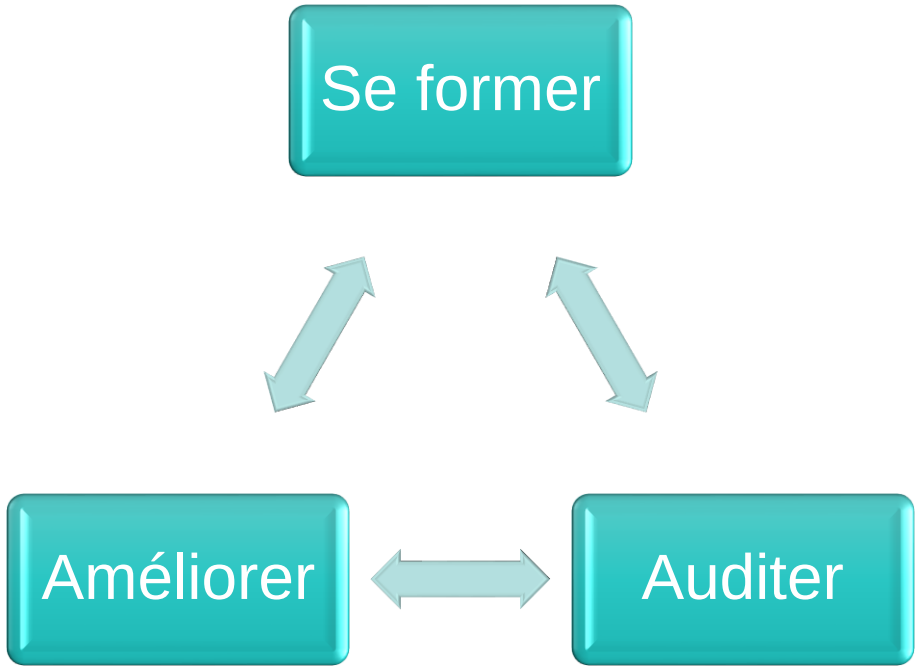
Le paradoxe de l'iBM i

- L'IBM i est probablement l'un des systèmes les plus sûrs du marché
- Mais probablement l'un des moins bien protégés !
- Statistiques personnelles
  - 80 % des IBM i que j'ai *audité* ont un niveau de Sécurité inexistant à faible
  - 10 % ont un niveau acceptable
    - Prise de conscience, maitrise des grands principes
  - 10 % préoccupation sérieuse
    - Réelle politique de gestion et d'amélioration de la Sécurité
- La faute à qui ?

Négliger la Sécurité

- Pêcher par omision !
- Pas de politique Sécurité. Absence de :
  - RSSI (Responsable de la Sécurité des Systèmes d'Information)
  - Audit (manque d'une vision claire des facteurs de risques)
  - Définition d'objectifs
    - Durée d'arrêt tolérée pour chaque application ou chaque service hébergé
    - Niveau de confidentialité des données (cryptage ?)
    - Traçabilité
- Manque de compétences
  - Principes de Sécurité de l'IBM i
  - Réseau
  - …

Que faire ?



- Définir un Plan de Reprise d'activité (PRA)

2 – Négliger les mots de passe

Mots de passe

- Le moyen le plus utilisé pour s'authentifier
  - Couplé à un identifiant (le profil utilisateur)
- C'est le « sésame » qui permet de rentrer dans un système
- Trop souvent les mots de passe sont mal gérés
  - Tout le monde connait le mot de passe de son voisin de bureau
  - Le même pour toute sa vie dans l'entreprise
  - Identifiant / mot de passe partagé entre plusieurs personnes
  - Ou alors politique trop compliquée, donc contournée
    - Post it sous le clavier…
- Par défaut, circule en clair sur le réseau
  - Telnet, FTP, SMTP…

Mots de passe : les soucis

- Mots de passe identique au profil
  - Profils courants : PCS, CA400, IBM
  - Souvent avec de forts privilèges
- Absence de stratégie de mots de passe
  - Durée de validité !
    - A vie…
  - Pas de conformité avec autres environnements (Active Directory…)

Que faire ?

- Avoir une vraie politique de mots de passe
  - Valeurs systèmes QPWD…
  - QPWDRULES à partir de la V6R1
- Mise en place d'un SSO
  - EIM : excellente solution !
  - C'est l'Active Directory qui gère l'authentification (donc le mot de passe)
  - Possibilité d'avoir *NONE au niveau du mot de passe IBM i
  - Tout est en standard dans l'IBM i (et l'AD) !
- Mise en place de SSL
  - Cryptage des informations qui circulent sur le réseau (donc ID/PWD)
  - S'appuie sur des certificats
  - Tout est en standard dans l'IBM i !

3 - Oublier les droits sur les objets (et l'IFS)

Droits sur les objets

- Tout objet dispose de droits pour
  - Le propriétaire
  - Certains utilisateurs (groupes). Ce sont les droits **privés**
  - Les autres. Ce sont les droits **publics**

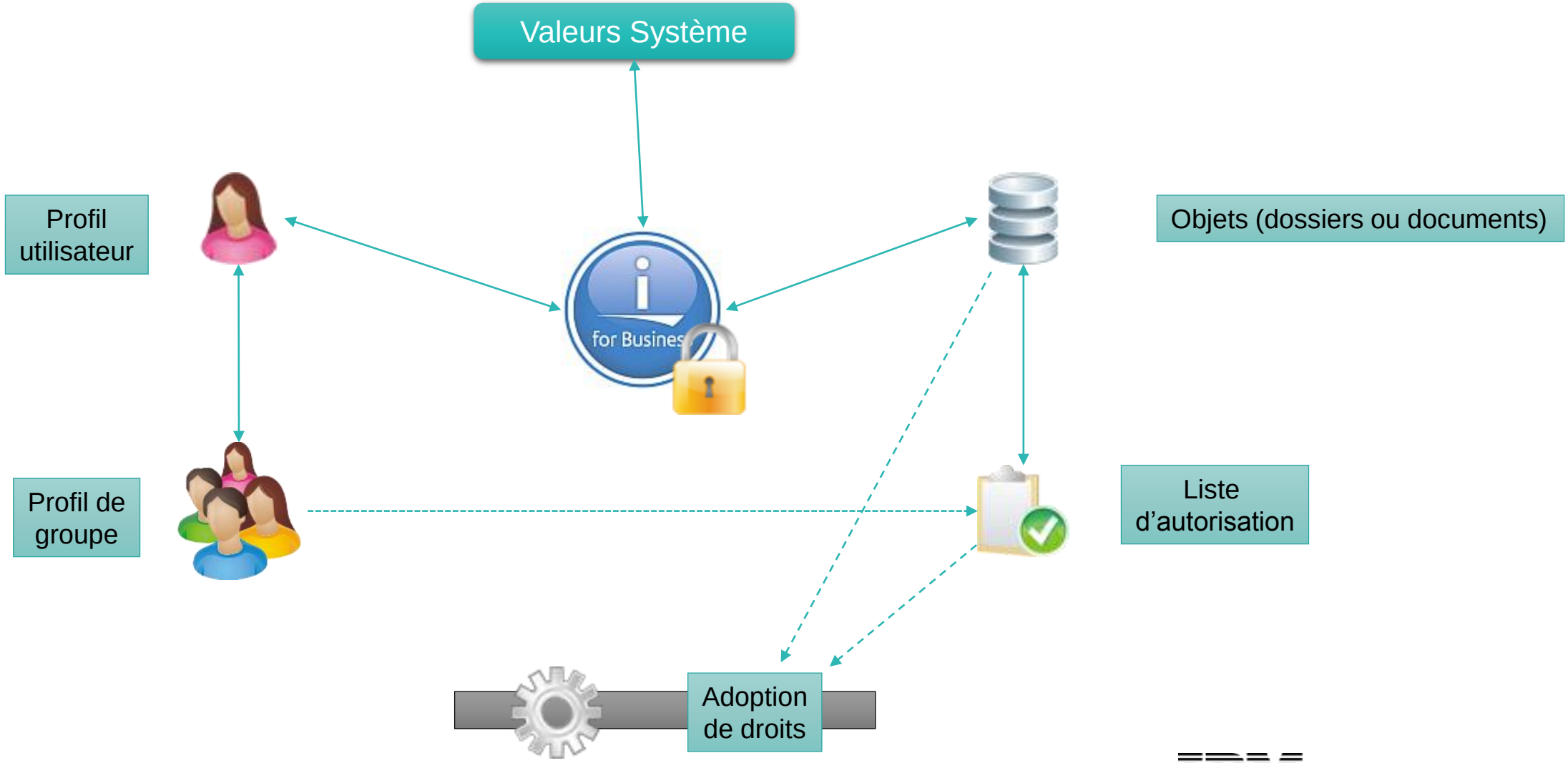
Droits publics

- *PUBLIC
  - Devraient être à *EXCLUDE
  - Souvent *CHANGE
    - *CHANGE : tous les droits sur les données (suppression, ajout, modification, lecture)
    - Valeur par défaut pour tout nouvel objet dans la valeur système QCRTAUT

Que faire ?

- Les commandes de gestion
  - EDTOBJAUT, WRKAUT, GRTOBJAUT, RVKOBJAUT
- Profils de groupe
  - Simplifie la codification des droits privés
  - Des profils utilisateurs sont rattachés à un (ou plusieurs) profil(s) de groupe
    - Le profil hérite des droits du groupe
- Listes d'autorisation
  - Rationalise la mise en place de la sécurité sur les objets
  - Contient des droits privés et publics
- Adoption de droits

Organisation de la Sécurité



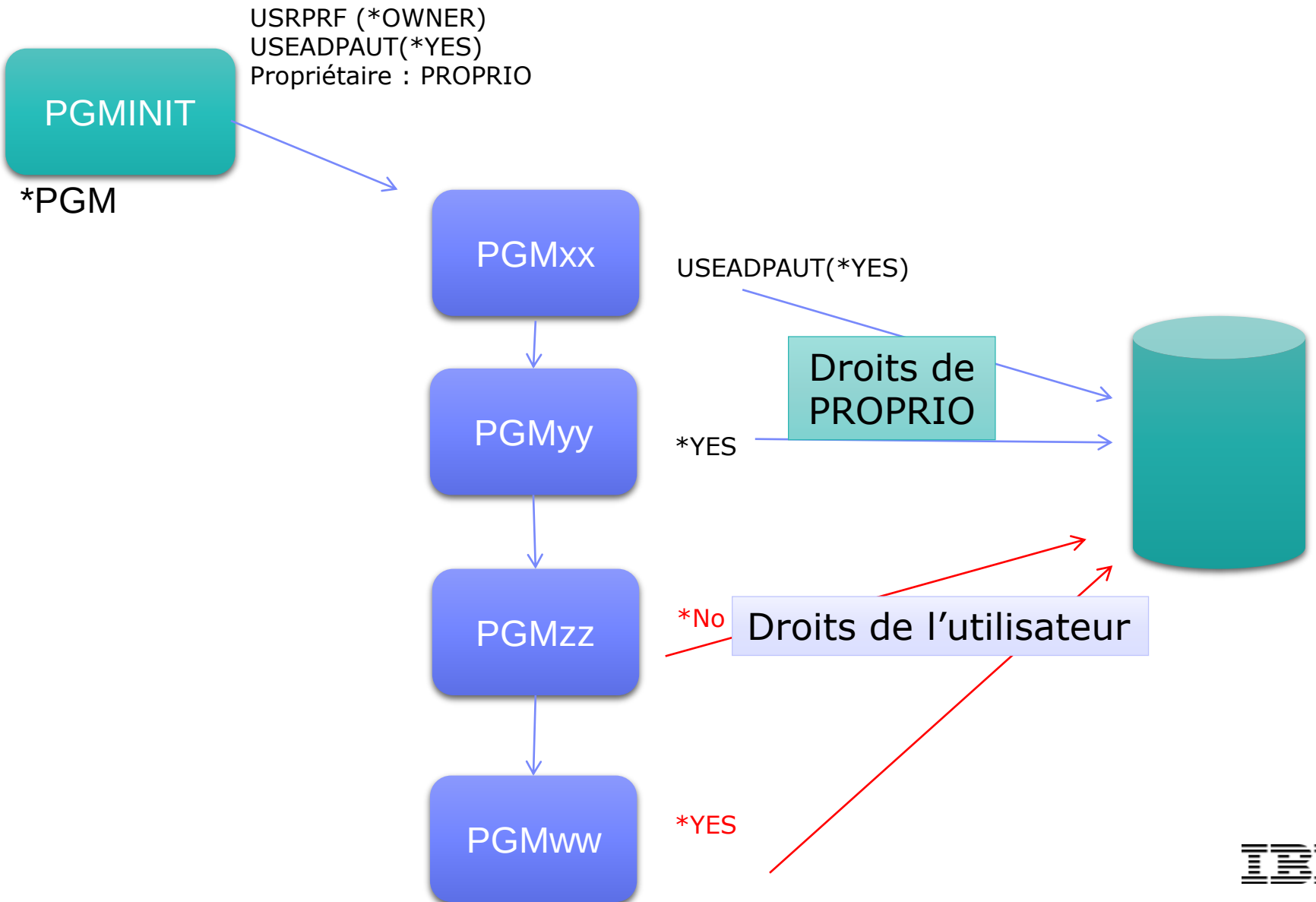
Adoption de droits

- Pendant l'exécution d'un programme l'utilisateur dispose des droits du créateur du programme !
- Paramètre USRPRF (*OWNER) lors de la compilation du PGM
- Intéressant mais à utiliser avec attention !
  - Peut créer des trous de Sécurité si mal utilisé
    - Il ne faut pas de ligne de commandes dans le programme appelé
  - Limiter les droits du profil propriétaire
    - Il doit juste avoir les droits sur les objets (propriétaire !) et disposer du minimum de droits spéciaux nécessaires à l'exécution du programme
  - Ne fonctionne pas avec l'IFS !
- C'est mieux que d'avoir le profil appartenant au groupe propriétaire des objets
  - En dehors du programme l'utilisateur n'a aucun droit avec l'adoption
- DSPPGMADP USRPRF(PROFIL)
  - Pour visualiser les programmes (et autres) utilisant l'adoption de droits

Paramètre USRPRF

```
                        Créer un programme CL (CRTCLPGM)

Indiquez vos choix, puis appuyez sur ENTREE.

Programme  . . . . . . . . . . . > TESTADP       Nom
  Bibliothèque . . . . . . . . . >   DGAYTE       Nom, *CURLIB
Fichier source . . . . . . . . . > QCLSRC        Nom
  Bibliothèque . . . . . . . . . >   DGAYTE       Nom, *LIBL, *CURLIB
Membre source  . . . . . . . . . > TESTADP       Nom, *PGM
Texte 'descript' . . . . . . . .   *SRCMBRTXT


                          Autres paramètres

Options pour liste source  . . .                 *SOURCE, *NOSOURCE, *SRC...
            + si autres valeurs
Options de génération  . . . . .                 *NOLIST, *LIST, *NOXREF...
            + si autres valeurs
Profil utilisateur . . . . . . .   *USER        *USER, *OWNER
Consigner les commandes  . . . .   *JOB         *JOB, *YES, *NO
                                                                  A suivre...
F3=Exit   F4=Invite   F5=Réafficher   F12=Annuler   F13=Mode d'emploi invite
F24=Autres touches
```

Adoption de droits



4 - Attribuer des droits spéciaux (trop élevés)

Droits spéciaux

- Prérogatives affectées à un profil utilisateur (ou a un groupe)
- Les plus préoccupants
  - *ALLOBJ : autorisé à accéder à tous les objets
    - Impossible d'interdire un objet à un profil *ALLOBJ
  - *JOBCTL : autorisé à gérer les travaux
  - *SPLCTL : autorisé à accéder à tous les spools

Que faire ?

- Planifier régulièrement des revues de profils
- Faire la chasse absolue aux *ALLOBJ
  - Attention aux groupes propageant ce droits à de nombreux profils
  - Attention aux profils/mot de passe embarqués en clair dans les applications
    - ODBC, JDBC, FTP
- Vérifier si les profils disposant de droits spéciaux en ont réellement besoin

Power Systems

for Business

5 - Mal configurer les profils utilisateur

IBM

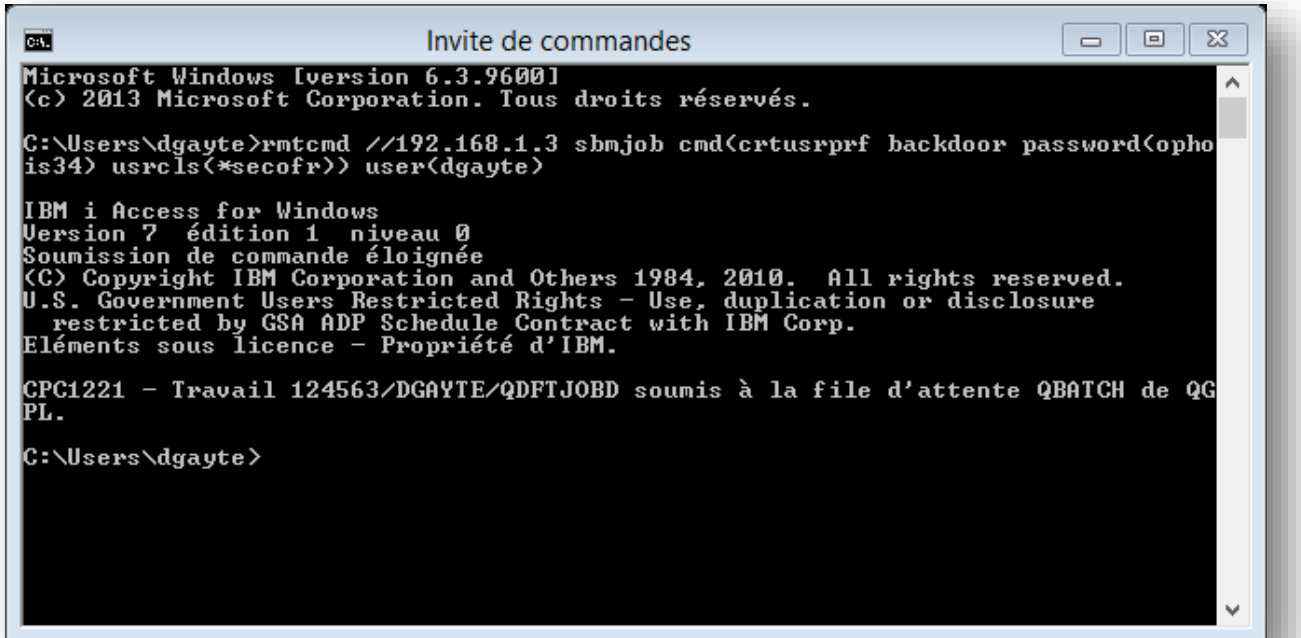
Configuration des profils utilisateurs

- Les droits spéciaux ont été décrits précédemment
  - Ne pas se fier à la classe de l'utilisateur
- Objectif : éviter la ligne de commandes !
- Programme initial
  - Doit être obligatoire pour les profils non système
  - Ne fonctionne qu'avec l'écran vert
- Menu initial
  - Devrait être à *SIGNOFF pour les profils non système
- Possibilité restreinte
  - *YES

Possibilités restreintes - limites

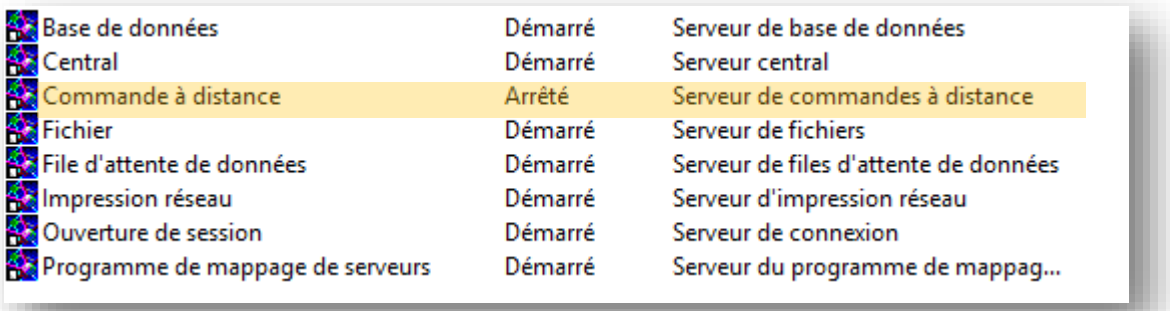
- Ne fonctionne qu'avec la ligne de commandes de « l'écran vert »
- N'est pas pris en compte avec les fonction réseau
  - RMTCMD
  - REXEC

```
C:\>rmtcmd //192.168.1.3 sbmjob cmd(crtusrprf backdoor password(monpwd) usrcls(*secofr)) user(dgayte)
```



Que faire ?

- Planifier régulièrement des revues de profils
- Vérifier les paramètres des profils
  - Programme initial
  - Menu initial
  - Possibilités restreintes
- Pour RMTCMD
  - Arrêter le **Serveur de commandes à distance**
  - Mais attention car il peut être indispensable pour certaines applications !



Power Systems

for Business

6 - Ne pas tracer

La traçabilité pour comprendre ce qui s’est passé

IBM

Traçabilité

- Comprendre après coup ce qui s'est passé
  - Qui, quand, comment ?
- Nombreuses possibilités dans l'IBM i
  - Journalisation
    - Fichiers, de l'IFS…
  - Audit système
  - Trigger
  - Programmes d'exit
  - IDS (Système de détection d'intrusions)

Que faire ?

- Définir ce qui doit être tracé
- Pour le coté système
  - Mettre en place l'audit système
  - Programmes d'exit
    - Ils ont aussi une fonction de protection en interdisant certaines opérations
      - Connexions FTP, requêtes SQL en ODBC…
- Pour les données
  - Journalisation des fichiers, IFS…
  - Trigger
- Avoir une stratégie de sauvegarde de ces traces
  - Cartouche dédiée

Power Systems

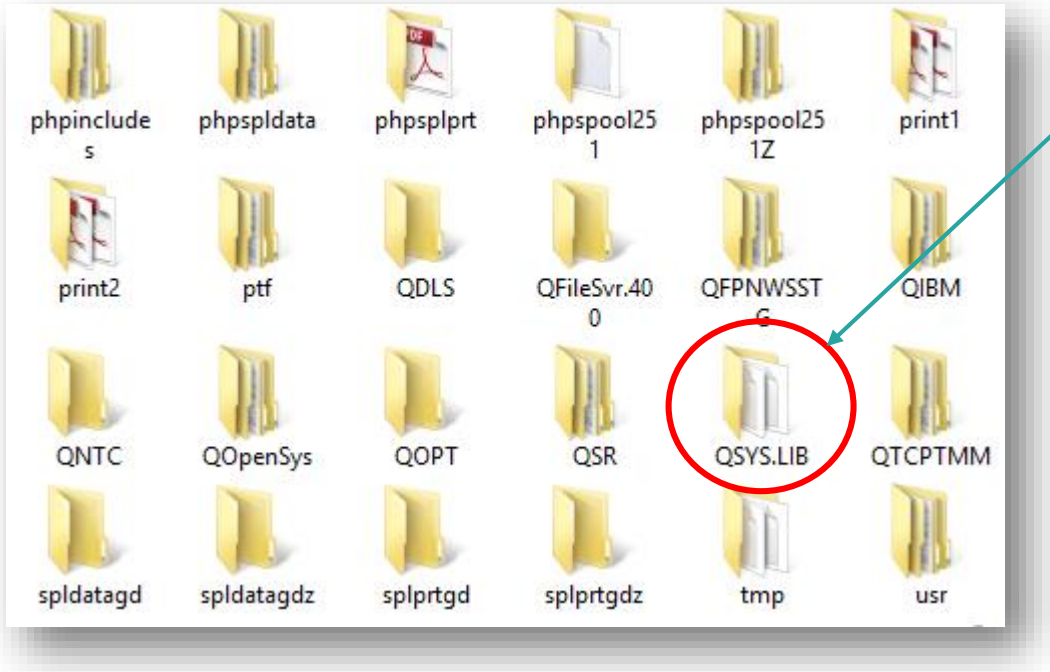
for Business

7 – Abuser des partages Windows

IBM

NetServer

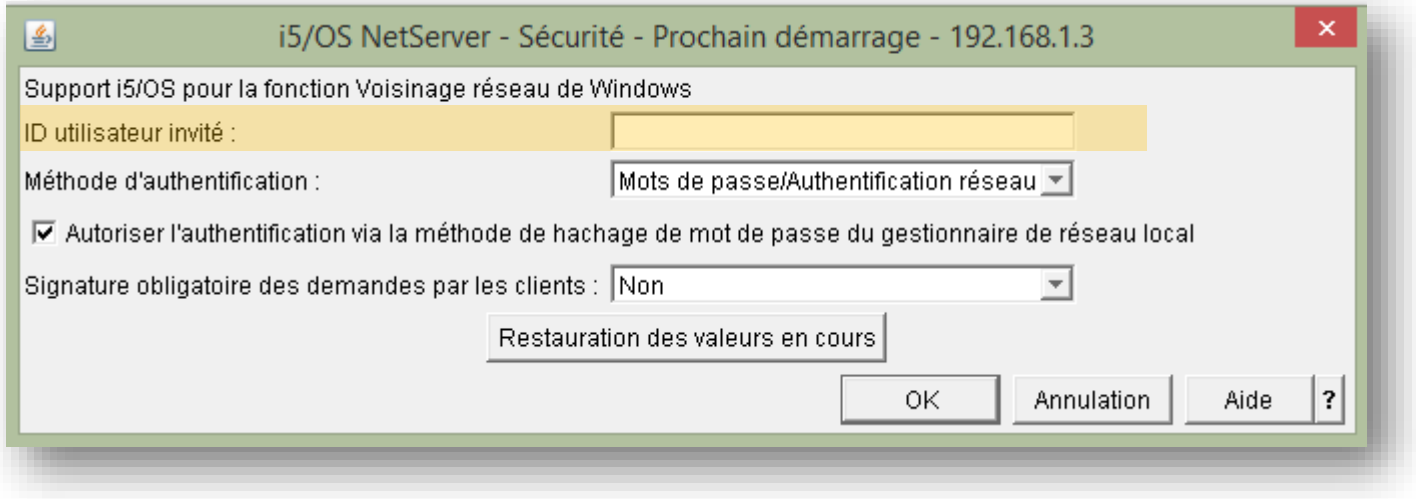
- Trop de dossiers partagés en écriture
  - Root ! Accès à tout l'IFS (y compris QSYS !)



Toute la bibliothèque QSYS

Profil Invité

- Le profil invité permet de se connecter au partage de l'IFS sans avoir de profil utilisateur
- Défini dans les propriétés de NetServer



Que faire ?

- Supprimer le profil « Invité »
- Vérifier les droits sur les dossiers
  - Attention il faut disposer du droit *X sur toute la hiérarchie de dossiers pour accéder à un fichier de l'IFS
- Limiter les partages à ce qui est essentiel
  - Surtout en écriture
- Toujours partager le niveau le plus bas de l'arborescence
- Programmes d'Exit

Power Systems

for Business

8 - Trop exposer l'IBM i sur le réseau

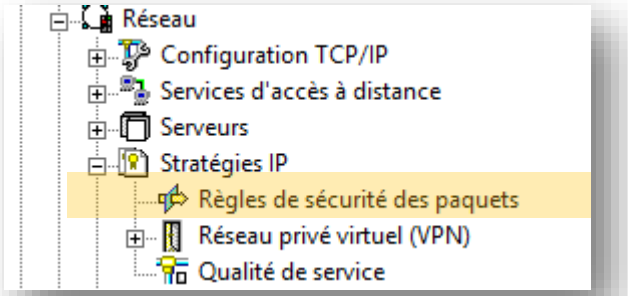
IBM

Réseau

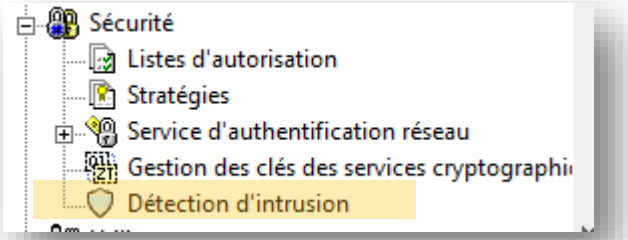
- De nombreux serveurs TCP/IP sont démarrés inutilement
  - Pas toujours très bien configurés
- De plus en plus d'IBM i sont directement connectés à Internet
  - Souvent sans que ce soit conscient. Il suffit :
    - Que le routeur par défaut ouvre la route vers Internet
    - Que le DNS configuré dans l'IBM i résolve les noms « Internet »
  - Vérification : faites un ping à partir de l'IBM i
    - Sur un nom de système qui répond au ping (www.ibm.com)
    - Sur une adresse IP si c'est négatif avec le nom

Que faire ?

- Isoler physiquement les réseaux
- Configurer TCP/IP (CHGTCPA) pour éviter le routage
  - IP Forwarding et IP Source Routing si possible
- Protéger la connexion Internet avec le parefeu intégré

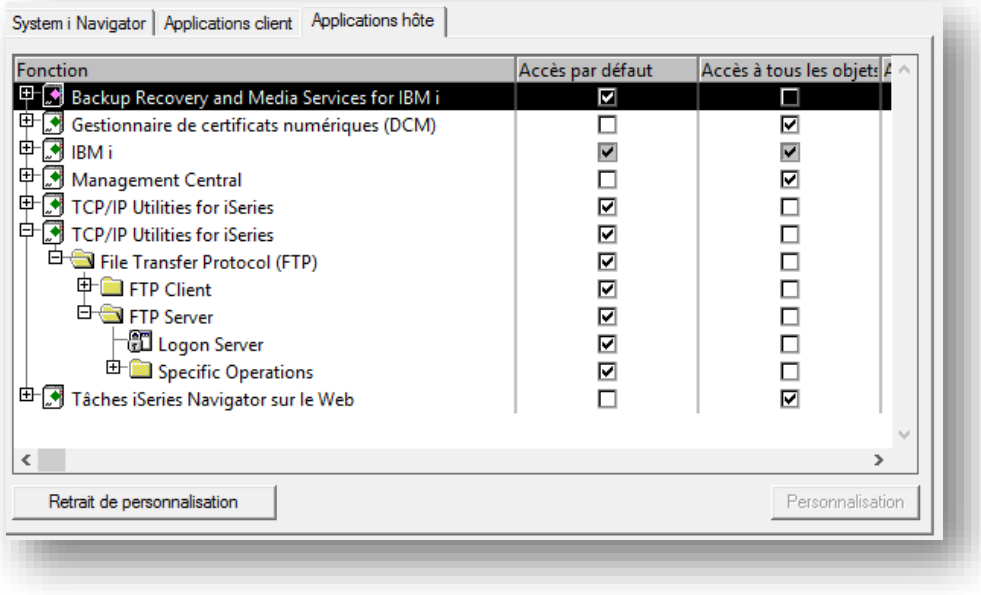


- Utiliser SSL pour les protocoles qui le supportent
- Tracer avec la Détection d'intrusion (IDS)

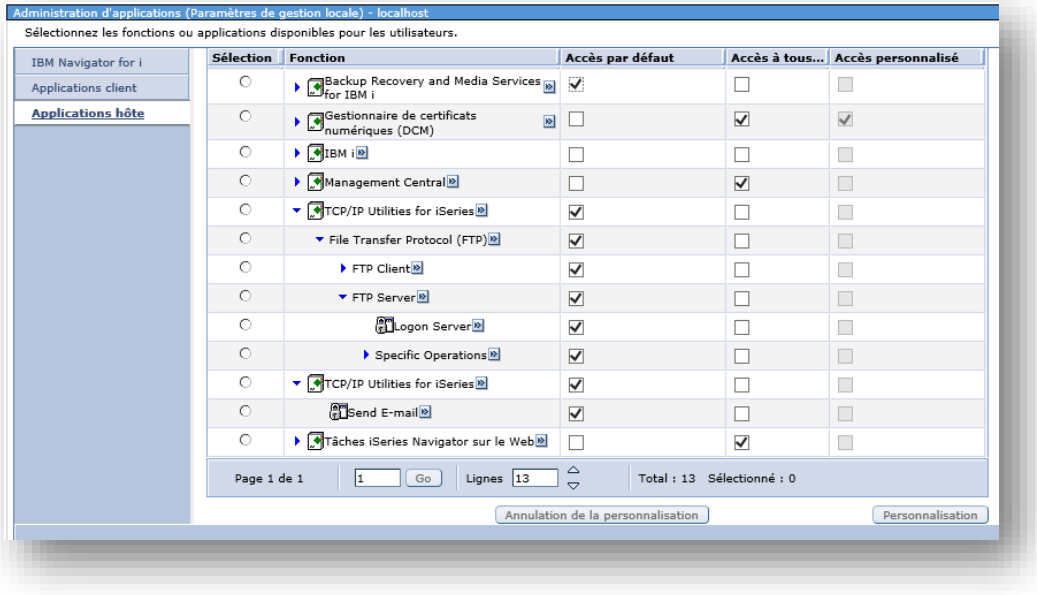


Que faire ?

- Limiter les serveurs TCP/IP démarrés à ce qui est essentiel
  - Vérifier les configurations
  - Protéger par des programmes d'exit et l'administration d'applications



System i Navigator



IBM Navigator for i

Power Systems

i for Business

9 – Sous évaluer les risques liés aux spools

IBM

Les Spools

- Les spools peuvent contenir des données essentielles
  - Bulletins de salaire
  - Listes de prix (de vente, de revient…)
  - Informations système vitales
- Attention aux profils *SPLCTL
- Et aux profils *JOBCTL pour les OUTQ qui ont OPRCTL(*YES)
- Et aux OUTQ ayant DSPDTA(*YES) et *PUBLIC différent de *EXCLUDE

Que faire ?

- Identifier les spools critiques
- Placer les OUTQ sensibles dans des bibliothèques avec des droits d'accès très limités
  - *PUBLIC *EXCLUDE
- Penser aussi à sauvegarder (et archiver) les spools qui ne peuvent être reproduits

Power Systems

i for Business

10 – Penser que les sauvegardes appartiennent au passé

IBM

Les nouveaux contextes

- Outils de réplications
  - Données dupliquées quasiment en temps réel
  - Sur 2 systèmes distants
- Données dans des SAN externes
  - Disques fortement protégés
- Dans ce contexte les sauvegardes sont elles toujours utiles ?

OUI !

Les sauvegardes indispensables…

- Indispensables pour conserver des historiques de versions des objets
  - En cas de suppression accidentelle, elle est automatiquement répliquée
  - Sans sauvegarde, pas de possibilité de retour à une version antérieure
- Indispensables pour externaliser les données
  - En cas d'acte malveillant, il peut être réalisé sur les différents environnements
  - Les sites de PRA sont parfois rapprochés. Un évènement important peut affecter les deux sites
- Indispensables pour conserver la traçabilité

Que faire ?

- Sauvegarder !
  - Quotidiennes
  - Hebdomadaires
  - Mensuelles ? Souvent ne sont plus utiles car réalisées en hebdomadaire
    - Ou pour un stockage à long terme
  - Traçabilité
    - Récepteurs de journaux
    - Fichiers de traces
- Externaliser les sauvegardes
- Conserver les bandes de traçabilité

Power Systems

i for Business

Merci pour votre écoute !

Des questions ?

Dominique GAYTE - dgayte@notos.fr
04 30 96 97 33
www.notos.fr

IBM