



iBelieve

Présent et Futur de l'IBM i 2022

Evènement
on-line
17 Nov. 22

Sécurisez votre IBM i de manière pragmatique et opérationnelle

- Guy MARMORAT -

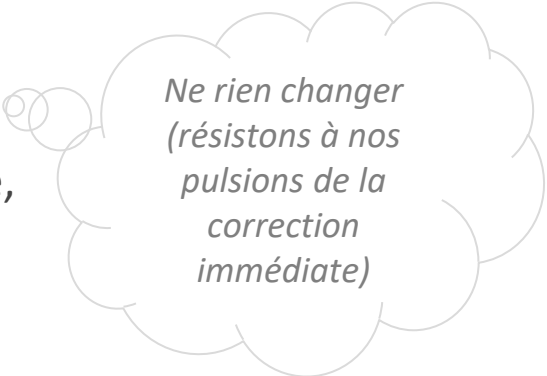
AGENDA

- 1 Analyser, planifier (audit de sécurité)
- 2 Préparer la remédiation
- 3 Remédier en Production
- 4 Les applications externes
- 5 Les applications externes (confiance ou pas?)
- 6 Règles d'or du contrôle d'accès via les points d'exit
- 7 Focus 7.5



Analyser, planifier (audit de sécurité)

- Identifier les failles, vulnérabilités, trous de sécurité, défauts de configuration.
- Décrire la faille (si besoin, comment peut-elle être utilisée pour compromettre la sécurité, l'intégrité, la confidentialité)
- Lui affecter un niveau de risque



*Ne rien changer
(résistons à nos
pulsions de la
correction
immédiate)*



BON SENS

Proposer toutes les remédiations possibles

- Leur affecter un niveau d'effort estimé (incluant le risque de la remédiation elle-même)
- Lister les points de vigilance, anticiper tous les impacts possibles

Affecter une priorité

Ne pas oublier : Garder toutes les évidences, y compris les valeurs ne nécessitant aucune correction. Il se passe en général du temps entre la publication des résultats de l'audit et la remédiation ! Cela pourrait bouger...

Préparer la remédiation

- Vérifier que la faille est dans le même état
- Coder (Merci SQL !)
- Tester le processus complet de remédiation (bac à sable)
- Tester le processus complet de remédiation (recette)

Mesurer les effets de la remédiation

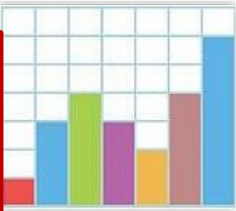
- Vérifier les effets positifs directs (preuve, éducation, ...)
- Identifier les effets négatifs directs
- Identifier les effets indésirables collatéraux



Envisager une éventuelle procédure de rollback

Mesures post-remédiation :

- Identifier les nouvelles déviations si elles devaient arriver
- Etre en capacité d'identifier des effets collatéraux plus insidieux
- Ne plus permettre à la faille de réapparaître



Bien documenter l'ensemble

Remédier en Production

Vérifier que la faille est dans le même état

Communiquer !

Lancer la procédure

- Choisir le bon moment en fonction des contraintes liées au type de remédiation. (IPL, changement dans d'autres serveurs & devices, changement dans des applications de gestion, etc...)
- Tester (Utilisateurs d'applications d'astreinte pour rejouer des transactions)
- Surveiller !



La remédiation est potentiellement une action **impactante et risquée**.
Découper un gros sujet en parties autonomes, les plus petites possibles, car **des solutions différentes** peuvent être apportées à chacune des parties.



Remédier en Production

Exemple : Suppression et/ou mitigation du droit spécial *ALLOBJ - Comment s'y prendre ?

- 1^{ère} étape : Nettoyer les profils inutiles
- 2nd étape : Classifier les profils et leur affecter des groupes
- 3^{ème} étape: Analyser le comportement des utilisateurs (authority collection, journaux, exit point) sur une période assez longue
- 4^{ème} étape : Proposer les remédiations adaptées et/ou les contrôles supplémentaires

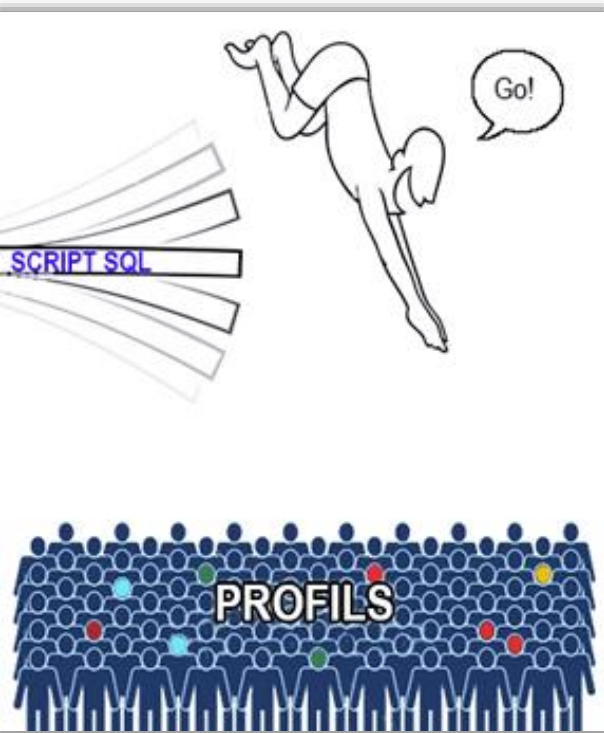
Ceci n'est qu'un exemple, à adapter à chaque situation et aux besoins de sécurité et de mise en conformité avec certaines réglementations.

Exemple :

Suppression et/ou mitigation du droit spécial *ALLOBJ Comment s'y prendre ?

~~*ALLOBJ~~ Supprimé

*ALLOBJ 👤 Sous surveillance



Categories d'utilisateurs	Ce qu'ils ont / n'ont pas le droit de faire sur les partitions de Production	Propositions de remédiation globale	Propositions de remédiation spécifique	
Business application	Utilisent exclusivement des applications de gestion. De façon exceptionnelle et contrôlée, certains d'entre eux peuvent exporter/importer des données pour certains besoins de gestion justifiés.		Authority collection et positionnement des droits Contrôle des imports/exports de données	*ALLOBJ
Admin	Administrent le système et parfois aussi la base de données. Ne devraient pas lancer des processus de gestion. Ne devraient pas modifier ou voir les données.		Audit complet (joblog, journal système, journaux base de données, exit point, écrans) Autorisations à la demande de certaines commandes et/ou types d'accès	*ALLOBJ 👤
Support Exploitation	Suivent la bonne utilisation du système. Peuvent modifier des données dans certains cas et de façon contrôlée. Ne devraient pas lancer des processus de gestion.		Audit complet (joblog, journal système, journaux base de données, exit point, écrans) Emballage de certaines commandes utilisées régulièrement	*ALLOBJ
R&D	Ont besoin de rechercher des contextes d'erreurs, parfois de debugger. De façon exceptionnelle et contrôlée, ils peuvent restaurer des objets et corriger manuellement des données.	Affecter des profils groupe le plus possible (comme marqueur et porteur de droits)	Elévation de droits à la demande et session auditée	*ALLOBJ
Comptes de service	Sont utilisés pour des process automatiques qui requièrent une connexion à l'IBM i, tout en respectant des règles d'isolation. Ne devraient jamais être utilisés en dehors de ce cadre.	Contrôler les créations, modification, restaurations de profils	Contrôle des connexions inbound Contrôle des protocoles et fonctions utilisées Authority collection et positionnement des droits	*ALLOBJ 👤
Comptes batch	Sont utilisés pour des process automatiques qui ne requièrent aucune connexion à l'IBM i. Ne devraient jamais être utilisés en dehors de ce cadre.	Contrôler les connexions	Pas de mot de passe Pas de connexion Contrôle de la source (call stack, WRKJOBSCDE, ...) Authority collection et positionnement des droits	*ALLOBJ 👤
Profils propriétaires	Profils techniques dont le seul but est d'être propriétaires d'objets et éventuellement de participer à un mécanisme d'élévation de droits (adoption ou swap). Ne devraient jamais être utilisés en dehors de ce cadre.	Interdire les délégations d'utilisateurs (SBMJOB, APIs de swap) ou les justifier/contrôler	Aucune connexion Aucune utilisation	*ALLOBJ
Profils de groupe	Profils techniques dont le seul but est de regrouper des profils par rôle et donc de participer au mécanisme de sécurité des objets. Ne devraient jamais être utilisés en dehors de ce cadre.		Aucune connexion Aucune utilisation	*ALLOBJ
Profils IBM réservés	Profils internes IBM. Ne devraient pas être modifiés et utilisés.		Aucune connexion Aucune utilisation autre système	*ALLOBJ 👤
Consultants externes	Leur tâche varie en fonction de leur domaine de compétence. Leur activité doit être auditée.		Audit complet (joblog, journal système, journaux base de données, exit point, écrans) Elévation de droits à la demande et session auditée	*ALLOBJ
QSECOFR	Dans la mesure du possible, réserver ce profil pour des tâches purement systèmes telles que l'application de PTF, des changements dans l'OS et touchant le hardware. Son activité doit être auditée.		Audit complet (joblog, journal système, journaux base de données, exit point, écrans)	*ALLOBJ 👤

Remédier en Production

- Pas d'idéologie, on n'écarte aucune méthode à priori (exit point, adoption, swap, SIEM, MFA, ...)
- Mais... l'achat d'un package de sécurité ne règle pas tous les cas par miracle
- Attention aussi aux outils gratuits d'analyse : souvent limités, orientés, et non contextualisés

- Investir dans le maintien d'une partition de recette à l'image de la production (ROI)
- Dire plutôt « environnement » de recette d'ailleurs

- Focus sur les failles à risque élevé, à effort faible à moyen
- Paralléliser les tâches en fonction de l'effort estimé

Les applications externes

Première installation/Mise à jour/Correctif :

Conserver systématiquement l'audit trail complet (joblog, journaux, exit point)

Les applications externes

Exemple d'un questionnaire à adresser à l'éditeur

Lister les nouveaux éléments :

- les bibliothèques
- les répertoires IFS
- les objets restaurés dans d'autres bibliothèques existantes
- les objets restaurés dans d'autres répertoires IFS existants
- les profils avec leurs attributs
- les listes d'autorisation
- les sous-systèmes

.....

Décrire et justifier les modifications apportées au système :

- programmes d'exit
- fonction usage (ex : RCAC)
- valeurs système
- autres éléments (sous-systèmes existants, QAQQINI, TCP/IP, DDM, SST users IDs, etc...)

.....

Décrire le schéma général de la sécurité au niveau des bibliothèques, objets, IFS en détaillant :

- les droits publics
- les éventuels droits privés
- la propriété
- les listes d'autorisation
- les exceptions

.....

Les applications externes

Exemple d'un questionnaire à adresser à l'éditeur (suite)

Expliquer si les profils ont des droits spéciaux
Expliquer si des commandes sont en ALWLMTUSR(*YES)	
Expliquer si des programmes adoptant des droits élevés existent et confirmer que ces programmes n'ouvrent pas de ligne de commande	
Expliquer si des programmes utilisent les APIs de swap pour élever leurs droits et confirmer que ces programmes n'ouvrent pas de ligne de commande	
Décrire la gestion de la journalisation des données
Décrire le principe d'enregistrement des utilisateurs finaux
Donner les différentes valeurs des registres client si application ODBC, JDBC
Justifier si l'installation patche des objets système qui apparaîtraient en erreur avec CHKOBJITG



Les applications externes (confiance ou pas?)



Software Supply Chain Attacks



Une seule attaque = De multiples sites infectés et/ou accessibles via des back doors, la propagation étant assurée par des canaux de confiance

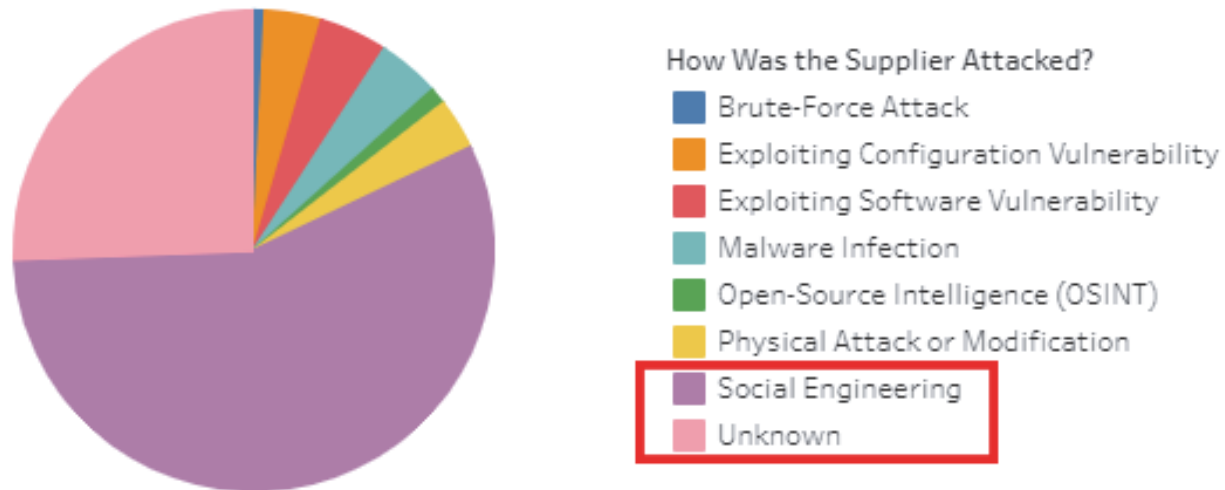
Les applications externes (confiance ou pas?)

Cas connus récents :

SolarWinds, Kaseya, Codecov, ua-parser-js

Open-Source: Log4j, Zlib, OpenSSL

Supplier Attacks-Type



Source : <https://www.comparitech.com/software-supply-chain-attacks/>

Les applications externes (confiance ou pas?)



Les éditeurs ne se sentent pas encore complètement concernés....
Le renforcement des tests de sécurité s'améliore timidement....

Nouveau comportement à adopter :

1. Challenger les éditeurs
2. Monitorer les activités d'installation, mise à jour, application de correctifs
3. Tendre vers le Zero-trust

Règles d'or du contrôle d'accès via les points d'exit

Que faire avec un programme d'exit :

- Rejeter certaines connexions et/ou transactions
- Loguer les tentatives rejetées
- Loguer certaines connexions et/ou transactions au caractère sensible (user admin, table critique, IP non recensée, call stack non applicatif, etc...)
- Déclencher des actions (envoi dans une SIEM, alerte, remédiation automatique, challenge MFA, interagir avec un SOAR, etc...)

Le programme d'exit est appelé avant le « authority-checking process ».

Règles d'or du contrôle d'accès via les points d'exit

Choisir le bon compromis pour la protection des profils de service :

A la connexion :

- Très contraignant (contrôle a minima sur le couple user-IP-protocole)
- Intransigeance sur les connexions « manuelles » avec des comptes de service

A la transaction :

- Définir la granularité de la règle (en fonction des ressources pour suivre les remontées, de la criticité des données, ...).
- Le vocabulaire peut être vaste : l'utilisateur et ses attributs, le protocole et la fonction, le fichier DB2, son membre et sa bibliothèque, le chemin IFS, le contexte (date/heure, job, call stack, IP, registre), l'iASP, le détail de l'instruction (phrase SQL complète, commande complète, programme avec les paramètres, ...)
- Mode forteresse ou Zero-trust
- Isolation : inbound/outbound (prod avec prod, recette avec recette, dev avec dev)
- Listes blanches, noires ou combinaison ?

Règles d'or du contrôle d'accès via les points d'exit

Contexte d'analyse déjà complexe et ça continue! Merci IBM  (SQL & Open-source)

- Instructions SQL complexes (jointures, fonction scalaire qcmdexc, alias, noms longs/courts, tables non qualifiées, troncatures des buffers, ...)
- Renforcer certaines connexions (MFA, registres client, ...)
- PASE & QSH

Critères de choix d'un package de sécurité

- Tests de résistance
- Attention au STRDBMON *ALL/*ALL/*ALL – utilisez les filtres !
- Impact CPU
- Orientation « data_centric » (DB2 & IFS)

Focus 7.5

Mes favoris apparus en 7.5 :

- Listes d'autorisation appliquées à NetServer et aux partages
- Le point d'exit QIBM_QPOL_OBJ_OPEN "Integrated File System Object Open"

7.5 TR1 & 7.4 TR7 - Dispo le 02/12/2022



FIN !

**MERCI
DE VOTRE ATTENTION**

