Power Week

Université IBM i 2019

22 et 23 mai

IBM Client Center Paris

i for Business

RAZ-LEE

S30 – Les nouvelles menaces et le défi de la règlementation RGPD

Nissim Ménashé | VP Operations & Marketing
Raz-Lee Security Ltd.
+33 1 77 47 07 16
nissim@razlee.com

Bruno Leconte | Data Protection Officer
Raz-Lee Security Ltd.
+33 6 08 50 42 85
Bruno.leconte@razlee.com

Raz-Lee Security

- Fondée en 1983
- L'offre sécurité la plus large du marché
- 100% focalisée sur IBM i (AS/400)
- Bureaux: Israel, USA, Italie, Allemagne
- Partenaire IBM
- Produits installés dans plus de 40 pays, plus de 12 000 licences
- Partenariats avec les fournisseurs majeurs de solutions SIEM & DAM
- Produits uniques: Anti-Ransomware, Change Tracker, Capture, Authority Inspector, Safe Update, ICAP client for AntiVirus.

Plan de la présentation

- Introduction
  - La Sécurité et la Fiabilité de l'IBM i sont inégalées
  - Architecture
  - L'interconnexion du 'i' a un Coût en Sécurité
- L'IBM i est hautement sécurisable
- Vulnérabilités de l'IFS
- Cyberattaques en chiffres
- Anti-Ransomware
- Le défi de la règlementation RGPD
- Raz-Lee Security: les expert de la sécurité IBM i

Intro: La Sécurité et la Fiabilité de l'IBM i sont inégalées

- Réputation enviable dans le monde des serveurs professionnels


Sécurité


Fiabilité


Aucun virus connu


Faible nombre de violations

- Cette position ignore le fait suivant


Systèmes IBM i


Banque et Finance


Difficulté

Ceci suggère qu'il y a quelque chose de plus fondamental à la réputation du système d'exploitation.

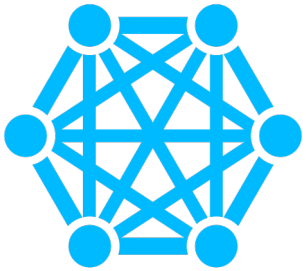
Intro: Architecture

- un profile utilisateur (*USRPRF)
- un programme compilé (*PGM)
- un fichier de base de données (*FILE)
- une bibliothèque (*LIB)
- une commande (*CMD) ou … la liste continue

Qui peut y accéder?

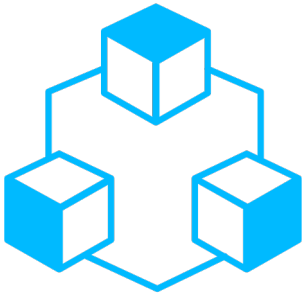
Pour altérer les paramètres de sécurité, un pirate devra mettre la main sur les outils de services, **mais bien sûr l'accès à des outils aussi puissants devrait être restreint.**

Intro: L’interconnexion du ‘i’ a un Coût en Sécurité



Monde interconnecté

Plus de forteresse



Connectivité IBM i

L’IBM i est hautement sécurisable (1)

L’IBM i bénéficie toujours d’une réputation enviable pour sa sécurité et sa fiabilité.

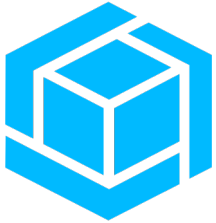
Cependant, les utilisateurs tendent à surestimer la sécurité inhérente au système d’exploitation!

En conséquence, ne prennent pas les précautions nécessaires pour empêcher une attaque ou une violation de données.

L’IBM i est hautement Sécurisable (2)

La meilleure façon d’atténuer les problèmes de sécurité liés à l’IBM i est:

Politique Sécurité de l’Entreprise



Contrôle d’Accès des Objets

Protection anti-virus

Cryptage

Audit

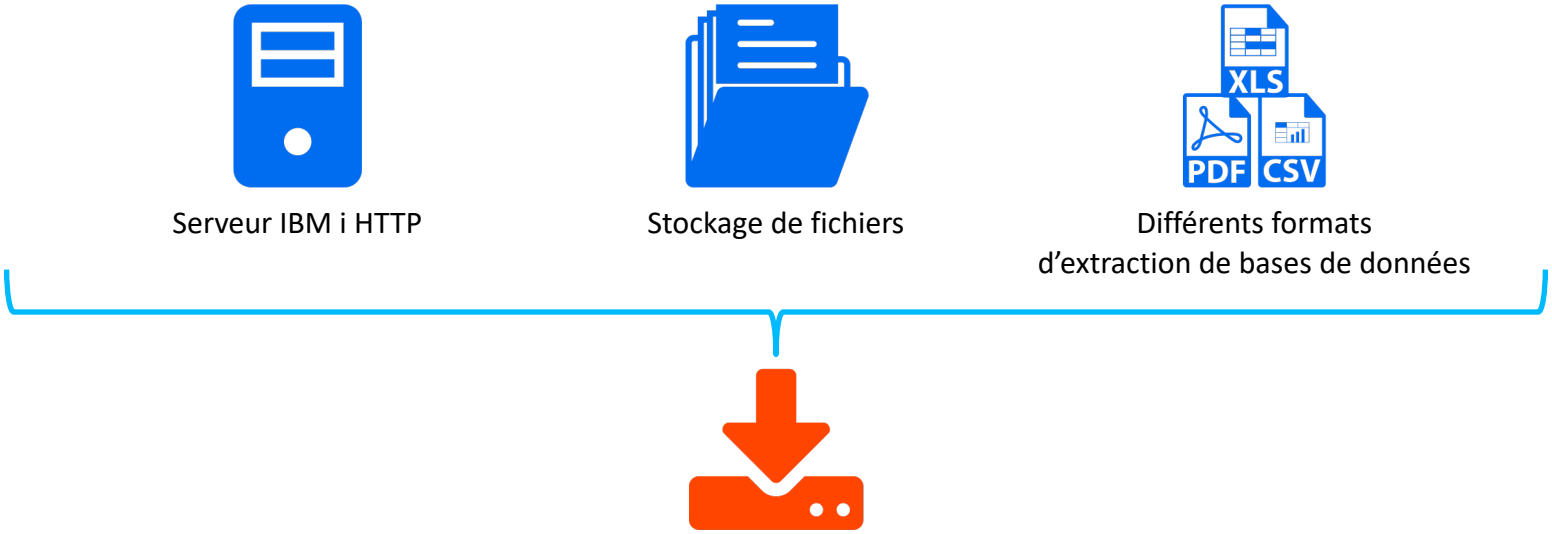
L’IBM i est hautement sécurisable!

Pour le garder sécurisé, les faiblesses de sécurité inhérentes à la plateforme IBM i doivent être gérées en permanence.

L’incroyable iSecurity Firewall

Vulnérabilités de l'IFS (cause)

En 1994 en plus de la bibliothèque QSYS, IBM introduit pour la première fois **l'Integrated File System (IFS)** avec la version V3R1.



Vulnérabilités de l'IFS (effet)

Cas d'école:

- Les fichiers de configuration TCP/IP sont stockés dans le répertoire **QIBM/Userdata**. Les fichiers d'accès client sont stockés dans le répertoire QIBM/Proddata.

Si lors de la mise a jour automatique du Client Access ce setup.exe avait eté infecté, cela aurait infecté tous les PCs.

- Les fichiers d'administration et de configuration du serveur HTTP sont stockés dans le répertoire **QIBM/Userdata**.

Si ces fichiers sont supprimés ou modifiés, le serveur HTTP peut être désactivé et l'ensemble du site Web nécessite une réinstallation complète.

La liste des problèmes potentiels avec l'IFS continue.

Vulnérabilités : Pas Seulement dans l'IFS

L'IFS n'est pas la menace la plus importante

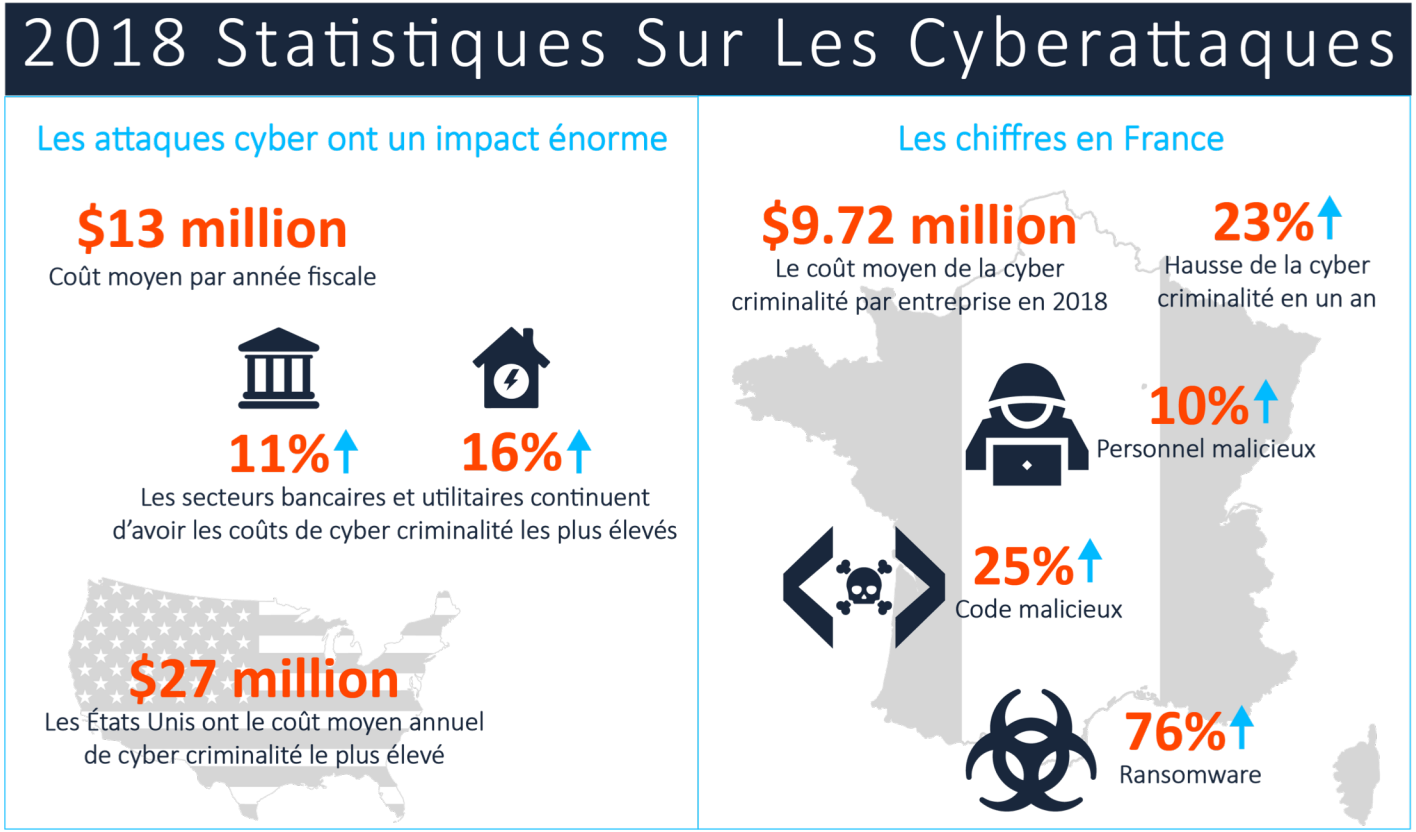
Les plus gros risques de vols de données et la déficience potentielle du serveur viennent de:

Privilèges de l'utilisateur
(erreurs)

Equipe technique
(erreurs)

Intention illicite

Les Cyberattaques (Accenture)

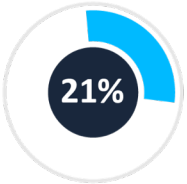


Source: Accenture 9th Annual Cost of Cybercrime Study in France

2018 Cyberattaques en France

RAZ-LEE

Un coût de 10 000 à 100 000 euros pour les PME



d'entre elles ont été victimes d'une attaque l'an passé.

des entreprises attaquées ont perdu moins de 10 000 euros

plus de 51 000 euros

plus de 100 000 euros

Les responsables identifient 5 risques principaux

52% les e-mails frauduleux

51% le piratage de données

41% les malwares

26% la perte ou le vol de matériel informatique

24% la fraude-malversation-escroquerie

Source: https://bfmbusiness.bfmtv.com/entreprises/cyberattaques-une-facture-moyenne-de-86-millions-pour-les-entreprises-francaises-1664768.html

Ransomware dans l’actualité (Avril 2019)

2 Avril 2019

la firme Arizona Beverages

16 Avril 2019

L’association du Mémorial Stone Mountain victime d’une attaque ransomware

“L’organisation d’état qui gère le Parc de Stone Mountain a été victime d’une attaque ransomware — similaire à celle qui a affecté les operations de la ville d’Atlanta l’année dernière.”

ordinateurs qu’il peut atteindre.”

Ransomware dans l'actualité (Avril 2019)

13 Mai 2019 Un ransomware chiffre 80% des données du négociant pétrolier Picoty

"Picoty SA, une société française localisée dans la Creuse à la Souterraine spécialisée dans le négoce de produits pétroliers, a été ciblé par un rançongiciel. Les pirates demandent une rançon de 500 000 euros, qui pourrait être doublée d'ici la fin de la semaine, pour déchiffrer 80% de ses données déjà chiffrées."

La menace des Attaques cyber est très réelle pour l'IBM i (source : Mars 2018)

- 26 Décembre 2017 LinkedIn, John Rockwell

  "Une des sociétés dans laquelle j'ai travaillé récemment **a été contaminée par le virus Cryptolocker 3 fois**. Puisque tous les PCs étaient connectés au réseau et les dossiers My Documents folders étaient pointés vers l'IFS, cela s'est avéré être un problème."

- 10 Avril 2017 IT Jungle

  "Auriez-vous préférer **payer une rançon de 200 000 $ ou** avoir votre serveur inutilisable pendant un mois ? C'est le résultat de deux récentes attaques ransomware sur des serveurs IBM i, que les cyber-criminels peuvent commencer à cibler."

- 2017 State of IBM i Security Study

  "Une entreprise a analyser l'IBM i à la recherche de virus pour la première fois, et a été choquée de trouver près de **250 000 fichiers infectés par le virus CryptoWall**. Si quelqu'un doute sur le besoin d'une protection contre les virus, cet exemple prouve que le risque est réel."

- 16 Mars 2016 IT Jungle

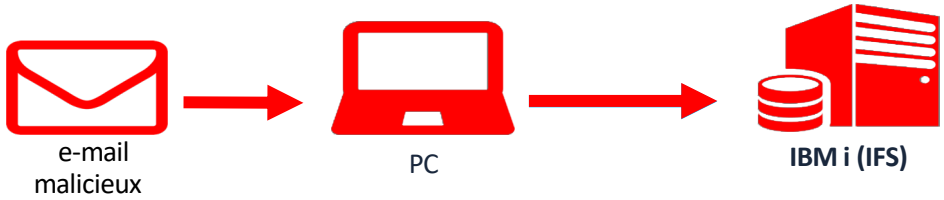
  "Des cyber-intrus ont réussi à accéder à un **AS/400 au sein d'un distributeur d'eau et** ont manipulé le flux de produits chimiques dans l'approvisionnement en eau publique. Par chance, aucune personne n'a été blessé."

La menace du Ransomware

- Le ransomware est une attaque cyber qui bloque un système informatique ou des fichiers jusqu'au paiement d'une rançon.
- Le coût d'une attaque ransomware dépasse les 5 millions de Dollars (Ponemon Institute)
- Toutes les 14 secondes une attaque ransomware sur les entreprises est attendue (Cybersecurity Ventures)
- D'ici 2021, les attaques ransomware coûteront 6 Milliards de Dollars annuellement (Cybersecurity Ventures)
- Le ransomware est en tête de liste (40%) des logiciels malicieux (Verizon)

Comment le Ransomware fonctionne dans un environnement IBM i

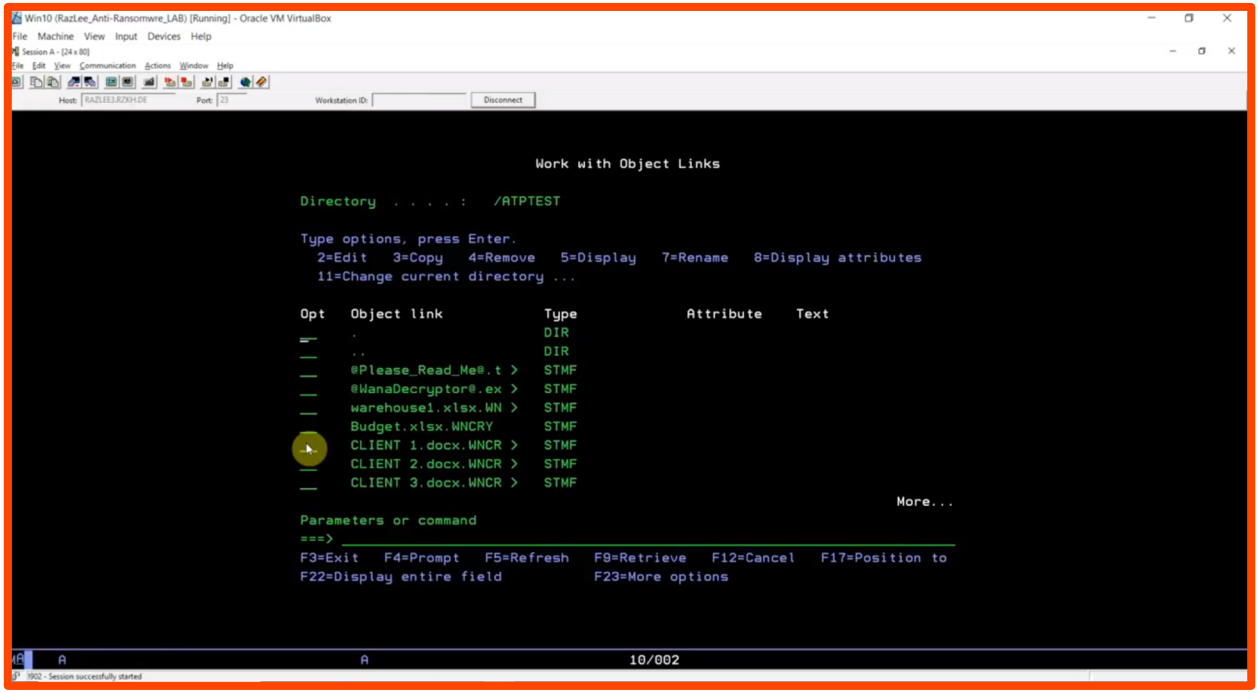
- Le dossier réseau correspondant à l'IFS apparait dans le PC comme un disque



- Le ransomware crypte tous les fichiers de données auxquels il a accès
- Les fichiers IFS deviennent inutilisables

Comment le Ransomware fonctionne dans un environnement IBM i

- Le ransomware crypte tous les fichiers de données auxquels il a accès
- Les fichiers dans l'IFS deviennent inutilisables



iSecurity Anti-Ransomware

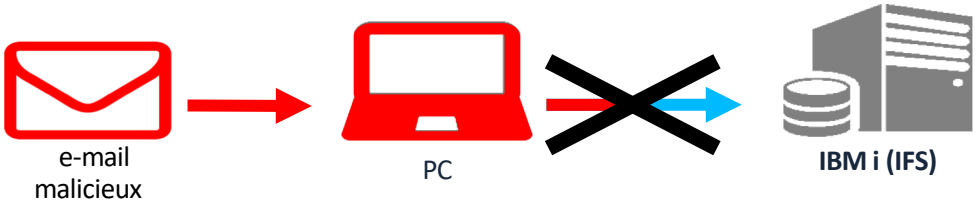
Détection
temps-réel

Arrêts et
alertes

Protège contre
connu et inconnu

- Réponses:
  - Informe l'Opérateur Système, l'Administrateur Sécurité, SIEMs (jusqu'à 3!) etc.
  - Informe le PC infecté qu'il est infecté
  - Déconnecte l'IBM i du PC infecté
  - Peut éteindre ou mettre en veille le PC attaquant
  - Différents types de réponses suivant les situations

iSecurity Anti-Ransomware & IBM i



Alerte: Message, Email, SIEM…

- Des outils de calibration vous permettent de régler la sensibilité par défaut.
- Les mesures prises sont aussi reglables

Le secret – de l’ iSecurity Anti-Ransomware

“S’il ressemble à un canard,
nage comme un canard,
et fait coin-coin comme un canard,
alors c’est probablement un canard."

James Whitcomb Riley (1849-1916)

“Cette citation s’applique au Ransomware."

Shmuel Zailer, CEO, Raz-Lee Security

Test réel

- Testé dans un laboratoire complètement isolé avec : (vidéo labo)
  - IBM i
  - PC Windows avec dossier réseau IBM i
  - Ensemble de 10+ vrais ransomwares (pas des émulateurs)

Sans protection

- Le PC et les fichiers IFS sont cryptés.
- Une demande de rançon apparait dans les deux endroits.
- Les fichiers sont complètement inutilisables.

Avec iSecurity Anti-Ransomware

- Les fichiers de données du PC sont cryptés.
- Quand les fichiers dans l'IFS sont attaqués, l'iSecurity Anti-Ransomware arrête l'attaque immediatement avant compromission du premier fichier.
- Une alerte est envoyée, et l'IBM i est déconnecté du PC attaquant.
- IBM i a survécu à l'attaque!

“Pôts de Miel” et l’Anti-Malware au travail

- Caractéristiques:
  - Pièges personnalisables par défaut
  - Système pour implanter des pièges là où c’est nécessaire
  - Les fichiers “Pots de Miel” sont identifiés même après avoir été copiés, renommés ou déplacés
  - Ils détectent les activités suspicieuses sur les fichiers “Pots de Miel” en temps réel
  - Des seuils assurent des faux positifs minimaux
  - Réponses configurables

Quelques mots supplémentaires…

- Les “pots de miel” Travaillent en parallèle avec les autres
  - Pare-feu
  - Anti-Virus
  - Programme de sortie écrit par l’utilisateur

- Utilisent plusieures méthodes de détection simultanément
- Une des méthodes est d’identifier les noms de fichiers et les extensions de fichiers qui sont utilisés par le ransomware
- Cette information est chargée depuis le web
- L’information peut-être tirée directement du web, ou par le proxy
- Ce site web est mis à jour toutes les 2 heures

- S’installe et fonctionne en moins d’une heure

Est-ce que Ransomware = brèche RGPD ?

- Probablement !
  - Vous devrez prouver que le fichier ne contenait AUCUNE donnée personnelle selon la classification des données de l'entreprise !
  - Même si vous payez la rançon – les données ont été violées
  - Quelqu'un est entré – Comment pouvez-vous être sûr qu'ils ont manipulé SEULEMENT les fichiers du Ransomware
    - Vous devez effectuer une enquête sur une violation de données !

- Votre Ransomware est rapporté sur le DARK Web
  - A tout moment cela peut être rapporté ou publié
  - Vous devrez montrer que vous avez réagi dans les 72 heures suite à la découverte de la violation
    - Vous devez effectuer une enquête sur une violaion de données ASAP

Objectifs de Sécurité du RGPD

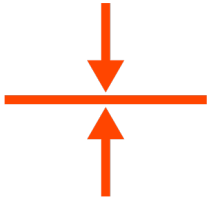
Droit fondamental

Protection des données personnelles

Processus, technologie & automatisation

Obligation légale

Responsabilité de l'entreprise



Base de référence pour la protection des données

Principes de protection des données

Amendes importantes

Principales exigences de sécurité du RGPD

Evaluation

Prévention

Détection

Principales exigences de sécurité du RGPD: Evaluation

- Effectuer des analyses d'impact lorsque le traitement pose un risque majeur aux personnes concernées
- Evaluer également les processus et les profils de l'entreprise
- Articles 35, 84

Evaluation

Analyse approfondie de l'ensemble des forces et faiblesses de la sécurité IBM i, identifiant les risques de sécurité à prendre en compte.

Evaluateur de conformité

Fournit des vérifications de conformité en un coup d'oeil, évaluant l'état de la sécurité, ses forces et ses faiblesses, en fonction des politiques du secteur et de l'entreprise.

Data Discovery

Fournit aux organisations une vue claire et précise de l'emplacement des données réglementées et sensibles présentes sur l'IBM i de leur entreprise.

Authority Inspector

Aide les organisations à minimizer les menaces posées par les autorisations utilisateur trop fortes.

Principales exigences de sécurité du RGPD: Prévention

- Chiffrement – annule la nécessité pour une entreprise d'informer un client d'une violation
- Anonymisation des données – rendre les données incompréhensibles, peu claires
- Pseudonymisation – reduire la possibilité de liaison des données avec l'identité d'une personne
- Contrôle de l'Accès des Utilisateurs Privilégiés
- Minimisation des données – limiter autant que possible la quantité de données à caractère personnel conservées et la durée pendant laquelle elles sont conservées.
- Article 5, 6, 25, 28, 29, 32, 64, 83

Anti-Virus

Protection contre les virus compatibles Windows et les programmes utilisés ou stockés sur le serveur IBM i. Effectue des analyses périodiques pré-programmées automatiques.

Anti-Ransomware

Anti-Ransomware protège les données critiques en détectant et en empêchant, en temps reel, la menace d'endommager l'IBM i et en envoyant un message d'alerte au SIEM.

Encryption

Protège les données sensibles à l'aide d'un chiffrement renforcé (jusqu'à AES 256), gestion des clés et audit intégrés.

Firewall

Un système complet pour la prévention des intrusions qui sécurise tout type d'accès interne et externe au serveur IBM i.

Authority on Demand

Simplifie le processus d'octroi d'autorisations temporaires lorsque celà est nécessaire, économise un temps précieux et des ressources, et impose la séparation des tâches.

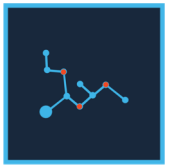
Principales exigences de sécurité du RGPD: Détection

- Données d'Audit– RGPD exige un enregistrement et un audit inattaquables des activités sur les données personnelles
- Surveiller et alerter en temps reel – Les activités relatives aux données personnelles doivent être surveillées en permanence
- Articles 30, 33, 34

Audit
Améliore l'audit natif de l'IBM i en surveillant et en rendant compte de toutes les activités de l'environnement IBM i

AP-Journal
Protège les informations critiques de l'entreprise des menaces internes et des atteintes à la sécurité externe

SIEM/DAM Support
Envoie des alertes en temps réel à des destinataires spécifiques



Change Tracker
Surveille et enregistre automatiquement les modifications d'objet, en particulier celles apportées aux bibliothèques de production

Capture
Effectue la capture, la sauvegarde et la lecture en mode silencieux des sessions utilisateur

Règlementations et Mise en Application de la Protection des Données dans le Monde

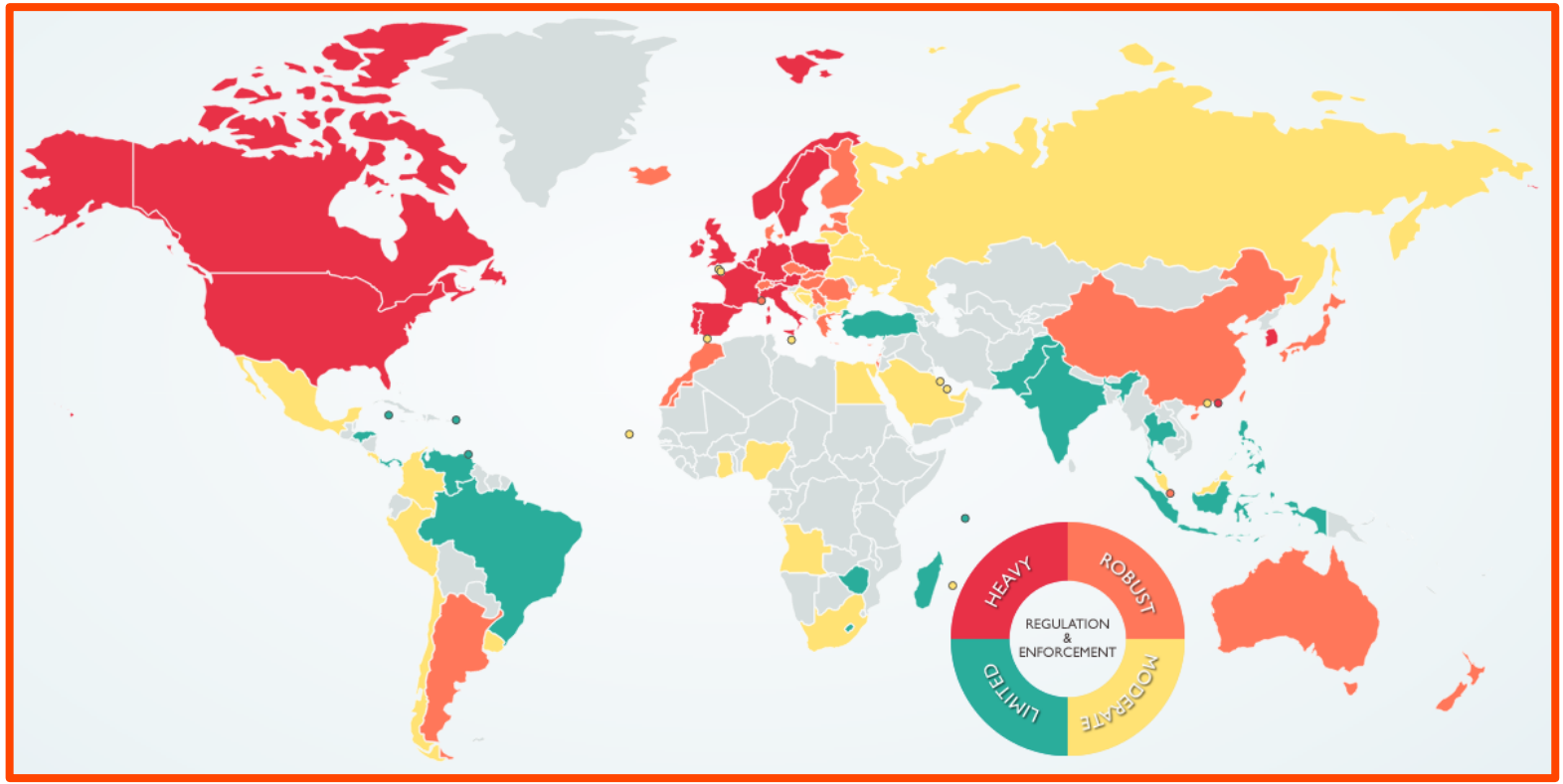


Tableau des Principales Exigences du RGPD

	ARTICLE	POINTS IMPORTANTS	EXIGENCES de SECURITE	iSecurity
EVALUER	Evaluation d'impact de la protection des données *Art. 35 et 84	Evaluation de l'objectif, portée et risque associés au traitement des données	Inventaire des données personnelles dans l'organisation, droits d'accès aux données, et risques associés avec cet accès	▪ Data Discovery ▪ Assessment ▪ Authority Inspector ▪ Compliance Evaluator
PREVENIR	Sécurité du traitement *Art. 5, 6, 26, 28, 29, 32, 64 et 83	Mettre en oeuvre les contrôles de sécurité techniques et organisationnels pour protéger les données personnelles contre les pertes accidentelles ou illicites, destruction, altération, accès ou divulgation	▪ Pseudonymisation et cryptage ▪ Protection en continu ▪ Tests et verifications réguliers	▪ Anti-Ransomware ▪ Encryption ▪ Firewall ▪ Anti-Virus ▪ Authority on Demand
DETECTER	Notification de violation de données *Art. 30, 33 et 34	Notification dans les 72 heures à l'Autorité de Protection des Données après la découverte de la violation des données, et notification aux personnes concernées	Le rapport doit inclure: ▪ Que s'est-il passé (les faits) ▪ Nombre de personnes concernées ▪ Quelle donnée a été violée	▪ Audit ▪ AP-Journal ▪ Capture ▪ SIEM / DAM Support ▪ Change Tracker

iSecurity Field Encryption

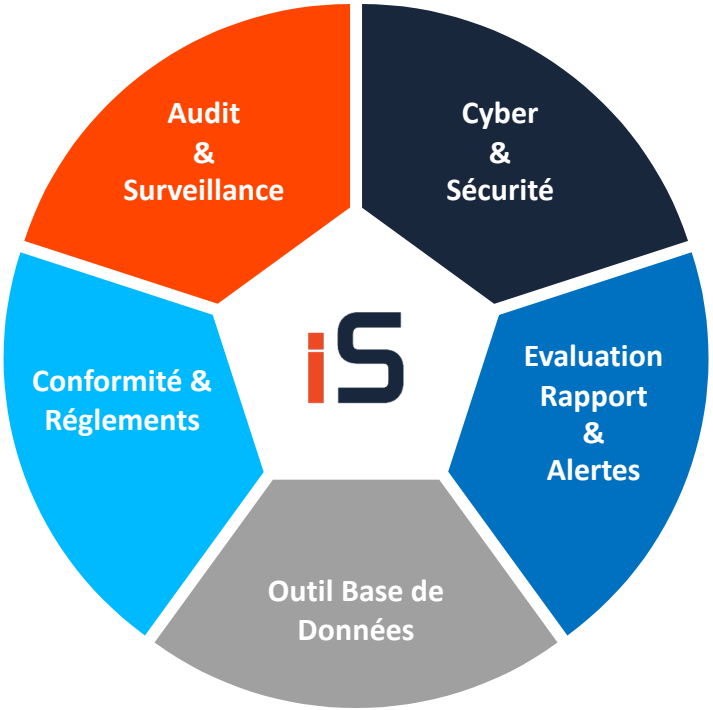
Cybersécurité : Bonnes pratiques et rester informé

Etant donné le besoin urgent qu'ont les entreprises à détecter et arrêter les attaques cyber avant que celles-ci les démolissent, voici 4 conseils que les entreprises de taille petite & moyenne peuvent mettre en pratique pour combattre les attaques cyber.

Les 4 recommandations pour améliorer les bonnes pratiques de cybersécurité :

1. Définir votre structure organisationnelle pour traiter la cybersécurité
2. Identifier les menaces et les opportunités pour améliorer la cybersécurité
3. Dispenser une éducation quotidienne concernant la cybersécurité
4. Mobiliser votre organisation pour la cybersécurité

Solutions iSecurity



- Surveillance base de données
- Audit des systèmes
- Sécurité écran utilisateur
- Gestion de la politique de sécurité

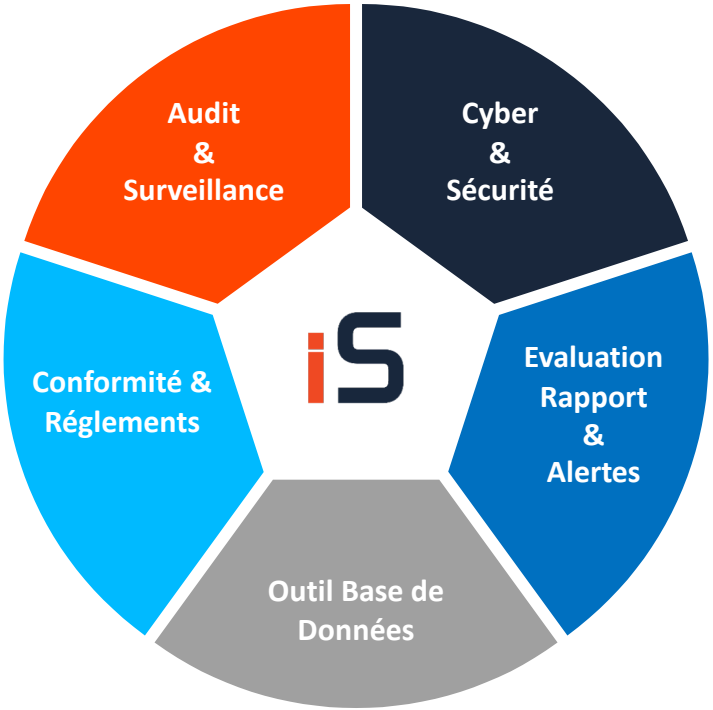
- Protection avancée contre menaces
- Protection des données
- Sécurité du réseau
- Gestion des autorités et utilisateurs

- Evaluation des risques
- Gestion des accès aux données
- Business intelligence
- Evaluation de conformité

- Accès base de données à distance
- Manipulation de données
- Multi-LPAR

- Evaluation
- Détection
- Prévention - protection

Produits iSecurity



- Audit
- AP-Journal
- Change Tracker
- Capture
- Compliance Management

- Firewall
- Encryption
- ATP: Anti-Ransomware, Anti-Virus
- Authority on Demand
- Command
- Password Reset

- Security Investigator
- SIEM/DAM Support
- Compliance Evaluator
- Visualizer

- Update Control
- DB-Gate
- FileScope
- Central Admin

- Assessment
- Detection
- Protection

Partenariats

OEM

imperva

Partenaires Techniques

IBM

McAfee™

Supportés

LogRhythm™

RSA®

QRadar®

splunk>

HP OpenView

ArcSight™ An HP Company

GFI®

Q1 Labs Total Security Intelligence

Tivoli® software

Ils nous font confiance

IPLS et Raz-Lee Experts de la sécurité IBM i

- Audit et conformité
- Monitoring, reporting et alertes
- Prévention et protection contre les menaces
- Accompagnement par les leaders de la sécurité sur IBM i


MERCI