Power Week

Université IBM i 2019

22 et 23 mai

IBM Client Center Paris

S45 - Enjeux de cybersécurité et de conformité sur IBM i : la vision d'un tiers de confiance

Marc LEBRUN, Charles d'AUMALE
DIGITEMIS
contact@digitemis.com

La société DIGITEMIS

DIGITEMIS Cybersecurity & Privacy

CYBERSÉCURITÉ

Sécurité des systèmes d'informations

JURIDIQUE

Protection des données personnelles

FORMATIONS

Formations et sensibilisations

SOLUTIONS

Nos outils innovants d'évaluation, de pilotage et de sensibilisation

LABEL CNIL AUDIT DE TRAITEMENTS N°2016-192 EXPIRE : 30/06/2019

Assurance

LABEL CNIL AUDIT DE TRAITEMENTS N°2016-193 EXPIRE : 30/06/2019

Logement social

LABEL CNIL AUDIT DE TRAITEMENTS N°2016-194 EXPIRE : 30/06/2019

Compteurs communicants

LABEL CNIL AUDIT DE TRAITEMENTS N°2016-195 EXPIRE : 30/06/2019

Informatique & libertés

LABEL CNIL FORMATION N°2017-004 EXPIRE : 12/01/2020

Gestion des données personnelles

LABEL CNIL FORMATION N°2017-005 EXPIRE : 12/01/2020

Devenir Délégué à la Protection des Données

LABEL CNIL GOUVERNANCE RGPD N°2018-242 EXPIRE : 24/05/2021

Gouvernance RGPD

VISA DE SÉCURITÉ — ANSSI — Agence nationale de la sécurité des systèmes d'information

FRANCE CYBER SECURITY

PARTENAIRE RESERVE MILITAIRE de la DEFENSE

PASS FRENCH TECH Accompagner l'hyper-croissance

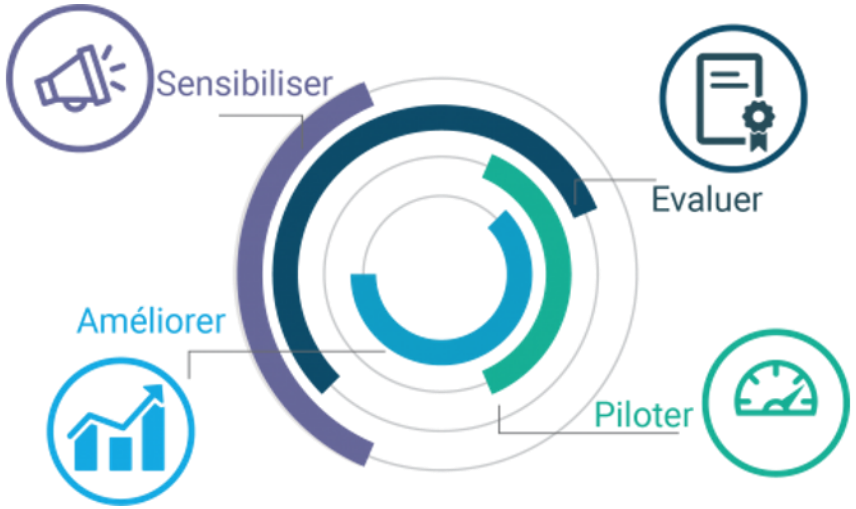
bpifrance

EXCELLENCE 2018

Nos produits logiciels

PERIDIAG®

Un outil fiable d'évaluation et de pilotage de la Cybersécurité des fournisseurs et filiales

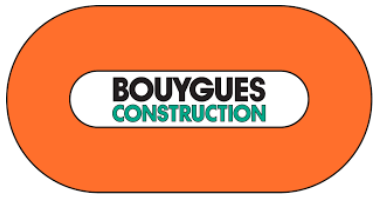


BookMyData®

Solution de gestion de la conformité avec le RGPD

Parmi nos références









Cour des comptes

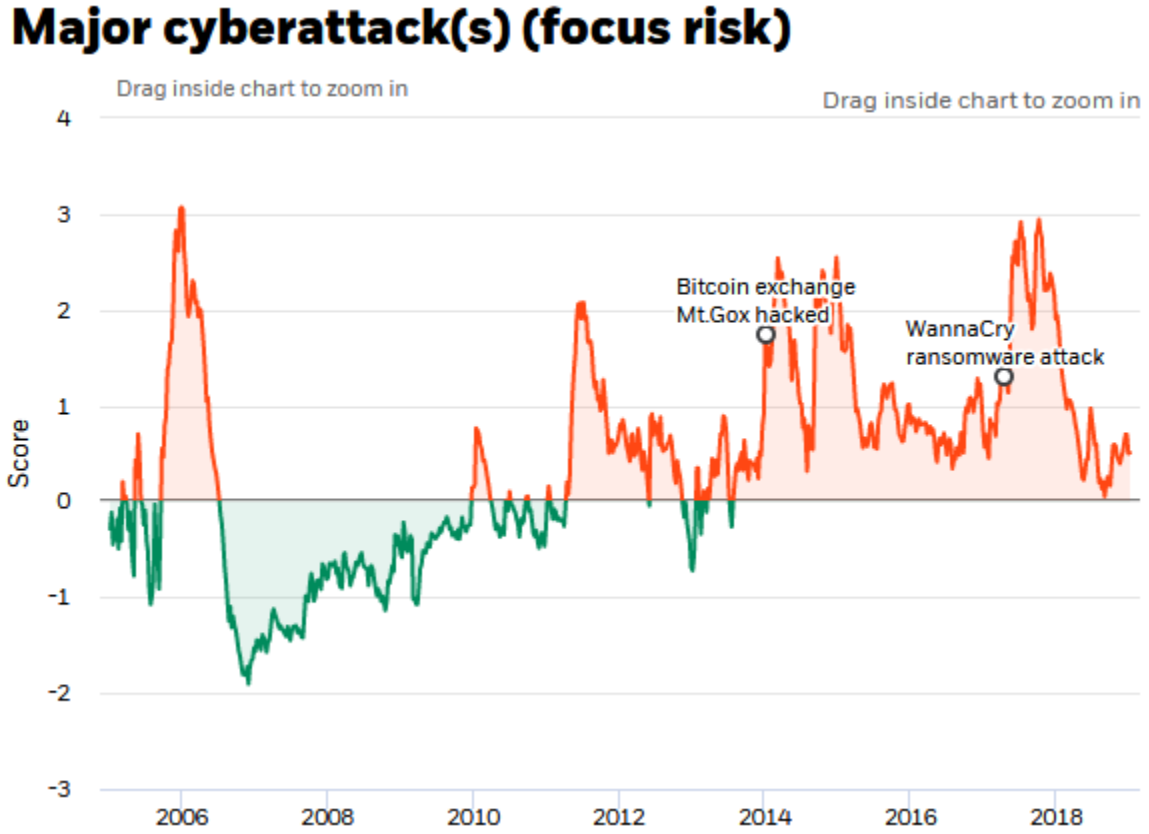
Pourquoi des exigences de sécurité?

La cyber vue par les investisseurs - Blackrock

Top 10 risks, select to view

Sort order: BGRI level

- Global trade tensions
- U.S. - China relations
- Gulf tensions
- European fragmentation
- Major cyberattack(s)
- North Korea conflict
- South China Sea conflict
- Russia - NATO conflict
- LatAm populism
- Major terror attack(s)



https://www.blackrock.com/mx/recursos/herramientas/blackrock-geopolitical-risk-dashboard

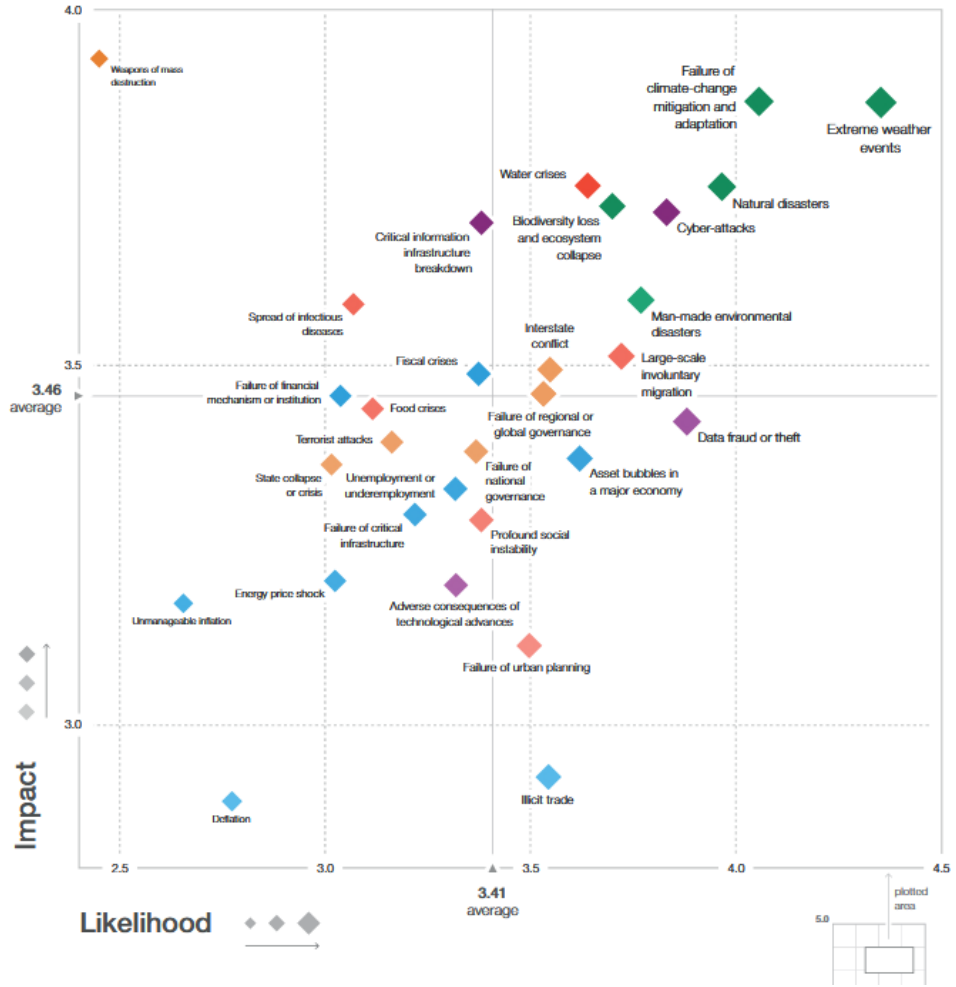
La cyber vue par les dirigeants - World Economic Forum

Cyber et fraudes dans le top 5 des risques

Top 10 risks in terms of **Likelihood**	Top 10 risks in terms of **Impact**
1 Extreme weather events	1 Weapons of mass destruction
2 Failure of climate-change mitigation and adaptation	2 Failure of climate-change mitigation and adaptation
3 Natural disasters	3 Extreme weather events
4 Data fraud or theft	4 Water crises
5 Cyber-attacks	5 Natural disasters
6 Man-made environmental disasters	6 Biodiversity loss and ecosystem collapse
7 Large-scale involuntary migration	7 Cyber-attacks
8 Biodiversity loss and ecosystem collapse	8 Critical information infrastructure breakdown
9 Water crises	9 Man-made environmental disasters
10 Asset bubbles in a major economy	10 Spread of infectious diseases

http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

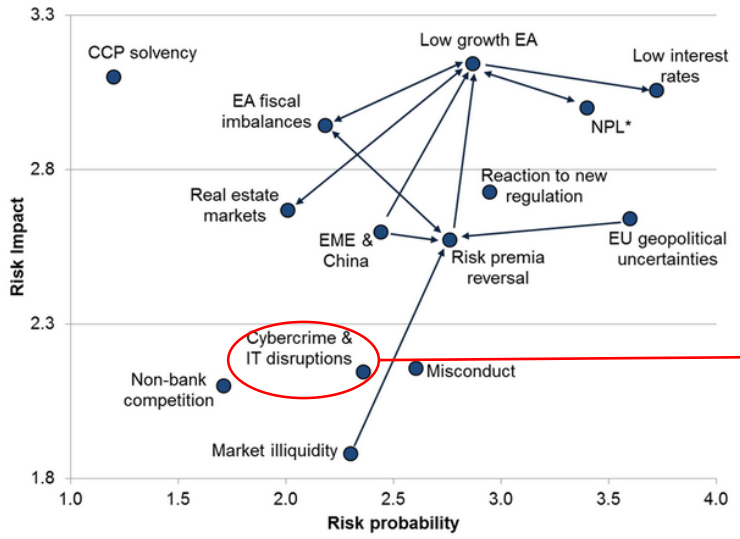
Figure I: The Global Risks Landscape 2019



Cyber et interruption IT – dans le TOP 3 des risques pour la BCE et l'ACPR

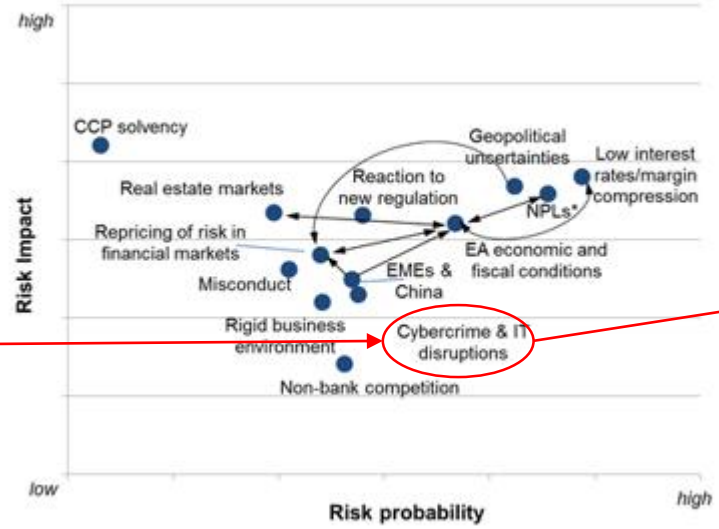
2017

Risk map of the SSM banking system 2017



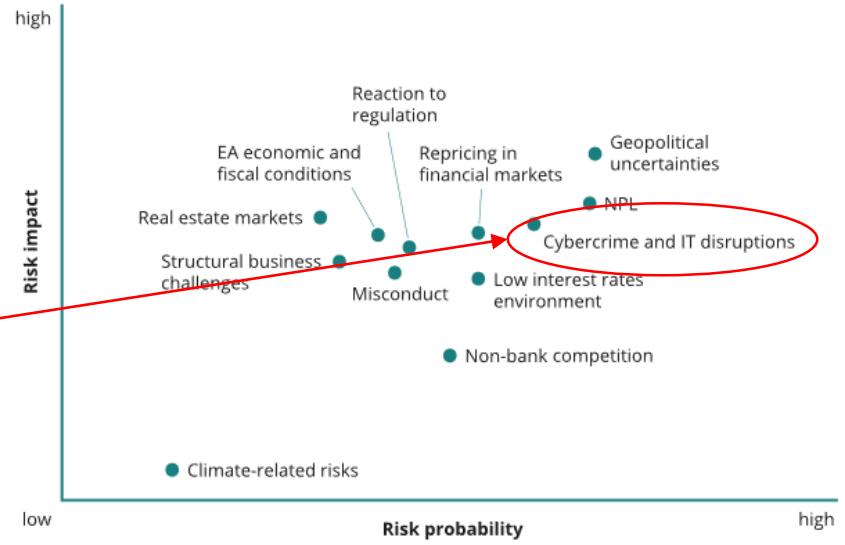
2017

SSM risk map 2018 for euro area banks



2017

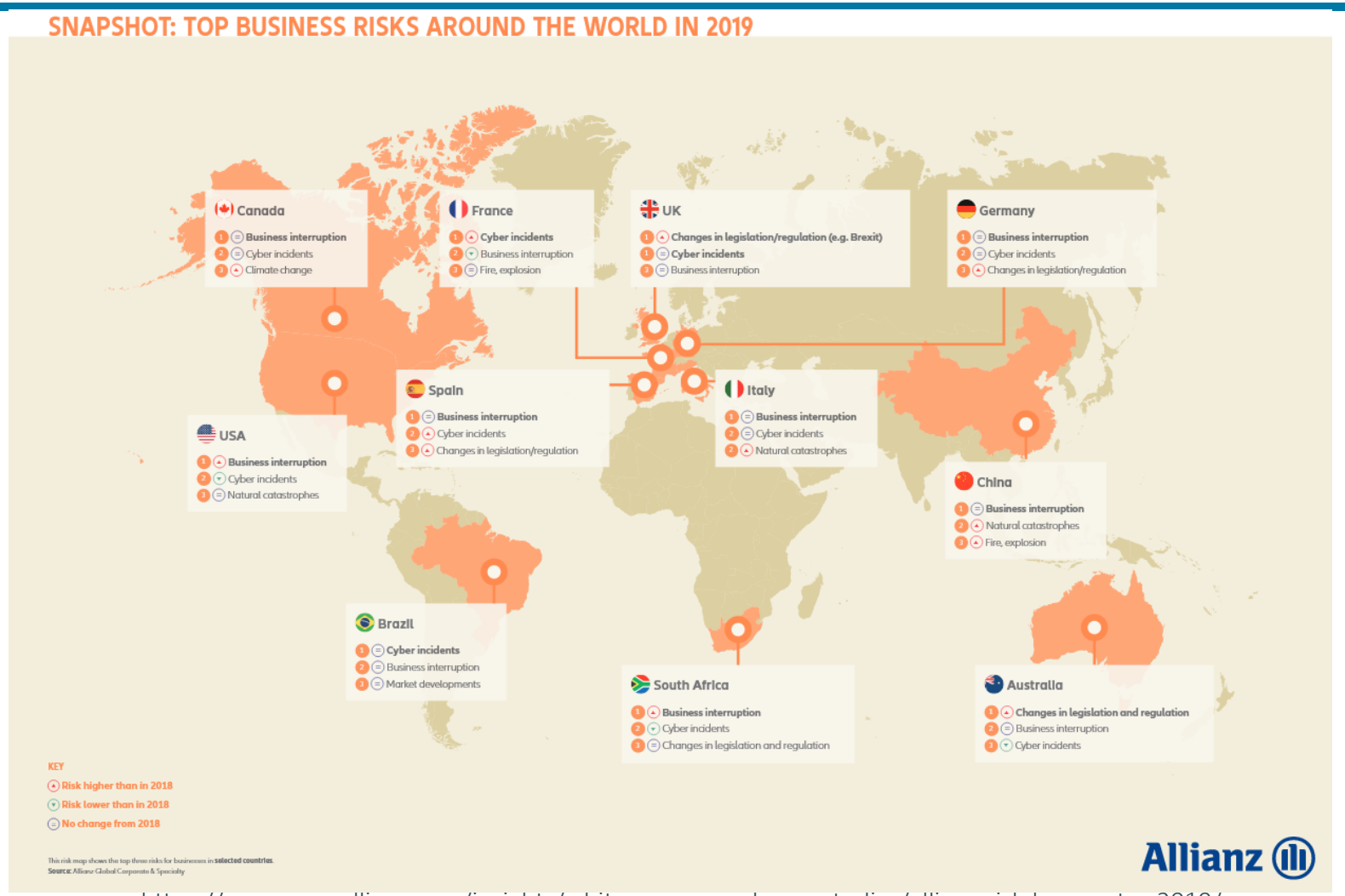
SSM Risk Map for 2019



https://www.bankingsupervision.europa.eu/banking/priorities/risk_assessment/html/index.en.html

https://acpr.banque-france.fr/intervention/quelques-enjeux-pour-le-systeme-bancaire-en-2019

Business interruption et *cyber incidents* en tête des risques en occident



https://www.agcs.allianz.com/insights/white-papers-and-case-studies/allianz-risk-barometer-2019/

Le risque cyber – premier risque en France

TOP 10 RISKS IN FRANCE

Source: Allianz Global Corporate & Specialty.

Figures represent how often a risk was selected as a percentage of all responses for that country.

Respondents: 86

Responses: 106

More than one risk and industry could be selected. Figures don't add up to 100% as up to three risks could be selected.

Rank		Percent	2018 rank	Trend
1	**Cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)**	**41%**	2 (46%)	▲
2	Business interruption (incl. supply chain disruption)	**40%**	1 (47%)	▼
3	Fire, explosion	**29%**	3 (21%)	=
4	Natural catastrophes (e.g. storm, flood, earthquake)	**28%**	4 (21%)	=
5	Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)	**26%**	4 (21%)	▼
6	Market developments (e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)	**18%**	6 (18%)	=
6	New technologies (e.g. impact of increasing interconnectivity, nanotechnology, artificial intelligence, 3D printing, autonomous vehicles, blockchain)	**18%**	8 (14%)	▲
8	Loss of reputation or brand value	**12%**	9 (13%)	▲
8	Product recall, quality management, serial defects	**12%**	7 (16%)	▼
10	Theft, fraud, corruption	**10%**	9 (13%)	▼

https://www.agcs.allianz.com/insights/white-papers-and-case-studies/allianz-risk-barometer-2019/

Le risque cyber – premier risque en France

TOP 10 RISKS IN FRANCE

Source: Allianz Global Corporate & Specialty.

Figures represent how often a risk was selected as a percentage of all responses for that country.

Respondents: 86

Responses: 106

More than one risk and industry could be selected. Figures don't add up to 100% as up to three risks could be selected.

Rank		Percent	2018 rank	Trend
1	**Cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)**	**41%**	2 (46%)	▲
2	Business interruption (incl. supply chain disruption)	**40%**	1 (47%)	▼
3	Fire, explosion	**29%**	3 (21%)	=
4	Natural catastrophes (e.g. storm, flood, earthquake)	**28%**	4 (21%)	=
5	Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)	**26%**	4 (21%)	▼
6	Market developments (e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)	**18%**	6 (18%)	=
6	New technologies (e.g. impact of increasing interconnectivity, nanotechnology, artificial intelligence, 3D printing, autonomous vehicles, blockchain)	**18%**	8 (14%)	▲
8	Loss of reputation or brand value	**12%**	9 (13%)	▲
8	Product recall, quality management, serial defects	**12%**	7 (16%)	▼
10	Theft, fraud, corruption	**10%**	9 (13%)	▼

https://www.agcs.allianz.com/insights/white-papers-and-case-studies/allianz-risk-barometer-2019/

Une multitude d'exigences de conformité

Petit Quizz d'introduction

Que veut dire EBA?

- ❑ European Banking Association
- ❑ European Banking Authority
- ❑ European Burns Association

Pourquoi il faut suivre leur activité?

EBA publishes clarifications to a third set of issues raised by its Working Group on APIs under PSD2 , April 26th 2019

ESAs publish Joint Advice on Information and Communication Technology risk management and cybersecurity , April 10th 2019

EBA consults on guidelines on ICT and security risk management , Dec 13th 2018

…

Une première application concrète avec l'annonce de Bruno Lemaire le 13 mai 2019 avec renfort de la coopération dans le secteur bancaire et test de cyberattaque par la Banque de France

https://www.informanews.net/cybersecurite-du-secteur-financier-cooperation/

Petit Quizz d'introduction

Combien de sociétés européennes concernées par la directive NIS?

- ❑ 10
- ❑ 100
- ❑ 1 000
- ❑ 10 000

Comment suivre le déploiement de la directive?

State-of-play of the transposition of the NIS Directive

https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive

ECS EUROPEAN CYBER SECURITY ORGANISATION DIGITALEUROPE

NIS Implementation Tracker

https://www.digitaleurope.org/resources/nis-implementation-tracker/

Foisonnement de sources d'exigences

Données personnelles

GDPR

General Data Protection Regulation

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

edpb European Data Protection Board

ico. Information Commissioner's Office

An Coimisiún um Chosaint Sonraí Data Protection Commission

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS

Secteur financier

EUROPEAN CENTRAL BANK EUROSYSTEM

EBA EUROPEAN BANKING AUTHORITY

ACPR BANQUE DE FRANCE

esma European Securities and Markets Authority

U.S. SECURITIES AND EXCHANGE COMMISSION

AUTORITÉ DES MARCHÉS FINANCIERS AMF

Autorités SSI

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION ANSSI

enisa European Network and Information Security Agency

U.S. DEPARTMENT OF HOMELAND SECURITY CISA CYBER+INFRASTRUCTURE

Bundesamt für Sicherheit in der Informationstechnik

Standards

NIST National Institute of Standards and Technology U.S. Department of Commerce

ISO 27001

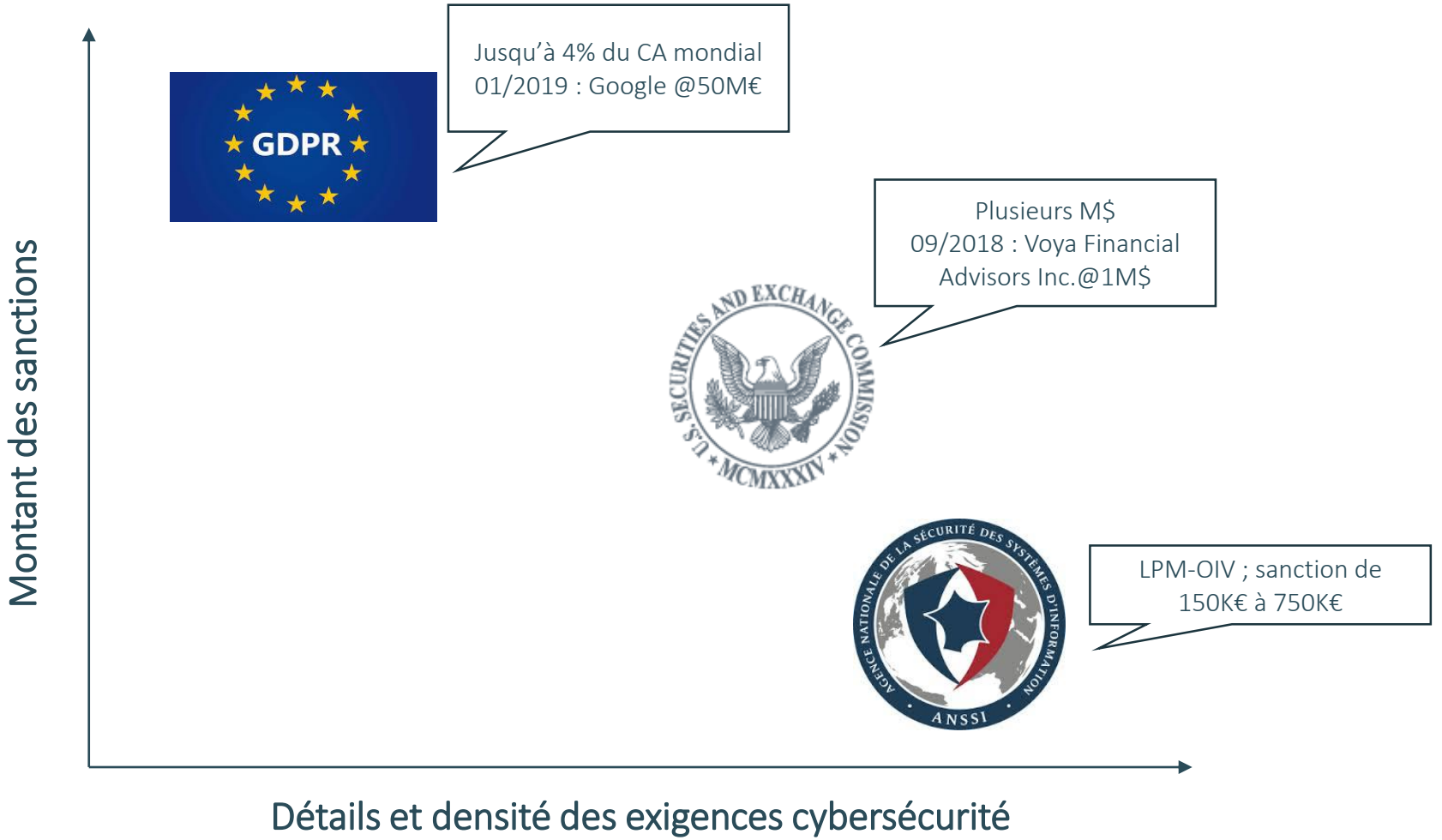
PCI Security Standards Council

ETSI

afnor GROUPE

ISO 26262 Road Vehicles - Fuctional Safety

Densité des exigences et montant des sanctions



Les audits PASSI

- Audit d'architecture
- Audit organisationnel et physique
- Audit de code
- Test d'intrusion
- Audit de configuration

Audit sur IBM i

DIGITEMIS
CYBERSECURITY & PRIVACY

In the Wild

Water treatment plant hacked, chemical mix changed for tap supplies

Well, that's just a little scary

By John Leyden 24 Mar 2016 at 12:19 82 SHARE ▼

Hackers infiltrated a water utility's control system and changed the levels of chemicals being used to treat tap water, we're told.

The cyber-attack is documented in this month's IT security breach report (available here, registration required) from Verizon Security Solutions. The utility in question is referred to using a pseudonym, Kemuri Water Company, and its location is not revealed.

https://www.theregister.co.uk/2016/03/24/water_utility_hacked/

KWC asked Verizon to conduct a cybersecurity assessment as part of their normal operations. As Verizon conducted that assessment they discovered a threat actor was at work stealing financial records and manipulating industrial control parameters used to purify water.

https://www.vericlave.com/wp-content/uploads/2018/10/Vericlave_WhitePaper_KemuriWater_1018_F.pdf

In the Wild

The Internal AS400 Server Compromise

Internal server credentials in plaintext were found on the public facing web server.

Perimeter network access controls allowed direct login from the internet to the internal AS400 server.

Customer Data Compromise

The AS400 server hosted KWC's payment/financial system, which the attackers were able to authenticate due to coincidental and/or available credentials found on the server.

The AS400 server hosted KWC's SCADA control applications, which the attackers were able to authenticate due to coincidental and/or available credentials found on the server.

Accessing the AS400 server provided attackers with approximately 2.5 million customer records, the ability to manipulate SCADA controls (valves, chemical mixtures, and water flow), additional password files, back-office system configuration settings, and other sensitive data.

https://www.vericlave.com/wp-content/uploads/2018/10/Vericlave_WhitePaper_KemuriWater_1018_F.pdf

In the Wild

- Deux principaux profil d'attaquants
  - *Advanced Persistent Threats*
  - Opportunistes : « Si l'ennemi laisse une *porte ouverte*, il faut s'y précipiter »

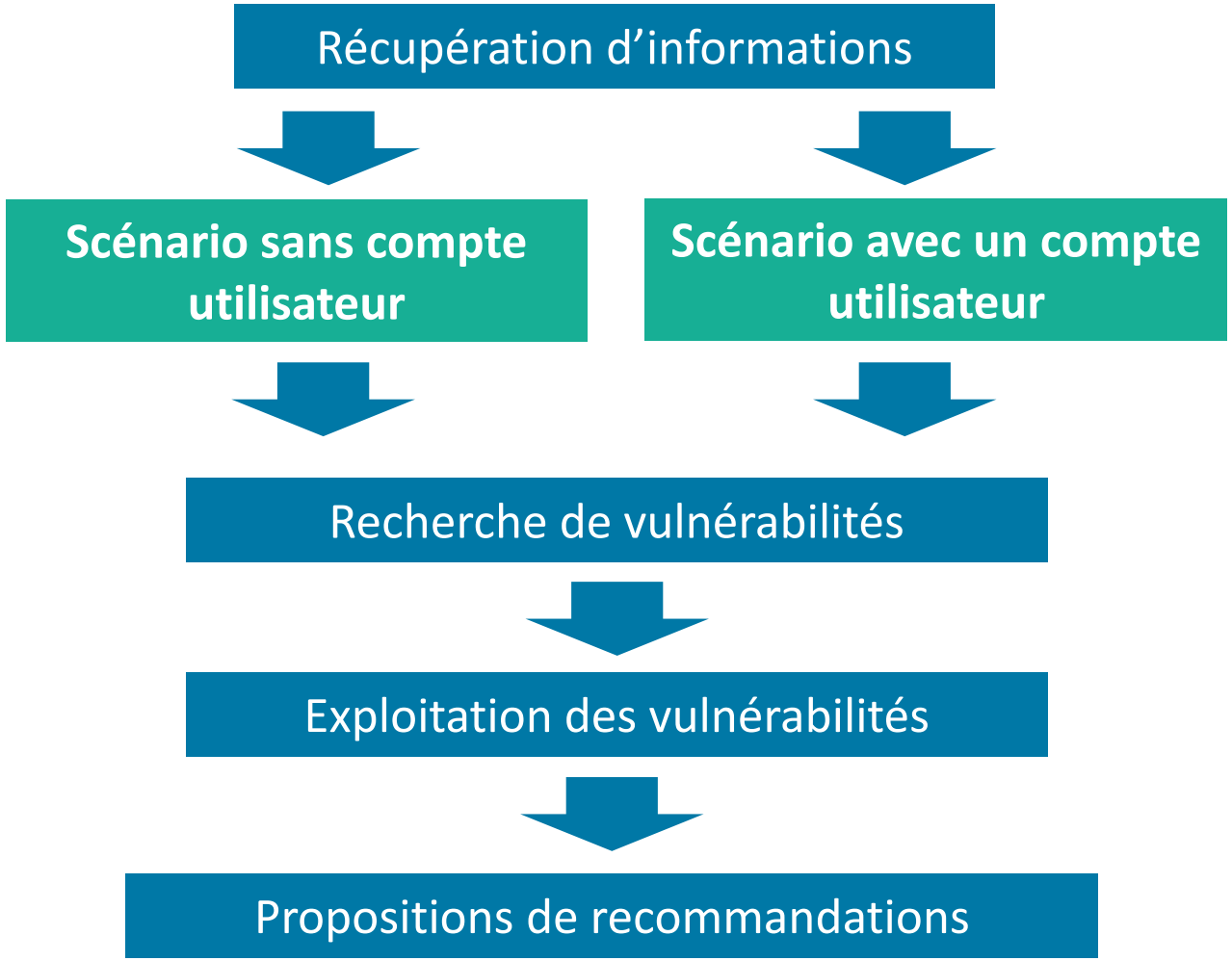
- Se prémunir
  - Défense en profondeur
  - À défaut : détecter, contrer et rétablir
  - Limiter son exposition
  - Durcir les équipements sensibles

Audits techniques sur IBM i

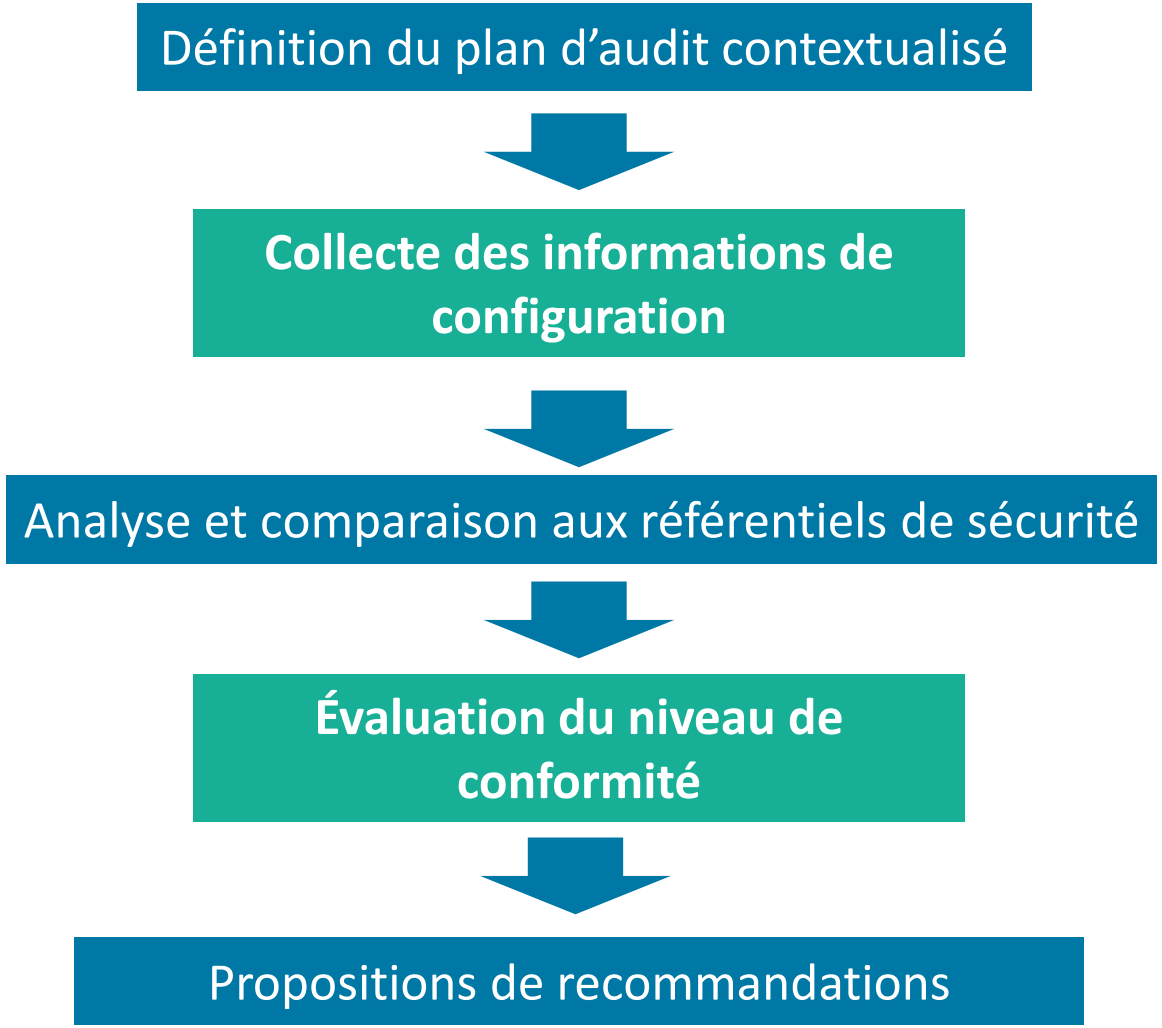
- Deux approches complémentaires

Modéliser des scénarios d'attaque réalistes Approche pragmatique	Tests d'intrusion Boîte noire / grise
Assurer la conformité Confronter l'existant à un référentiel sécurité	Audit de configuration Boîte blanche

Méthodologie d'intrusion



Méthodologie d'audit de configuration



Approche Audit Technique

- IBM i du point de vue du pentester / auditeur
  - Les spécificités
  - Techniques d'attaque particulières
  - Outils d'analyse et d'intrusion

- Comme d'habitude :
  - Protocoles non sécurisés
  - Mots de passe triviaux
  - Attaques sur Websphere
  - Bases de données

Quels référentiels ?

OWASP
Open Web Application Security Project

OSSTMM
www.osstmm.org
Open Source Security Testing Methodology Manual

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

SANS INSTITUTE

IBM Knowledge Center

Home > IBM i 7.4 > Security > Security reference >

Introduction to IBM i security

https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_74/rzarl/rzarlintro.htm

Retours d'expérience : Tests d'Intrusion

- Failles liées aux usages
  - Comptes faibles
  - Accès anonymes
  - Partages réseau permissifs
  - Profils utilisateurs

Table 1. Passwords for IBM-supplied profiles

User ID	Password	Recommended value
QSECOFR	QSECOFR[1]	A nontrivial value known only to the security administrator. **Write down the password that you have selected and store it in a safe place.**
QSYSOPR	QSYSOPR	*NONE[2]
QPGMR	QPGMR	*NONE[2]
QUSER	QUSER	*NONE[2], [3]
QSRV	QSRV	*NONE[2]
QSRVBAS	QSRVBAS	*NONE[2]

The Submit Job (SBMJOB) command allows a job that is running to submit another job to a job queue

User (USER)

Specifies the name of the user profile for the job being submitted.

https://www.ibm.com/support/knowledgecenter/

Retours d'expérience : Tests d'Intrusion

- *Legacy* / rétrocompatibilité
  - Protocoles non sécurisés
  - Paquets logiciels obsolètes

Oracle » JRE : Vulnerability Statistics

Vulnerabilities (**607**) CVSS Scores Report Browse a

Related OVAL Definitions : Vulnerabilities (839) Patc

Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow
2010	1		1	
2011	3			
2012	59	3	1	
2013	180	1	10	4
2014	115	1	1	
2015	80			
2016	37		1	1
2017	69	14		
2018	55	17	2	
2019	8	1		
Total	607	37	16	5

https://www.cvedetails.com/vulnerability-list/vendor_id-93/product_id-19117/Oracle-JRE.html

Retours d'expérience : Tests d'Intrusion

- Applications Web
  - Serveurs applicatifs (interfaces d'administration) non sécurisés
  - Vulnérabilités applicatives

Retours d'expérience : Audit de configuration

- QSECURITY : arbitrage entre conformité et productivité

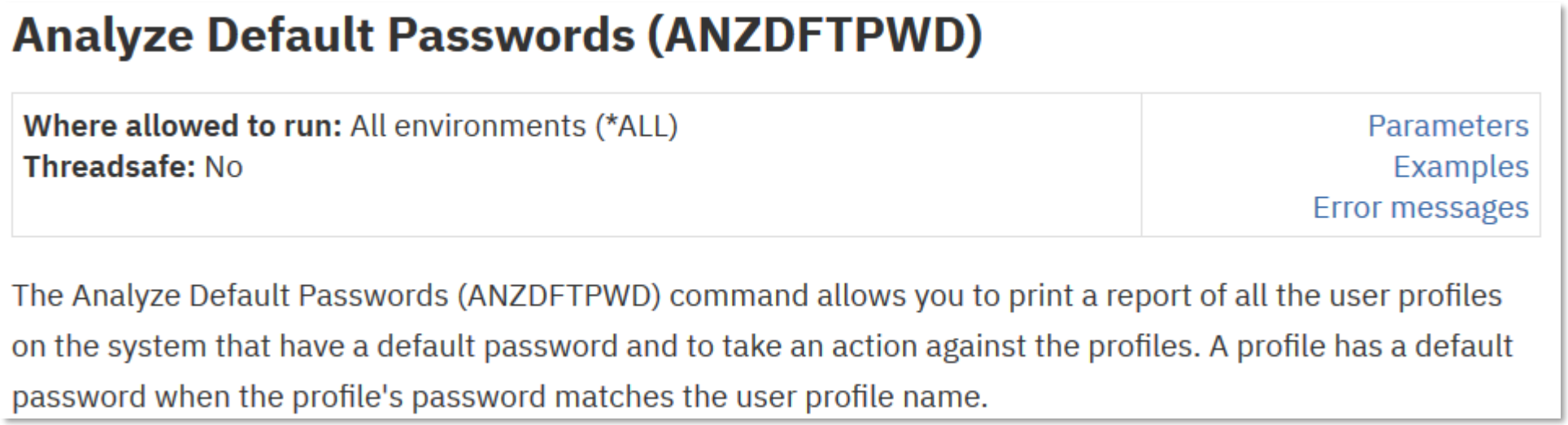
> At security level 30 and below, signing on by pressing the Enter key without a user ID and password is possible with certain subsystem descriptions. At security level 40 and higher, the system stops any attempt to sign on without a user ID and password.

> If a user profile name is used as the value for the User field in a job description, any jobs submitted with the job description can run under that user profile. Thus an unauthorized user might submit a job to run under the user profile specified in the job description.
>
> At security level 40 and higher, the job will fail unless the user submitting the job has *USE authority to both the job description and the user profile specified in the job description. At security level 30, the job runs if the submitter has *USE authority to the job description.

https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_74/rzarl/rzarlseclvl.htm

Retours d’expérience : Audit de configuration

- Politique de mots de passe : des outils efficaces



Analyze Default Passwords (ANZDFTPWD)

Where allowed to run: All environments (*ALL)
Threadsafe: No

Parameters
Examples
Error messages

The Analyze Default Passwords (ANZDFTPWD) command allows you to print a report of all the user profiles on the system that have a default password and to take an action against the profiles. A profile has a default password when the profile's password matches the user profile name.

https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_74/cl/anzdftpwd.htm

Retours d'expérience : Audit de configuration

- Défauts de contrôles d'accès
  - Partages, ressources locales
  - Fonctions système sensibles : CRTUSRPRF, CHGSYSVAL, …
- Excès de droits sur les profils d'utilisateurs
  - Beaucoup de profils à auditer…
- Supervision des évènements de sécurité balbutiante
  - Configuration des files d'attentes de message
  - Centralisation sur un serveur tiers
  - Traitement humain, corrélation

RGPD & IBM i

- Article 32 : « Sécurité du traitement »
  - Chiffrement des flux
  - Chiffrement des données
  - Sauvegardes
- Anonymisation / pseudonymisation
- Conservation
- « Tester, analyser et évaluer l'efficacité des mesures techniques et organisationnelles »

Soyez moteur dans la gouvernance SSI

DIGITEMIS
CYBERSECURITY & PRIVACY

La check list de la gouvernance SSI

- Conformité et amélioration continue
  - Plan d'action et suivi
  - […]
- Organisation et responsabilités
  - Y a-t-il une organisation à 2 ou 3 niveaux de supervision (opérations / risques / audit)
  - Qui est responsable de la sécurité opérationnelle? De la supervision de la sécurité?
  - Combien d'échelon entre RSSI et CEO?
  - Est-ce que le COMEX et le BOARD ont une vision régulière de la SSI?
- Budget SSI
  - 5 à 10% du budget IT
- Valorisation
  - Méthodologie AMRAE / FERMA sur l'évaluation des risques et assurance cyber avec réduction des risques
  - Marketing et mise en avant de certifications

contact@digitemis.com

+33 9 72 46 39 78

www.digitemis.com

DIGITEMIS
CYBERSECURITY & PRIVACY