FAIRE FACE À DES
FAILLES DE SÉCURITÉ
FUITES DE DONNÉES PERSONNELLES

« DÉCRYPTAGE ET PRÉVENTION DES CYBER ATTAQUES »

CNEJITA 18 JUIN 2018
ESSEC CNIT
PARIS LA DEFENSE

Bruno HAMON
bhamon@mirca.fr

Fondateur et PDG de MIRCA : Audit, Conseil et Formation

- gestion risques IT - cyber risques
- sécurité patrimoine informationnel / systèmes d'informations
- gestion de crise / cyber crise

Diplômé de l'Institut National des Hautes Etudes de la Sécurité et de la Justice

- Fichiers de police (2014) / Cybercriminalité (2015)

Enseignant grandes écoles et instituts

Membre actif de l'AFNOR depuis 2005

- PCA (Réf. BP Z74-700 Mars 2011) : Plan de Continuité d'Activité
- DLP (Réf. BP Z90-001 Déc. 2014) : Prévention et Gestion de la Fuite d'Information
- APTs (Réf. BP Z90-00é Janv. 2018) : Prévention, Détection Traitement des Nouvelles menaces

Animateur / Conférencier en gestion des risques

- Afnor / Assises de la Sécurité / Clusif / FIC / Isaca / Medef/ Security Day ..

SCENARIO d'un Exercice de GDC avec PMR
(Pression Médiatique Réelle)

CNEJITA EXPERTS

MIRCA BUSINESS DATA SECURED

FLASH INFO

xxxxxx, le banquier du cinéma, victime de hackers

Ces derniers menacent de révéler sur les réseaux sociaux des données ultraconfidentielles de clients de la banque

FLASH INFO

C'est confirmé !

xxxxxx, le banquier du cinéma, est victime de hackers

Des données ultraconfidentielles de clients sont actuellement révélées sur les réseaux sociaux

FLASH INFO

xxxxxxxx, le banquier des stars du cinéma, vraiment dans la tourmente

Des N° de comptes bancaires avec le montant de leurs avoirs associés sont désormais en ligne sur plusieurs sites

Plusieurs noms circulent parmi lesquels des personnalités emblématiques du cinéma

FLASH INFO

Une dizaine de célébrités ayant des avoir chez xxxxxx viennent de faire savoir par la voix de leurs avocats leur intention de quitter l'établissement

Ils menacent de porter plainte

FLASH INFO

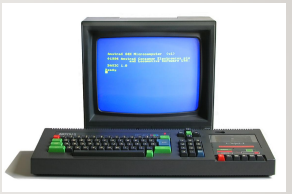
Sur le site 01Net.com, un expert en sécurité de l'ANSSI pose la question à la direction générale ainsi qu'à celle des systèmes d'information de xxxxxxxxx :

« Comptez-vous et comment allez-vous régler cette fuite ? »

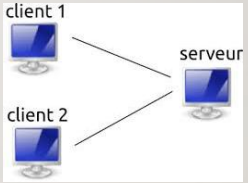
REVOLUTIONS TECHNOLOGIQUES

CES 25 DERNIÈRES ANNÉES

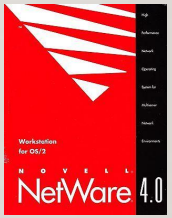
- 1980 : le monde du PC



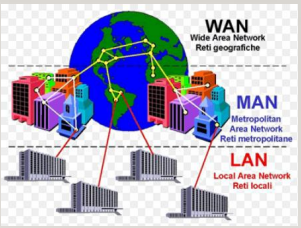
- 1985-1990 : l'Architecture Client-Serveur



- 1990 -1995 : le réseau Lan



- 1995 - 2000 : le WAN - le MAN

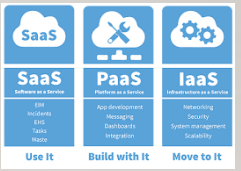


CES 25 DERNIÈRES ANNÉES

- 1994 - 2018 : Internet - Sécurité - e-Commerce

- 2003 : la Mobilité - les Smartphones

- 2010 : le Cloud



- 2015 : les IOT

- 2010- 2018 : la Transformation Numérique

MOBILITE : 20 ANNÉES D'ÉVOLUTION

OBJET CONNECTE : 15 ANNÉES D'ÉVOLUTION

PIRES SCÉNARIOS : ET SI DEMAIN …..

Exploitation de faille de sécurité dans un barrage pour l'ouverture de vannes ?

Contrôle à distance de transformateurs de centrale nucléaire ?

PIRES SCÉNARIOS : ET SI DEMAIN …..

Pour un état, perte du contrôle du trafic aérien au profit d'un autre ?

Déviation d'un bateau pour le lancer sur un port !

Exemple : Méthanier

(345m Long - 54m large; + grand que Charles De Gaulle- 266000 m3 GNL (= consommation ville de Lyon / un an)

Cyber-attaque sur un sous-marin dans un port avec un réacteur allumé !

Enjeux
d'aujourdhui et de demain

AUJOURD'HUI

Internet World Stats
Usage and Population Statistics

WORLD INTERNET USAGE AND POPULATION STATISTICS DEC 31, 2017 - Update						
World Regions	Population (2018 Est.)	Population % of World	Internet Users 31 Dec 2017	Penetration Rate (% Pop.)	Growth 2000-2018	Internet Users %
Africa	1,287,914,329	16.9 %	453,329,534	35.2 %	9,941 %	10.9 %
Asia	4,207,588,157	55.1 %	2,023,630,194	48.1 %	1,670 %	48.7 %
Europe	827,650,849	10.8 %	704,833,752	85.2 %	570 %	17.0 %
Latin America / Caribbean	652,047,996	8.5 %	437,001,277	67.0 %	2,318 %	10.5 %
Middle East	254,438,981	3.3 %	164,037,259	64.5 %	4,893 %	3.9 %
North America	363,844,662	4.8 %	345,660,847	95.0 %	219 %	8.3 %
Oceania / Australia	41,273,454	0.6 %	28,439,277	68.9 %	273 %	0.7 %
WORLD TOTAL	7,634,758,428	100.0 %	4,156,932,140	54.4 %	1,052 %	100.0 %

Internet Stats and Facebook Usage in Europe December 2017 Statistics					
EUROPE	Population (2018 Est.)	Internet Users, 31-Dec-2017	Penetration (% Population)	Users % in Europe	Facebook 31-Dec-2017
France	65,233,271	60,421,689	92.6 %	8.6 %	33,000,000

1 MINUTE SUR INTERNET ! (2018)

1991 = 1er site Web (poignée users) **2018 = + 1,2 milliard de sites Web**

ACTUALITÉS DE NOS CHERS MÉDIAS !

IL Y A QUELQUES MOIS ! TRIBUNE DE GENÈVE 05.04.2016, 21H28

« Enorme » fuite de données

à Panama : 12 chefs d'Etat touchés,

des hauts dignitaires, des hommes d'affaires, mais aussi des criminels

- Sur la période de juin à déc. 2015, + de 2,6 To de données sensibles ont été exfiltrées peu à peu du cabinet d'avocats Mossack Fonseca

- 11,5 M de fichiers, concernant des grandes fortunes et leurs placements financiers opaques, plus ou moins légaux

IL Y A UN MOIS ! (14/05/2018 - 16H47)

Nouvelle annonce sur la Fuite de données : 3 millions d'utilisateurs touchés !

Des DP (test de personnalité) accessibles en ligne pendant 4 ans !
(identifiant + MDP : accès à la base - disponibles en ligne durant ces années sur un site dédié aux développeurs)

De nouvelles accusations pour Facebook

SAVEZ VOUS


Top 10 des menaces pour une entreprise
1st Cyber attaque
2nd Violation des données
3rd Panne informatique ou de télécommunication
4th Acte de terrorisme
5th Incident de sécurité
6th Interruption des services publiques
7th Pertubation de la chaîne d'approvissionnement
8th Conditions climatiques défavorables
9th Disponibilité des talents / des compétences clés
10th Incidents liés à la santé et la sécurité
Source : Horizon scan report 2016

PROTECTION DU PATRIMOINE INFORMATIONNEL

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

IL Y A COMME UN PROBLÈME !

IL Y A COMME UN PROBLÈME

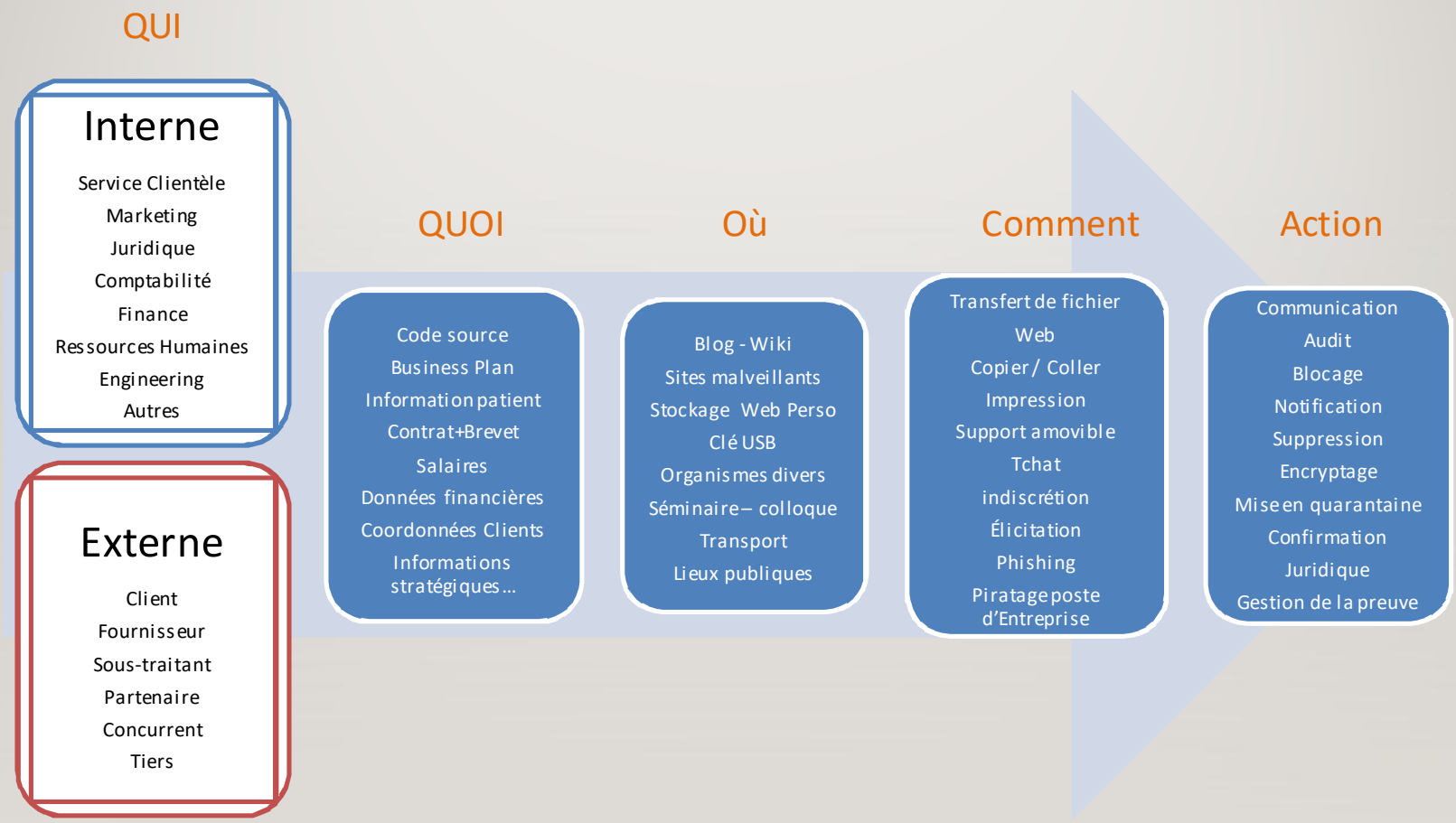
DÉFINITION : LE DATA LEAK PREVENTION (DLP)

- **AFNOR BP Z 90 -001 v1.0**

« Ensemble de mesures organisationnelles et techniques visant à identifier, surveiller, et protéger l'information qu'elle soit stockée, en mouvement ou en cours d'utilisation »

« La prévention et la gestion de la fuite de l'information sont basées sur des politiques centralisées et une analyse approfondie du contenu et de son contexte »

ETAPES DE LA FUITE DE DONNÉES



INFORMATIONS/ DONNEES « SENSIBLES »

- **Informations auxquelles une organisation attache une forte importance, quel que soit le motif de son attachement.**
- **Informations confidentielles :**
  - **Relevant du secret des affaires,**
  - **Secret professionnel,**
  - **Offrant un avantage concurrentiel,**
  - **Protégées par un droit de propriété intellectuelle,**
  - **DP (au sens CNIL)**
  - **Autres ….**

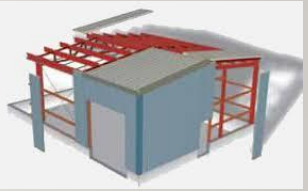
90 % des données dans le monde ont été produites sur les 2 dernières années !

70 % des données en entreprises ne sont pas utilisées

Il appartient à chaque organisation de déterminer elle-même l'importance qu'elle attache à quelles informations.

DIFFÉRENTS VECTEURS DE FUITES DE DONNÉES

- **Structures du bâtiment :**
  - **Fenêtres, portes, parois, tuyaux, radiateurs,**



- **Médias : Les câbles, les ondes, les réseaux**
  - **Réseaux électriques, téléphoniques, informatiques, hauts parleurs, sonorisations, vidéo portiers, vidéo surveillance, alarmes, télésurveillance,**

- **Facteur humain : le maillon faible ?**
  - **Principaux moteurs de motivation : argent, pouvoir, sexe, vengeance.**
  - **Distraction, étourderie, maladresse (parfois liés à la fatigue, le stress ou le surmenage).**

NOUVELLES GENERATIONS DE MENACES

UNE CHOSE TRÈS IMPORTANTE

La 1ère question à vous poser n'est pas tant :

« Puis-je être victime d'une nouvelle menace ? »

ou

« Quand vais-je l'être ? »

mais plutôt

« Ne le suis-je pas déjà ? »

10 + GRANDES CYBERATTAQUES EN 2017

N°1 Mai 2017 : WannaCry / NSA : + importante cyberattaque ransomware de l'histoire.
Quelques heures = + 300 000 PCs dans + 150 pays (faille déjà identifiée par Microsoft mais patch correctif pas suffisamment installé !) Coûts = environ 1 milliard $

N°2 Juin 2017 : Petya / NotPetya : Petya : ransomware (faille sécurité Windows). Rançon = 300 $ (bitcoins) pour récupération fichiers.
NotPetya : virus déguisé en ransomware : 1 seul poste non mis à jour sur un réseau => ensemble du réseau compromis.
Environ 2 000 sociétés infectées (ex. Saint-Gobain et un coût de 220 millions €). NB : impossible pour les victimes de payer la rançon (clé décryptage) : adresse mail associée à l'attaque invalide !

N°3 Septembre 2017 Deloitte : accès informations privées (via identifiant + mdp admin) + accès à Cloud Azure (Microsoft) : plateforme hébergement data Deloitte.

N°4 Septembre 2017 Equifax : société crédit US (spécialité : protection des données !) .
Informations de + 140 millions d'américains + 200 000 N° CB consultés par les pirates.
Exploitation d'une faille applications de Equifax. NB : Après attaque : démission PDG

N°5 Septembre 2017 Netflix : campagne scam vers millions users via mails depuis l'adresse supportnetflix@com.
Communiquer : coordonnées bancaires (éviter la clôture)

10 + GRANDES CYBERATTAQUES EN 2017

N°6 Octobre 2017 : DoubleLocker : ransomware vers les appareils mobiles /Androïd.
1ère fois : un virus parvient à changer le code PIN. Puis chiffrement données. Pas d'autres choix : payer

N°7 Novembre 2017 : PowerShell : campagne APT massive de cyber-espionnage
Dirigée contre Arabie Saoudite via logiciel Powershell (très difficile à détecter)

N°8 Novembre 2017 Imgur : site de partage d'images (date de 2014 et découverte qu'en 2017).
Près de 1,7 millions victimes (dérober leurs DP : adresses email + mdp)

N°9 Novembre 2017 Uber : 57 millions comptes utilisateurs piratés.
UBER aurait pris la décision de payer. Rançon = 100 000 $ (échange destruction données piratées, sans avoir l'assurance que celle-ci soit réellement effectuée).
Affaire mise sous silence pendant 1 an = éveil des consciences (enjeu majeur).

N°10 Décembre 2017 NiceHash : plateforme slovène de minage de Bitcoins .
Victime d'une cyberattaque : 4 700 bitcoins dérobés (équivalant : 64 millions $)

DÉFINITION APT = ADVANCED PERSISTENT THREAT

A pour « AVANCEE » qui signifie :

- utilise tout un arsenal de techniques d'attaques et d'outils pour atteindre son objectif
- unitairement les composants d'une telle attaque ne sont pas forcément "évolués" techniquement (phishing, malware, XSS, etc.)
- Des outils de génération de composants d'attaques existent (ex. Poison Ivy, etc.)

La combinaison des méthodes
et outils d'attaques en font une attaque avancée.

DÉFINITION APT = ADVANCED PERSISTENT THREAT

P pour « PERSISTANTE » qui signifie :

- a réussi à passer outre vos équipements de détection
- est basée sur une stratégie dont l'objectif est de rester le plus longtemps possible sans éveiller les soupçons (furtivité) (par opposition à une attaque "opportuniste")
- est scénarisée par ses attaquants avec des objectifs précis (compromission de tout ou partie de la chaine des systèmes)

L'objectif consiste à rester sous les "radars" ("low and slow")

DÉFINITION APT = ADVANCED PERSISTENT THREAT

T pour « THREAT / MENACE » qui signifie :

- Implique une coordination de moyens techniques et humains
- Préparée, ciblée, travaillée
- Généralement peu automatisée
  (bien que certaines compromissions de systèmes puissent l'être)

Les attaquants sont motivés !

Ils se dotent de compétences techniques
et de moyens inhabituels.

PROFILS CYBER ATTAQUANTS

Cyber violents visent les personnes, les internautes
(menaces, insultes, diffamations, harcèlements)

Cyber escrocs appât du gain
(relèvent d'une délinquance à grande échelle organisée)

Cyber espions s'approprier données sensibles
(stratégiques/économiques)

Cyber mercenaires : proposent services sur Darknet
(perpétrer attaques pour états, individus ou organisations)

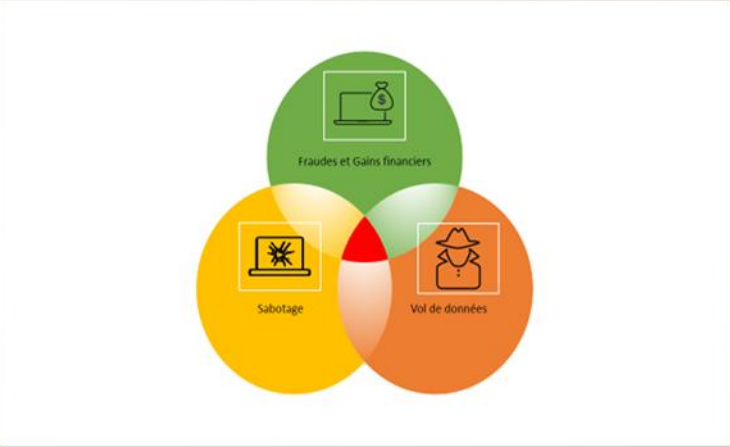
Cyber terroristes : idéologies extrémistes
(utilisent Internet comme tribune / moyen de radicalisation)

OBJECTIFS ET PROFILAGE DES NOUVELLES CYBER-MENACES

Risques se matérialisent de manière unitaire et/ou par le jeu de combinaisons

Parmi ces grands risques, on distingue :

- Sabotage / panne
- Fraude / gain
- Exfiltration / exploitation de données



Autres finalités : blocage, destruction, notoriété, intérêt personnel, chantage, vol de données, intelligence économique ou même cyber-guerre (cyberattaques d'Etat)

Et autres motivations :

- raisons politiques
- raisons morales (Ashley Madison, …)
- réputation (Sony,..)
- parfois simplement par « jeu » !

ENJEUX DES 20 PROCHAINES ANNÉES

- Cyberéconomie, Cybercommerce, Cyberconsommation
- Cybermenaces, Cybercriminalité, Cyberguerre,
- Cyberincidents, Cybersécurité, Cyberconférence,
- Cyberdéfense, Cyberattaque, Cyberconflits,
- Cybercollaboration, Cyberdémocratie, Cyberjustice,

Le « Tout Cyber » : la norme pour le futur

Aujourd'hui, aucune crise dans le monde de quelle nature que ce soit ne présente pas une cyber-dimension, ou un cyber-aspect !

COMMENT FAIRE FACE AUX NOUVELLES MENACES

Face à l'évolution constante des nouvelles typologies d'attaque comme de leur multiplication, nécessité de :

1. réviser les stratégies : SSI, CA, DLP, GdC (en coord. avec : RSSI, RPCA, DPD)

2. se poser de nouvelles interrogations :
   - *mon PCA actuel qui couvre les sinistres classiques permet-il également de répondre à une cyberattaque ?*
   - *mon SI actuel peut-il devenir un facteur d'aggravation d'une crise cyber ?*
   - *mon organe de GdC actuel est-il adapté pour gérer une crise cyber ?*
   - *plus globalement, mon organisation est-elle prête / cyber résiliente ?*

Réponses : investiguer de nouvelles pistes de travail

SE POSER DE NOUVELLES INTERROGATIONS !

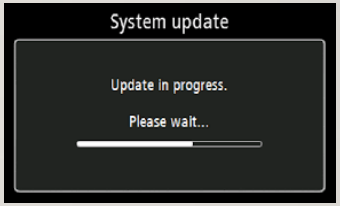
1. Quelles sont les nouvelles menaces qui pourraient impacter mon SI ?
2. Sur quel périmètre ces nouveaux types d'attaques pourraient-ils m'impacter ?
3. En cas d'activation, comment m'assurer de l'intégrité de mon SI ?
4. Quelles seraient/pourraient être les solutions complémentaires à mettre en œuvre ?
5. Les acteurs de mon organisation sont-ils sensibilisés aux spécificités d'une attaque cyber ?
6. En cas d'attaque avérée, qui peut/doit veiller à conserver un maximum de trace ?
7. Comment qualifier l'attaque (sabotage, fraude, vol de données) et son impact ?
8. Ais-je réalisé un test dans mon organisation avec pour scénario une cyber attaque ?

Indispensable et forte collaboration entre métiers et équipes SSI
Prise de conscience et implication forte de la DG

DES MOYENS DE PROTECTIONS

Maintenir à jour ses systèmes

- *Systèmes et applications (Java, IE, PRA, etc.)*
- *Protection périmétriques (Firewall, IDS, IPS, DLP, etc.)*



- *Solutions antivirales, antimalware, ..*
- *Pour mémoire :*
  - *L'attaque Aurora aurait pu être stoppée, ou ralentie si des utilisateurs n'utilisaient pas IE6.*

DES MOYENS DE PROTECTIONS

Sensibiliser les utilisateurs

- *A être vigilent*

- *A remonter toutes anomalies*
  - – Compte bloqué
  - – Problème à l'ouverture d'un fichier (PDF ou autres)

- *Aux bonnes pratiques en matière d'hygiène de sécurité*

QUELQUES PISTES / SOLUTIONS

Exemples

- ❑ Créer des « Masters Sains »
- ❑ Déployer et mettre à disposition rapide des stations de travail virtualisées
- ❑ Isoler / Compartimenter des réseaux / sous réseaux
- ❑ Faire des tests chronométré (chercher un temps record) pour :
  - Remonter un parc contaminé
  - Récupérer un serveur Métier essentiel via un « Master Sain »

Partir du concept de « la promesse client » pour :

- ➢ ***Aller à l'essentiel***
- ➢ ***Savoir s'adapter***
- ➢ ***Faire preuve d'agilité, de pragmatisme, de flexibilité***

AUTRES OUTILS

- ANSSI : l'Agence nationale de la sécurité des systèmes d'information
- Prestataires de services de confiance qualifiés :
  - Prestataires d'audit de la sécurité des systèmes d'information PASSI
  - Prestataires de détection d'incidents de sécurité PDIS
  - Prestataires de réponse aux incidents de sécurité PRIS
  - Computer Emergency Response Team CERT / CSIRT
- Instituts, Ecoles, Threat Intelligence
- Normes : ISO, AFNOR, BSI, …
- CLUB / FORUM / ASSOCIATION
- Méthodes : EBIOS, MEHARI, …


CONCLUSION : ENJEUX & DIFFICULTES

La prise en compte des futures générations de cybermenaces demeure une réelle nécessité et peut devenir un réel atout

- *évite à une organisation de devenir victime et par conséquent d'en subir les impacts et conséquences (Deni d'image, incapacité à délivrer un service, à gérer la crise, …)*
- *sensibilise les collaborateurs à la sécurité au sein de son organisation comme à l'extérieur (risques pas seulement professionnels mais aussi personnels)*
- *présente un avantage rassurant dans son écosystème (clients, fournisseurs, partenaires, …) voir un argument concurrentiel*

CONCLUSION : ENJEUX

La cybersécurité n'est plus une option !
(condition nécessaire pour toute activité mettant en œuvre des procédés numériques)

Le prochain demi-siècle devrait voir une évolution en matière de confiance numérique par la mise en place progressive de cadres et d'organisations acceptés par tous les États (confiance juridique des Échanges)

Les questions de cybersécurité et de ses réglementations :

- Place de + en + importante dans l'OMC ou dans le Forum Économique Mondial
- Cyberattaques figurent parmi le top 5 des risques pour 27 Économies
- Sont aujourd'hui au cœur d'enjeux géopolitiques majeurs

CONCLUSION : DIFFICULTÉS

Nouvel ordre numérique : reste encore à être inventer et à être mis en œuvre

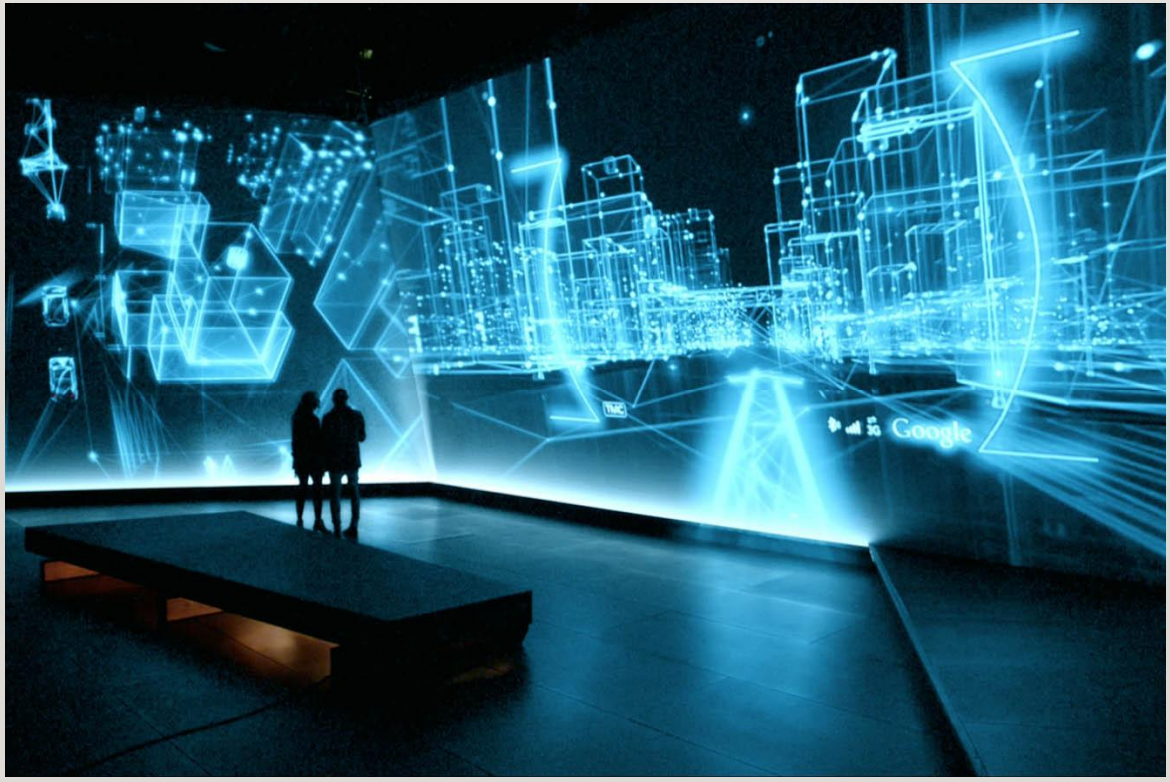
Formidable opportunité : pour tous pays, dès lors qu'ils échangent !

Nombreuses faiblesses persistent et représentent de véritables risques et menaces pour les années à venir.

Pour les PME : 3 x aspects principaux

1. pénurie des compétences
2. marché international trop fragmenté et dispersé
3. entreprises souvent sous-dimensionnées, fragiles financièrement et vulnérables

REVOLUTIONS POUR DEMAIN



NOUVELLES REVOLUTIONS

- BlockChain
- Big Data
- Cloud Computing
- Intelligence Artificielle
- 5G
- Nanotechnologies
- Drônotique (L'autodrône)

et pour chacune d'entre-elles, nous devrons pouvoir compter sur des Experts en SSI

20 MÉTIERS EXPERTS EN CYBERSECURITE

La cybersécurité constitue une filière d'avenir

1. Technicien support
2. Auditeur, contrôleur, évaluateur
3. Opérateur
4. Intégrateur
5. Délégué à la protection des Données
6. Cryptologue
7. Chef de projet sécurité
8. Analyste SOC
9. Chargé de la Réponse aux Incidents
10. Développeur de sécurité
11. Architecte de sécurité
12. Expert en sécurité des systèmes d'information
13. Expert des tests d'intrusion
14. Consultant
15. RSSI
16. Spécialiste en gestion de crise
17. Juriste spécialisé
18. Community Manager spécialisé en e-réputation
19. Correspondant informatique et libertés
20. Formateur, instructeur

GERER DE NOUVELLES CYBER-ATTAQUES

Objectif : capacité de déclencher des réactions en chaîne « risque systémique »

Secteurs touchés : tous sans exceptions !

Une Priorité absolue : La « Santé Connectée », du fait de la dématérialisation et du partage des résultats d'examens

Cibles probables :

- matériels implantables pilotés à distance (implants cérébraux)
- pace-makers,
- membres artificiels,

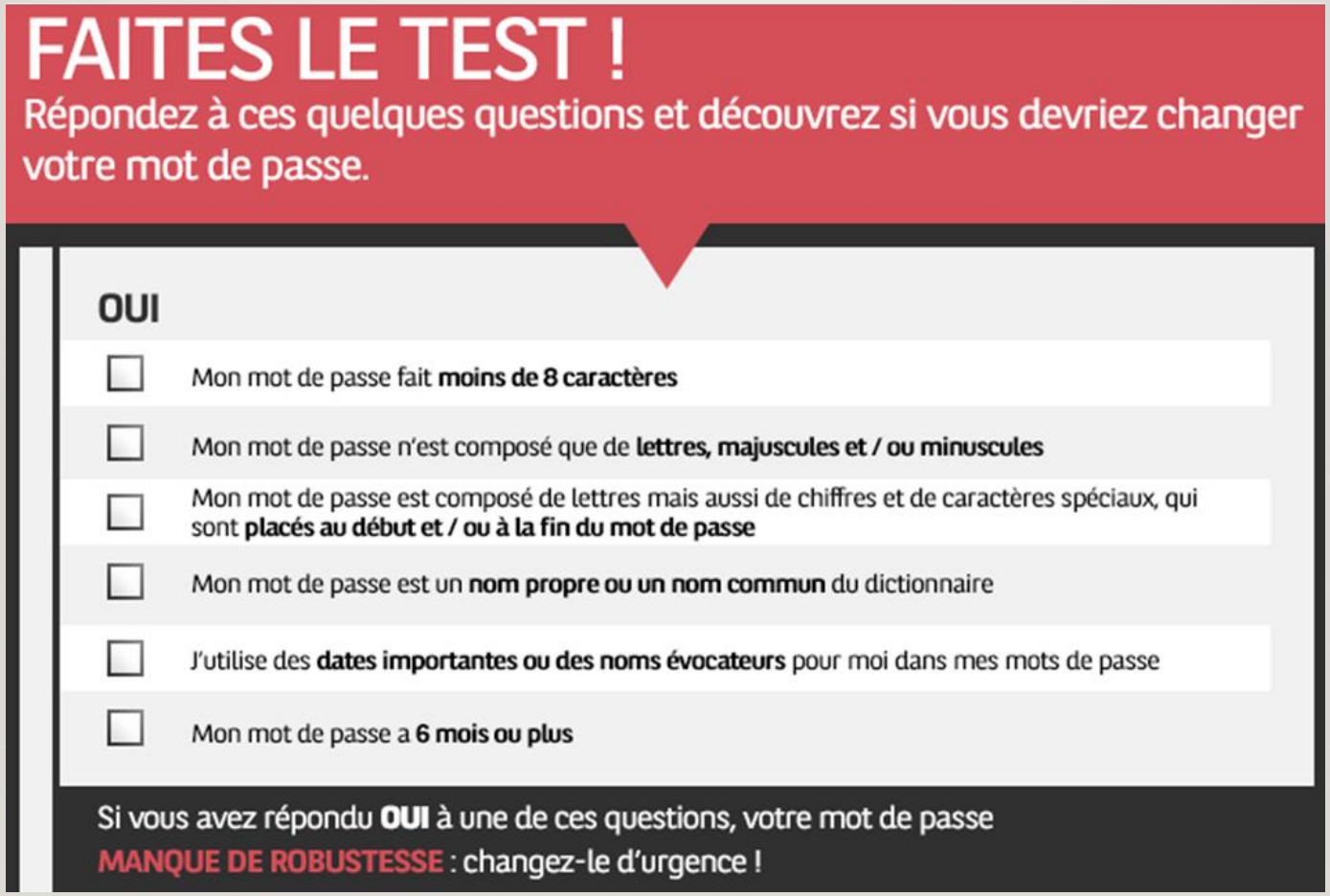
APPORTER DE NOUVELLES SOLUTIONS

- Analyse comportementale : Serveur – Machine – PC …
- A terme, fin des MdP ⏭ Authentification continue et multi-modale (reconnaissance faciale, vocale, rythme cardiaque, bijou connecté, implants, ..)
- Adaptation dynamique politiques en fonction facteurs de risque
- Isolation – Compartimentation : machines / réseaux infectés
- Blocage attaques à déplacements latéraux
- Analyses Forensiques, autres……

SYNTHESE

- Déterminer et maintenir une organisation relatives au processus de gestion du risque
- Identifier des responsabilités (RPCA, DPO, CISO, CySE…)
- Disposer d'un PCA/PRA et le maintenir en condition opérationnelle
- Mettre en place une politique de gestion et de prévention de la fuite d'information
- Créer un centre de commandement des incidents cyber (SIEM, SOC,…)
- Implanter une cellule de GdC au sein de votre organisation
- Maintenir à jour tous vos systèmes de protection et vos machines dans votre entreprise
- ESF : Eduquer , Former , Sensibiliser
- Traiter les aspects juridiques
- Impliquer tous vos collaborateurs

UN TOUT DERNIER CONSEIL : CHANGEZ REGULIEREMENT VOS MDP




MERCI!
THANK YOU!
FRAPAR.

MANAGEMENT DE L'INFORMATION, DU RISQUE ET DE LA CONTINUITÉ D'ACTIVITÉ

CNEJITA EXPERTS

MIRCA BUSINESS DATA SECURED