CINQUIEME PARTIE

LA SECURITE DES SI

INTRODUCTION

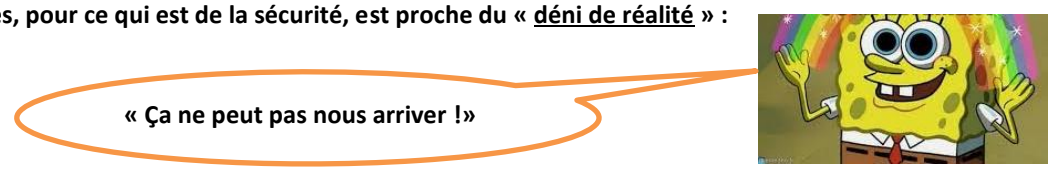
Dans un contexte de concurrence croissante, d'intelligence économique croissante et de sécurité informatique croissante, l'objectif de ce chapitre est de **comprendre le fonctionnement d'une infrastructure de confiance**. Nous allons expliquer pourquoi le fait de sécuriser son patrimoine informationnel est nécessaire dans un écosystème de plus en plus complexe.

CONSTATS

1/ Nous voulons des systèmes **rapides, réactifs** et de prime abord **ouverts (sur internet).**

2/ On souhaite faire confiance au SI, les données doivent donc être sécurisées (au sens DIPCR) !

3/ Cependant, une majorité d'entreprises, pour ce qui est de la sécurité, est proche du « déni de réalité » :



→ Les attaques sont de plus en plus pernicieuses et fréquentes, visant principalement les données et **l'effondrement du SI**

- o **Le périmètre des menaces évolue et augmente continument**
- o De nouvelles formes d'attaque (Botnets), sur les mobiles (Jailbreak de l'iPhone), de nouvelles menaces, sur les smartphones, les serveurs virtualisés, les navigateurs, les virus industriels (Flame après Stuxnet et Duqu) ..

→ Messagerie, Portables, Mobiles, sont devenus les talons d'Achilles du SI

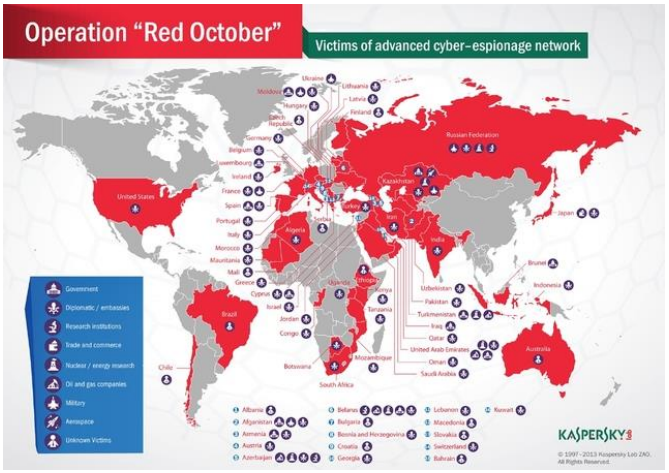
→ **Qui sont les auteurs de ces problèmes de sécurité ?**

→ **La sécurité nécessite une approche globale** et il n'y a pas de solution sans adhésion des utilisateurs (cf. Charte de sécurité)

- * **10 à 12 % du budget à terme**
- * **Conformité à la CNIL et à l'ISO 27000**
- * **Respect strict de normes (PCI DSS pour e-paiement)**

→ Les attaques sont souvent difficilement détectables :

Octobre Rouge – Malware



→ Elles sont essentiellement de 3 ordres :

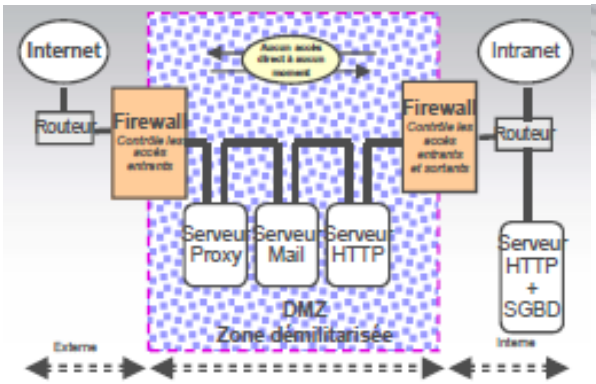
- o Infection par un ver, virus, ..
- o Attaque par déni de service
- o Attaque de type APT (Advanceds persistent Threat)

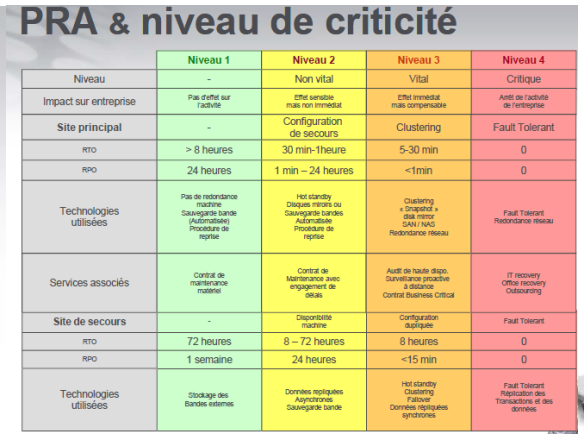
SECURISER LES OPERATIONS ET LES SITES

A chaque niveau de traitement ou de lieu, il existe des outils simples et efficaces à mettre en œuvre :

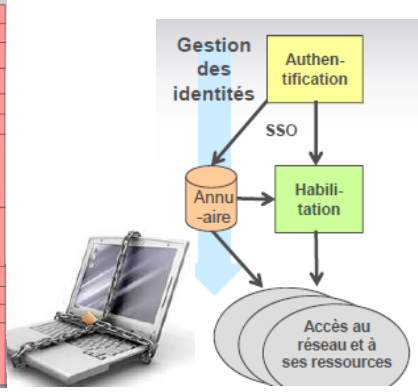
Niveau de Sécurité	Localisation	Moyens
Sécurité individuelle	Poste de travail	Antivirus, spam, Firewall, authentification et cryptage disque
Sécurité réseau	Connexion au réseau local	Sécurité de connexion (authentification), Cryptage des données transmises + VPN* si liaison extérieure
Sécurité passive	Globale entre réseau local et internet	DMZ* avec Firewalls, Proxy, détection d'intrusion…
Sécurité active	Individuelle par gestion des identités	Authentification, habilitation, Annuaire, gestion et fédération d'identités
Sécurité serveurs	Serveurs, centre de calcul et centre de secours	Firewalls, Antivirus, spam PCA* et PRA* pour les centres de secours

** VPN : Virtual Private Network, réseau privé virtuel*
** DMZ : De-Militarized Zone*
** PCA : Plan de Continuité d'Activité*
** PRA : Plan de Reprise d'Activité*





	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Niveau	-	Non vital	Vital	Critique
Impact sur entreprise	Pas d'effet sur l'activité	Effet sensible mais non immédiat	Effet immédiat mais compensable	Arrêt de l'activité de l'entreprise
Site principal	-	Configuration de secours	Clustering	Fault Tolerant
RTO	> 8 heures	30 min-1heure	5-30 min	0
RPO	24 heures	1 min – 24 heures	<1min	0
Technologies utilisées	Pas de redondance machine Sauvegarde bande (Automatisée) Procédure de reprise	Hot standby Disques miroirs ou Sauvegarde bandes Automatisée Procédure de reprise	Clustering « Snapshot » disk mirror SAN / NAS Redondance réseau	Fault Tolerant Redondance réseau
Services associés	Contrat de maintenance matériel	Contrat de Maintenance avec engagement de délais	Audit de haute dispo. Surveillance proactive à distance Contrat Business Critical	IT recovery Office recovery Outsourcing
Site de secours	-	Disponibilité machine	Configuration dupliquée	Fault Tolerant
RTO	72 heures	8 – 72 heures	8 heures	0
RPO	1 semaine	24 heures	<15 min	0
Technologies utilisées	Stockage des Bandes externes	Données répliquées Asynchrones Sauvegarde bande	Hot standby Clustering Failover Données répliquées synchrones	Fault Tolerant Réplication des Transactions et des données



A la base de la **sécurité active** : chiffrage asymétrique, PKI (Public Key Infrastructure) ou ***infrastructure à clé publique*** et **certificat** : mécanisme permettant le cryptage et l'authentification, non cassé (à ce jour).

*** Toute machine / service est doté de 2 clefs : privée (confidentielle) et publique (publiée dans un certificat « signé » par un tiers de confiance)**

* Tout ce qui est crypté avec l'une n'est décrypté que par l'autre

Une sécurité individuelle idéale repose sur 3 aspects :

→ ***Ce que je sais (ID + PSWD)*** *Problèmes : simplisme, trivialité, multiplicité, non renouvellement*

→ ***Ce que je suis (Biométrie)*** *La biométrie est l'ensemble des techniques qui cherchent établir l'identité d'une personne en mesurant certaines de ses caractéristiques physiques* ***:*** *empreinte digitale, géométrie de la main, iris, demain : la voix, l'image, la frappe au clavier,..*

→ ***Ce que je possède :*** *carte à puce, USB, en progrès, carte basée temps à jeton unique (OTP : One Time Password) en recul*


Clef USB

RESPONSABILITES : DROITS ET DEVOIRS EN MATIERE DE SECURITE

- Même s'il peut être *victime*, ***le chef d'entreprise*** reste responsable juridiquement - art. 1383 du Code civil (dommages causés à la société ou aux tiers du fait de sa négligence en cas de *preuve sur l'incapacité avérée et répétée*)
- ***Utilisation abusive*** (personnelle) sur le lieu de travail :
  - ***E-mail*** : l'employeur ne doit pas prendre connaissance des messages personnels
  - ***Dossier « personnel »*** : ne doit contenir aucun logiciel malveillant
- ***Obligation légale*** : "*loi relative à l'informatique, aux fichiers et aux libertés*" du 6 janvier 1978, qui institue la Commission nationale de l'informatique et des libertés (***CNIL***), autorité chargée de veiller à la protection des données personnelles et de la vie privée.

IMPACTS DU DENI

Une mauvaise sécurité entrainera certainement (à terme) des pertes :

Nature des Impacts	Type de pertes
Fonctionnels	De crédibilité
	D'exploitation (indisponibilité des outils)
	De compétitivité (vol d'informations)
	De savoir-faire (destruction de données)
Financiers	De valorisation boursière
	D'exploitation
	De compétitivité
	Détournement de fonds
Structurels	De confiance *interne* et *externe*
	De motivation

Remarque : le cadre juridique reste souvent limité, même s'il existe de nombreuses évolutions depuis la loi Godfrain.

COMMENT PROTEGER LES DONNEES ?

- Avoir une connaissance des valeurs à protéger (cf. PRA, référentiels de type ITIL et normes ISO)
- Effectuer une veille informatique efficace
- Connaître, gérer et remplacer son matériel
- Surveiller le réseau
- Changer les comportements humains
- Mettre en place un système de protection complet et évolutif

LA SIGNATURE ELECTRONIQUE

> *La **signature électronique** (ou **signature numérique**) désigne l'opération de codification d'un document avec une **clé de chiffrement** de manière à cacher le contenu du document, à protéger son intégrité et à en authentifier son auteur.*

OBJECTIFS DES NORMES ISO 27000

La norme ISO 27001 :2013* vise à évaluer la maturité des organisations, à analyser les risques qui les menacent et à constituer un portefeuille de risques, elle utilise la formulation : « établir, implémenter, maintenir, améliorer »
La norme ISO 27002 (ex. 17799) spécifie une Politique de Sécurité des SI, à un niveau plus fin que la précédente, se situant dans le registre du conseil (Guide de Bonnes Pratiques).

* La norme ISO 27001 publiée en octobre 2005 et révisée en 2013 succède à la norme BS 7799-2 de BSI (*British Standards Institution*). Elle s'adresse à tous les types d'organismes (entreprises commerciales, ONG, administrations…) La norme ISO/CEI 27001 décrit les exigences pour la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI). Le SMSI est destiné à choisir les mesures de sécurité afin d'assurer la protection des biens sensibles d'une entreprise sur un périmètre défini. http://fr.wikipedia.org/wiki/ISO/CEI_27001