



Sécurité des systèmes d'information: les enjeux 2009-2010

Réseaux-Télécoms.net

CIO

Le Monde Informatique.fr

Hervé Schauer

Paris, 23 juin 2009

Conférence sécurité

La sécurité est un facilitateur de business

Dépérimétrisation

- PC = Poubelle
 - Attaque des postes de travail via des sites web compromis
 - Vulnérabilités du butineur et de ses logiciels tiers
 - Flash, Acrobat, Quick Time, etc
 - Impossibilité de mise à jour des PC
 - Ou de le faire en temps utile
 - Interconnexion du PC d'entreprise avec outils personnels
 - USB, Firewire, WiFi, BlueTooth, SD-Card, etc

Infrastructures spontanées

- DSI de moins en moins sollicitée
 - Services en ligne
 - Stockage, partage, messagerie, agenda, bureautique
 - Matériel personnel
 - Accès internet personnel
 - ...
- Pas de réflexion
- Pas d'appréciation des risques

Cloud

- « ASP, Cloud computing, SaaS, Web 2.0, ... »
 - Infogérance choisie
 - Projet, MOA, MOE, contrat, SLA, etc
 - Infogérance subie
 - Infrastructures spontanées
 - « *Best effort* »
- Plat de spaguettis
 - Virtualisation, télémaintenance

Population se rajeunit

- Nouveaux profils d'utilisateurs
 - Utilisateurs nés avec le PC, le téléphone portable, le MP3 et ADSL 30 Mb/s
 - Comme d'autres étaient nés avec l'électricité, le téléphone fixe ou la télévision
 - Habitués à l'accès administrateur
 - Habitués à l'usage systématique des services en ligne sur internet
 - Messageries instantanées
 - Réseaux sociaux
 - Multitâches

Médiatisation des failles

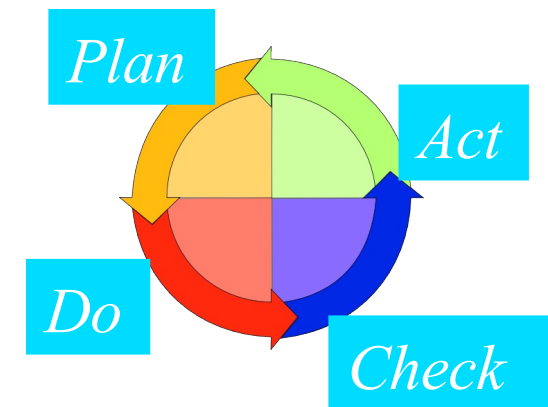
- Failles de sécurité surmédiatisées
 - Faille DNS
 - Faille TCP
 - Lundi noir des virus, MD5 cassé sur des PSP
- Manque de médiatisation d'autres
 - Mifare classic & RFID
 - Avis de sécurité concernant le poste client
 - Exemple Microsoft : MS08-067
- Médias
 - Vecteur de sensibilisation

Défense en profondeur

- Applications d'entreprise dans des bastions
- Accès sécurisé au bastion depuis le PC :
authentification forte et tunnel chiffré
 - Authentification d'entreprise
 - Authentification PC, PDA, Smarphone, etc
- Visualisation des applications d'entreprise sur le PC depuis un butineur lui aussi en bastion
- Protection périmétrique forte autour du bastion

RSSI 3.0

- Intégration dans la gouvernance d'entreprise
 - Gestion de risques
 - Conformité
 - Systèmes de management
- Intégration dans la gouvernance du SI
 - ISO 27001 / ITIL-ISO2000-1
- DSI
 - Gestion de la sécurité
 - Coeur de métier



RSSI 3.0

- RSSI fait avancer la SSI
 - SSI : ce qui permet de faire les choses
 - SSI : jamais un frein, toujours un équilibre
 - DG : arbitre
- RSSI concerné par tous les systèmes d'informations
 - Système informatique que la DSI connaît
 - Systèmes informatiques infogérés
 - Systèmes téléphonique, photocopie, ...
 - Système humain, papier, etc
 - « Quand on parle c'est en clair, ce n'est pas chiffré »
 - Infrastructures spontanées

Conclusion

- RSSI : allié de la DSI
 - Permet à la DSI de reprendre des projets
 - Ont intérêt mutuel à collaborer