



HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989

Spécialisé sur Unix, Windows, TCP/IP et Internet

Sécurité et Gouvernance du SI

Peut-on mixer "pari de la confiance" et "pari de la maîtrise" ?



Université du SI
Paris, 2 juillet 2009

Hervé Schauer
<Herve.Schauer@hsc.fr>

- Confiance
- Maîtrise
- Constats
 - PC = poubelle
 - Infrastructures spontanées
 - Cloud
 - Jeune génération
- Idées
 - Défense en profondeur
 - Gouvernance et SSI
- Conclusion

**Les transparents seront
disponibles sur
www.hsc.fr**

- Espérance solide en une personne ou une chose
- Assurance, sentiment de sécurité
- Présomption
- Dans les systèmes de management : « Apporter la **confiance** aux parties prenantes »

- Domination, autorité
- Habileté, supériorité
- Se dit de certaines charges ou dignités
- En Sécurité des Systèmes d'Information (SSI) : « **Maîtrise** des risques »

Quelques constats

- Attaque des postes de travail via des sites web compromis
- Vulnérabilités du butineurs et de ses logiciels tiers
 - Flash, Acrobat, Quick Time, etc
- Impossibilité de mise à jour des PC
 - Ou de le faire en temps utile
- Récurrence des failles
 - Exemple Microsoft : MS08-067

- Travail à la maison
- Interconnexion du PC d'entreprise avec outils personnels
 - USB
 - Firewire, WiFi, BlueTooth, SD-Card, etc
- Réciproquement, interconnexion du PC personnel avec les outils de l'entreprise
- ADSL perso au bureau
- Contournement de la protection périmétrique

- DSI de moins en moins sollicitée
 - Services & applications en ligne répondent aux besoins
 - Stockage, partage, messagerie, agenda, bureautique
 - Google XX, etc
- Matériel personnel
- Accès internet personnel
- Pas de réflexion
- Pas d'appréciation des risques

- « ASP, Cloud computing, SaaS, DLP, DLP, DLP »
 - Infogérance choisie
 - Projet, MOA, MOE, contrat, SLA, etc
 - Infogérance subie
 - Infrastructures spontanées
 - « *Best effort* »
- « Plat de spaguettis »
 - Virtualisation, télémaintenance
 - Fournisseurs en cascade

- Nouveaux profils d'utilisateurs
 - Nés avec le PC, MSN, le téléphone portable et le MP3
 - Comme d'autres étaient nés avec le téléphone fixe
- Habitués à l'accès administrateur
- Habitués à l'usage systématique des services en ligne sur internet
- Habitués à l'ADSL 30 Mb/s

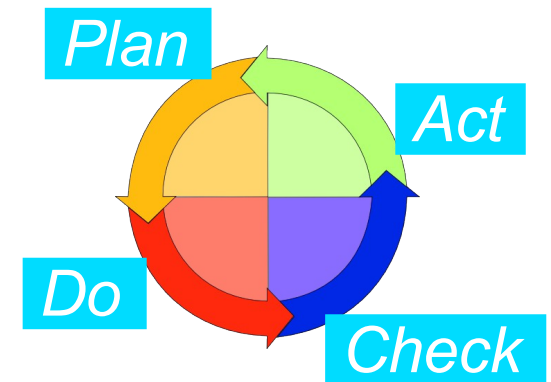
Pourquoi les IBM 3274 (couleur !) ont été remplacés par des PC ? Parce que la génération Nintendo/Sega ne voulait plus de terminaux !

Maîtrise ?

Quelques idées

- 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, annexes
- Visualisation des applications d'entreprise sur le PC depuis un butineur lui aussi en bastion
- Protection périmétrique forte autour du bastion
- Cloisonnement dans le SI

- Intégration de la SSI dans la gouvernance d'entreprise
 - Gestion de risques
 - Exemples : ISO 31000, Risques opérationnels, Risques SI ↔ ISO 27005
 - Conformité
 - Systèmes de management
 - Retour sur investissement
- Intégration de la SSI dans la gouvernance du SI
 - Etudes : CMMI ↔ ISO 27001 & ISO 27005
 - Production : ISO 20000 (ITIL) ↔ ISO27001
- 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

- Sans maîtrise des systèmes d'information, pas de confiance
 - Maîtriser est équilibrer et arbitrer en toute connaissance de cause
 - Maîtriser n'est pas contraindre
- Sans confiance, pas de business

Questions ?

www.hsc.fr

