



HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

Conclusion de la journée

De la SSI aux risques
et vice-versa

Journées
01

Mercredi 29 avril

4^e édition

sécurité

Anticiper les nouvelles menaces

Hervé Schauer

<Herve.Schauer@hsc.fr>

- Constats
 - PC = poubelle
 - Nouveaux mots (maux)
 - Infrastructures spontanées
 - Population se rajeunit
- Espoirs
 - Défense en profondeur
 - RSSI : rôle central
- Conclusion

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

- CERT-IST : « 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

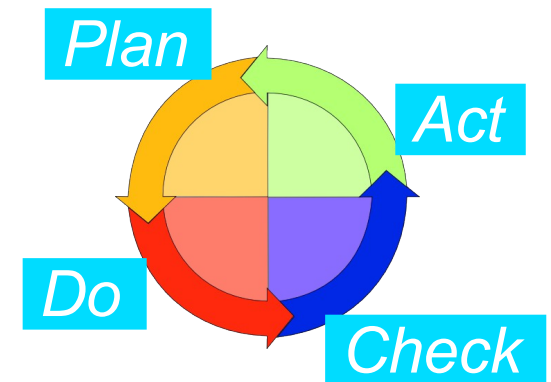
- « ASP, Cloud computing, SaaS, DLP, DLP, DLP »
- Réalité : **infrastructures spontanées**
- Dans une moindre mesure :
 - Encore des *firewalls*
 - « Bloque le PRA »
 - Infogérance
 - Virtualisation
 - « Solution pour votre PRA »
- **Anticipez** avant de suivre ou de tomber après-coup
- Intégrez la SSI

- Travail à la maison
- Interconnexion du PC d'entreprise avec outils personnels
 - USB
 - Firewire, WiFi, BlueTooth, SD-Card, etc
- ADSL perso au bureau
- Services en ligne
 - Stockage, partage, messagerie, agenda, bureautique
 - Google XX, etc
- Pas d'intervention de la DSI, pas demande du métier
- Contournement de la protection périmétrique

- Nouveaux profils d'utilisateurs
 - Nés avec le PC, 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
- **Culture à prendre en compte**

- 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
- Peugeot : « Cloisonnement à l'intérieur de nos systèmes d'informations »

- Systalians, Egencia : « politique de sécurité, appréciation des risques »
- RSSI est moteur dans la vision de son entreprise
- Doit structurer et formaliser la vision de la SSI dans l'entreprise
 - Penser avant d'agir
 - Plan avant Do
 - PDCA
 - ISO 27001
- Ne doit pas avoir l'image d'un technique en interne
 - Sans perdre la compétence et la compréhension des dispositifs techniques
 - Sans se laisser influencer par les fournisseurs



- Crestel : « réintroduisez de l'humain dans les process »
- RSSI doit avoir envie de faire avancer le schmilblick de la SSI
 - RSSI ne doit jamais être perçu comme un frein
- RSSI concerné par tous les systèmes d'informations
 - Système informatique que la DSI connaît
 - Système téléphonique
 - Système humain, papier, etc
 - EADS : « Quand on parle c'est en clair, ce n'est pas chiffré »
 - Aussi les infrastructures spontanées dont tout le monde se sert et pour lesquelles personne n'est au courant et qui demeurent invisibles
- Anticipation donc appréciation des risques en amont
 - CNAM-TS « ISO 27005 nous facilitera la justification régulière des dépenses »

- Pensez, analysez et organisez
- Anticipez et accompagnez
- Plus de budget ? Formations !

Questions ?

www.hsc.fr

ISO 27001 a son club !

Paris, Toulouse, Rennes, Marseille, ...

En projet : Lyon, Nantes
Mutualisation ITIL/itSMF

www.club-27001.fr



Club 27001



Club 27001

