



HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989

Spécialisé sur Unix, Windows, TCP/IP et Internet



La réponse des DSI et RSSI à la sécurité distribuée

Raphaël Marichez

<Raphael.Marichez@hsc.fr>

- Bilan de la matinée
- Nouvelles technologies, nouveaux risques
- Une gestion de la SSI multi-acteurs
- Evolution récente et future du métier de RSSI

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

- Des méthodes répondant aux nouveaux besoins :
 - La gestion des utilisateurs
 - Besoin de mobilité et de souplesse
 - La politique de contrôle d'accès : selon le poste client ou l'utilisateur ?
 - La gestion du poste client
 - Une passoire
 - Séparer professionnel / privé : le poste client devient virtuel
- Distribuer pour mieux régner ?
 - Questions de fonds : Où ? Qui ? Responsabilités ?
 - A quand une gestion des prestataires de service ?

- Efficacité de ces méthodes ?
 - Risques résiduels
 - Etanchéité des VM, évasion, risques non traités par le prestataire...
 - Nouveaux risques
 - Mutualisation des ressources
 - Augmentation de la surface d'exposition
 - Augmentation de l'impact en cas d'incident
 - Traçabilité ?
 - Dépossession des données
 - Localisation ?
 - Responsabilité ?
 - Traçabilité ?
 - Nouvelles méthodes
 - Bonnes pratiques, conformité, contrôle

- « Sécurité distribuée »
 - JRES 1999 Montpellier
- Complexité des infrastructures
 - Maîtrise de son activité ?
 - Dé-périmétrisation
 - Virtualisation des réseaux
 - Points d'accès externes
 - Télé-maintenance
 - « C'est quoi ce câble-là ? »
 - Prestataires / Partenaires
 - Infogérance



- « Infrastructures spontanées »
 - Ca **doit** marcher comme à la maison
 - La sécurité ne peut **plus** être un frein
 - => « Solution clé en main pour votre PRA »
 - => contournement de la DSI
 - => Google Apps, Services en ligne, BlueTooth, USB, ...
- Mélange des genres
 - Le test du PRA qui laisse un trou béant dans le firewall...
 - Un branchement de téléphone qui met à terre le réseau...
 - Un scanneur de vulnérabilités qui plante l'alarme incendie à 10.000 km...
- **Sécurité distribuée = sécurité diluée ?**

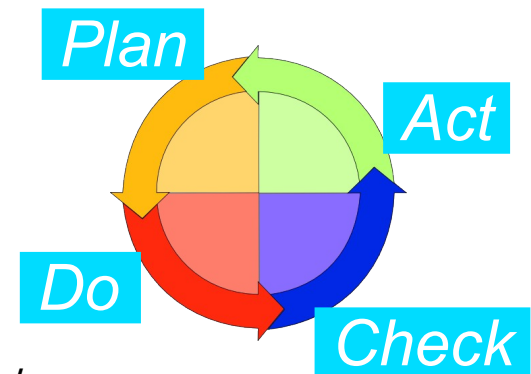


- Externaliser une partie de son activité
 - Externaliser les vulnérabilités
 - Distribuer pour être conforme
 - Titrisation de la sécurité
- Faites votre analyse de risques
 - On achète un produit... (site web)
 - ...qui intègre d'autres produits...
 - Hébergeur, backups, mail, DNS...
- Pyramide des risques
 - « Produits structurés » ?
- Perte de maîtrise : exemples
 - Sauvegardes externalisées
 - Test de vulnérabilité récurrent (TSAR) qui ne trouve jamais rien

© NEA, Inc.



- Le RSSI dans son organisme
 - Le RSSI est un vendeur
 - Il rend compte au DSI, ou au DG, selon le cas
 - De plus en plus souvent, au DG
 - Outils :
 - Appréciation de risques SI : **justification des budgets**
 - Guides de bonnes pratiques SSI reconnus
 - Système de management (SMSI) : amélioration continue (ISO 27001)
 - Moyens :
 - Point de vue externe (consultants) : indépendance ?
 - Faire mieux que les autres filiales / agences / régions / pays
 - Vulgarisation des risques SI (sensibilisation : ne pas oublier la DG)
 - Certifications (des personnes, des systèmes de management, des services)



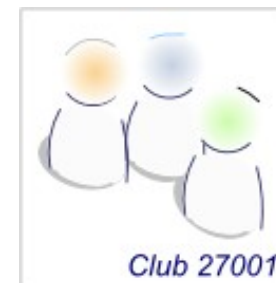
- Le RSSI dans son organisme
 - Le RSSI est un acheteur
 - Produits, prestataires, infogérance
 - Marchés publics
 - Lourdeur : projets à échéance entre 9 mois et 2 ans
 - Mais la SSI a besoin de rapidité ! (deadlines : élections, ...)
 - Formalisme et dé-personnalisation de l'acte d'achat
 - Permet des relations plus cordiales avec les prestataires
 - Bien élaborer son CCTP sinon... c'est trop tard
 - Privé
 - Souple mais copinage possible



- Le RSSI en dehors de son organisme
 - Groupes sectoriels
 - Exemple : en milieu bancaire, les RSSI ont les mêmes problèmes

- Associations

- CLUSIF, OSSIR, Club 27001, ...



- Groupes restreints

- GITSIS, Netfocus, ...



- Domaines connexes

- Normalisation, FNTC...
 - Continuité d'activité, santé, données personnelles...



- Associations régionales...

- Autour de l'organisme
 - La loi (pour tous)
 - Exemple : hygiène et sécurité au travail
 - La Défense
 - Protection pénale du secret de la Défense Nationale
 - Cascade HFDS → FSSI → AQSSI → RSSI → CFSSI
- Le règlement sectoriel
 - Loi pour la Sécurité Financière, Bâle II, SOX, PCI-DSS...
 - La santé (CNAM, hôpitaux), les Douanes...
- L'autorité ou la pression des clients, actionnaires ou utilisateurs
 - Certification, labellisation, contrôle ...

- Distribution du SI

- Le SI devient accessible depuis n'importe quel point du globe
- Nombreux acteurs : les responsabilités sont distribuées diluées
- Tous les métiers sont concernés

- Tout anticiper

- Messagerie bloquée deux jours au Minefi pour un oubli sur l'anti-spam :

```
relaismsg.minefi.gouv.fr[194.250.149.46] said: 554 Service unavailable;  
Client host [129.104.xx.xx] blocked using relays.ordb.org; ordb.org was  
shut down on December 18, 2006. Please remove from your mailserver.
```

- Utiliser son budget

- Justifier un budget précaire dans le privé
- Optimiser l'emploi d'un budget rigide dans le public

- Avoir une vision long-termiste

- vs. la vision « quarter » des CEO

- Secteurs privés sensibles (banques, santé...)
 - Nombreux groupes de travail
- Collectivités locales
 - SSI très décentralisée, très en retard
 - Les RSSI des CG commencent à travailler ensemble... à imiter !
- Universités et recherche
 - Cas du CNRS : cadre SSI centralisé, réunions régulières des RSSI
 - RENATER impose un minimum de fait
- Dans tous les cas : **travaillez ensemble !**

- Réaction à l'incident
 - Culture de la transparence vs. Culture du secret
 - Cas particulier en France : le CERT Renater
- Influences étrangères
 - Anglo-saxons : transparence, importance des données personnelles
 - En Californie : hôpital condamné à 250.000 \$ d'amende le 15 mai dernier
 - Habitudes des utilisateurs : responsabilisation
 - Culture de l'intelligence économique

- Le passé
 - La **conformité** : incite à déléguer (déplacer le problème)
 - Les rationalisations, les consolidations
 - → **Externalisation du SI**
 - Externalisation de la sécurité
- Aujourd'hui
 - La **Conformité** est progressivement remplacée par le **Contrôle**
 - Identifier les risques pour les **exprimer**
 - En prenant en compte la sécurité **externalisée**

- Le futur ?
 - Le RSSI dans un rôle central
 - De la sécurité des systèmes d'information à la **sécurité de l'information**
 - Quitte le giron de la DSI
 - Défense « en profondeur »
 - Pour réduire les risques encore et encore
 - Anticipation
 - **Connaître les risques et les réduire à un niveau acceptable**
 - **Demain : le RSSI distribué, mais pas dilué !**