CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS


# Administration du SI

## *Périmètre et Risque*

**Lazaro Pejsachowicz**

Président

CLUb de la Sécurité de l'Information Français

# De qui/quoi parle-t-on?

- *En informatique, le titre d'**administrateur systèmes** désigne la personne responsable des serveurs d'une organisation (entreprise, association, administration).*
- *Il travaille au sein d'une DSI (Direction des Systèmes d'Information) ou d'une SSII (Société de Services en Ingénierie Informatique). Son rôle ne se limite pas à la résolution des problèmes, mais il doit proposer des solutions en adéquation avec les besoins de son client.*
  *(Wikipedia)*
- Mais, au delà de ce personnage si mystérieux, on veut traiter les risques inhérentes à l'existence d'utilisateurs privilégiés.

# Utilisateur privilégiés?

- Ils ont un accès au système d'information avec des droits supérieurs à ceux correspondant à une utilisation normal d'une application.
- Ces « privilèges » peuvent être au niveau d'une application (gestion des utilisateurs, par exemple) ou au niveau système, dans quel cas elles vont au-delà du contexte applicatifs.
- C'est surtout de ces derniers que je voudrais parler, la gestion de privilèges à l'intérieur d'une application peut être géré par celle-ci.
- Il s'agit donc, d'abord, du mystérieux Administrateur Système qui pour l'informatique moderne est découple en un certain nombre de rôles: installation, DBA, monitoring,…tous ayants des privilèges plus ou moins importants même si parfois, il n'ont pas accès à la toute puissance: le dieux grec ROOT appelé SysAdmin ou simplement Admin chez les Romans.
- Par simplicité du langage nous allons appeler « administrateurs » à cette myriade de « privilégies techniques ».

# Faut-il se méfier de son admin?

- **Oui**, il a trop de droit
- **Non**, vous perdez votre temps, il a trop de pouvoir et heureusement pour vous
- Orange Book: l'administrateur d'un système (et même tout ingénieur système) appartient à la « Trusted Computer Base (TCB) »
- Mais le SI et avec lui le SSI a fait des progrès depuis: vous pouvez embaucher un Admin sans enquête « de moralité approfondie » ☺
- Vous ne pouvez pourtant lui faire « confiance » mais plutôt une « confiance raisonnable »
- Et s'est la bonne connaissance des VOS au niveau de l'administration du SI que donnent la mesure du « raisonnable »

# Comment avoir une confiance raisonnable?

- La clé est dans la compréhension qu'aucun contrôle d'accès peut gérer la règle du « besoin d'en connaître » (ou besoin d'agir)
- Pour un Admin suprême, le dieux « root » supprime toutes vos contrôles.
- Il faut donc une sage combinaison de « a priori » (contrôle d'accès ) et à posteriori (les traces).
- Et dans les deux cas, la maitrise des actions d'administration nécessite un outillage adéquat: IAM spécifique, gestions des traces plus détaillées (commandes), éloignement des traces par rapport au domaine de compétence de l'administrateur,
- Etc Etc Etc
- Parlons deux minutes du Clusif, pour nourrir vos questions:

# Le CLUSIF : *agir pour la sécurité de l'information*

Association **sans but lucratif** (créée en 1984)

~500 adhérents (pour 50% prestataires et fournisseurs de produits et/ou services, pour 50% RSSI, DSI, FSSI…)

**Partage de l'information**

Échanges homologues-experts, savoir-faire collectif, groupes de travail

**Valoriser son positionnement**

Retours d'expérience, visibilité créée

Annuaires (formations, membres offreurs)

**Anticiper les tendances**

Le « réseau », faire connaître ses attentes auprès des offreurs

**Promouvoir le sécurité**


**Logo pour vos actions commerciales, votre site web…**

**Adhérer…**

# Groupes de travail

## Les groupes actifs en 2013

- Codes malveillants : malware
- Evaluation Financière des Incidents de Sécurité - EFIS
- Fiches de sécurité pour la micro-informatique
- Incidents de sécurité et l'ISO/IEC 27035
- Panorama de la cybercriminalité
- PCI-DSS
- Sécurité des Applications Web : Défense en profondeur des applications Web
- Sécurité des Outils de Communication
- Sécurité SCADA
- SSI Santé

## Espaces de travail actifs en 2013

- Espace MEHARI
- Espace Menaces
- Espace RSSI

*Suivez-nous sur facebook, twitter, linkedIn et abonnez-vous à nos flux RSS*

# Quelques documents publiés

. Téléchargez tous ces documents gratuitement sur http://clusif.fr/

Contrôle d'accès, Chiffrement, Lutte antivirale

Gestion des secrets cryptographiques (PKI)

**Panorama de la Cybercriminalité**

**Menaces Informatiques et Pratiques de Sécurité** en France - Edition 2012

Brève étude de la norme ISO/IEC **27003**

Défense en profondeur des **applications Web**

Aider l'auditeur pour les revues de **sécurité physique**

**Gestion des incidents** de sécurité du système d'information

**PCI DSS** v2.0 : quels changements ?

Et aussi : l'infogérance, Communication Voix, Sécurité des applications Web, Chiffrement des données locales, Bots et Botnets, Fraude interne…

et 100+ vidéos

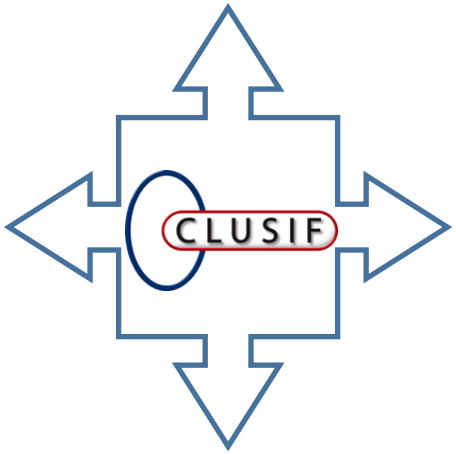
+ la méthode d'analyses de risques MEHARI

(40 documents en 11 langues)

# Une collaboration à l'international…












*Des créations en cours : Ethiopie, pays du Maghreb…*

# Des actions en région


CLUSIR TAHITI

CLUSIR RÉUNION