



HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989

Spécialisé sur Unix, Windows, TCP/IP et Internet

# Forum Alger IT-Sécurité solutions

18 Janvier 2004

# Logiciels libres et Sécurité

**Hervé Schauer**

<Herve.Schauer@hsc.fr>

- x Logiciel libre
- x Sécurité
- x Processus de décision
- x Le logiciel libre en sécurité
  - x Adaptation, pérennité, support
  - x Savoir comment ça marche
  - x Développer en toute liberté
  - x Adapter et corriger
- x Exemples de logiciels libres en sécurité
- x Conclusion

- x Liberté d'utilisation d'un programme
- x Liberté de distribution d'un programme
- x Liberté d'étudier et modifier un programme
- x Liberté de distribuer les modifications d'un programme

- x La sécurité est définie dans une politique de sécurité qui applique la vision de l'organisme à la valeur de ses actifs avec le soutien de la direction
- x La sécurité est un équilibre entre application de la politique de sécurité et convivialité d'utilisation du système d'information
- x La sécurité est un processus, une organisation à mettre en place et à maintenir
- x La sécurité s'établit par un minimum de confiance dans son système d'information
- x La confiance s'établit par
  - x Un système d'information qui répond comme attendu
  - x La compréhension de ce qui se passe sur le système
  - x La possibilité de prouver que cela fait bien ce qui est prévu

- × Il faut partir des besoins des utilisateurs, du métier
- × Il ne faut pas partir d'une liste de produits et chercher lequel répond aux besoins
- × Spécifier ses besoins
- × Choisir la solution qui répond
  - × Aux besoins du métier
  - × A l'application de la politique de sécurité
  - × Aux moyens
    - × Humains
    - × Financiers

- x Possibilité d'adapter le logiciel
  - x Adaptation à sa politique de sécurité
  - x Toujours possible de changer la version standard
  - x Toujours possible d'intégrer une fonctionnalité de sécurité spécifique
  
- x Maîtrise de la pérennité
  - x Pas de disparition
  - x Pas de fusion
  - x ...

- x Disponibilité de services de support et de maintenance concurrents
  - x Possible d'avoir un support autre que celui du fournisseur ou ses partenaires agréés
    - x Partenaire local
  - x Possible d'acheter un support qui comprenne votre besoin d'appliquer une politique de sécurité
    - x Une majorité des services de support de logiciels propriétaires commencent par ouvrir le système et supprimer le contrôle d'accès en cas de problème

- x Possibilité de lire, analyser et comprendre le source
  - x Les logiciels libres sont indépendants
    - x Indépendants sur les plans politique, économique, ...
- x La documentation correspond aux fonctionnalités
- x Les normes et standards annoncés comme respectés le sont
  - x Les normes et standards sont un cahier des charges pour les logiciels libres
  - x Pas d'incompatibilité, pas d'ajout cassant l'interopérabilité

- x Capacité à développer en toute liberté
  - x Utilisation du temps nécessaire
  - x Ré-écriture et reconception quand nécessaire
  - x Besoin de code accessible à des tiers
    - x Modulaire, lisible, commenté, de qualité
  - x Relecture du code et confrontation des idées

- x Qualité
  - x Evaluation de la sécurité sans tricher
  - x Plusieurs projet d'évaluation de logiciels libres vis-à-vis des critères communs
- x Réactivité aux problèmes de sécurité
  - x La correction des failles ouverte à tous
    - x Y compris à un cabinet de conseil et d'expertise en sécurité
  - x Dynamisme de la communauté
    - x Validation et contrôle important et rapide
- x Pas de marketing

- x Application de votre politique de sécurité
  
- x Pas d'application d'une autre politique de sécurité à votre insu

- x Serveurs de noms (DNS) : Bind
- x Messagerie
  - x Serveur de messagerie : Postfix
  - x Anti-spam : spamassassin
  - x Anti-virus : amavisd-new et clamav
- x Gestion des journaux : Acid, OWL, IPFC, ...
- x Détection d'intrusion : Prélude, Snort
- x Contrôle d'intégrité : AIDE
- x Analyse réseau : Ethereal, tcpdump

- x Tests de vulnérabilités : Nessus
- x Système de gestion de fichier chiffrés
- x Tunnels : IPsec, ssltunnel, ...
- x *Firewalls*
  - x Filtrage IP : netfilter, packet filter, IP filter
  - x Relayage et filtrage HTTP : Squid, Apache
- x Gestion des authentifications : Openldap, Freeradius
- x Serveur de services pour Windows : Samba
- x Serveurs web : Apache & zeus
- x ...

Le logiciel libre est indispensable à la sécurité

Questions ?

[www.hsc.fr](http://www.hsc.fr)

- x Evolutions des technologies et sécurité, Hervé Schauer, Séminaire EADS, 11/03,  
<http://www.hsc.fr/ressources/presentations/eads03>
  
- x Sécurité et logiciel libre, Cédric Blancher, RMLL, 07/03,  
[http://www.netexit.com/~sid/pres/0307\\_LSM03\\_Libre\\_Secu.pdf](http://www.netexit.com/~sid/pres/0307_LSM03_Libre_Secu.pdf)
  
- x L'intérêt du logiciel libre en sécurité, Hervé Schauer, Linux-Expo 06/99, <http://www.hsc.fr/ressources/presentations/libre2>