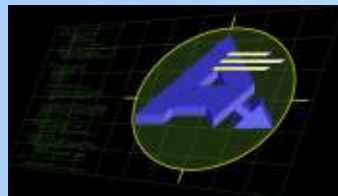


Sécurité et logiciels libres

Sébastien Heitzmann - Jean-Marc Boursot



<<http://www.2le.net>>



<<http://www.ankeo.com>>

Sécurité et logiciels libres

- **Présentation des sociétés**
- **Logiciels libres**
 - historique
 - philosophie
 - avantages et inconvénients
- **Sécurité**
 - buts et principes
 - ouverture, obscurité, avantages et inconvénients
 - exemples de logiciels de sécurité
- **Conclusion**

Ankeo

- Société indépendante spécialisée en sécurité informatique et réseau
- Audit, conseil, ingénierie en sécurité système et réseau
- Installations, tests de vulnérabilités et d'intrusions, veille technologique, etc.
- Conseil, ingénierie en logiciel libre

2LE

- Logiciel libre pour l'entreprise
- Développement en environnement Linux
- Spécialisé application web (php)
- Logiciels industriels. Python – OpenGL

Logiciels libres - historique

- 1984 – Richard Stallman - Projet GNU
- 1991 – Linus Thorvald - Première version de Linux
- 1998/99 – Popularisé auprès de la presse et du public
- 2001 – Support de linux par les grands constructeurs

Logiciels libres - libertés

- Le droit d'utiliser pour tous usages
- Le droit de modifier
- Le droit de redistribuer
- Le droit d'améliorer et de publier les améliorations

Ouverture du code source

Logiciels libres - philosophie

- Protégé par le droit d'auteur
- Développement collaboratif
- Auteurs aux quatre coins du monde
- Management de projet par despote éclairé

Logiciels libres - avantages/inconvénients

- Avantages :
 - Pérennité, respect des standards
 - Co-propriété des sources pour le client
 - Facilité de gestion des licences
 - Richesse du choix
- Inconvénients :
 - Technicité plus forte
 - Offre de support difficilement identifiable
 - Philosophie différente
 - Absent de certains domaines (vidéo, prépresse)

Logiciels libres - applications phares

- Linux
- Apache, Php, Mysql, Sendmail
- OpenOffice, The Gimp, Mozilla, VNC

- Calcul des effets spéciaux de Titanic
- Google, cluster de plus de 10 000 serveurs
- Boursorama

Sécurité

- « *La sécurité n'est pas un produit mais un processus...* »
- La sécurité 100% n'existe pas
 - stratégie de gestion des risques, non d'élimination
 - adéquation entre la valeur des données à protéger et le coût de cette protection
- Trop de sécurité tue la sécurité
 - complexité, convivialité
 - chiffrement vs analyse de contenu (encapsulation)

Sécurité - buts

Buts de la sécurité :

- Disponibilité
- Intégrité
- Confidentialité
- Identification

Sécurité - principes 1/2

4 grands principes :

- **Prévention**

politique de sécurité, durcissement, séparation des tâches, réduction des privilèges, formation et sensibilisation des utilisateurs, penser sécurité dès le développement, sauvegarde

- **Protection**

firewall, antivirus et filtrage de contenu, authentification et chiffrement

Sécurité - principes 2/2

4 grands principes :

- **Détection (et évaluations)**
surveillance et journaux, contrôle d'intégrité, système de détection d'intrusion, audit, veille technologique
- **Correction (et réponses)**
mise à jour des logiciels, modification de la politique de sécurité, mise en adéquation des règles, de l'organisation, restauration

Sécurité - ouverture vs obscurité

- Ouverture

- tout le monde peut connaître mes faiblesses mais tout le monde peut aussi les corriger
- l'outil est connu, pas ses réglages

- Obscurité

- problème d'audit et de validation (la CE et Echelon)
- cacher d'éventuels défauts ne les enlève pas (IIS)
- fausse sécurité : changements de ports, utilisateur « *toor* », code de César (rot3)

Logiciels libres pour la sécurité

- **Prévention**
xinetd, pam, « *chroot* », services et daemons
- **Protection**
NetFilter, IP-Filter, Packet Filter, Squid, Squidguard, GnuPG, OpenSSL, OpenSSH
- **Détection (et évaluations)**
Syslog-ng, Logcheck, IPPL, IPTraf, MRTG, Snort, Prelude, Nessus, Nmap, AIDE
- **Correction (et réponses)**

Sécurité et logiciels libres

- Avantages :
 - liberté de correction et d'adaptation importante
 - audit du code source possible (contre failles, *backdoor*)
 - indépendance et respect des standards
 - durée de vulnérabilité (pas le nombre, ni la gravité)
- Inconvénients :
 - inertie sur les IDS et les scanners
 - pas d'antivirus

Conclusion

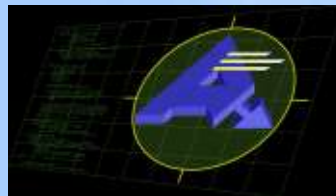
- Neutralité et indépendance
- Richesse de choix (pas toujours complet)
- Avantage structurel du libre pour la sécurité mais pas forcément qualitatif
- Panachage libre et propriétaire

Sécurité et logiciels libres

Sébastien Heitzmann - Jean-Marc Boursot



<<http://www.2le.net>>



<<http://www.ankeo.com>>