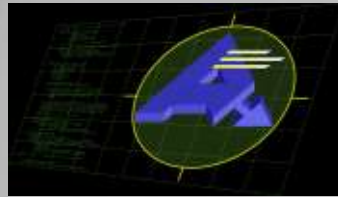


Sécurité et obscurité

Jean-Marc Boursot



<http://www.ankeo.com>

© Ankeo 2003 - reproduction interdite

La sécurité par l'obscurité?

- **Présentation de la société**
- **Rappels**
 - quelques formules...
 - buts et principes
- **Le côté obscur...**
 - exemples
 - revue de détail
- **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

Quelques formules...

- « *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

Obscurité...

- Mécanismes visant à améliorer ou garantir une meilleure sécurité via la rétention ou la falsification d'informations
- Une des 2 grandes « écoles » en matière de sécurité
- Souvent opposée à la divulgation
- Parfois opposée à l'ouverture
- Souvent lié au propriétaire

Le côté obscur...

Exemples :

- utilisation de ports non standards
- altération des versions ou des noms des logiciels
- changement du nom de l'administrateur
- codes ou chiffrements douteux
- boîtes noires et autres firewalls
- propriétaire (par opposition au libre)

Le côté obscur... en résumé

- Politique de l'autruche
- Je sous estime l'attaquant et les risques
- J'accorde ma confiance à un slogan ou une marque (propriétaire comme libre)
- Correction au lieu de prévention

Vous avez dit optimiste? Démonstration...

Porter un masque?

(changement du port, du nom, de la version ou du nom d'utilisateur)

- Souvent utilisé au détriment d'une vraie mesure de sécurité
- Ne résiste pas à un scanner ou une attaque systématique
- Peut attirer l'attention
- Pas très pratique

Donc, à éviter mais peut être envisagé en complément.

Codage et chiffrement?

- Exemples : code de César, décalage de bits, chiffrements faibles
- Vous connaissez le truc? L'attaquant (et ses outils) aussi!
- Ne résiste pas à un examen méthodique
- Peut provoquer l'imprudence

Choisir les bons, proscrire les mauvais!

Ayez confiance...

- *J'ai un firewall!* Il ne vous manque plus que l'architecture réseau, la politique de sécurité, la configuration, les mots de passe, l'administration et le suivi
- *Je n'ai jamais eu de problème et je suis trop petit pour intéresser quelqu'un!*
- *C'est une bonne marque / ça m'a coûté cher!*
Et le contrat de licence, de maintenance?

Doutez, formez vous et informez vous!

Vive le propriétaire? 1/2

- L'ouverture du code génère plus de failles?
 - cacher une faille ne veut pas dire qu'elle n'existe pas et n'empêche pas qu'on la découvre
 - on ne connaît pas mes réglages
 - on peut auditer le code (moins de risque de *backdoor*)
 - on peut m'aider à corriger (meilleure réactivité)
- Un éditeur m'offre plus de garanties?
 - sécurité plus réactive que proactive
 - avez-vous lu les contrats de licence?
 - rapport prix / gain en sécurité

Vive le propriétaire? 2/2

- Il n'y a pas d'équivalent libre
 - vrai dans le domaine des IDS, des antivirus et de certaines fonctionnalités de firewall
 - beaucoup de logiciels/systèmes propriétaires utilisent ou sont basés sur du libre
 - des logiciels libres ont porté des fonctionnalités inventées par des logiciels propriétaires

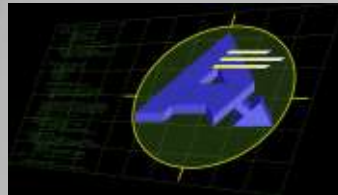
Oui pour les fonctionnalités (suivant les cas),
non parce que pas de gain grâce à l'obscurité

Conclusion

- Pas de plus value (et parfois moins value) en terme de sécurité à cacher les choses.
- La connaissance de l'anatomie ne fait pas tomber malade mais son ignorance empêche de soigner
- Information et formation
- Néanmoins, accepter l'obscurité :
 - pour obtenir des fonctionnalités
 - pour compléter une *vraie* politique de sécurité

Sécurité et obscurité

Jean-Marc Boursot



<http://www.ankeo.com>

© Ankeo 2003 - reproduction interdite