

Les Logiciels Libres au Service de la Sécurité

Retour d'expérience sur le déploiement de logiciels libres pour la sécurité des systèmes d'information

Cédric BLANCHER

`cedric.blancher@eads.net` -- <http://sid.rstack.org/>
Centre Commun de Recherche
EADS FRANCE

Journée sur les Logiciels Libres, Rabat
26 juillet 2005



Expérience personnelle

Déploiement de logiciel libre pour :

- SI complets de petites et moyennes entreprises
- Plate-forme d'hébergement complète
- Services en ligne bancaires et administratifs

Introduction

Les logiciels libres peuvent nous aider à améliorer la sécurité

- En tant que socle logiciel du système d'information
- En tant que socle applicatif des services proposés
- En tant qu'outils imposant les contraintes de sécurité
- En tant qu'outils de supervision du système
- En tant qu'outils d'évaluation de la sécurité

- 1 Le socle système
- 2 Le socle applicatif
- 3 Les outils de sécurité
- 4 Indépendance

Plan

- 1 Le socle système
- 2 Le socle applicatif
- 3 Les outils de sécurité
- 4 Indépendance

Le système d'exploitation

Le système d'exploitation : le socle de base

- Noyau + applications/bibliothèques de base
- C'est la première brique de la sécurité
- C'est l'endroit le moins difficile à protéger (domaine circonscrit)
- C'est l'endroit où les mesures de protection ont le plus d'effet (point de passage incontournable)

C'est un élément incontournable de la sécurité

GNU/Linux

GNU/Linux est populaire, son développement est actif et varié
Pour la sécurité :

- Linux est extrêmement portable (22 architectures supportées, plus de 60 sous-architectures et optimisations)
- Des distributions orientées sécurité
- Des modèles de sécurité additionnels
- Des outils et modèles de sécurité propres

GNU/Linux permet d'atteindre des niveaux de sécurité extrêmement pointus et résistants

Fonctionnalités

On peut configurer les systèmes pour des tâches variées

- Filtrage de paquets
- Gestion de la QoS
- Gestion de la haute disponibilité
- VPN
- Serveur sécurisé
- Station de travail sécurisée
- Etc.

Plan

- 1 Le socle système
- 2 Le socle applicatif**
- 3 Les outils de sécurité
- 4 Indépendance

Les applications

Les applications fournissent les services accessibles

Ces applications doivent fournir un niveau de sécurité important

- Minimiser les failles possibles
- Minimiser l'impact de ces failles

Services de base

Tous les services de base sont disponibles en logiciel libre

- Socle (DNS)
- Diffusion et échange de contenu (WWW, FTP)
- Messagerie (SMTP, POP/IMAP)
- Gestion de données (SGBDR)
- Etc.

Mécanisme de sécurité

- Intégrés au niveau de l'implémentation du logiciel
- Accès au service
- Accès aux données

Plan

- 1 Le socle système
- 2 Le socle applicatif
- 3 Les outils de sécurité**
- 4 Indépendance

Outils de sécurité

Le logiciel libre fournit des logiciels permettant d'imposer la politique de sécurité

- Sécurité réseau
- Sécurité système
- Poste de travail
- Évaluation de la sécurité
- Autres...

sécurité réseau

Outils de sécurité réseau

- Filtrage réseau (*firewall*)
- Analyse de flux
- Filtrage applicatif
- Analyse de contenu (*antivirus, antispam, etc.*)
- Protection des flux (*VPN*)

Sécurité système

Plusieurs niveau d'action

- Utilisation des fonctionnalités du socle système
- Utilisation des fonctionnalités des applications
- Authentification
- Protection des données
- Ajouts de restrictions additionnelles

Évaluer sa sécurité

Le monde du logiciel libre fournit de nombreux outils pour évaluer sa sécurité

- Scanners de vulnérabilité
- Scanners divers
- Pleins de petits outils très spécialisés

Tous ces outils permettent de vérifier l'application de la politique de sécurité et d'évaluer son niveau de sécurité

Supervision

Une bonne sécurité s'entretient

La supervision du système fait partie du process de sécurité pro-actif

- Gestion des journaux d'activité
- Détection des anomalies de sécurité
- Vision de l'état du système

Les capacités d'interopéabilités et d'adaptabilité sont essentielles

Plan

- 1 Le socle système
- 2 Le socle applicatif
- 3 Les outils de sécurité
- 4 Indépendance**

Indépendance

Le logiciel libre permet le niveau d'indépendance désiré

- Choix de logiciels
- Choix des fournisseurs
- Choix des prestataires
- Choix des améliorations
- Etc.

Indépendance

Impacts négatifs possibles de la dépendance

- Disponibilité des correctifs de sécurité
- Test et déploiement des correctifs de sécurité
- Ajout de fonctionnalités
- Montée en charge des infrastructures
- Résolution des pannes et bugs majeurs
- Etc.

Conclusion

Le logiciel libre est une réponse à prendre en compte

- Solutions pertinentes
- Solution efficaces
- Solutions ouvertes

Ressources

Retrouvez cette présentation sur :

- <http://sid.rstack.org/>

Découvrez deux autres présentations plus détaillées :

- Logiciel Libre et Sécurité Informatique
http://sid.rstack.org/pres/0502_JIA_Libre_Secu.pdf
- Outils Libres pour la Sécurité Informatique
http://sid.rstack.org/pres/0502_JIA_Outils.pdf