Logiciel libre et sécurité

- Retour d'expérience -

Sébastien DELCROIX
seb [at] citic74.fr

CITIC74

- Établissement Public local sous tutelle du CG74.
- Développement des usages pour les services publics de la Haute-Savoie.
- FAI et FSI.
- Infogérence des parcs informatiques des collèges.
- > 500 serveurs sous Linux.
- 1700 postes sous Win XP (~3000 pour 2009).
- Développement de PingOO, distribution Linux.

Enjeux

- Utilisateurs sensibles
  - Protection des mineurs (écoles, collèges, lycées).
- Collectivités
  - Images, données sensibles.

Risques

- Plusieurs critères
  - Résistance aux attaques
    - Malwares, DOS, remote exploit
  - Disponibilité
    - Uptime, bug

Cible privilégiée ?

- Parc poste de travail faible (~ 1%).
- Serveurs « internet » (40 à 50%)
  - Apache/MySQL/Php
- Applications web (blog, CMS, forums)
- Applications classiques
  - Firefox (> 20%)
  - OpenOffice

Mythes ou réalité

Les logiciels libres sont-ils plus sûrs que les logiciels propriétaires ?

Malwares

- Windows => applications tournant souvent sous un ID avec privilèges.
- Unix/linux => applications tournant sous le user (périmètre limité d'une attaque).
- Linux => infection par des malwares possible.

Suite Office

- Virus Macro dans les suites libres aussi.
- Macro verrouillée par défaut dans OOo.

Navigateurs

- IE => ActiveX.
- Firefox => Extension
  - Effort consenti dans la V3 pour faire un nettoyage des extensions.

Temps correction faille

- Propriétaire => dépend de l'éditeur !
- Libre => dépend du développeur ou du distributeur ou de soi-même.
- Windows => failles corrigées au bout de 6 mois.
- Debian => failles kernel non corrigées.
- Libre => très souvent corrigé très vite.

Gestion des mises à jour

- Windows
  - plusieurs éditeurs.
  - Tous les éditeurs ne packagent pas leurs softs avec du MSI.
  - Une signature par éditeur.
- Linux
  - Packaging par un distributeur.
  - Signature par le distributeur.
  - Package possible hors distributeur (signature différente !).

Transparence

- Propriétaire => aucune garantie sur la communication des failles corrigées.
- Libre = on sait forcément ce qui a été corrigé.

Transparence protocoles

- Libre
  - Pas de sécurité par l'obscurité.
  - Utilisation de protocoles ouverts.
  - Crypto utilisée : connue et éprouvée.
- Propriétaire
  - Aucune visibilité sur ce qui est utilisé (ex : crypto maison de certaines cartes « contactless »).
  - Aucune visibilité sur l'implémentation des protocoles.

Ouverture du code

- Pirate :
  - trouve les failles plus rapidement (pas de reverse engineering compliqué nécessaire).
- Hacker (White Hat) :
  - trouve les failles plus rapidement pour les corriger.
- => un mal pour un bien !

Installation par défaut

- **En général**
  - Windows
    - Trop souvent pas de sécurité par défaut
      - Services inutiles qui tournent.
      - Ports ouverts.
  - Linux
    - Sécurité/verrouillage par défaut.
    - Mais beaucoup d'applications installées.

Maîtrise : systèmes, applis

- On sécurise mieux un système que l'on connaît.
- Syndrome du « Click & Play » .
- Logiciel libre : en général meilleure maîtrise des systèmes et des applications.

La faille de l'année

- Debian / Initialisation clés openSSL
  - Changement de notre CA.
  - Serveurs SSH etc.
  - Openvpn : anciennes captures wifi .

Cas concrets au CITIC74

- Serveur : tout est libre
  - Sauf la sauvegarde
    - Une partie libre (rsync over ssh).
    - Une partie propriétaire (sauvegarde sur bande).
- Correction de la faille de webcalendar
  - Trop lourd à migrer à la version N+1.
  - Patcher par nos soins.
- Poste windows
  - pas d'antivirus : fonctionnement « à la linux », droits restreints pour les users, limitation d'exécution.

Conclusion

- Les logiciels libres sont loin d'être aussi sûrs qu'on le laisse entendre.
- À choisir entre le cheval borgne et l'aveugle !

Questions ?