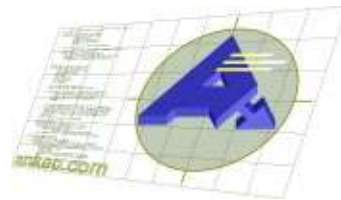




Le logiciel libre face à la sinistralité

Jean-Marc Boursot



<http://www.ankeo.com>

© Ankeo 2005 - reproduction interdite



Le logiciel libre face à la sinistralité

- Présentation
- Le rapport du Clusif
 - Quelques chiffres
 - Sinistralité
- Les solutions libres
- Conclusion
- Questions



Ankeo

- Société de conseil spécialisée en sécurité informatique et réseau
- Audit, conseil en sécurité des réseaux et systèmes d'information, tests de vulnérabilités, veille technologique
- Firewalls, AV, VPN, déploiement de solutions
- Conseil, ingénierie en logiciel libre



Principes de sécurité [1]

La sécurité 100% n'existe pas donc:

- réduction des risques (et gestion)
- minimisation des pertes (financières, image, savoir-faire, etc.)
- maximisation de l'efficacité d'utilisation



Principes de sécurité [2]

Améliorer:

- Disponibilité des ressources, continuité de service
- Intégrité des données
- Confidentialité des échanges
- Identification des acteurs et traçabilité



Principes de sécurité [3]

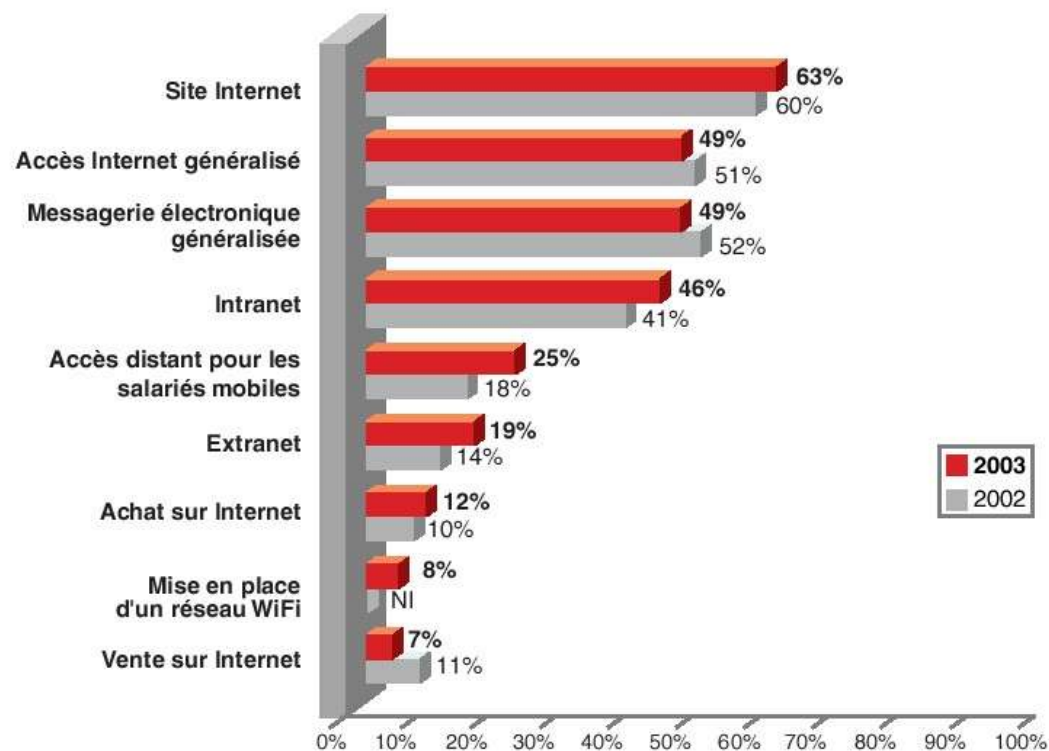
« Plan - Do - Check - Act »

- **Planification** (prévention, politique et objectifs de sécurité, formations, etc.)
- **Mise en oeuvre** (protections firewall, antivirus, chiffrement, authentification, etc.)
- **Vérification, surveillance** (exploitation journaux, audit, veille technologique, IDS, etc.)
- **Amélioration** (mise à jour des logiciels, changements des paramètres, adaptation de l'organisation, etc.)

Chiffres [1]

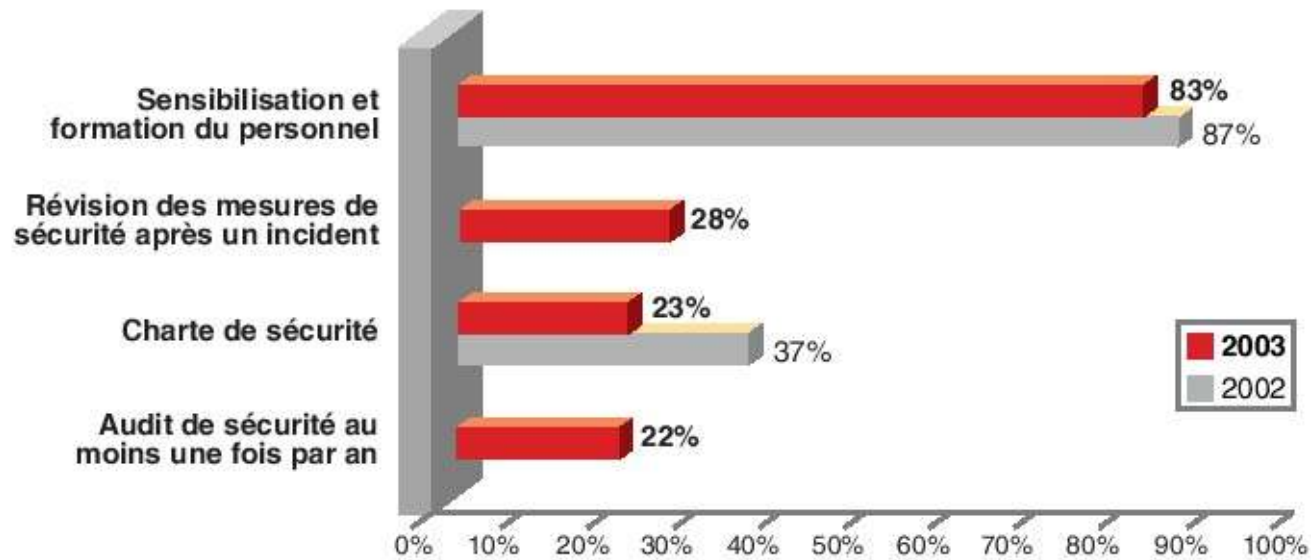
Etude CLUSIF 2003 (29/06/2004) (*Club de la Sécurité des Systèmes d'Information Français* - <http://www.clusif.asso.fr>)

- Ouverture vers l'extérieur



Chiffres [2]

- Management de la sécurité



Chiffres [3]

- Sécurité logique

	De 10 à 199	De 200 à 499	De 500 à 999	Plus de 1.000
Logiciel antivirus	90 %	95 %	89 %	94 %
Mot de passe non trivial	84 %	89 %	92 %	93 %
Pare-feu (firewall)	44 %	83 %	88 %	93 %
Surveillance du réseau contre les intrusions, système d'alerte	34 %	48 %	54 %	73 %
Réalisation de tests (intrusion, vulnérabilité...)	12 %	11 %	16 %	14 %
Chiffrement de données	9 %	13 %	15 %	19 %
Authentification renforcée par un dispositif électronique	8 %	20 %	20 %	38 %

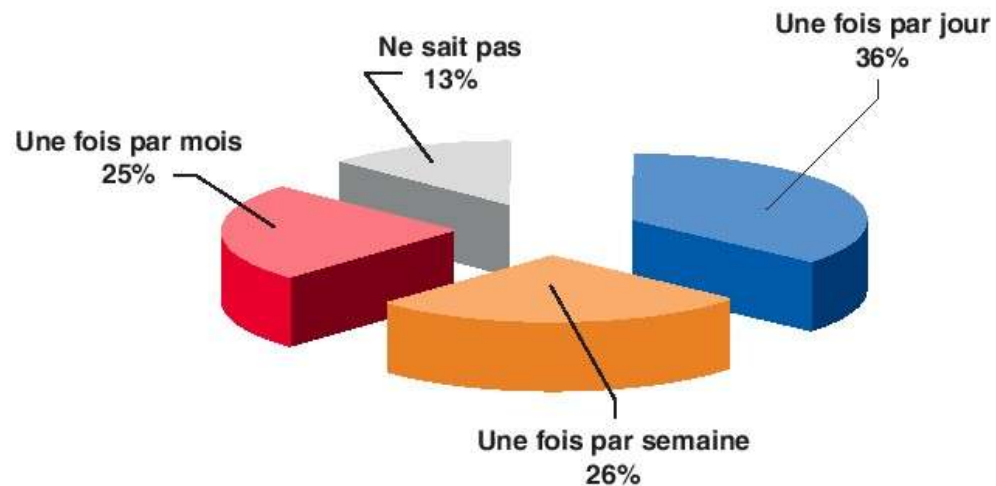
Chiffres [4]

- Mises à jour

Mise à jour des systèmes par les *patches* :

	De 10 à 199	De 200 à 499	De 500 à 999	Plus de 1000
Oui	50 %	59 %	62 %	77 %
Non	50 %	41 %	38 %	23 %

Fréquence des mises à jour de l'antivirus :





Sinistralité [1]

Sinistres:

- Virus 17,6%
- Panne interne 10,7%
- Perte de services essentiels 6,9%
- Erreur de manipulation 6,6%
- Vol 4,8%
- Evènement naturel (2,5%), erreur de conception (1,4%), accident physique (0,6%), dénigrement (0,6%), etc.



Sinistralité [2]

- Intrusions et attaques ciblées ne représentent que 0,7% (cumulés)
- Les problèmes liés au Wifi ne représentent que 0,1%.
- Le risque estimé porte sur les virus, les pannes internes et les attaques.



Solutions libres

- Sécurité par l'obscurité vs ouverture
- Avantages intrinsèques
 - audit du code (OpenBSD)
 - réactivité face aux failles
 - adaptabilité
 - indépendance du support (support professionnel par éditeurs, constructeurs et SSII)
- Certification



Virus

- Filtrage des emails (virus et spam)
- Contrôle de navigation via un proxy
- Surveillance du poste client
- Exemples: ClamAV (moteur), Mailscanner - Amavisd (email), DansGuardian - SquidClam (navig), mod_clamav (serveur web), ClamWin (poste client), SpamAssassin - Razor (antispam)
- Attention aux mises à jour
- Problème des spyware



Accidents

**pannes internes, pertes de services
essentiels, évènements naturels**

- Audit et évaluations
- Sécurité physique (accès restreint, vidéosurveillance, onduleurs, etc.)
- Redondance et sauvegarde
- Exemples: clusters, RAID, Backuppc - Amanda - Bacula (sauvegarde), rsync (synchronisation)



Erreurs de manipulation

- Cloisonnement
 - réseaux
 - droits
- Authentification
- Sauvegarde
- Exemples: kerberos - LDAP - PAM - radius (authentification), ACL (droits)



Attaques

Risque faible mais emblématique

- Mises à jour système
- Cloisonnement
- Durcissement et chiffrement
- Système de détection d'intrusion
- Exemples: netfilter - ipfilter/pf - ipfw (filtrages), snort - prelude (NIDS), AIDE - Tripwire (IDS), GnuPG - ssh - ssl (chiffrement), Kame/Racoon - OpenSwan (IPSec), tcp_wrapper - xinetd - tiger - bastille (durcissement)



Autres solutions [1]

- Site Internet, partage d'accès et messagerie sont très bien pourvus et sécurisables « de l'intérieur » (apache, php, postfix, qmail, sendmail, samba, etc.)
- Firewalls de type filtrant ou mandataires (squid, squidguard, delegate, etc.).
- Technologies utilisées dans de nombreux firewalls ou produits propriétaires
- Filtrage niveau 7 (I7-filter, hogwash, flexresp, guardian, etc.)



Autres solutions [2]

- Outils de suivi (logcheck, iptraf, etc.)
- Outils d'évaluation (tcpdump - ethereal - dsniff, kismet - airtsnort, nessus, nmap, netcat, john, etc.)



Limites actuelles

- Antivirus sur poste client
- Inspection de niveau 7 (deep packet inspection, intrusion prevention system)
- Suivi pour les signatures des virus, les signatures d'attaques (IDS), les scanners
- Parfois difficulté de mise en oeuvre ou d'interopérabilité (notamment standards non suivis par les logiciels propriétaires)
- Corrélation d'évènements
- Manque d'outils sur poste client



Conclusion

- Avantage intrinsèque de l'ouverture
- Offre technique très riche et complète
 - Offre égale ou supérieure aux versions propriétaires dans certains cas (antispam et authentification par exemple)
 - Quelques lacunes ou limites (niveau antivirus et inspection niveau 7 par exemple)
- Libre ou pas, le suivi est essentiel



Questions

Le logiciel libre face à la sinistralité

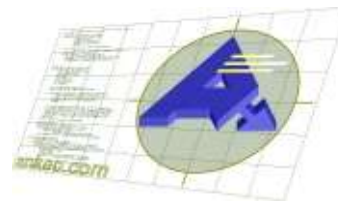
Merci de votre attention. Merci aux organisateurs.

Remerciements au CLUSIF pour son rapport.

Jean-Marc Boursot

<http://www.ankeo.com>

© Ankeo 2005 - reproduction interdite





Annexes [1]

- Systèmes de firewalls:
Netfilter (Linux) - <http://www.netfilter.org/>
PF (OpenBSD) - <http://www.openbsd.org/faq/pf/>
IPFilter (FreeBSD) - <http://coombs.anu.edu.au/~avalon/>
IPFW - http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/firewalls-ipfw.html
- Proxies et contrôle de contenu:
Squid - <http://www.squid-cache.org/>
Squidguard - <http://www.squidguard.org/>
DansGuardian - <http://dansguardian.org/>
Delegate - <http://www.delegate.org/delegate/>
- Antispam:
SpamAssassin - <http://spamassassin.apache.org/>
Razor - <http://razor.sourceforge.net/>



Annexes [2]

- Contrôle Antivirus:
ClamAV (moteur) - <http://www.clamav.net/>
Mailscanner - <http://www.mailscanner.info/>
Amavisd - <http://www.ijs.si/software/amavisd/>
SquidClam (Squid) - <http://squidclam.sourceforge.net/>
mod_clamav (Apache) - http://software.othello.ch/mod_clamav/
ClamWin (poste client) - <http://www.clamwin.com/>
- Sauvegarde:
BackupPC - <http://backuppc.sourceforge.net/>
Bacula - <http://www.bacula.org/>
Amanda - <http://www.amanda.org/>
- Détection d'intrusions:
Snort - <http://www.snort.org/>
Prelude - <http://www.prelude-ids.org/>
AIDE - <http://www.cs.tut.fi/~rammer/aide.html>
Tripwire - <http://www.tripwire.org/>



Annexes [3]

- Authentification et droits:
 - Kerberos - <http://web.mit.edu/kerberos/www/>
 - LDAP - <http://www.openldap.org/>
 - PAM - <http://www.kernel.org/pub/linux/libs/pam/>
 - Radius - <http://www.freeradius.org/>
 - ACL - <http://www.suse.de/~agruen/acl/linux-acls/online/>
- Chiffrement:
 - GnuPG - <http://www.gnupg.org/>
 - SSH - <http://www.openssh.com/fr/>
 - OpenSSL - <http://www.openssl.org/>
- VPN:
 - Kame/Racoon - <http://www.kame.net/>
 - OpenSwan - <http://www.openswan.org/>



Annexes [4]

- Redondance:
HA - <http://www.linux-ha.org/>
RAID - <http://www.freenix.fr/unix/linux/HOWTO/Software-RAID-HOWTO.html>
rsync (synchronisation) - <http://samba.anu.edu.au/rsync/>
- Durcissement:
tcp_wrapper - http://www.ja.net/CERT/Hinxman/TCP_wrapper.html
xinetd - <http://www.xinetd.org/>
Tiger - <http://www.net.tamu.edu/network/tools/tiger.html>
Bastille - <http://www.bastille-linux.org/>
- Filtrage niveau 7 / IDS proactifs :
I7-filter - <http://I7-filter.sourceforge.net/index.php.fr>
Hogwash - <http://hogwash.sourceforge.net/oldindex.html>
flexresp / guardian - cf. Snort



Annexes [5]

- Surveillance:
Logcheck - <http://logcheck.org/>
IPTraf - <http://iptraf.seul.org/>
IPBand - <http://ipband.sourceforge.net/>
- Evaluation:
Tcpdump (sniffer) - <http://www.tcpdump.org/>
Ethereal (sniffer) - <http://www.ethereal.com/>
DSniff (sniffer) - <http://www.monkey.org/~dugsong/dsniff/>
Kismet (Wifi) - <http://www.kismetwireless.net/>
Airsnort (Wifi) - <http://airsnort.shmoo.com/>
Nessus (scanner) - <http://www.nessus.org/>
nmap (scanner de ports) - <http://www.insecure.org/nmap/>
john (mots de passe) - <http://www.openwall.com/john/>

Cette liste n'est évidemment pas exhaustive mais donne un aperçu de ce qui existe dans les différentes catégories.