Autodéfense pour les PC

Protégez totalement vos postes de travail avec la sécurité comportementale

5 minutes pour comprendre :

- Le problème
- Les menaces
- Les vulnérabilités
- Les limites des outils actuels
- La solution StormShield®
- Les bénéfices de StormShield®

Le problème

- Les techniques de sécurité traditionnelle ne parviennent plus à endiguer les nouvelles attaques
  - Indisponibilité des systèmes informatiques en 2004 : agences de presse, transport aérien et ferroviaire, opérateurs télécom, distributeurs bancaires, centrales électriques... Tous les secteurs sont concernés.
  - Espionnage industriel et détournement d'information : codes sources de logiciel, données client, mots de passe, courrier électronique confidentiel...
  - Les postes clients sont de plus en plus utilisés comme vecteurs d'attaques, contournant les défenses réseau de l'entreprise.

*Selon l'étude 2004 du ministère du commerce britannique, **99%** des grandes entreprises ont des défenses antivirales en place...*

*...pourtant **68%** ont subi des pertes financières suite à des attaques en 2003.*

Department of Trade and Industry

La menace

- Les attaques des systèmes informatiques continuent à croître en nombre, en vitesse de propagation, en complexité et en dangerosité
  - Plus de 100 000 virus dans la nature, plus de 30 nouvelles variantes chaque jour.
  - La vitesse de propagation peut dépasser 100 000 PC à l'heure. Le ver Slammer s'est répandu dans le monde entier en 10 minutes.
  - Nouvelles formes d'agression : prise de contrôle de réseaux de machines infectées (botnets), capture de la frappe au clavier (keylogger), phishing...
  - Nouveaux canaux de diffusion : messagerie instantanée, P2P, corruption des services réseaux de Windows...

En 2004, le coût des virus par entreprise dépasse la moyenne de 200 000 dollars.

Pour la première fois, les virus sont devenus le ***facteur n°1*** *de perte financière liée à la sécurité des systèmes d'information.*

CSI COMPUTER SECURITY INSTITUTE

FBI San Francisco

Les vulnérabilités

- Les failles logicielles se multiplient
  - Plus de 50 failles sont identifiées chaque semaine.
  - Le délai d'exploitation malveillante des failles se raccourcit.
- Les postes de travail ne sont pas mis à jour
  - La diffusion des patchs correctifs sur chaque poste est une charge trop lourde pour être effectuée systématiquement.
  - En 2003, une cinquantaine de mises à jour de sécurité pour Microsoft seulement.
- Les postes mobiles sont plus exposés
  - A l'extérieur de l'entreprise, les PC portables sont peu protégés. Une fois infectés, ils deviennent une menace pour tout le réseau lorsqu'ils s'y reconnectent.

35% des attaques réussies exploitent des défauts logiciels.

Gartner

Le coût d'application des correctifs dépasse aujourd'hui celui des licences.

ORACLE

Les postes de travail deviennent un vecteur d'attaque privilégié.

IDC

Les limites des outils actuels

- Les antivirus sont trop lents
  - Le délai moyen de mise à jour des signatures virales est d'environ 12 heures. C'est trop long face à la rapidité de propagation des nouveaux vers !
  - Les attaques ciblées se multiplient, pour lesquelles aucune signature n'est jamais disponible.
- Les défenses réseau sont contournables
  - Les postes mobiles sont peu protégés car ils peuvent se connecter à des fournisseurs d'accès privés.
  - L'analyse du trafic réseau ne suffit pas pour identifier avec certitude toutes les attaques, les firewalls et IPS réseau sont donc limités dans leur capacité de filtrage et de blocage.

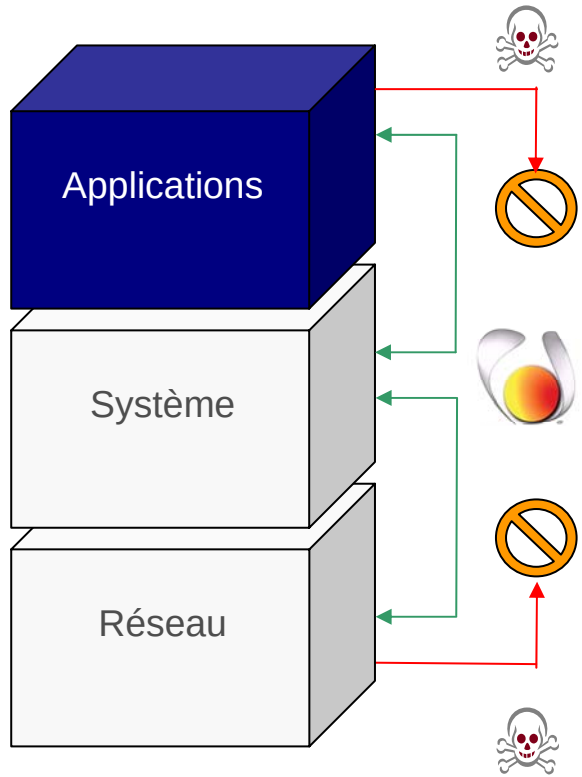
Nous devons commencer à concevoir différemment la protection vis-à-vis des virus et des programmes malveillants.

Il n'est plus suffisant de penser la protection anti-virale sur la seule base de technologies réactives.

ICSA Labs - février 2004

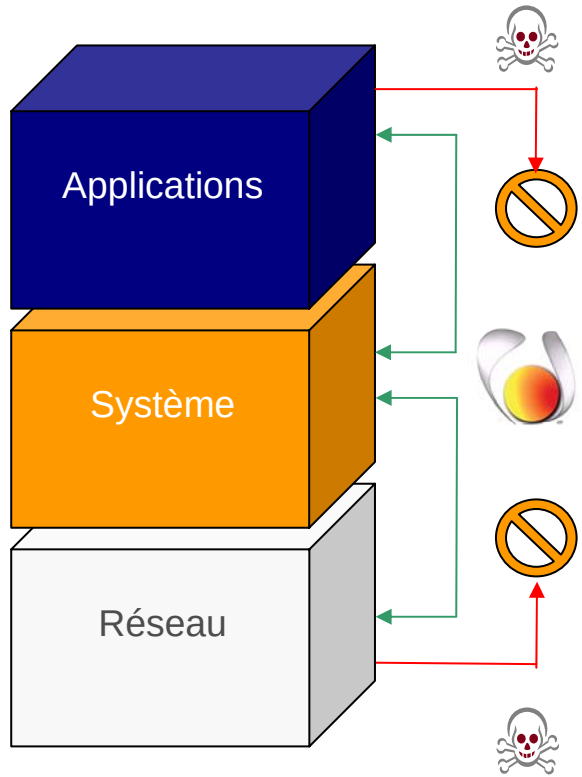
La solution StormShield

- Protection Applicative
  - La protection applicative assure l'intégrité des applications sans interrompre ni perturber le travail des collaborateurs.
  - Elle s'appuie sur la définition de politiques de sécurité applicative définies par l'administrateur et sur la capacité de StormShield de contrôler de façon automatisée le comportement des applications du poste de travail.



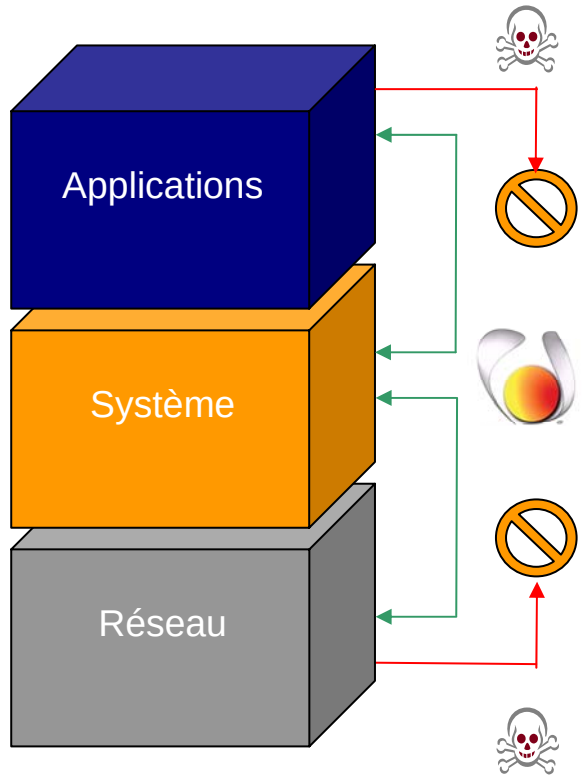
La solution StormShield

- Protection Applicative
- Protection Système
  - La protection système bloque toute tentative de corruption ou d'utilisation anormale du système.
  - Elle surveille en permanence les points névralgiques du système et stoppe immédiatement toute activité dangereuse telle que l'injection de code non autorisée ou les reboots non initiés par l'utilisateur.



La solution StormShield

- Protection Applicative
- Protection Système
- Protection Réseau
  - La protection réseau contrôle les communications et l'environnement du poste de travail et le protège des tentatives d'usurpation d'identité.
  - Un firewall réseau associé aux contrôles comportementaux permet de bloquer dynamiquement les communications en fonction des ports, adresses IP, adresses MAC ou points d'accès Wi-Fi.



Les avantages

- 5 produits en 1:
  - Firewall réseau inviolable (Host IPS)
    - *Evite toute sortie d'informations illicite ou intrusion*
  - Firewall système niveau kernel
    - *Evite toute prise de contrôle à distance ou corruption d'application*
  - Anti-spyware comportemental
    - *Evite toute installation inopinée de mouchards sans mise à jour de liste*
  - Contrôle d'usage des applications
    - *Permet d'interdire ou de restreindre l'usage d'applications, fichiers ou types de fichiers*
  - Protection Wi-Fi
    - *Contrôle l'environnement voisin, évite toute usurpation*

- Les attaques contrées par StormShield
  - Vers (Netsky, Blaster, etc et leurs variantes) et nouveaux exploits de failles
  - Attaques hybrides et ciblées (Trojans multi-tâches, keyloggers…)
  - Installations de programmes illicites ou dangereux (barres dans IE…)
  - Destruction ou diffusion de documents sensibles
  - Attaques « over the air » (Man in the middle, Hijacking, Dos, Rogue AP…)

Bénéfices

- Sécurité proactive
  - Stoppe immédiatement les nouveaux virus exploitant les failles du système ou des applications.
  - Protège des attaques ciblées et furtives pour lesquelles aucune signature ne sera forgée.
- Protection dans tous les contextes
  - Protège les postes mobiles et la connectivité sans-fil, même hors de l'entreprise.
  - Contrôle l'accès au système même quand l'utilisateur est administrateur de son poste.
- Productivité de l'administrateur
  - L'auto-défense évite le recours systématique à l'administrateur lors d'une alerte.
  - Application rationnelle et économique des patchs, plus de "mode panique".
- Productivité des utilisateurs
  - Contrôle l'utilisation des nouveaux outils de communication (P2P, messagerie instantanée..).
  - Permet de bannir les DivX et autres fichiers multimedia.

StormShield est simple à mettre en oeuvre :

- *Aucune perturbation pour l'utilisateur*
- *Administration centralisée*
- *Déploiement GPO*
- *Configurations prédéfinies*
- *Complémentaire à l'existant*

SkyRecon

SkyRecon en Bref

- Editeur de logiciels de sécurité comportementale
  - Société Anonyme française
  - Expansion européenne, investisseurs européens
- Une technologie unique et innovante
  - Soutien ANVAR et Direction Générale de l'armement
  - Parmi les 70 sociétés européennes les plus prometteuses (Commission Européenne – IST Prize)
  - Technologie brevetée
- Notre Mission
  - Assurer la continuité de travail pour chaque collaborateur, en préservant l'intégrité et des données et des applications sur chaque poste client.

7TH INTERNATIONAL VENTURE CAPITAL SUMMIT

ANVAR

10th EDITION Capital-IT Autumn 2003 Best IT

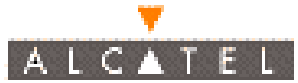
THE EUROPEAN IST PRIZE NOMINEE

Taste of entrepreneurship

Parmi nos clients et partenaires

- Quelques clients

- Quelques partenaires



Contact

Quoc-Viet NGUYEN HUU

Business Development Director

+33 6 68 52 81 22

qvnguyen@skyrecon.com