Université
De Boumerdes

Université
De Limoges

Département d'informatique
M2

Protections

Réalisé par : Dr RIAHLA
Docteur de l'université de Limoges (France)
Maitre de conférences à l'université de Boumerdes

Université
De Boumerdes

Université
De Limoges

Département de physique/Infotronique
IT/S6

Introduction

Réalisé par : Dr RIAHLA

2008/2009

On considère généralement que la majorité des problèmes de sécurité sont situés entre la chaise et le clavier).

Quelles sont les solutions donc !!!

Université
De Boumerdes

Université
De Limoges

FORMATION DES UTILISATEURS

Réalisé par : Dr RIAHLA

2008/2009

FORMATION DES UTILISATEURS

la sensibilisation des utilisateurs :

- A la faible sécurité des outils de communication
- A l'importance de la non divulgation d'informations par ces moyens.

- Il est souvent trop facile d'obtenir des mots de passe par téléphone ou par e-mail en se faisant passer pour un membre important de la société.

FORMATION DES UTILISATEURS

Virus :

- Selon une étude, 1/3 des utilisateurs ouvriraient encore une pièce jointe d'un courrier nommé « i love you »

- La moitié ouvriraient une pièce nommée « ouvrez-ça » ou similaire… !

- **L'information régulière du personnel est donc nécessaire.**

FORMATION DES UTILISATEURS

Charte d'entreprise :

Obliger les employés à lire et signer un document précisant (**Charte**):

- Leurs droits
- Leurs devoirs
- Montrer leurs responsabilités individuelles.

Université De Boumerdes

Université De Limoges

POSTE DE TRAVAIL

Réalisé par : Dr RIAHLA

2008/2009

POSTE DE TRAVAIL

- Il reste un maillon faible de la sécurité.

- Le projet **TCPA** *(Trusted Computing Platform Alliance) a pour but d'améliorer sa sécurité en dotant le PC d'une puce* dédiée à la sécurité.

- Elle sera chargée de vérifier l'intégrité du BIOS, du chargement de l'OS,..etc

POSTE DE TRAVAIL

Les postes de travail Windows doivent être protégés individuellement par des:

- Antivirus
- Anti Spywares
- Firewall personnels (Firewall Windows)
- Mise à jour de correction des vulnérabilités

POSTE DE TRAVAIL
Exemples d'actions

- Vérifier et mettre en place le cavalier interdisant la reprogrammation du BIOS sur tous les postes.

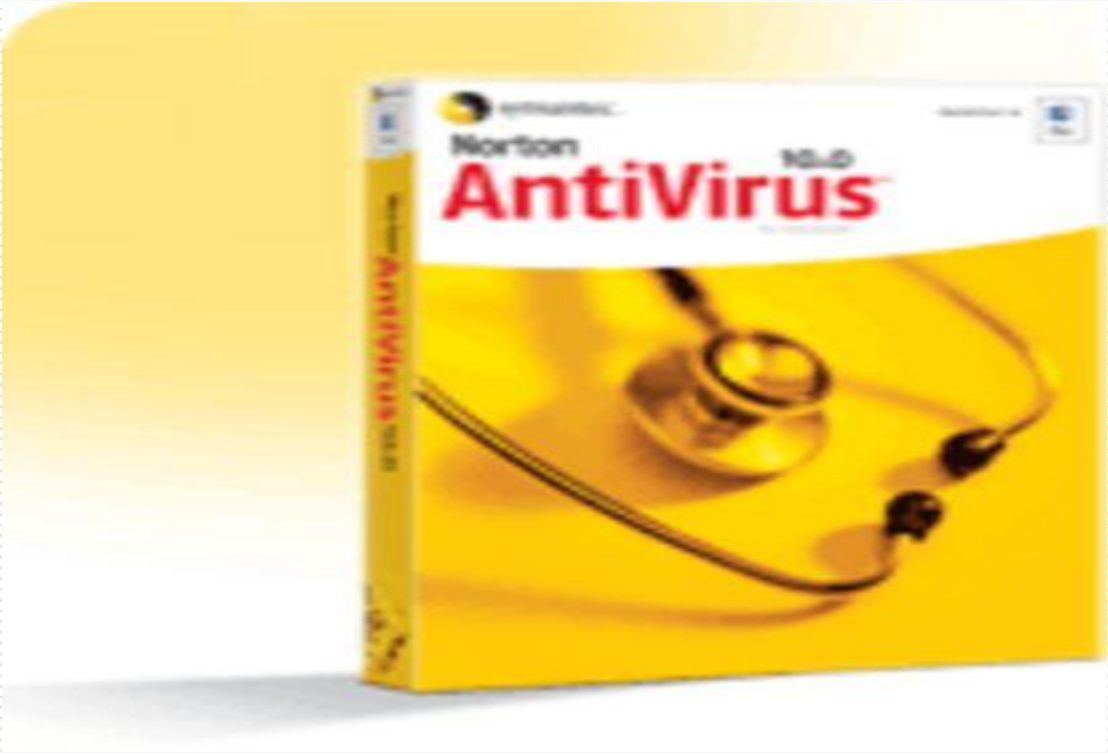
- Interdire le Boot disquette.

- Effectuer des Backups réguliers et sécuriser les informations essentielles.

- Eviter le Multi-boot car la sécurité globale du poste est celle de l'OS le plus fragile

- …etc

ANTIVIRUS



ANTIVIRUS
Méthodes de détections

Analyse des signatures
Utilise une base de données de signatures

Analyse du code
Analyse du code statique
Analyse du code dynamique (analyser le comportement des applications)

Contrôle d'intégrité
vérifier si les fichiers exécutables du système ont été modifiés.
...etc

ANTIVIRUS
Analyse du code

Méthodes approximatives qui utilise les méthodes heuristiques

Avantages

- N'a pas besoin de base de signatures
- Détecter les nouvelles attaques non reconnu par les antivirus par signature

Inconvénients

- Mathématiquement la solution n'est pas parfaite.
- Génère beaucoup de fausses alertes

ANTIVIRUS
Solution

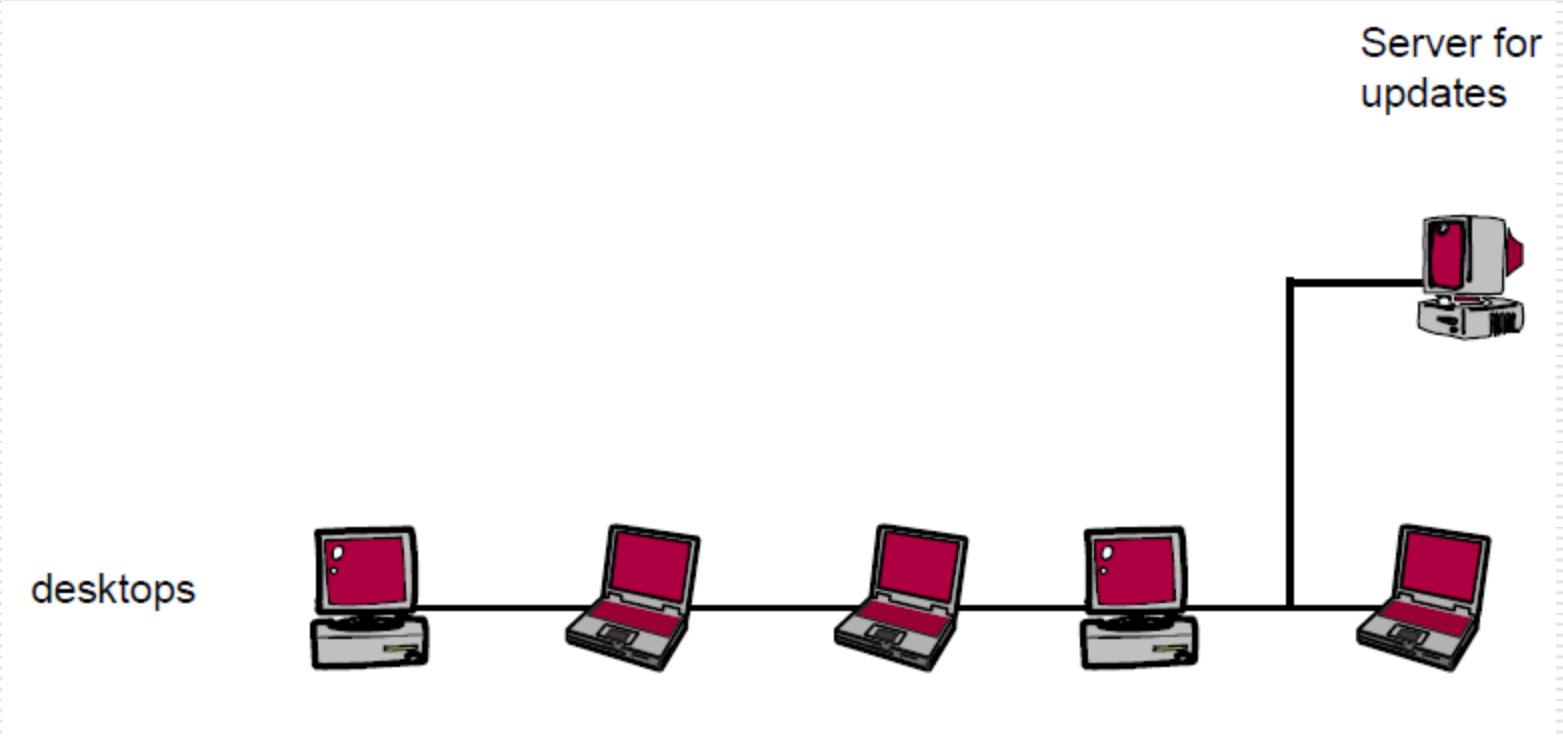
- Utiliser les méthodes de détections conjointement.

- Un antivirus doit être mis à jour et vérifier automatiquement

- Un antivirus doit être utiliser à tous les niveaux du réseau d'une entreprise

- **Tous les niveaux????**

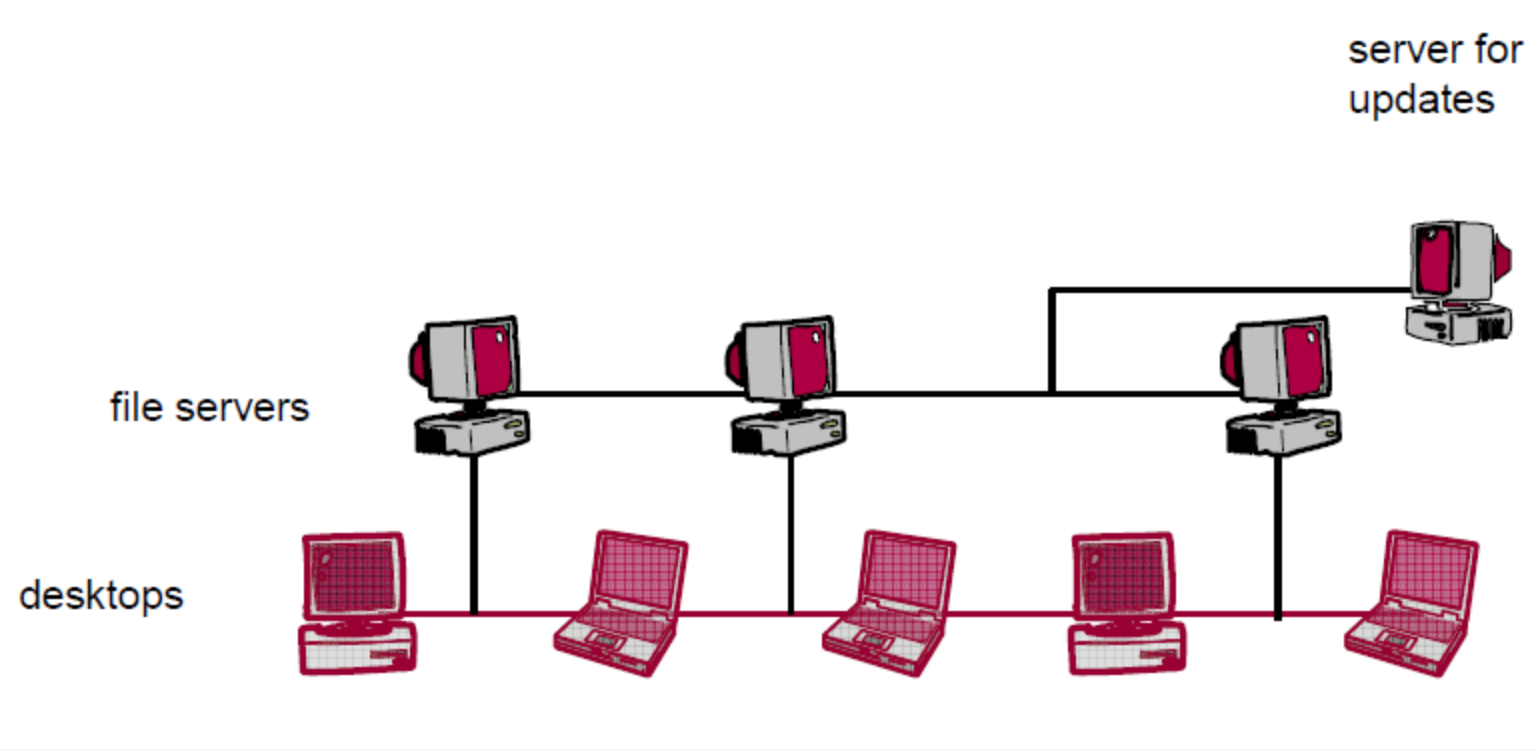
Niveau 1: Postes de travail



Niveau 1: Postes de travail

- Tous les ordinateurs de bureau doivent être protégés par un antivirus
- La mise à jour doit être automatique
- Il faut gérer le cas des nouvelles machines insérées (les laptops surtout)

Niveau 2
Les serveurs de fichiers



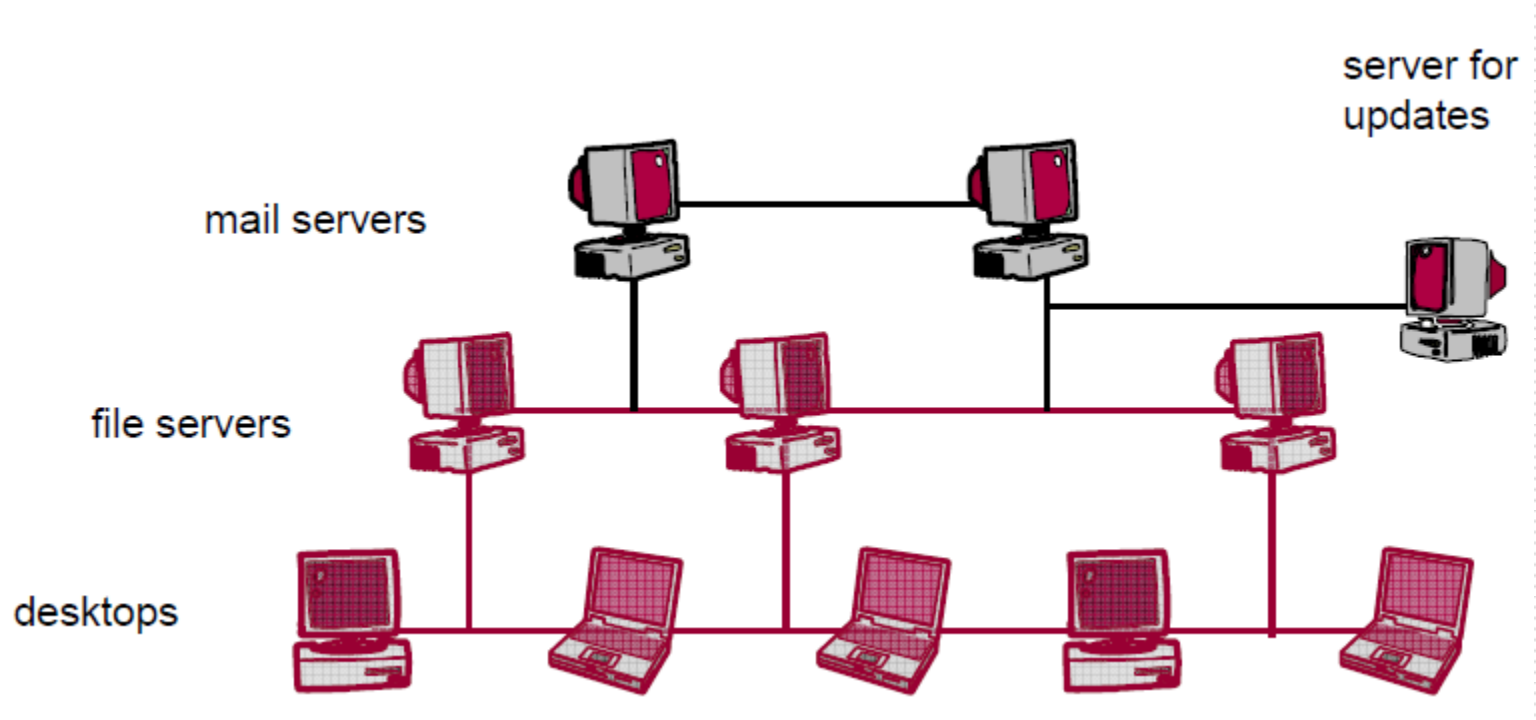
Niveau 2
Les serveurs de fichiers

- Les serveurs de fichiers contiennent des fichiers de plusieurs utilisateurs
- Une infection peut être très dangereuse

Il faut donc:

- Analyser tous les fichiers lors de l'écriture ou de la lecture
- Des MAJ automatiques et quotidiennes
- Une Analyse automatique des logs

Niveau 3
Les serveurs mails



Niveau 3
Les serveurs mails

- Il faut analyser les emails avant de les placés dans la boîte du destinataire

- Le logiciel antivirus doit être capable de faire face à tout type de pièces jointes (même les fichiers zippés)

- Le logiciel antivirus doit éliminer les virus détectés et doit informer l'expéditeur, le destinataire et l'administrateur par e-mail

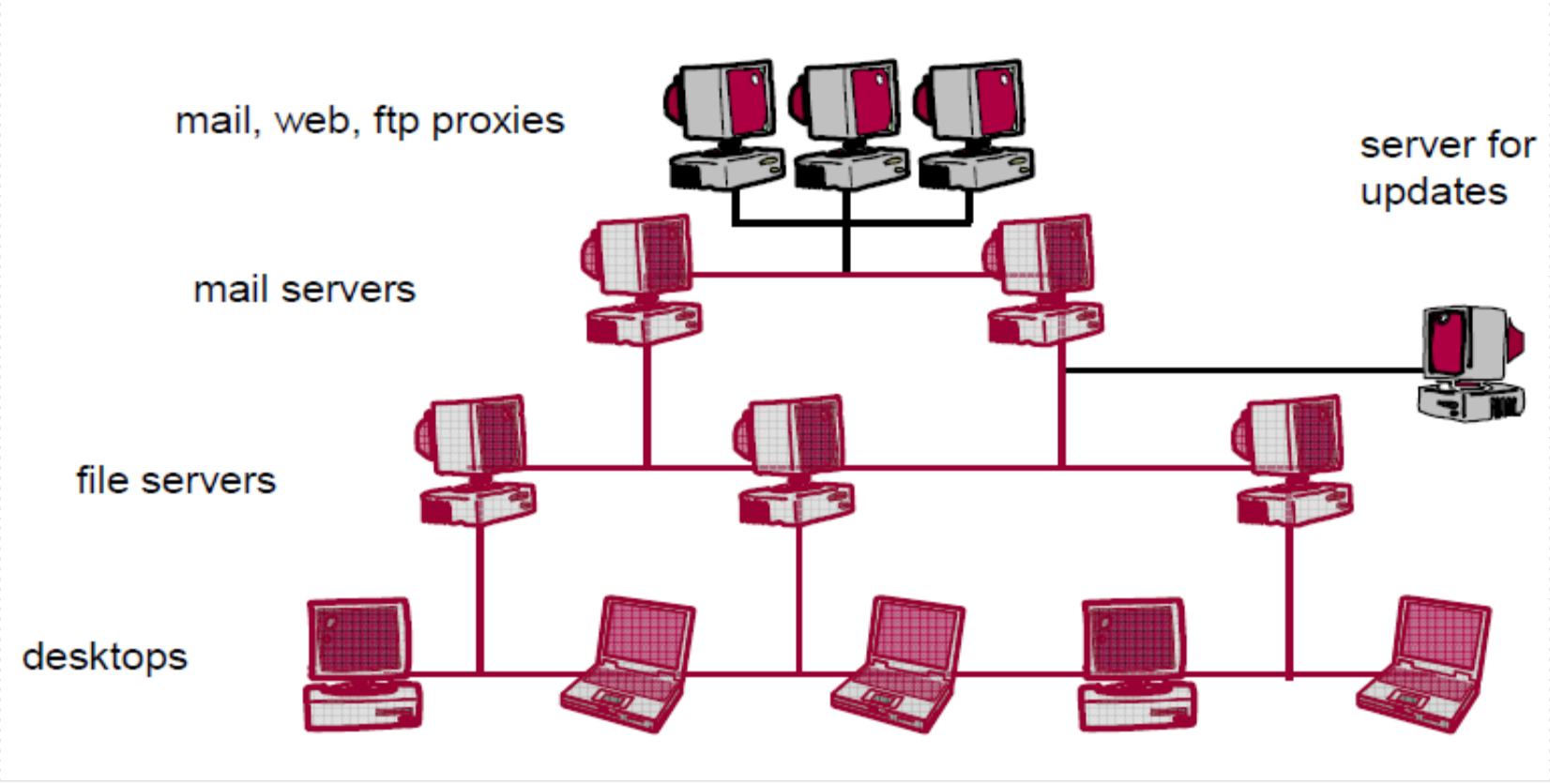
Niveau 3
Les serveurs mails

- L'expéditeur malveillant peut être mis sur une liste noire

- Une mises à jour quotidiennes de l'antivirus est recommandée

- Régulièrement, une mises à jour du logiciel de serveur mail est nécessaire

Niveau 4
Les proxies: mail, web, ftp



Niveau 4
Les proxies mail

- Isoler les serveurs de messagerie de l'Internet
- Les attaques (DOS et autres) touchent le proxy et non pas les serveurs internes.

- Interception de virus avant même qu'ils ne pénètrent dans le réseau interne

- Le proxy est sous la responsabilité d'une seule équipe donc est facile à gérer.

Une maintenance 24/7 et une mise à jour sont nécessaire

Niveau 4
Les proxies web et ftp

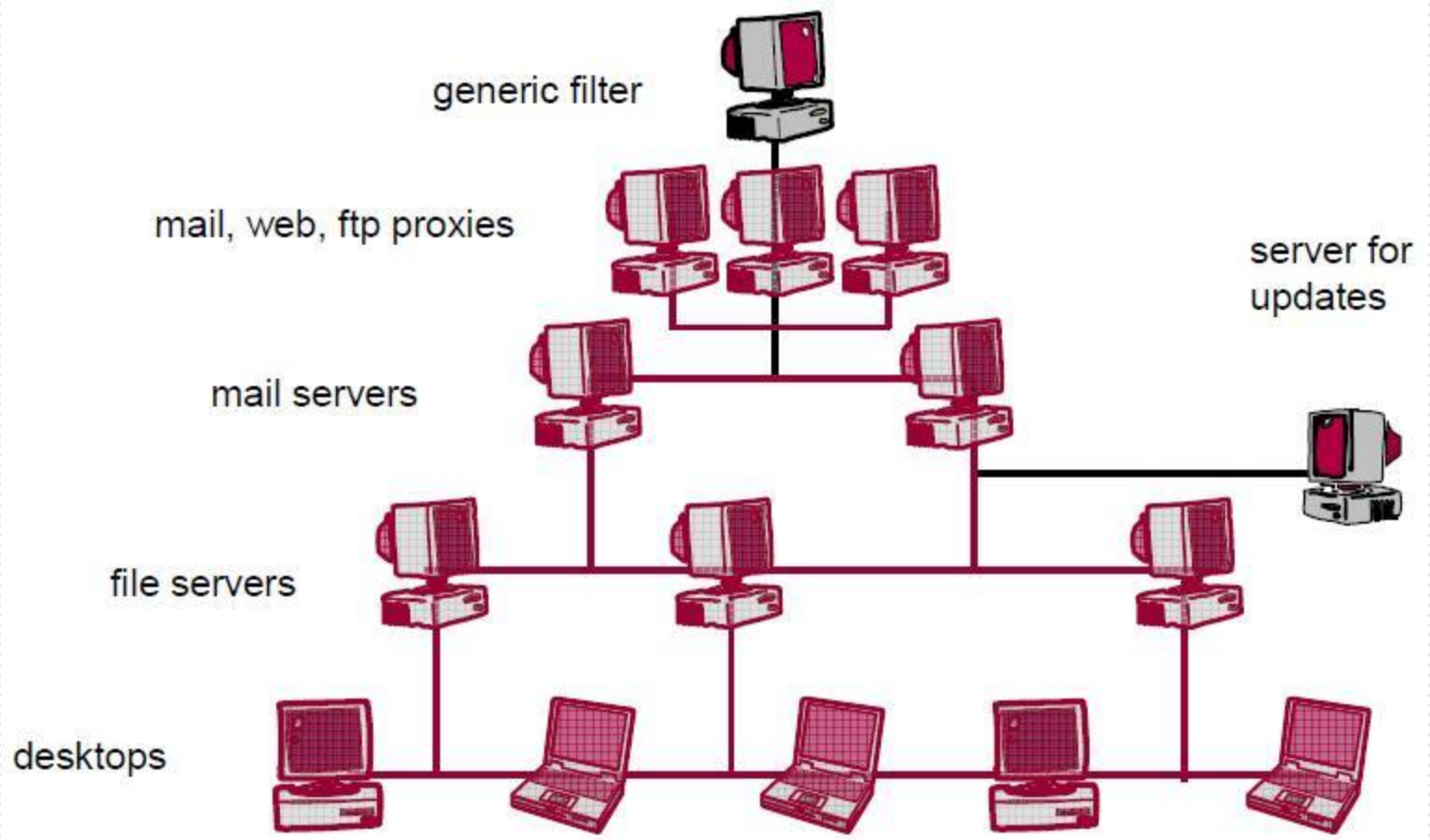
- On peut télécharger des logiciels potentiellement infectés par l'intermédiaire du Web et par ftp.

- Nous pouvons également recevoir des e-mails sur le Web(yahoo, Hotmail,…etc.).

- Les pages Web peuvent contenir des virus (par le biais d'une infection)

- **Les proxies web et ftp analysent tous les documents accessibles et éliminent les virus détectés**

Niveau 5


generic filter
mail, web, ftp proxies
server for updates
mail servers
file servers
desktops

Niveau 5

- Le filtre général permet le blocage des nouveaux virus avant même que le logiciel antivirus est mis à jour

- Il filtre les pièces jointes qui ne sont pas utiles .exe .bat .vbs,.pif , .scr, .shs

- **Principe**: Interdire par défaut, et préciser les types autorisés .doc, .xls,…etc

- Le filtre doit être installé sur tous les Proxies

Code Mobile

Attention aux:

- **Applets JAVA**
- **Active X**