RéSIST

Protection virale

- Où en est-on ?
  - Constats
- Où va-t-on ?

RéSIST

Constat

- Nombre de virus/vers double chaque année
- Le concepteur de virus devient professionnel
- Le temps de réalisation d'un antidote est au minimum de 2 heures, plus généralement 4 heures.

RéSIST

Constat 2

- Le firewall ne suffit plus
- La mise à jour des antivirus ne suffit plus
- Le décalage horaire ne suffit plus.

RéSIST

Constat 3

- Les vers sont optimisés pour la propagation interne/externe
- Les virus ont coûtés 10 jours ingénieur + 20 jours techniciens cette année à l'UT1

RéSIST

Il faut se protéger en attendant

- Classiquement
  - Filtrage des ports (généralement microsoft)
- Moins classiquement
  - Protéger l'extérieur
    - Empêcher les sorties SMTP
- Mais cela ne suffit pas

RéSIST

Les comportements viraux

- Vers : scan de ports.
- Virus :
  - SMTP embarqué
  - Nombreux origines
  - Nombreux destinataires
  - Annexes dangereuses.

RéSIST

Limiter les virus

- Notion de greylisting (vis-à-vis de l'extérieur)
- Traitement particulier des pièces jointes
  - Eradication
  - Mise en attente

RéSIST

Repérer les machines infectés

- Sur les firewalls (individuels ou non)
  - Blocage avec log des communications interdites (en particulier le SMTP)
- Remontée des alertes vers un point de collecte

Mise en quarantaine

- Distribution de la liste des postes infectés
- Actions spécifiques ayant pour but
  - De limiter la propagation
  - D'avertir l'utilisateur

Exemple à l'UT1

RéSIST

La limitation des virus

- Greylisting sur un postfix : 75% de virus et de spams en moins (plus marquage)
- Mise en attente des annexes dangereuses. Et renvoi toutes les 6 heures
  - Evite de faire disparaître un mail
  - Evite les boules de neige
  - Affiche « l'efficacité » du service
- Utilisation d'un bayésien anti-spam

RéSIST

La prise d'alerte

- Le firewall
  - Remonte les alertes sur protocoles SMTP et Netbios (plus de 10 en 10000 lignes de logs)
- Les serveurs remontent toute tentative Netbios
- Les serveurs de messagerie
  - Remontée des postes avec plus de 3 expéditeurs en 10000 lignes de logs

La mise en quarantaine

- Blocage de la propagation
  - Interdiction d'envoi de mail (mais pas de récupération)
  - Interdiction de connexion au WWW (mise à jour virale)
- Avertissement du propriétaire
  - Redirection des page web vers une page d'explication pour la désinfection

Les résultats : positifs

- Baisse de la charge des serveurs
- Réaction automatique (blocage et déblocage) en moins de 30 minutes (pour un virus qui n'est pas encore connu)
- Les utilisateurs arrivent, parfois (30%), à se débrouiller seuls
- Le diagnostic est immédiat.

RéSIST

Les problèmes

- Attention aux protocoles et aux seuils de déclenchement (poste configuré avec un SMTP ou une imprimante SNMP extérieure)
- Attention aux applicatifs utilisant le protocole Netbios
- La notion de fenêtre temporelle glissante est insuffisamment gérée, empêchant toute réduction du temps de réaction

RéSIST

Les problèmes 2

- Il faut une structure adéquate (redirection web)