Situation de la messagerie électronique à l'IN2P3 : virus et spam

JI2006, Lyon-Valpré, du 18 au 21 septembre 2006

delaunay@in2p3.fr
Benoit DELAUNAY

Contenu de la présentation

- État des lieux des mécanismes de lutte contre les virus et les spams dans le(s) système(s) de messagerie utilisé(s) à l'IN2P3
- Repose sur les résultats d'une enquête auprès de 14 laboratoires
- Un indicateur à ajouter au tableau de bord maintenu par le chargé de mission à la Sécurité Informatique de l'Institut
- Une vue globale des technologies utilisées dans chacun des sites

Lutte contre les virus et les spams

- La lutte contre les virus et la lutte contre les spams sont souvent associées (mêmes canaux de diffusion, etc…).
- La propagation massive du virus « I love You » en mai 2000 amène à une prise de conscience collective des risques liés à l'utilisation non contrôlée de la messagerie électronique.
- Les JS organisées au Collège de France en octobre 2002, sont le point de départ au déploiement de mécanismes de lutte contre les virus à l'IN2P3.
- A l'automne 2002, trois laboratoires ont déjà des solutions opérationnelles (SUBATECH avec Interscan, CPPM avec Amavis/Sophos et le LAL)

Contenu de l'enquête

- Informations générales
  - Nom de domaine de messagerie, nombre d'adresses, volumes
- Passerelle de messagerie entrante
  - Types de MTA, description des moyens de lutte contre les virus et les spams, politique adoptée.
- Passerelle de messagerie sortante
  - Types de MTA, description des moyens de lutte contre les virus, politique, accès.

Présentation des résultats…

Structure du système de messagerie électronique

- Le domaine d'adresses « @in2p3.fr » est géré par le Centre de Calcul de l'IN2P3
  - Concrètement une liste d'alias
- Chaque laboratoire gère son propre domaine de mail, un sous domaine du domaine « in2p3.fr »
  - Ex. « @labo.in2p3.fr »
- Certains moyens sont mutualisés, mais pas tous.
  - Sur 14 sites ayant répondu à l'enquête, 8 utilisent la passerelle antivirus du Centre de Calcul
  - Le serveur de boites aux lettres IMAP du CC est utilisé par le CPPM

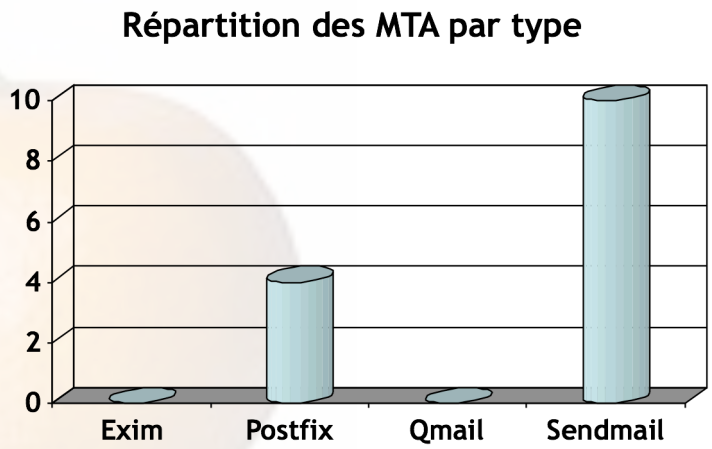
Nombre d'adresses et volume

- Plus de 5000 adresses sont gérées sur la totalité des sites de l'IN2P3
- Un volume quotidien moyen supérieur à 150000 courriers électroniques

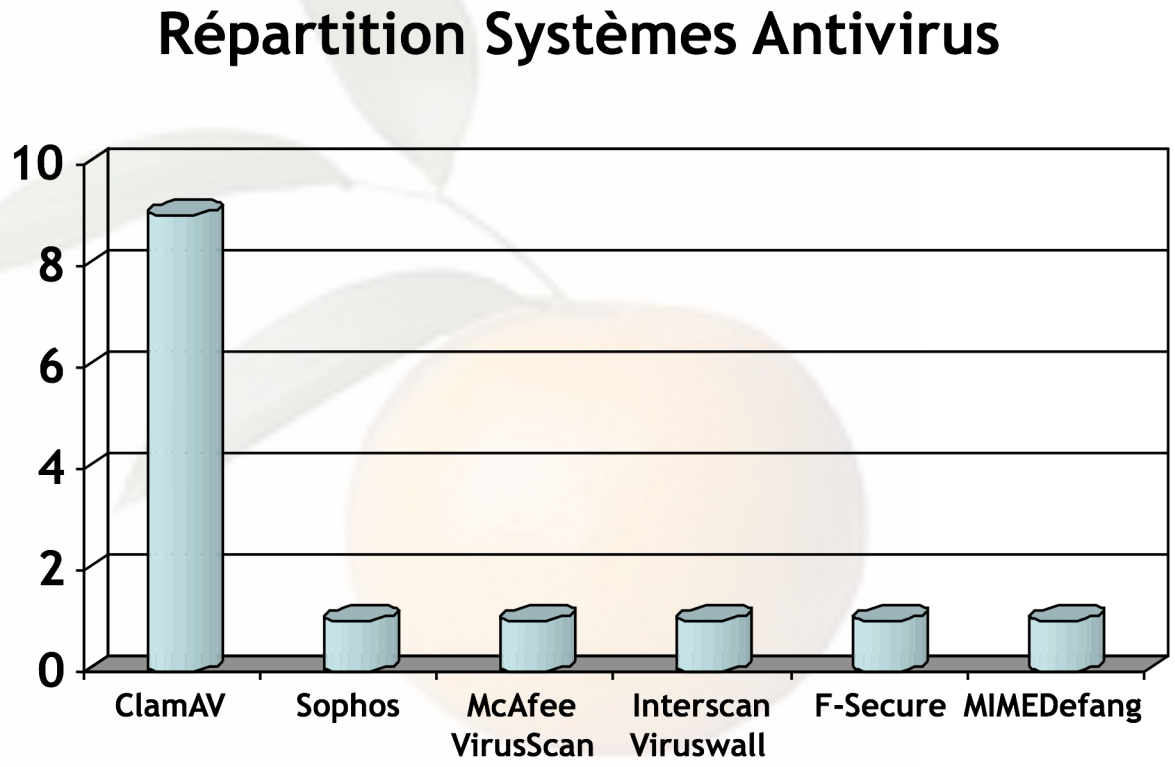
Mail Transfer Agent - MTA

- Sendmail et Postfix sont principalement utilisés sur les passerelles de messagerie des laboratoires.

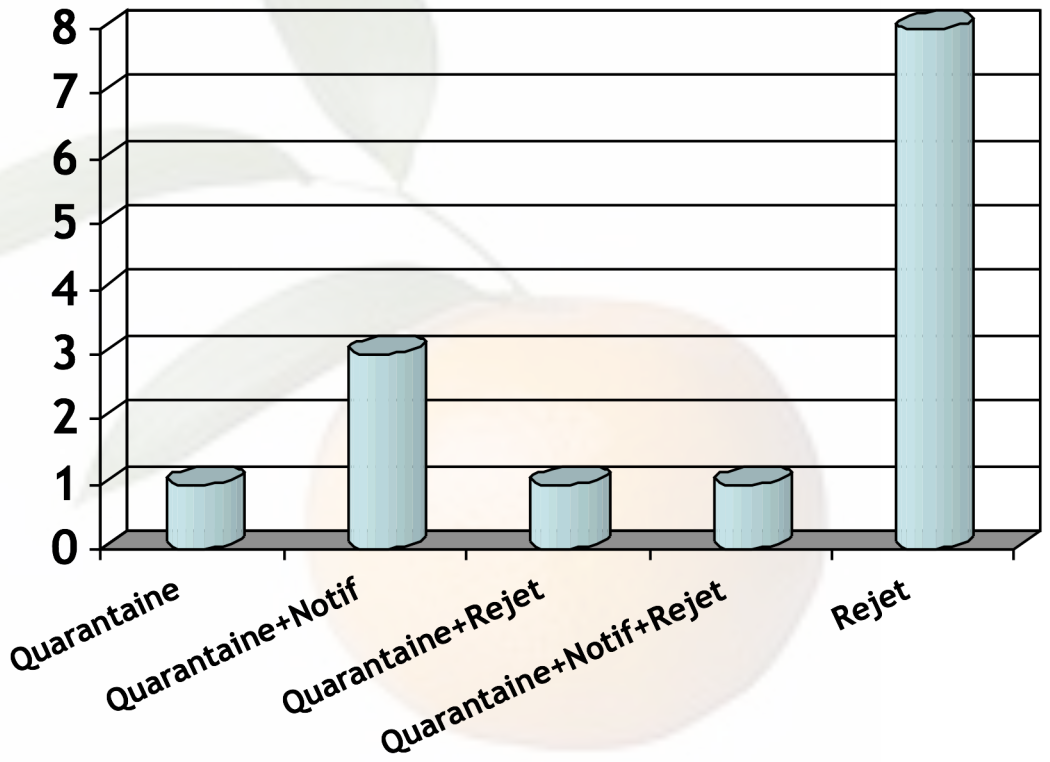
- http://www.sendmail.org
- http://www.postfix.org



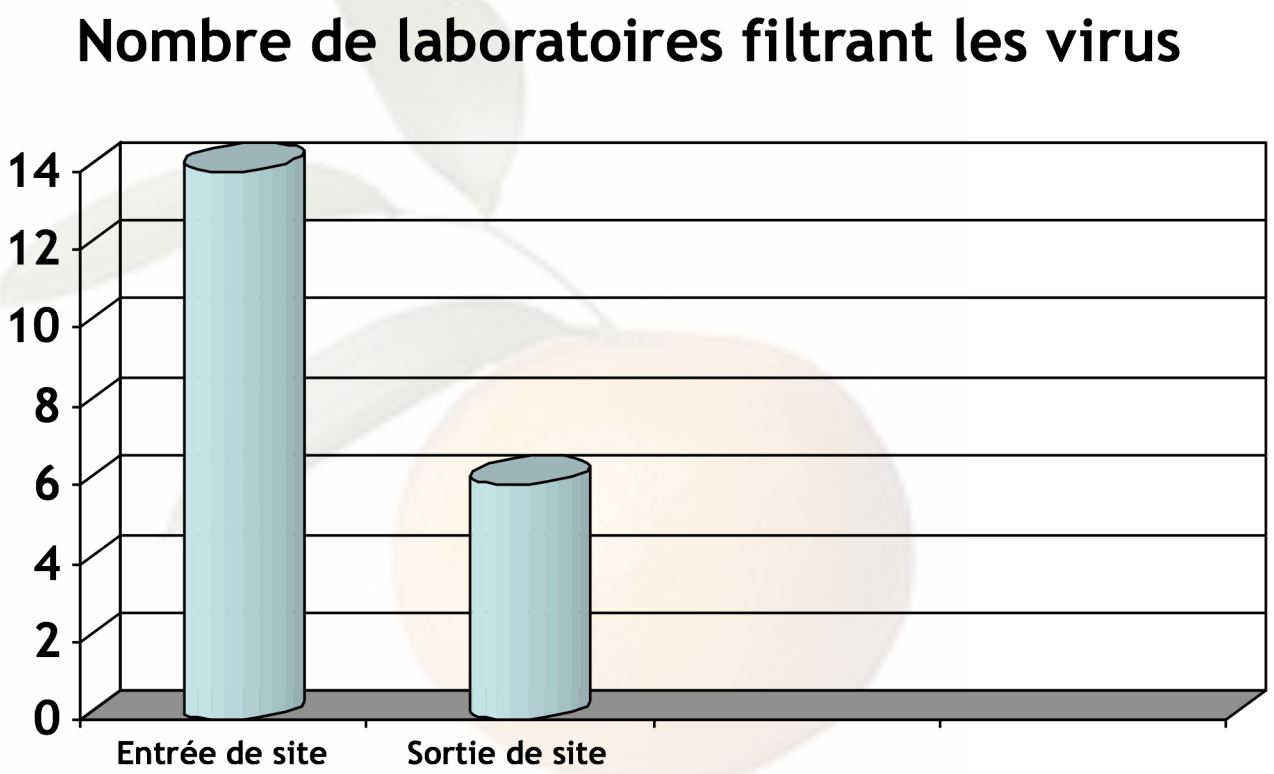
Origine des antivirus de messagerie



Action sur détection de virus



Filtrage des virus



Bilan antivirus 1/2

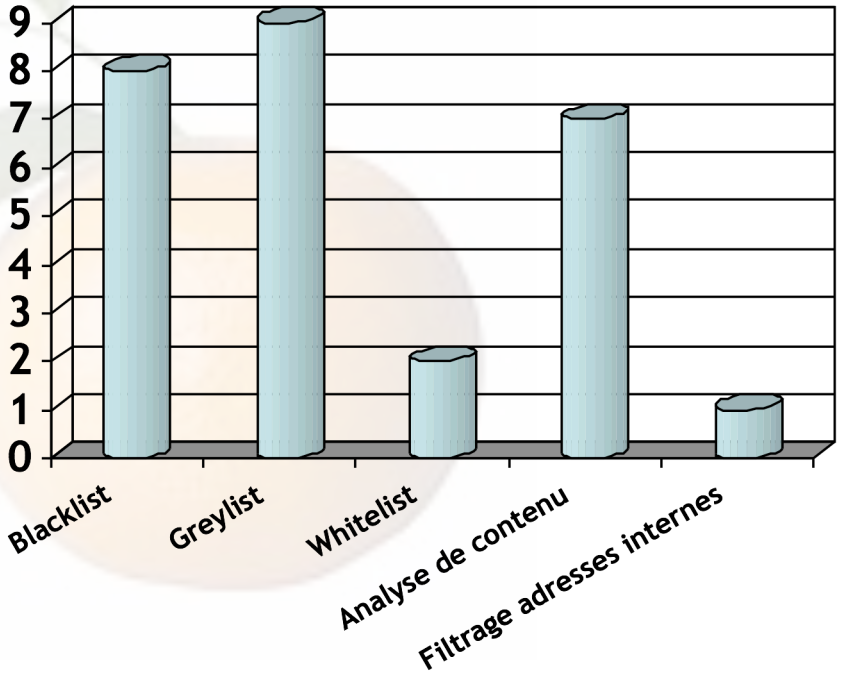
- La totalité des laboratoires de l'IN2P3 (ayant répondu) utilisent des mécanismes de lutte contre les virus en entrée de site.
- 1 laboratoire n'utilise pas d'antivirus basé sur la détection de signature, mais filtre les pièces jointes sur la nature des extensions.
- Tous les autres sites utilisent au minimum un antivirus commercial ou du domaine public.

Bilan antivirus 2/2

- 6 laboratoires font une vérification explicite du contenu des courriers en partance de leur site.
- La situation est a clarifier avec les 8 sites utilisant la passerelle antivirus du CC.

Lutte contre le spam

- Répartition des techniques utilisées de lutte contre la diffusion de courriers non sollicités à l'IN2P3



Bilan antispam

- Tous les laboratoires utilisent des techniques pour réduire la diffusion de courriers non sollicités.
- Il n'y a pas une technique miracle mais un ensemble de techniques complémentaires.
- Contrairement à la problématique de détection de virus, les techniques de lutte contre le spam doivent être en perpétuelle évolution.

Conclusion 1/2

- Tous les laboratoires de l'IN2P3 ont déployé des mécanismes de lutte contre les virus. Le bilan est tardif mais très positif !
- L'expérience de l'IPNL de filtrage du trafic sortant TCP/25 pour les machines autres que les passerelles de messagerie pourrait-elle être généralisée ?
- Le filtrage antivirus sur les passerelles de sortie de site devrait être global.

Conclusion 2/2

- Tous les sites utilisent des outils de lutte contre les spams.
- Si la lutte contre les virus est assez mature, la lutte contre la propagation des courriers non sollicités est un combat de chaque jour.