Anti Virus & Spam Management - The Microsoft Way

QUESTnet – July 2004

Raj Natarajan
National Technology Specialist
Enterprise & Partner Group
Microsoft Australia

Agenda

- Microsoft IT messaging hygiene overview
- E-mail Anti virus infrastructure
- Anti spam infrastructure
- Other messaging hygiene methods
- Futures

What is Messaging Hygiene?

- Goal: Keep corporate messaging environment free of malicious and unauthorised content
- Threats to messaging hygiene include
  - Virus infected e-mail
  - UCE/Spam e-mail
  - Denial of Service (DoS) attacks
  - Directory Harvesting (DHA) attacks
  - E-mail spoofing
  - Unauthorised mail submission

MS IT Messaging Hygiene in Numbers

- Overall Internet mail volume
  - 8,000,000-10,000,000 per day
- Spam/UCE
  - Heuristics based filtering - Intelligent Message Filter (IMF)
    - ~50% of all inbound Internet mail traffic
    - 4,000,000 messages per day filtered
  - Signature based filtering
    - up to 55% (of the remaining)
    - 2,000,000 + messages per day filtered
  - Sender/Recipient filtering
    - 1,500,000 message/day filtered
- Viruses
  - 10,000 – 100,000 viruses stopped at the e-mail edge

MS IT Messaging Hygiene in Numbers

- Platform
  - Windows 2003/Windows 2000
  - Exchange 2003 SP1
  - Client: Outlook 2003
- Topology
  - Multiple Exchange organisations
  - Virus scanning on all Internet mail entry and exit points
  - Spam blocking on major *published* mail entry points
  - Spam filtering is done topologically prior to virus scanning
- Infrastructure
  - 9 SMTP gateways dedicated for e-mail virus scanning
  - Regional SMTP gateways are enabled for virus scanning
  - 7 gateways performing anti spam functions

MS IT Messaging Hygiene

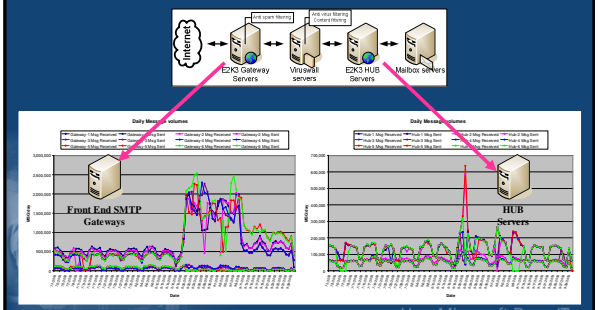
- Anti virus
  - Signature based
  - Attachment stripping
- Anti spam
  - Signature based
  - Heuristics based (Intelligent Message Filter - IMF)
- Static filtering
  - Sender/Recipient filtering
  - Custom Event sinks

Architectural Principles

- Anti spam and Anti virus MUST be present at the gateway level
- Anti spam MUST be topologically before anti virus
- Anti spam SHOULD be done for inbound mail only
- Anti spam filtering SHOULD remove vs. quarantine
- Anti virus MUST scan both inbound and outbound mail
- Anti virus MUST be mail direction aware
- Anti virus MUST follow “block on fail” rule
- Anti virus MUST include attachment stripping

Virus Attack – Live Primer

- August 2003: Sobig.F causes DoS effect (5xnormal load)

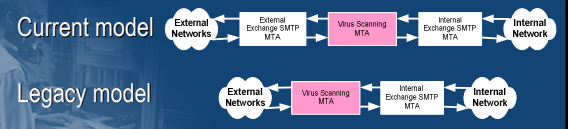


MS IT E-mail Anti Virus

- Gateway, transport, store and client
  - Defense in depth is key
- MS IT environment
  - Gateway level scanning (managed by Messaging)
  - Client level scanning (managed by CorpSec)
- MS IT dependency on Dogfooding

MS IT E-mail Anti Virus

- Existing environment
  - Gateway level scanning
  - Dedicated virus scanning SMTP MTA
  - Interoperability based on RFC 821

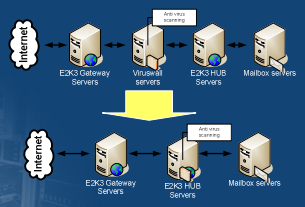


MS IT E-mail Anti Virus

- Attachment Security
  - Attachment stripping is done at the gateway
    - Protection from unknown malware
    - Stripped attachment is substituted with a text file
  - Topologically before virus scanning
    - Reduced performance overhead
  - List of stripped attachments includes Outlook 2003 Level 1 attachment list (Q829982)

MS IT E-mail Anti Virus

- Future direction
  - Leverage Exchange gateway as Anti virus platform
  - Use VSAPI 2.5 or transport event sink model
  - Retire dedicated virus scanning servers



Exchange Server 2003
- Virus Scanning API 2.5

- Message body and attachment scanning
- Native MAPI/MIME content scanning
- Scan Exchange Database & Transport
- Proactive Scanning
  - As messages arrive inbound to the server
- On Access Scanning
  - When messages are accessed via client or agent
- Background Scanning
  - Ongoing scanning of messages
  - Primarily used for re-scanning data when virus signatures are updated
- Scanner On-Demand Reload

MS IT Anti Spam

- MS IT anti spam components include
  - Heuristics based spam blocking
    - Intelligent Message Filter http://www.microsoft.com/exchange/techinfo/security/imfoverview.asp
  - Signature based spam blocking
- Installed at the outermost SMTP gateways
  - Topologically before Anti virus
  - Exposure to unaltered message headers
- Exchange 2003 is used as a platform

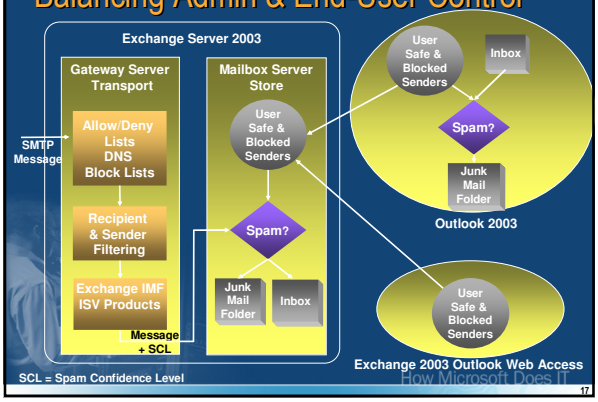
MS IT Anti Spam

- Integration with Exchange – transport event sinks
- Action on spam is "Remove"
  - Quarantine is too costly
- SCL (Spam Confidence Level)
  - Gateway level threshold (Remove)
  - Store level threshold (Junkmail)

Exchange Server 2003
- Intelligent Message Filter

- Built on SmartScreen Technology
  - Shipped in Outlook2003
  - Deployed at Hotmail (blocks ~3 billion+ messages / day; more than 95% of incoming spam at Hotmail)
  - In use at MSN8 & MSN Premium
- Extension to Exchange 2003 Server
- Leverages the SCL infrastructure with by supporting per message tagging
- Filter Updates
- Coexistence with 3rd party solutions
- Balances Administrative & End-User Control (effort to combat False Positives)

Balancing Admin & End-User Control



Quick Look – Exchange IMF

demo

Other Message Hygiene Methods Used

- Exchange sender and recipient filtering
- Exchange connection filtering
- Custom event sinks
- Exchange anti spoofing mechanisms
- Restricted and authenticated Distribution Groups (DGs)
- Outlook 2003/OWA features
- RBL is under consideration

Operations

- Regular signature/pattern file updates
- Automated checks for state of critical services
- Close monitoring of Internet mail patterns
- Areas of interest
  - Inbound message rate
  - Number and rate of inbound connections
  - Virus detection rate
  - Mail queue size and content

Futures - Exchange Edge Services

- Q1 CY2005
- New Exchange Server “Roles”
- Exchange Edge Services focus
  - SMTP Gateway – security/reliability
  - E-mail Hygiene – anti-spam and anti-virus
  - Routing - Mail flow policies and processing
- Extensible
  - Partners integrate and innovate

Questions?

- Additional content on Microsoft IT deployments and best practices can be found on Microsoft TechNet: http://www.microsoft.com/technet/itshowcase
- Want to know more about Exchange Server – read up at http://www.microsoft.com/exchange
- More information about our anti-spam efforts is available at http://www.microsoft.com/spam

Microsoft

Your potential. Our passion.™