Multilayer e-mail security
Multilayer email security

Jozef Kačala – Sales engineer EMEA, APAC
Multilayer email security

Agenda

- E-MAIL usage
- Importance of E-MAIL protection
- E-MAIL born attacks
- GFI MailEssentials + demo
E-MAIL usage

E-mail is the most widely used Internet function across the planet.

- 3.8 billion email users worldwide
- 1.75 e-mail accounts per user
- 212 billion business email sent every day
- 2 million e-mails sent every second
- 91% of people check their e-mail daily
E-MAIL usage

- People check their email an average of **74 times a day**!
- People are spending anywhere from **25 minutes to 2 hours a day** actively involved in their inbox.
E-MAIL born attacks

E-mail is #1 delivery vehicle for malware

- 60% of emails are spam
- 48% of organisations experienced phishing attacks
- 92.4% of malware is delivered via e-mail
E-MAIL born attacks

As one of the most popular services, e-mail has become a major vulnerability to users and organizations.

- Phishing
- Whaling
- Pharming
- Spyware
- Scareware
- Adware
- Spam
- DoS
- Man-in-the-middle attacks
- Credential reuse
The security system is only as strong as its weakest point.
SECURITY = wall + antivirus + ? + spam + search + settings + email + ...
Importance of e-mail protection

- Save resources
- Prevent brand damage
- Email is the most common IT security threat for organizations
- Email-based attacks affect the entire organization
- Save time
- Save money
- Email-based threats are evolving and increasing, putting more organizations at risk every year
- Basic anti-spam email filters are not enough
Malware protection

Unwanted (spam) e-mail protection

E-mail management

Content control
The user

Up to 99% spam filtered

The security system is only as strong as its weakest point
Malware protection

- Five antivirus engines
- Trojan and executable scanner
- E-mail exploit engine
- HTML sanitizer
Unwanted e-mail protection

- 15 anti spam engines
- Outlook integration
- Granular Whitelist and Blacklist
E-mail Management

- Disclaimer management
- E-mail monitoring functions
- Module for automatic replies
Content control

- Filtering incoming, outgoing and internal content
- Granular ruleset against users/groups
- Decompression and attachment filtering
- Advanced content filtering within documents
E-mail flow in GFI MailEssentials

1. SMTP level filters (Directory Harvesting, Greylist, IP Blocklist & IP DNS Blocklist)
2. Malware and content filtering scans
3. List server check
4. Other anti-spam scans
5. Auto replies (if configured)
6. E-mail monitoring (if configured)
7. New senders filter check

If email is not blocked by any scanning or filtering engine, it is sent to the user’s mailbox.
GFI MailEssentials – best practices

• Place IP blocklist on the first place so it will run during SMTP transmission rather than after the IP whitelist.

• When MS Exchange is used, best is to install GFI MailEssentials directly on MS Exchange servers with HUB transport role, Mailbox role or edge server role.

• Turn on bayesian filter after creating sufficient spam and ham database.
GFI MailEssentials – Live demo
Contact Us

salescz@gfi.com  www.gfi.com