



Results from ENISA 2007 survey on providers' security and anti-spam measures

Pascal Manzano

RIPE 55 Anti-spam Working Group
October 25, 2007

Goal of the survey

- Better understand security measures used by providers
- Promote and develop best practices
- Survey covers security and anti-spam measures, both from technical and organisational point of view

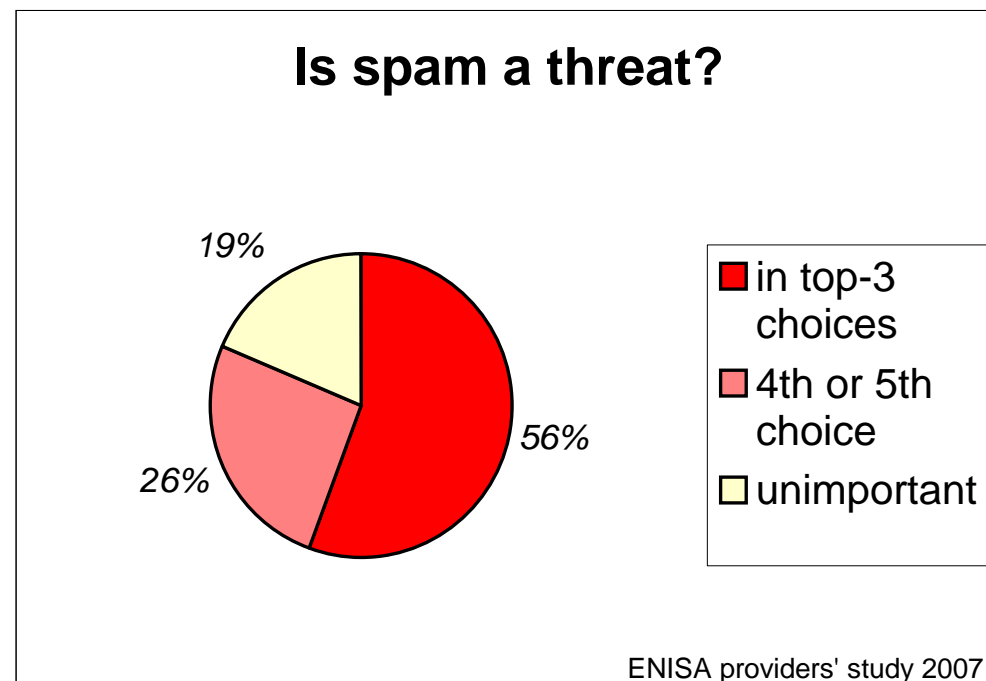
Method

- Online questionnaire available in June and July
- 21 multiple choice questions
- Contacts with providers' associations at European and national level
- Promotion of the questionnaire in newsletters, mailing-lists, ENISA contacts' network.

Representativeness

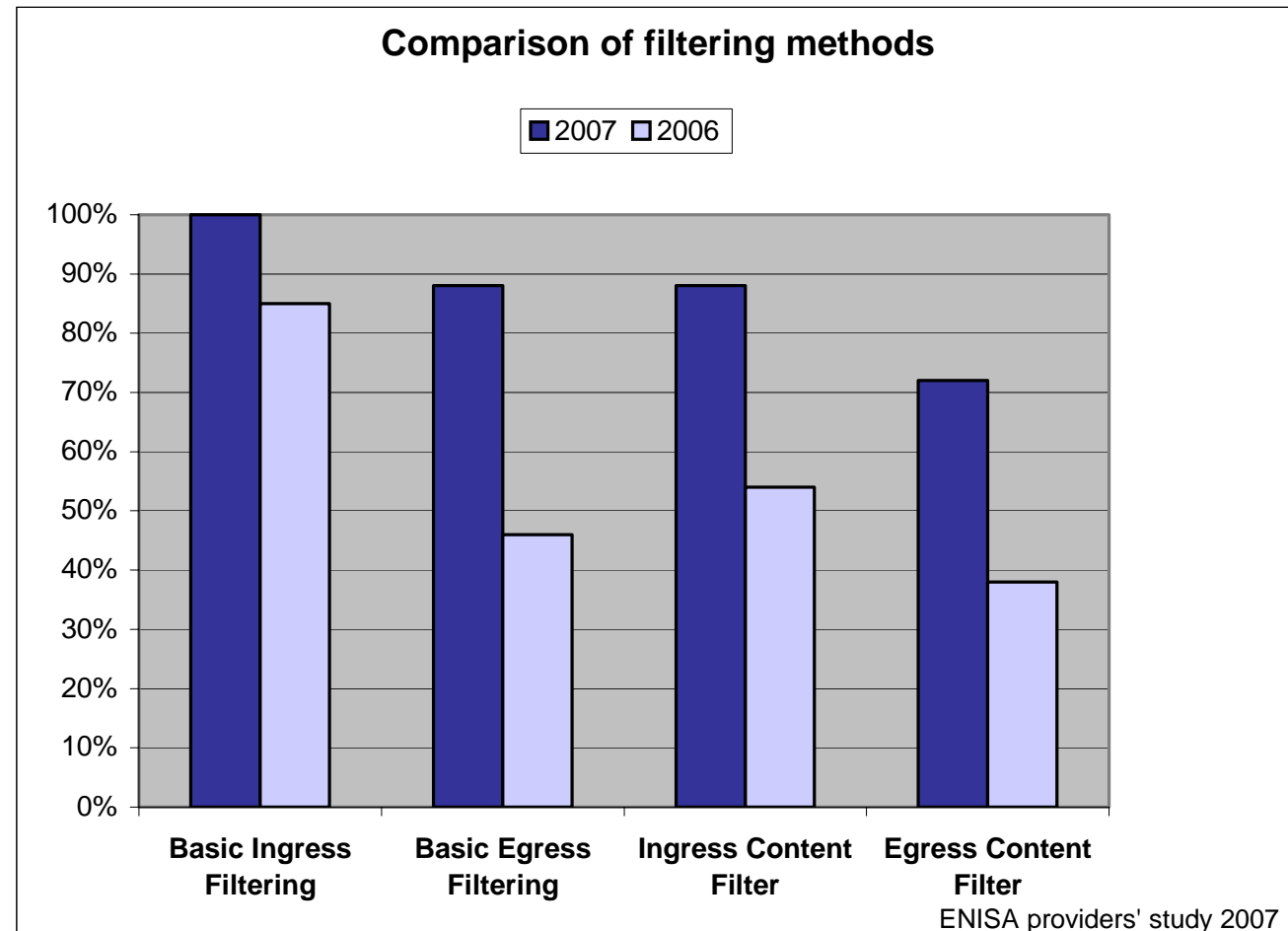
- 30 providers replied
- 86% are ISPs, 11% ESPs, 43% telco
- Wide variety of size (3 in European top10)
- 25 providers are from 16 of the 27 EU countries
- 3 from Norway, 1 from Iceland and 1 from US

- Most important threats identified by providers:
 1. Viruses
 2. Spam
 3. DDoS

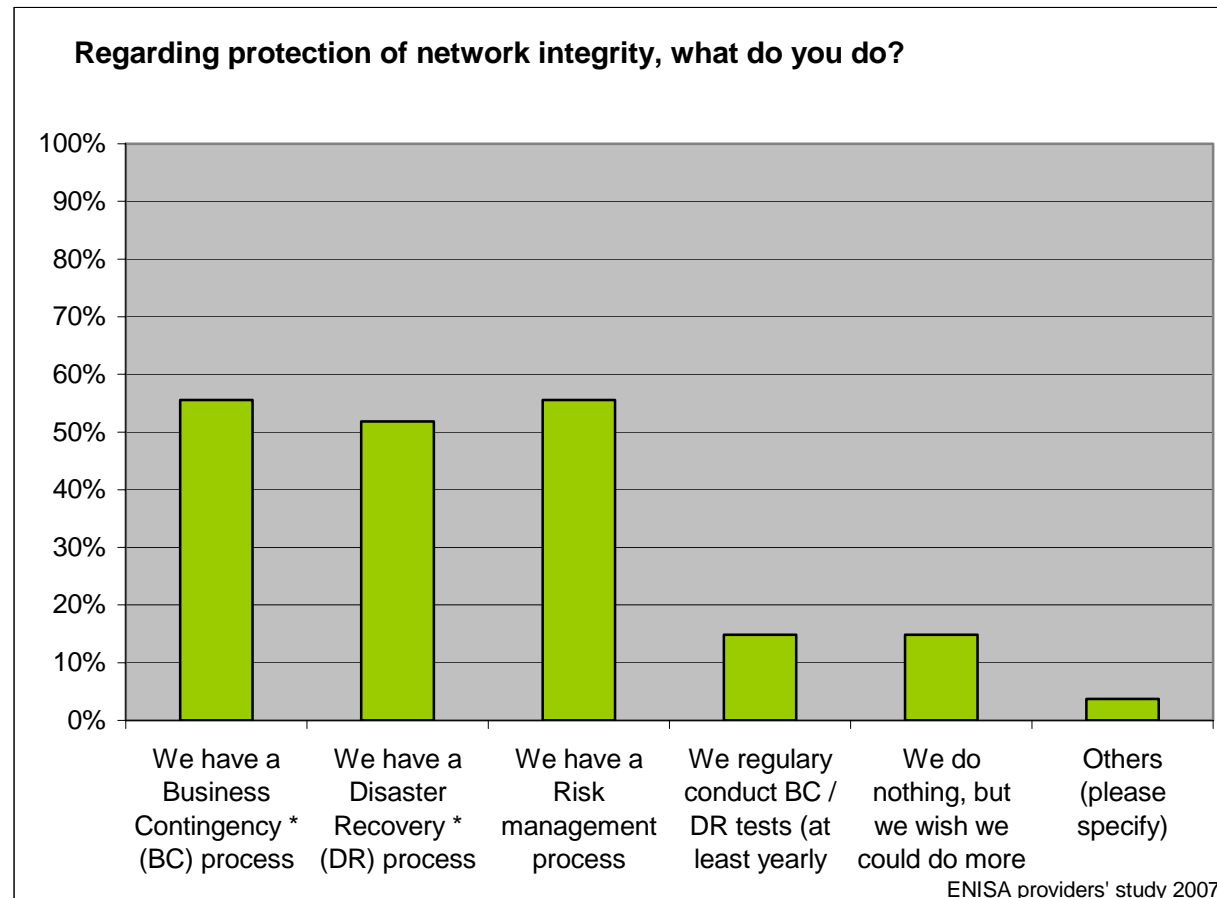


Filtering methods

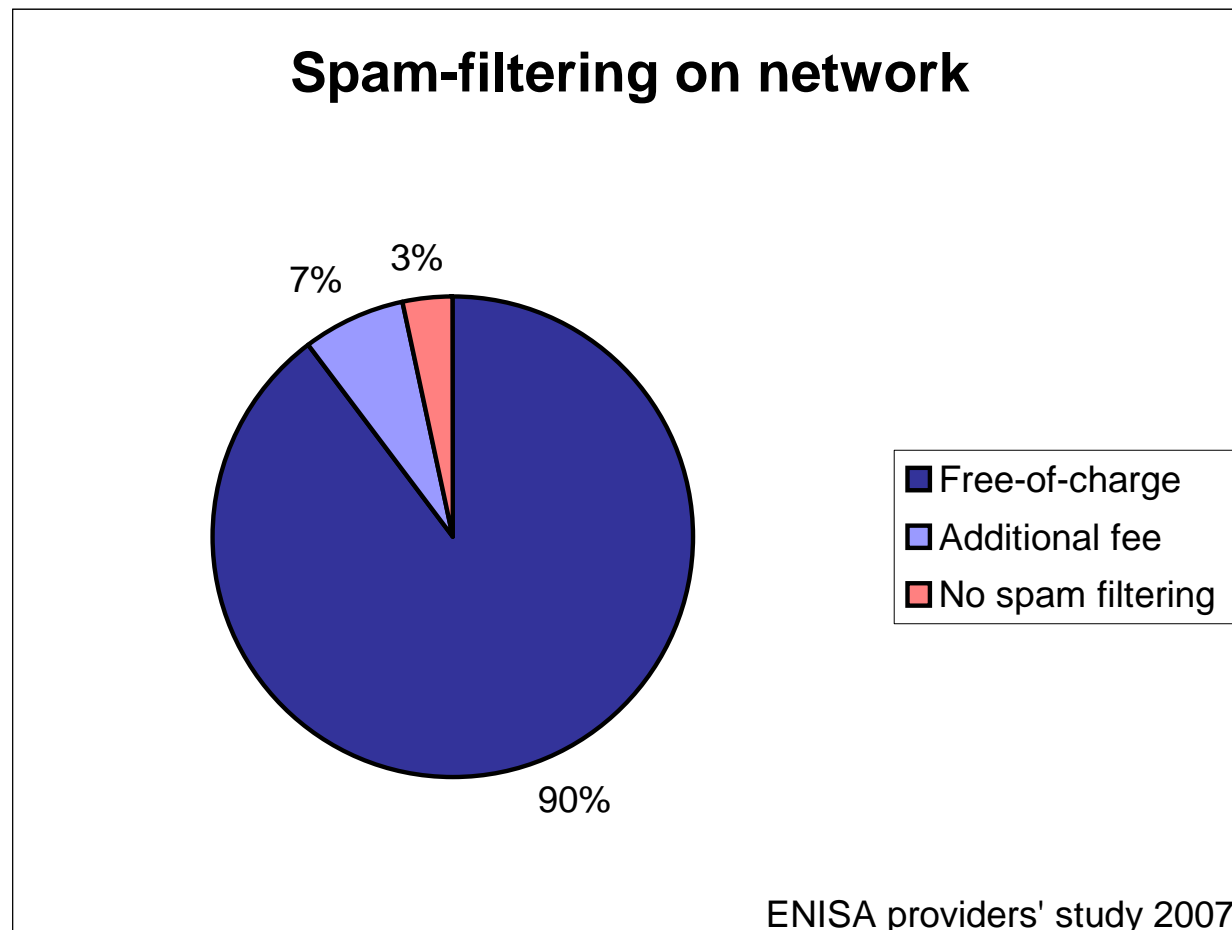
- Ingress
- Egress
- Basic
- Content
- Trend



- BC
- DR
- RM
- Testing

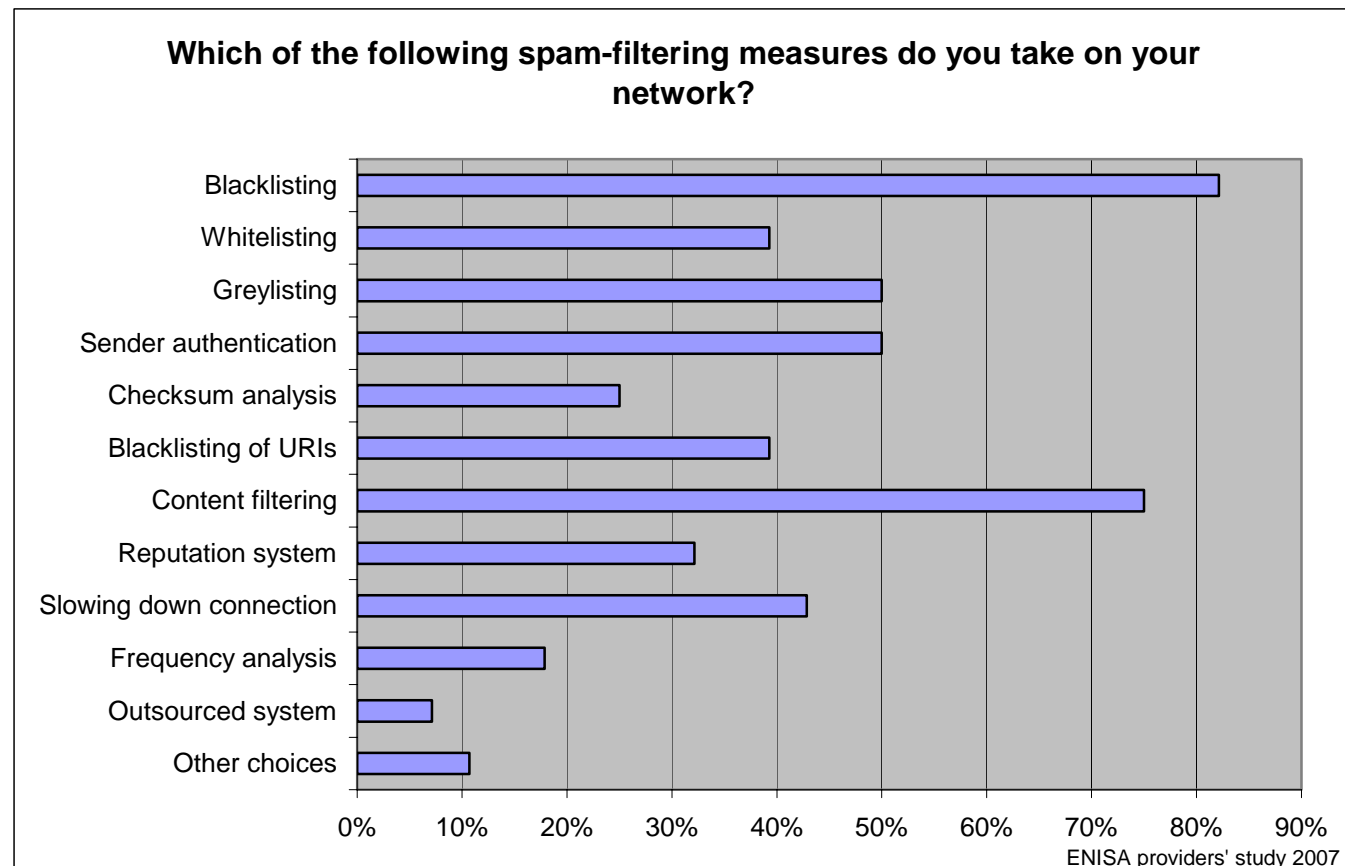


- Network
- Client



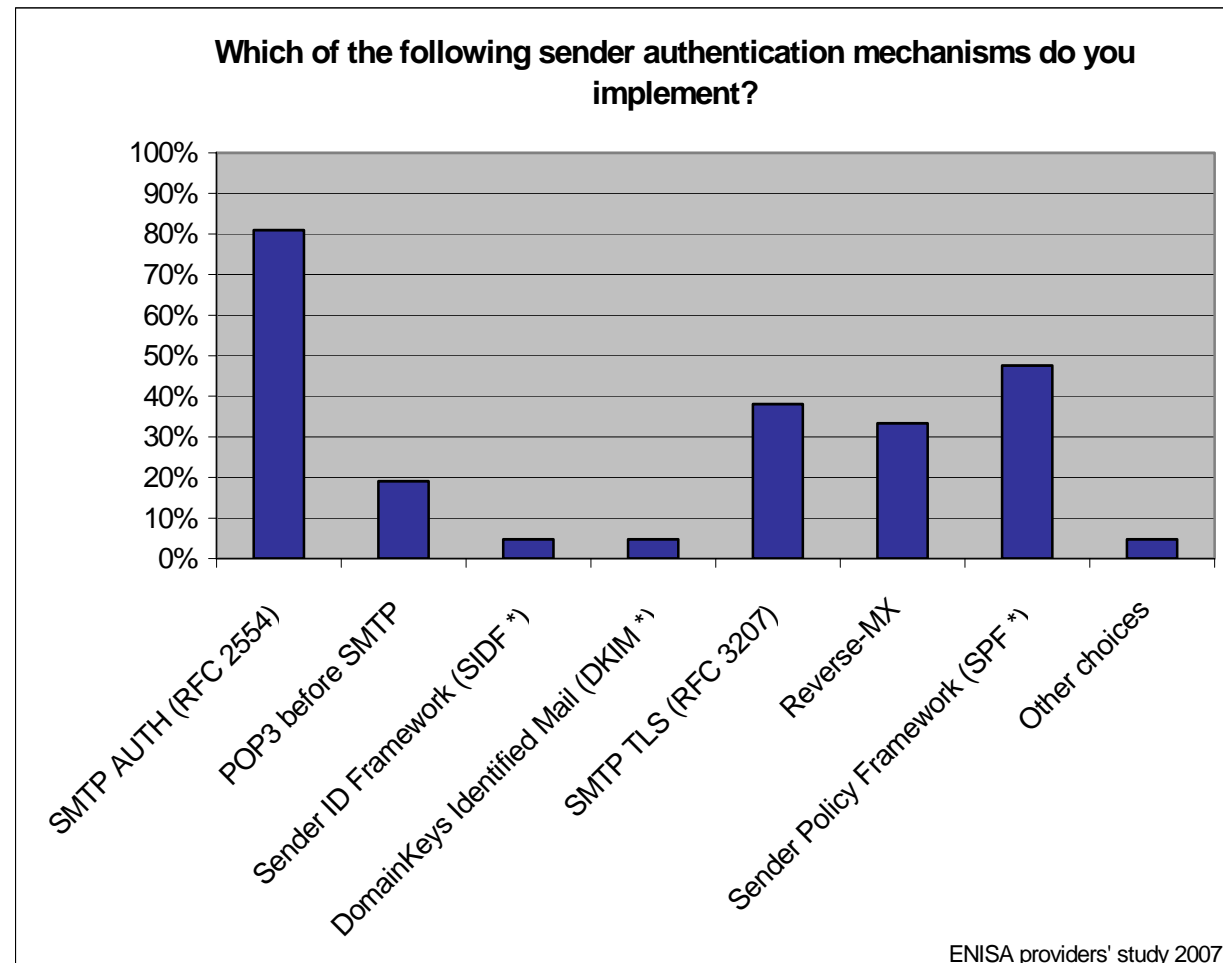
Spam filtering measures

- Blacklist
- Content
- 5 measures
- BL vs. WL
- Sender auth

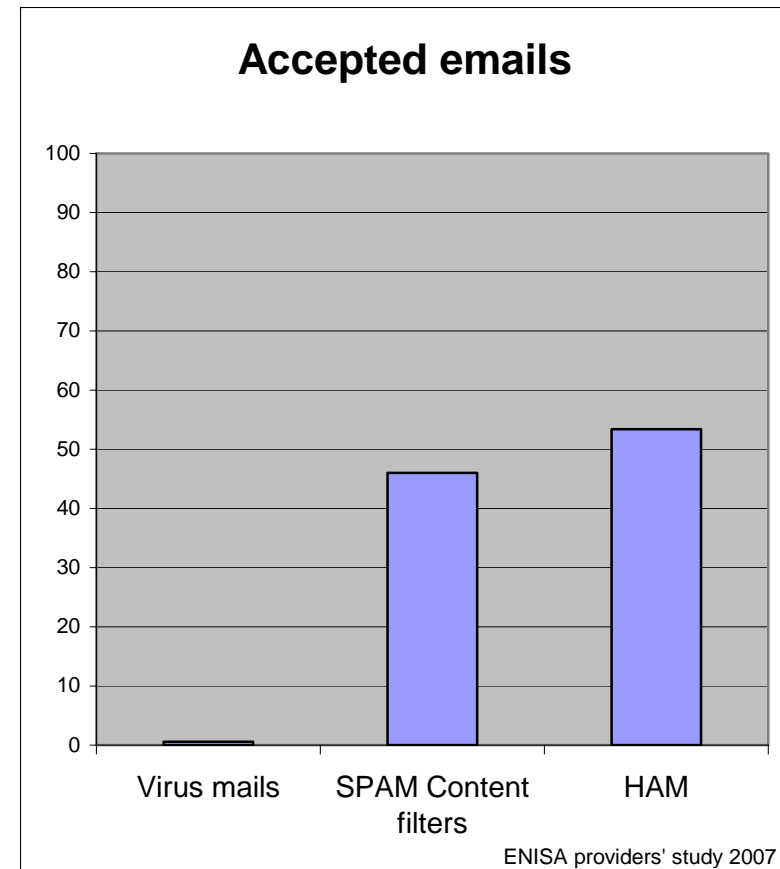
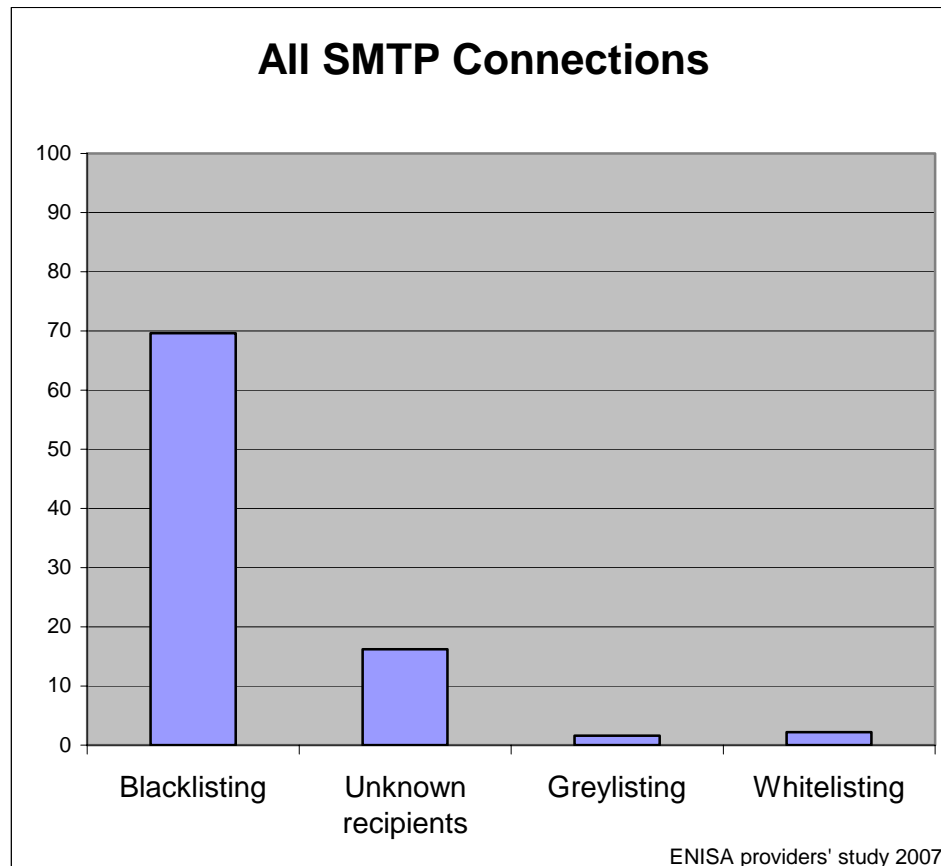


Sender authentication

- SMTP AUTH
- SMTP TLS
- SPF
- MTA auth
- DKIM

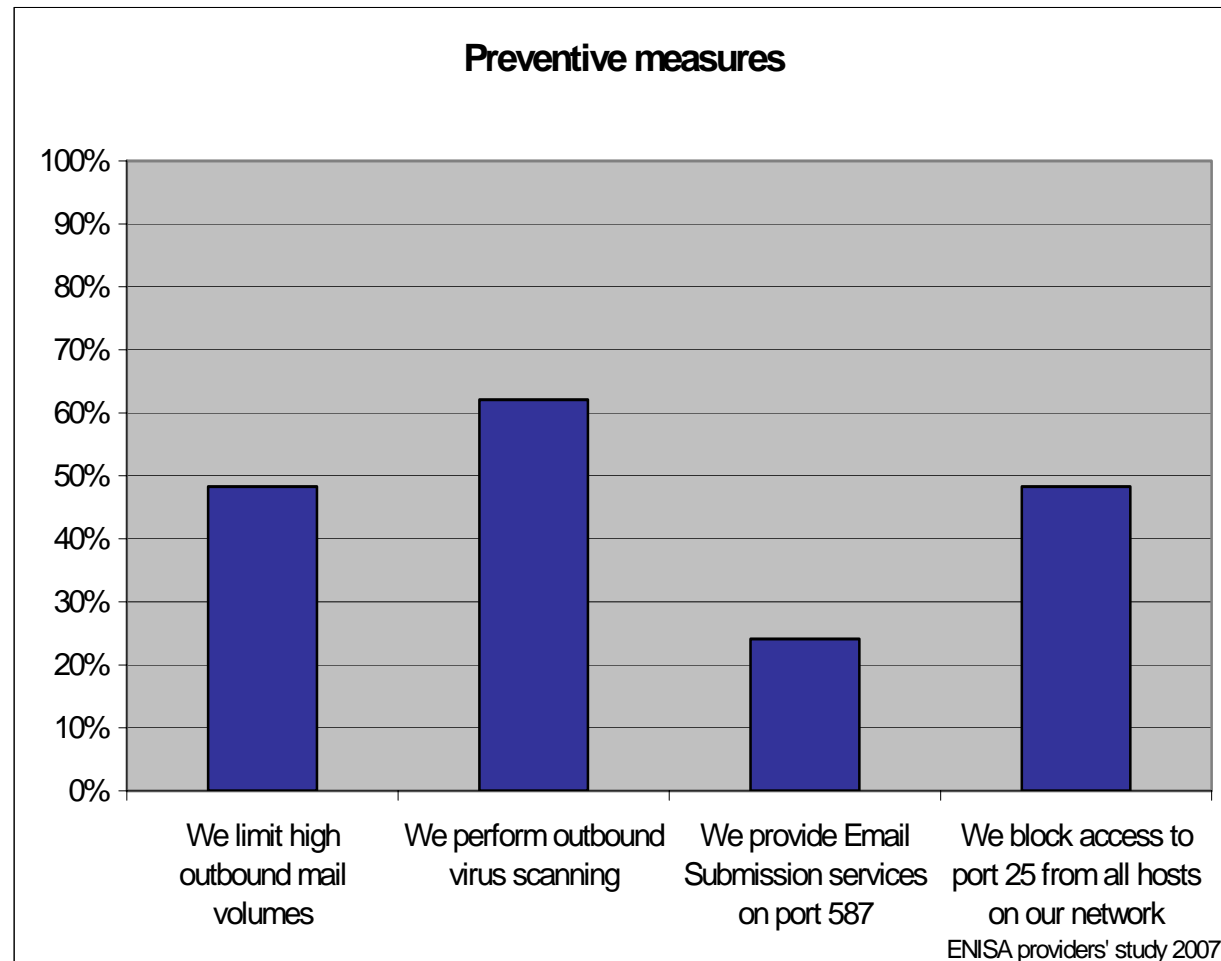


Effectiveness



Graph

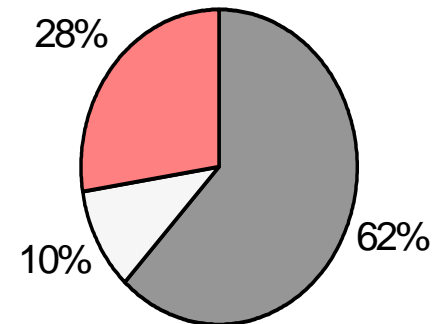
- Port 25
- Port 587
- EU spam
- Reputation



- Blacklist
- Whitelist
- Trend

Reactive measures

- We put a subscriber on a blacklist if the subscriber sent spam
- We put on a whitelist all subscribers who didn't send spam
- No technical measure



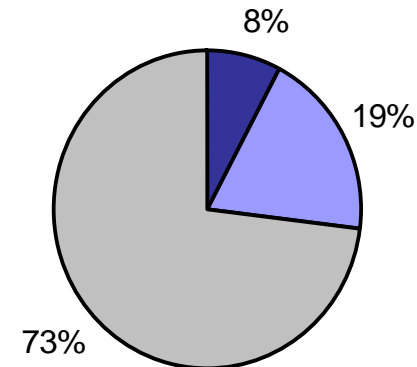
ENISA providers' study 2007

Abuse reports

- Manual
- ARF
- Mixing

Automated abuse-reports processing

- We use the ARF standard reporting format
- We use another reporting format or other automated
- We have no automated reporting format



ENISA providers' study

Legal aspects

- More than a third of providers see a conflict between their obligations and the use of spam filters
- A workshop will clarify the legal aspects of spam filtering and present new anti-spam methods
- Inbox-Outbox, London, November, 27th and 28th 2007

Summary

- Filtering
- Best practices
- Risk management
- Cooperation
- Awareness

- 2006 ENISA providers' study
 - http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_security_spam.pdf
 - http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_security_spam_part2.pdf
- ENISA <http://www.enisa.europa.eu/>
- Inbox-Outbox <http://www.inbox-outbox.com/index.htm>
- EuroISPA <http://www.euroispa.org/>
- eco <http://www.eco.de/>
- MAAWG <http://www.maawg.org/>
- IfIS <http://www.internet-sicherheit.de/>

Contact details

ENISA

(European Network and Information Security Agency)

Pascal Manzano

Expert - Information Security Policies

Technical Department

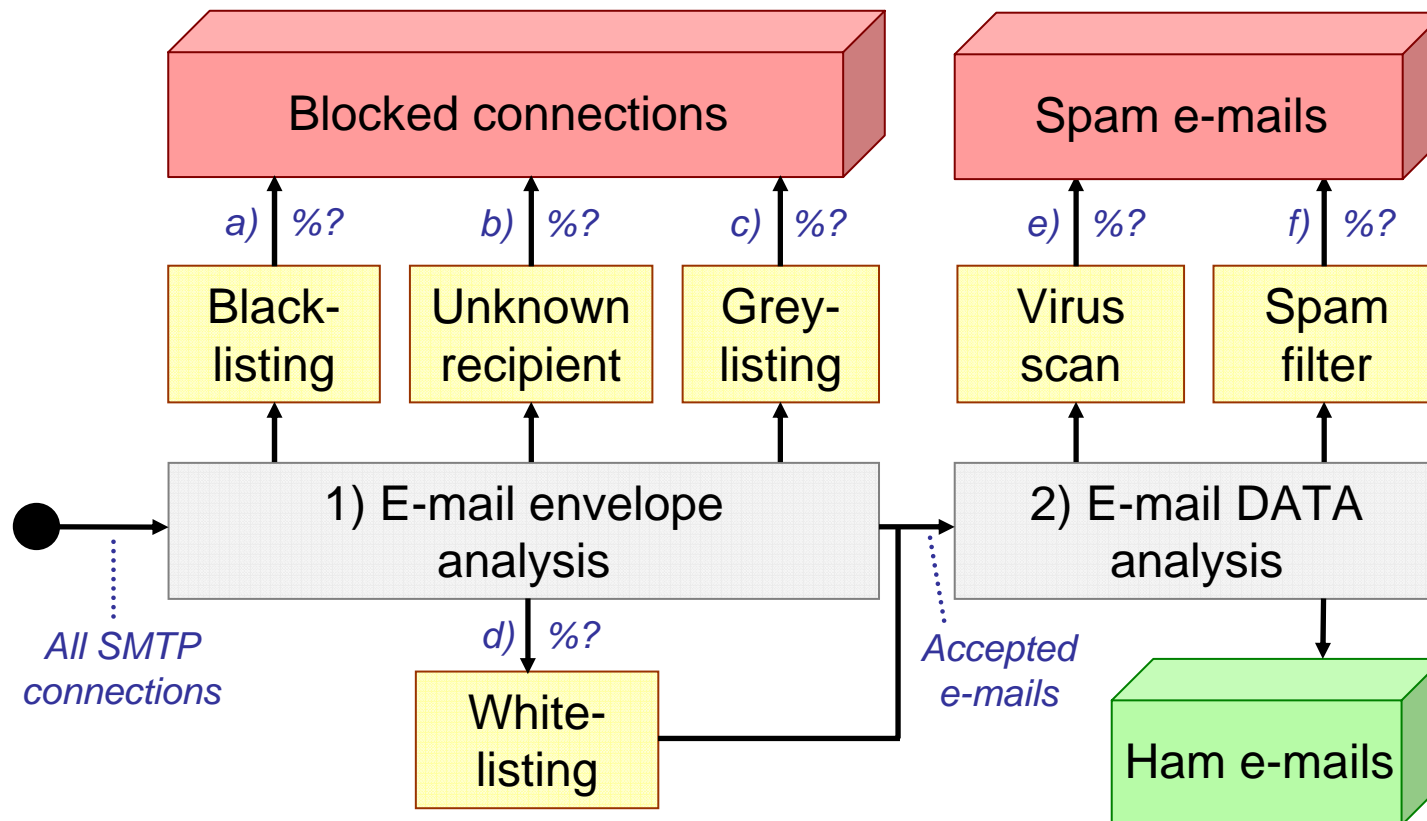
+30.2810.39.1366

pascal.manzano(-at-)enisa.europa.eu

Questions

?

Question 15



[Back](#)