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

Pascal Manzano

Internal presentation
20 February 2008, Heraklion

What's this?

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

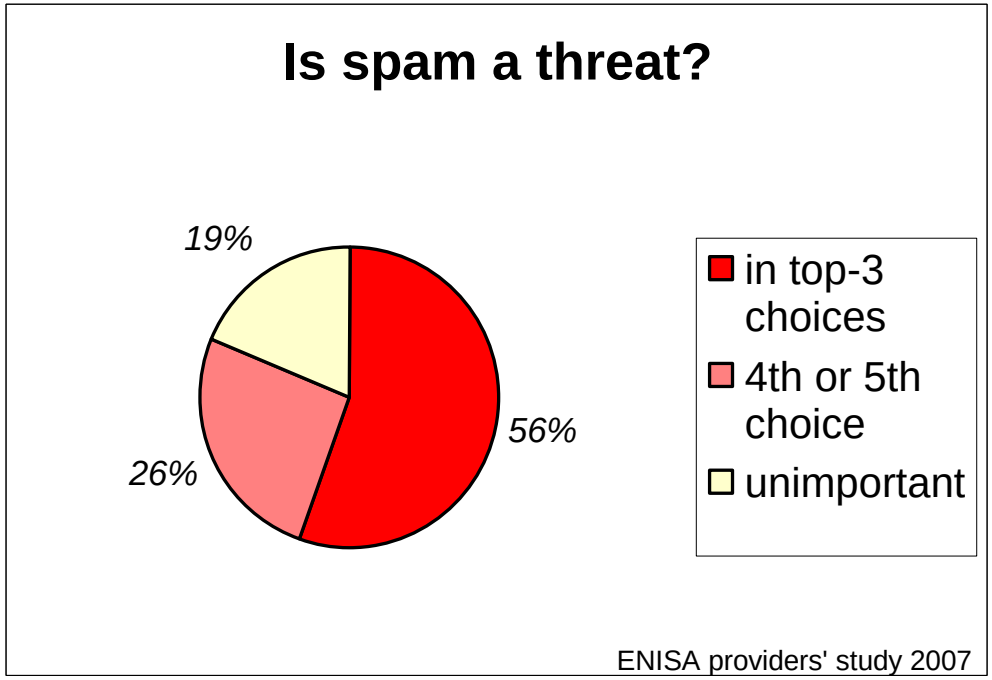
- Online questionnaire available in June and July
- 21 multiple choice questions
- Contacts with providers' associations at European and national level
- Promotion of the questionnaire in newsletters, mailing-lists, ENISA contacts' network.

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

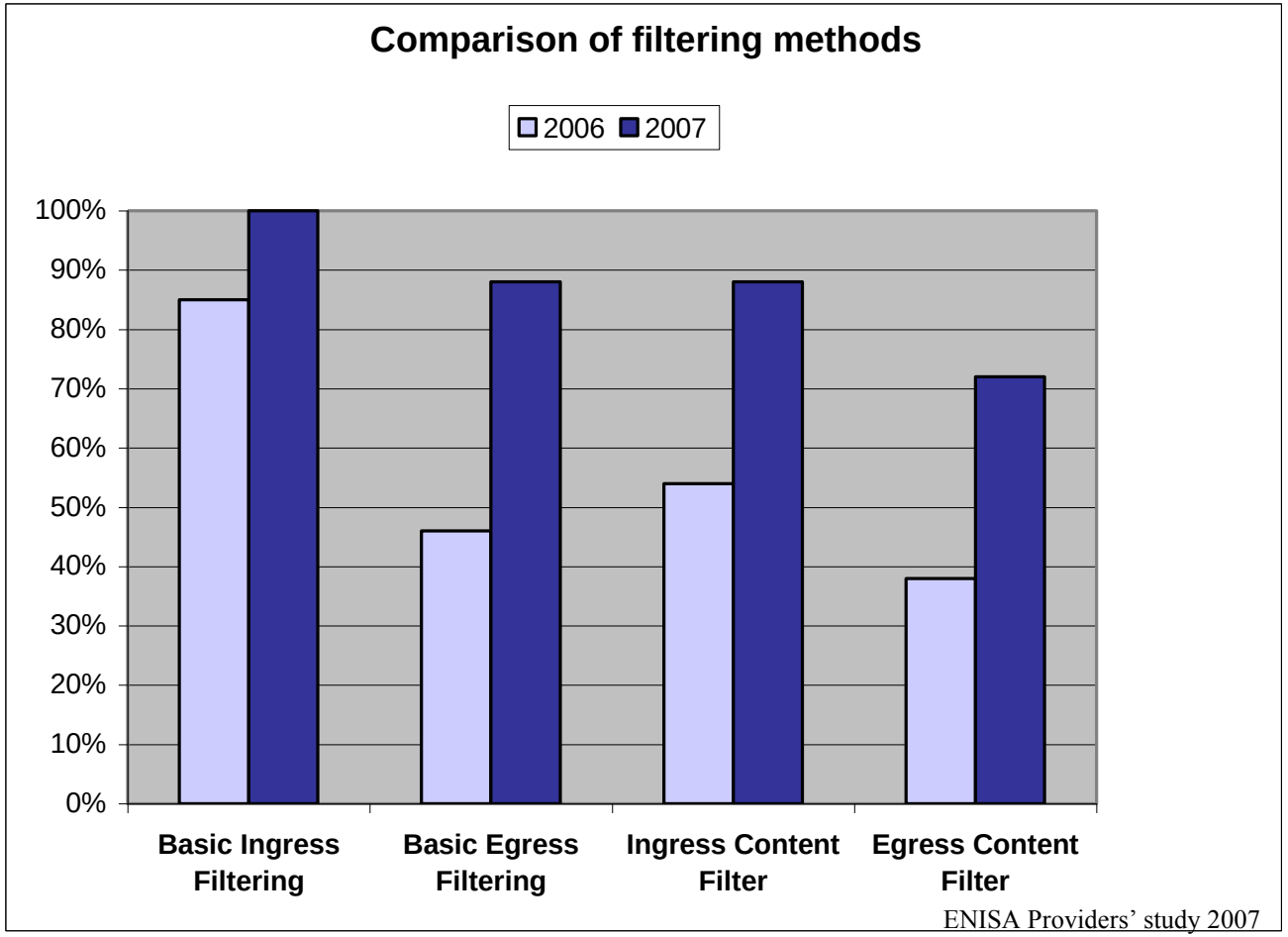
Threats

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



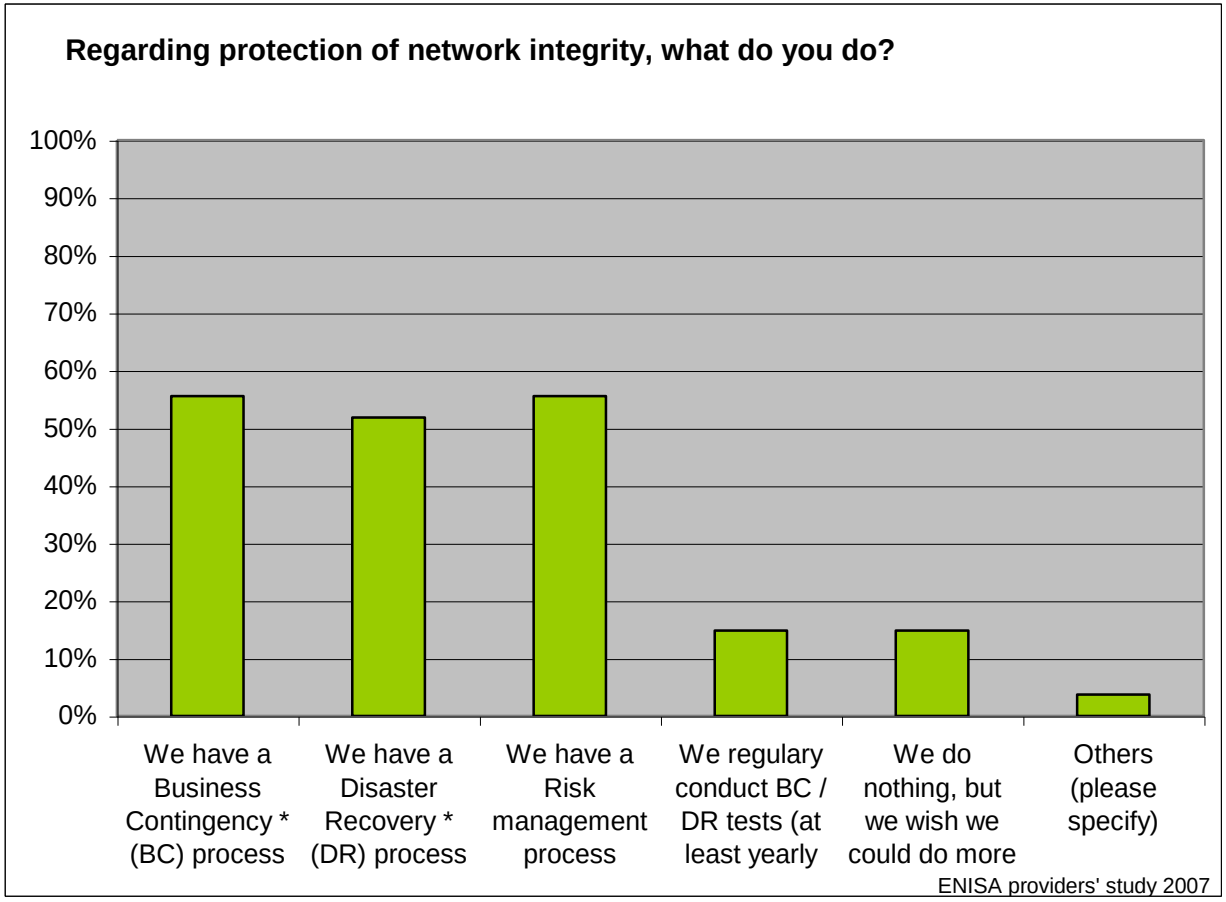
Filtering methods

- Ingress
- Egress
- Basic
- Content
- Trend



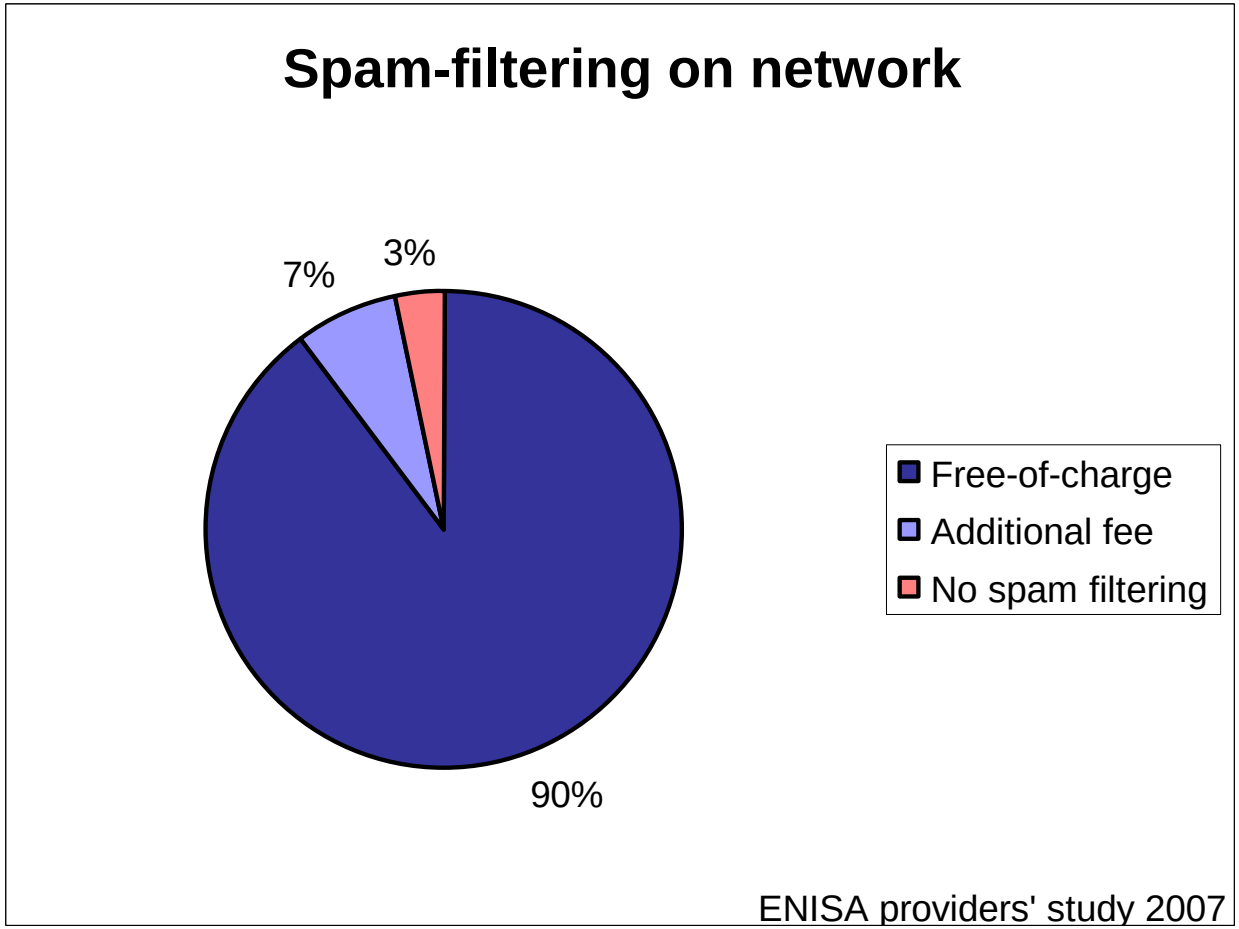
Network integrity

- BC
- DR
- RM
- Testing



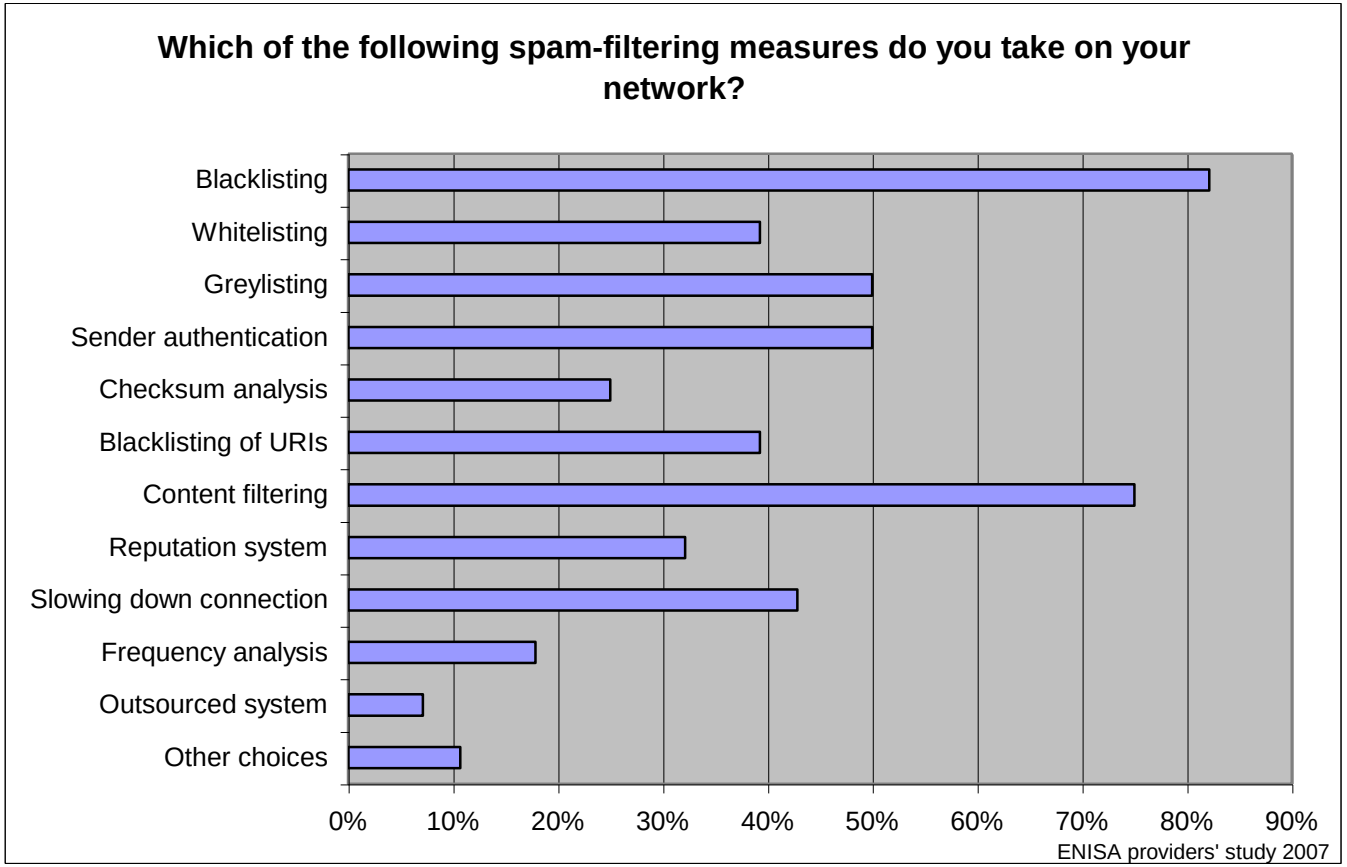
Preventing **receiving** spam

- Network
- Client



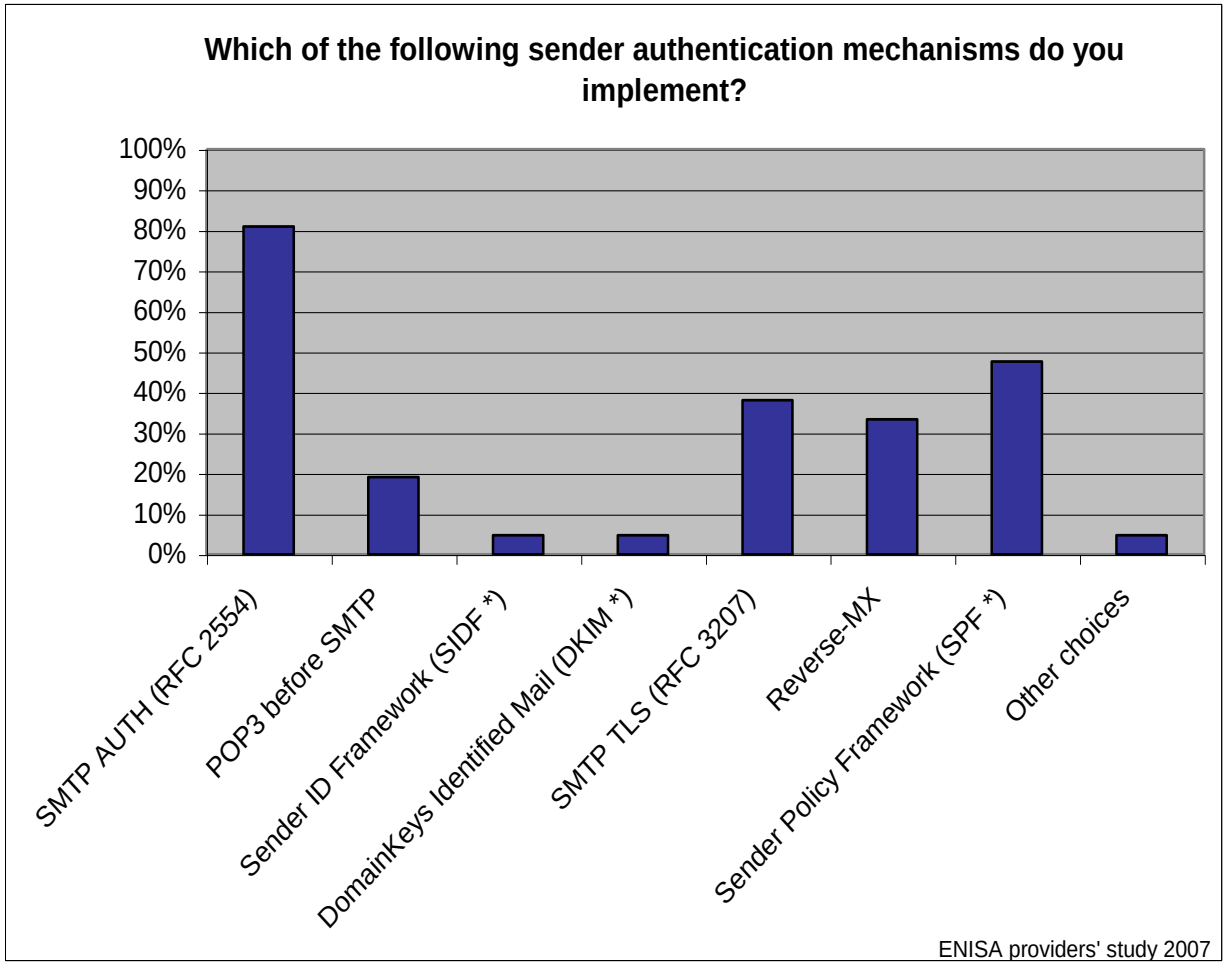
Spam filtering measures

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

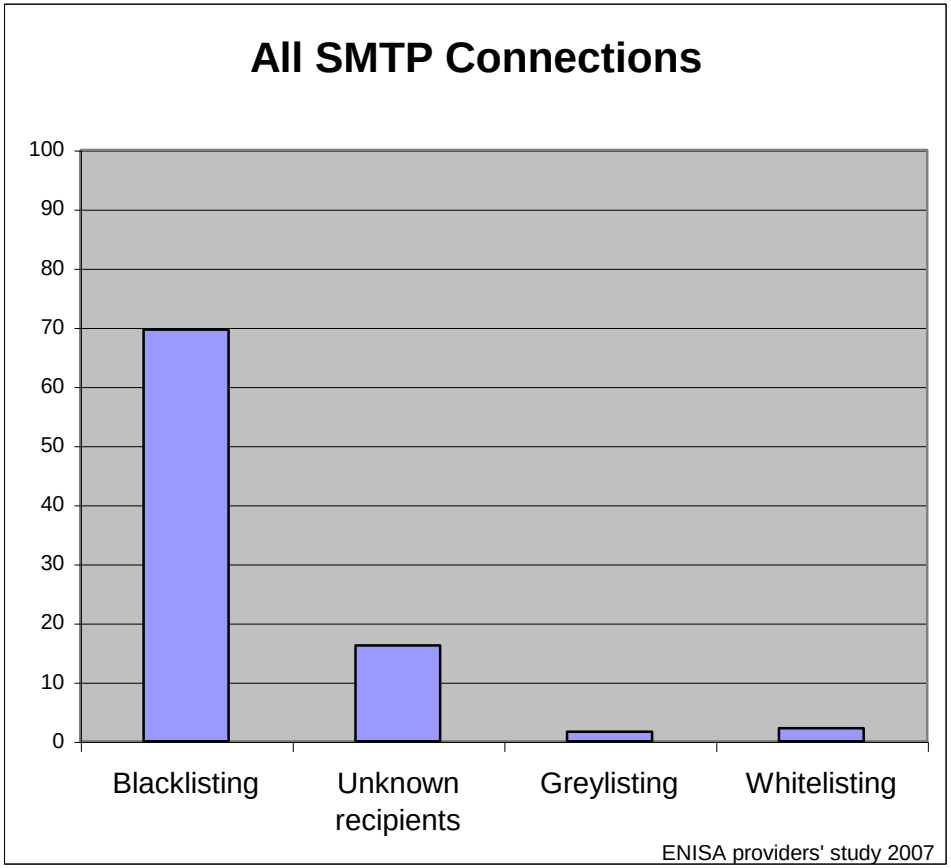


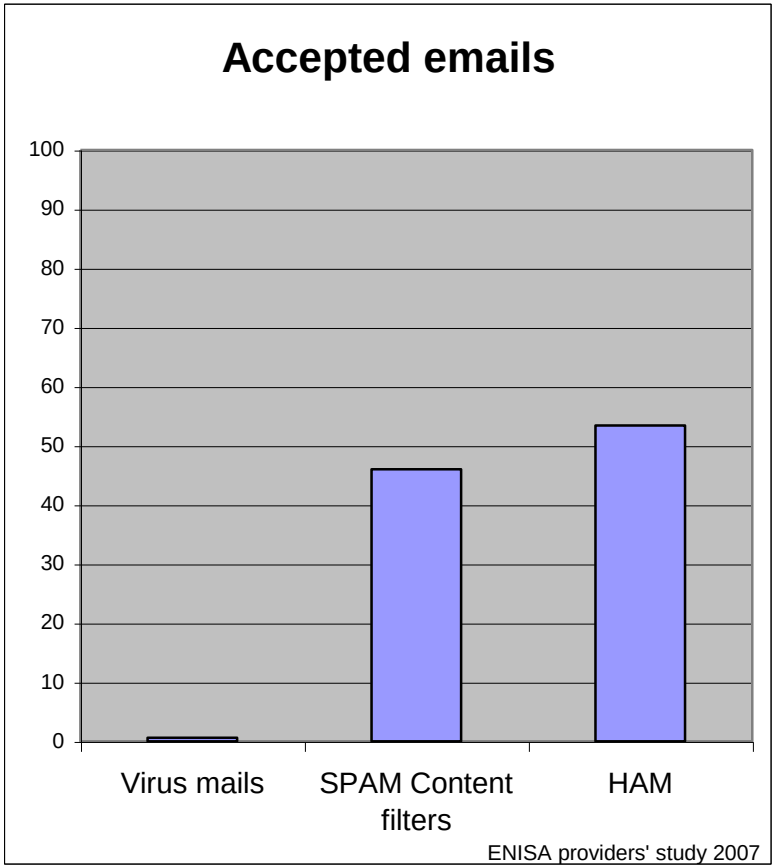
Sender authentication

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



Effectiveness

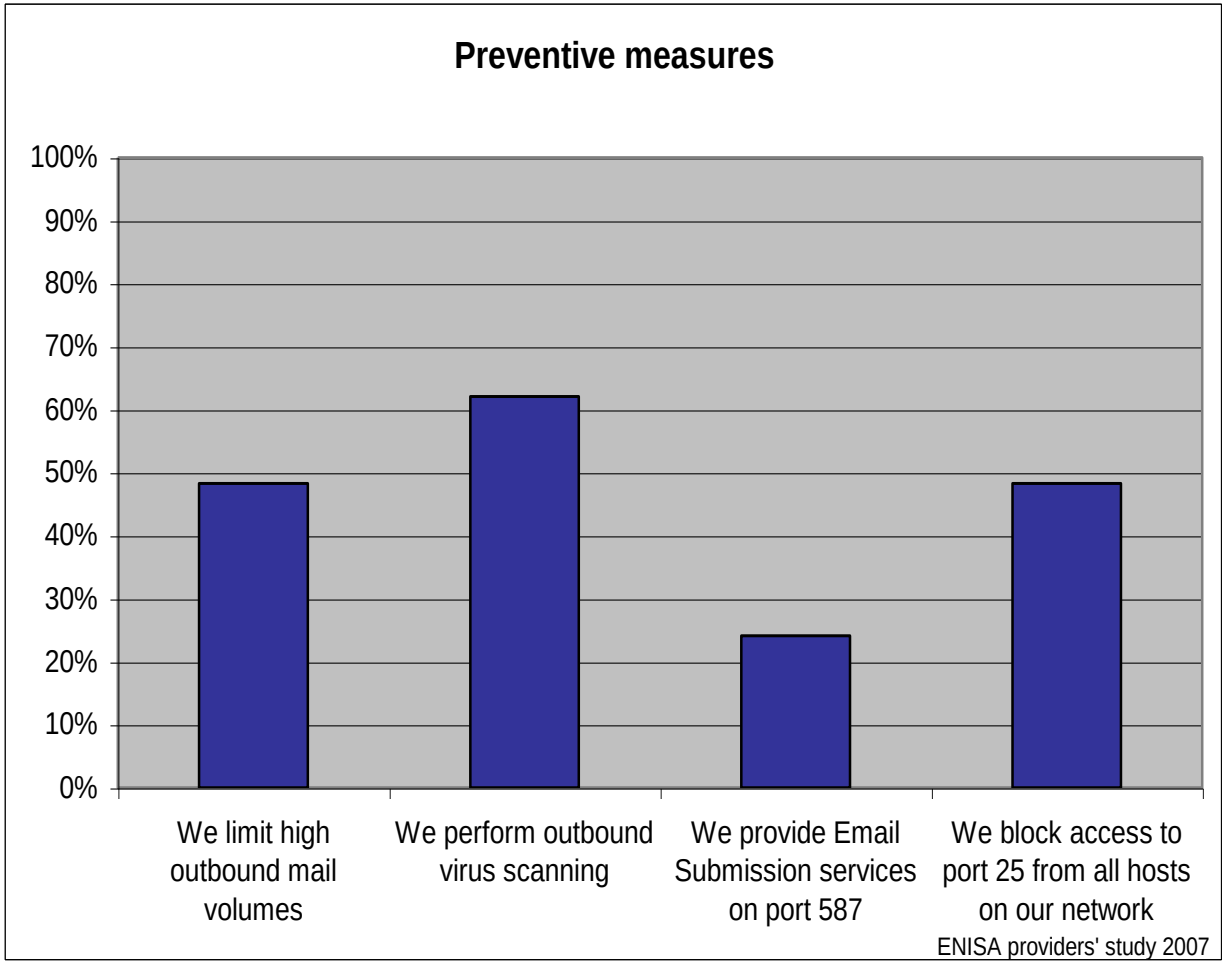




Graph

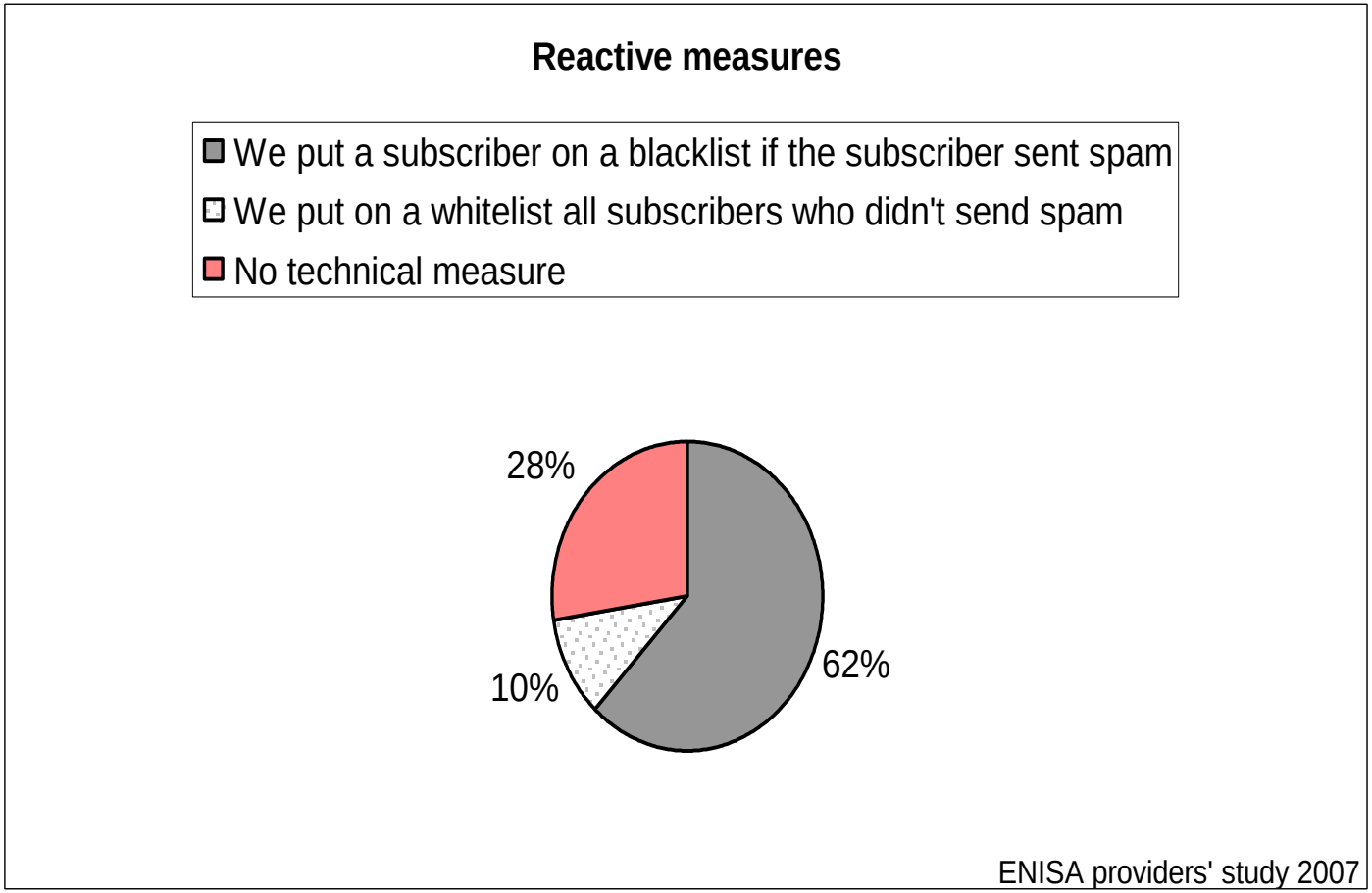
Preventing **sending** spam

- Port 25
- Port 587
- EU spam
- Reputation



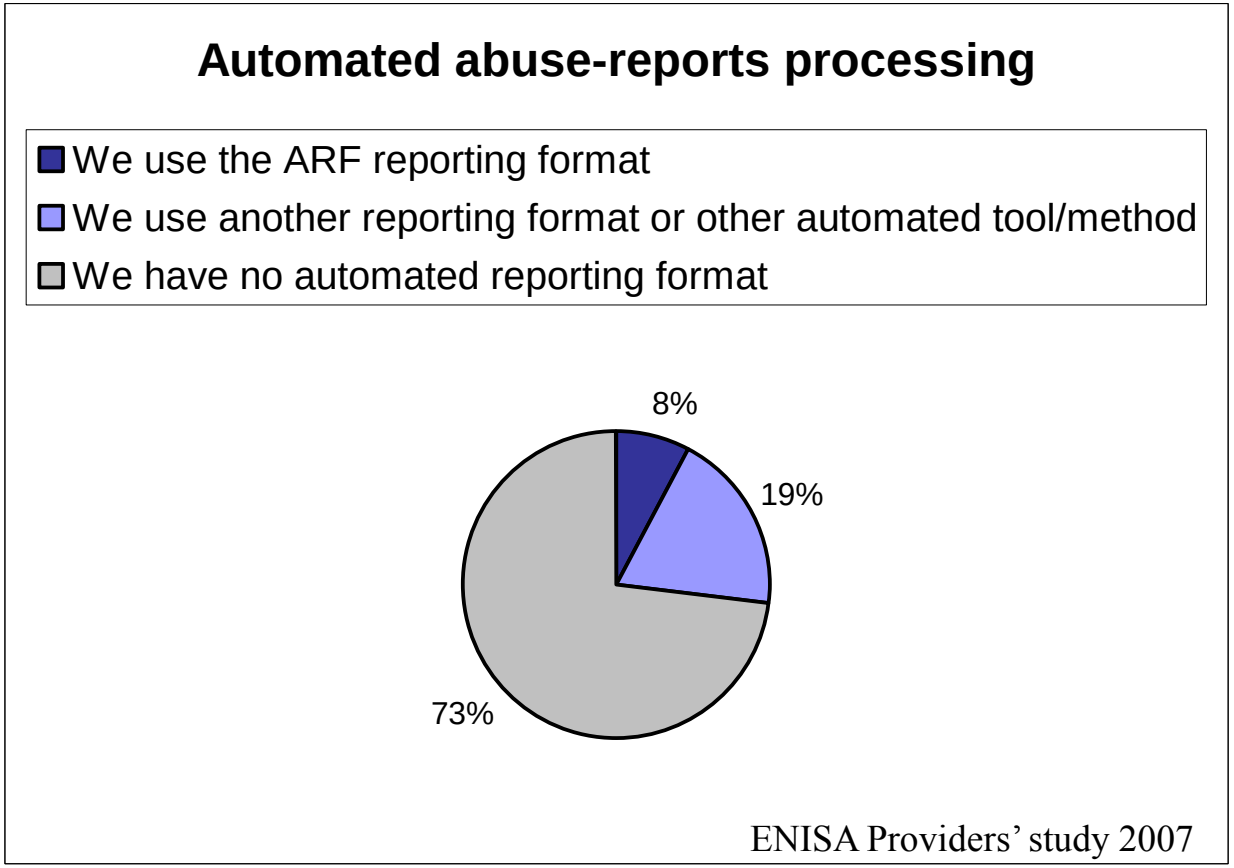
Preventing **sending** spam

- Blacklist
- Whitelist
- Trend



Abuse reports

- Manual
- ARF
- Mixing



Legal aspects

- More than a third of providers see a conflict between their obligations and the use of spam filters
- A workshop was organised end of November 2007 in London to help clarifying the legal aspects of spam filtering and present new anti-spam methods

Summary

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

Links

- ENISA anti-spam activities and 2007 study
  http://www.enisa.europa.eu/pages/spam/index.htm
- EuroISPA http://www.euroispa.org/
- eco http://www.eco.de/
- MAAWG http://www.maawg.org/
- ETIS http://www.etis.org/
- IfIS http://www.internet-sicherheit.de/
- Spotspam http://www.spotspam.net/