Provider Security Measures

Survey on Security and Anti-Spam Measures of Electronic Communication Service Providers

Deliverable 2.1.6 of ENISA’s Work Programme 2007
ENISA/TD/SP/07/0071

Pascal Manzano and Christian Rossow

European Network and Information Security Agency
Technical Department – Section Security Policies

September 2007
INDEX

1 EXECUTIVE SUMMARY 1

2 INTRODUCTION 2
  2.1 MOTIVATION 2
  2.2 THE STUDY 2
  2.3 METHODOLOGY 2
  2.4 OVERVIEW OF ANSWERS 3
  2.5 DOCUMENT ORGANISATION 3

3 SECURITY MEASURES 3
  3.1 ORGANISATIONAL ASPECTS 4
    3.1.1 Results from the survey 4
    3.1.2 Trend analysis 5
    3.1.3 Recent developments 5
    3.1.4 Comments 6
    3.1.5 Advice & proposals 6
  3.2 TECHNICAL ASPECTS 6
    3.2.1 Results from the survey 6
    3.2.2 Trend analysis 7
    3.2.3 Recent developments 7
    3.2.4 Comments 7
    3.2.5 Advice & Proposals 7

4 ANTI-SPAM MEASURES 8
  4.1 ORGANISATIONAL ASPECTS 8
    4.1.1 Results from the survey 8
    4.1.2 Trend analysis 9
    4.1.3 Recent developments 9
    4.1.4 Comments 9
    4.1.5 Advice & Proposals 10
  4.2 TECHNICAL ASPECTS 10
    4.2.1 Results from the survey 10
    4.2.2 Trend analysis 11
    4.2.3 Recent developments 12
    4.2.4 Comments 12
    4.2.5 Advice & Proposals 12

5 OUTLOOK 13

6 APPENDIX 14
  6.1 LIST OF RECOMMENDATIONS 14
    Advice & proposals to providers 14
    Advice & proposals to the European Commission 14
    Advice & proposals to the Member States 14
    Advice & proposals to other organisations 14
    Advice & proposals for ENISA 14
  6.2 QUESTIONNAIRE 15
  6.3 ADDITIONAL LINKS 24
1 Executive Summary

Providers of electronic communication services are a vital element of the security chain when users and enterprises connect to the Internet. This study, conducted by ENISA in June 2007, provides an overview of the measures service providers take to secure their services and to combat spam.

This is the second year that ENISA has conducted a survey in this field. It is based on 30 very detailed replies to a questionnaire circulated to providers in 19 different countries, mainly in Europe. The observations, facts, trends analysis and comments produced as a result of these replies are grouped under two main themes: Security measures and Anti-spam measures. These themes are then divided into organisational and technical aspects.

Security

Organisational aspects

Nowadays almost every provider publishes contact details to report security violations and e-mail abuse. Nearly half of the providers who responded provide training or awareness campaigns. Two-thirds of the providers have either a Business Contingency plan (BC) or a Disaster Recovery plan (DR). Implementation of these measures has increased since 2006. There are two interesting changes from last year’s study results as to how Internet Service Providers (ISPs) ensure an appropriate level of security. Firstly, there is a huge increase (from 38% to 65%) in the extent to which providers follow the guidance contained in national legislation. Secondly, there is a notable reduction in the extent to which they follow the guidance laid down in international standards, which has dropped from 46% to 35%. ENISA encourages providers to be involved in information-sharing by joining providers’ associations or working groups and by attending and presenting at security conferences so that they become better informed about new trends and best practices.

Technical aspects

Basic ingress filtering is applied by every provider. Basic egress filtering is now widely deployed, with nearly 90% of providers saying they deploy it. Egress filtering has nearly doubled since 2006, when it was only used by 46% of the providers. ENISA welcomes this behaviour, showing that providers are investing resources in the interest of the whole community. Last year, providers relied mainly on complaints from customers or other providers to detect anomalies. It was a reactive process. This year the decrease in tracking complaints and the increase in monitoring traffic peaks could be seen as a move from purely reactive behaviour to integrate more proactive initiatives.

Anti-spam

Organisational aspects

About 73% of all providers process abuse reports manually. Almost half of the providers contact an ISP directly when receiving spam from that network. Different laws, time zones and languages make communications complex for providers seeking to combat spam. ENISA supports the SpotSpam project that helps mitigate this problem by acting as an intermediary.

Technical aspects

On average, providers combine 5 different anti-spam methods. Although the best practice recommended by all providers’ associations is to manage port 25, only 50% of the providers do so. ENISA is convinced that applying best practices will significantly reduce the amount of spam both sent and received, and therefore encourages providers to implement e-mail management best practices.

---

1 The previous studies can be downloaded from: www.enisa.europa.eu/pages/spam/index.htm
2 Ingress filtering is applied to traffic coming from outside, whereas egress filtering is applied to traffic leaving the network.
3 The project SpotSpam: www.spotspam.net/
4 Many providers’ associations have agreed on such best practices; relevant links are provided within this study.
2 Introduction

2.1 Motivation
The use of the Internet for e-commerce is growing within Europe, demonstrating that, even if some fears remain, users seem to be becoming more confident. The Internet is also increasingly used to communicate with administrations. The availability of broadband access has doubled from 14% of households in the European Union (EU) in 2004 to 30% in 2006. Although spam is still common, considerable effort has been dedicated to limit its effect.

Internet Service Providers (ISPs) and E-mail Service Providers (ESPs) have a very important role to play in securing the Internet. They implement security measures to protect their infrastructures and the services they offer. These measures are the first levels of protection for their customers (end-users and businesses). Due to this crucial position, providers have been the main source of information for this survey.

This report provides information on existing security and anti-spam measures which have been implemented by providers, together with feedback on the implementation of best practices. Readers will obtain an overview of the actual security and anti-spam measures of providers’ network infrastructures.

2.2 The study
This study is referred to in ENISA’s 2007 Work Programme as “Yearly report on electronic communication security measures, detailing the measures implemented, trends and advice”. It follows the previous study conducted in 2006, which comprised two reports on the technical and organisational security measures adopted by providers to comply with legal requirements.

This report has been designed to bring concise and up-to-date information to the educated information security community. It is neither the definitive best practice guide on fighting spam, nor is it a general blueprint for future security legislation. It is merely a contribution to understanding the challenges that providers face, a catalogue of the solutions that leading providers apply – and that others may want to adopt – and an attempt to help readers (re-)gain trust in European electronic communications.

At the end of November 2007 ENISA is organising a workshop in London, inviting providers and other stakeholders to debate the effectiveness of current and future anti-spam measures and their compatibility with existing privacy regulations. More specifically, the workshop will address filtering methods, emerging anti-spam approaches, spamming trends and the privacy of users.

2.3 Methodology
ENISA used the same methodology in 2007 that it had already applied successfully in 2006, disseminating a multiple-choice questionnaire widely with an option to answer online. However, in 2007 ENISA complemented the questionnaire with more detailed and focused questions. This method enabled trend analysis, by comparing the current position with last year’s results. It also allowed new data to be collected.

ENISA created the questionnaire in April and transformed it into a web form in May. European Directive 2002/58/EC was used to create the questions, especially Article 4 (Security) and Article 13 (Unsolicited communications). Some providers’ best practices (MAAWG, OECD) were also taken into account, with the aim of obtaining feedback on their level of implementation.

The questionnaire was available online from the beginning of June to mid-July 2007. During July ENISA analysed the data that had been collected, and in some cases sought clarification from providers. The report will be made available first to the providers who replied to the questionnaire and later will be publicly available.

Most of the questions offered the option of selecting more than one answer; this is why, in some of the graphs, responses are above 100%.

---

5 The enterprises’ receipts from e-sales compared with total turnover were 2% in 2004 and 4% in 2006. For more details, see Eurostat figures at: http://epp.eurostat.ec.europa.eu/
7 The ENISA workshop on anti-spam measures will be held as a dedicated track within the Inbox-Outbox event. More details are available at: www.inbox-outbox.com/index.htm
8 See Appendix 6.1
9 MAAWG: www.maawg.org/port125/MAAWG_Port125Rec0511.pdf
2.4 Overview of answers
30 very detailed answers to the questionnaire were received, mainly from Internet Service Providers (ISPs) (half of which also provide telecommunications services), but also from E-mail Service Providers (ESPs). For the sake of simplicity, they are all called providers in this document.

The range of participants included providers of all sizes, from small to very large (3 providers are in the top 10 of European providers).

Coverage in terms of countries was also wide, with participation from providers in 16 EU countries as well as in Norway, Iceland and the US.

2.5 Document organisation
This document is organised in two major parts: security measures and anti-spam measures. For each of these main parts, the report provides “results” from the survey, “trend analysis”, “recent developments”, “comments” and “advice & proposals”.

The “results from the survey” sections give detailed information about the data collected from the questionnaire.

The “trend analysis” sections compare 2006 and 2007 data.

The “recent developments” sections are summaries of external data sources in the field which have been covered by the study. Rather than listing all available data, these sections focus on recent trends and interesting points. The information is provided as-is, with short references to the sources. A list of references including web links is attached as Appendix 6.3.

The “comments” sections are lists of comments on the facts presented in the previous sections.

The “advice & proposals” sections provide suggestions for possible actions, discussions and solutions for ISPs, Members States, the European Commission and ENISA.

Finally the “outlook” chapter provides an overview of future action to be taken by ENISA in the area of European ISPs’ security and anti-spam measures.

3 Security Measures
Providers have to secure their infrastructures, not only because this is often a mandatory requirement, but also because providing infrastructure is their core business. This part of the study provides information about the security measures that providers implement to protect their assets for the benefit of their customers.

To gain a better understanding of the risks that providers are facing, ENISA asked them to rank security threats from “most concerning” to “least concerning”. The survey demonstrates that the threat of viruses is ranked highest, followed by spam and Distributed Denial of Service (DDoS) attacks. In addition, nearly 60% of the providers selected spam as one of the three most concerning threats, as the following charts show.

For the organisational aspects, the study covered the measures providers have taken to protect their services and to inform their customers. It shows that “risk management” is implemented at a level comparable with other industry sectors. This represents an improvement on last year’s results.

Providing information to or raising the awareness of their customers are now more widely used as security measures by providers than in 2006. The number of organisations which report security breaches or risks to their customers is increasing. In Europe there is currently no regulation requiring breaches to be publicly reported when private data is involved, although ENISA encourages the reporting of all security breaches.

3.1 Organisational aspects
This chapter describes measures that providers take to secure their services, including, for example, a risk management process, awareness-raising activities and information dissemination.

3.1.1 Results from the survey
Organisational measures taken to secure communication services
- Almost every ISP provides contact details for e-mail abuse and for security violations.
- Written guidance is available for staff (80%), and 60% of ISPs replied that they also provide guidance for their subscribers. Half of the ISPs said that they have a policy which defines the permitted and prohibited uses of messaging services.
- Spamming is forbidden in most of the Terms and Conditions used by ISPs, and nearly half of the providers also inform their subscribers about the legal consequences of sending spam.
- Nearly half of the providers offer training or awareness campaigns.
- Nearly two-thirds of the ISPs provide information on security via their website or via e-mail.
- More than 80% of the ISPs keep their reverse Domain Name System (DNS) records up-to-date.

How do you ensure an appropriate level of security?
Providers were asked to choose only the three most appropriate options.

- “Following guidance from national legislation” is popular with 66% of providers which selected it as one of the three most appropriate options.
- “Following industry best practice” is also highly ranked with 58%.
- The use of security policy to ensure the appropriate security level was chosen by 40% of respondents.
- The “Following international standards” option received 35% of the votes.

When a particular risk of a security breach arises in your network, what do you do?

- More than two-thirds of the ISPs inform their subscribers directly e.g. via e-mail.
- Nearly half of them decide on a case-by-case basis how to inform their subscribers.
- Only 12% of all ISPs inform the public and only 8% inform their respective National Regulatory Authority.
- When there is a risk of a security breach, all providers inform their subscribers either directly or via their customer portal.

If the risk lies outside of the scope of measures you can take directly, what do you do?
- Almost all ISPs inform their subscribers of any remedies that they can take. Some providers also inform their customers about the associated costs of the remedies.
- More than half of them also inform their subscribers of the risk of not implementing countermeasures.
- More than one third of the providers stop servicing non-compliant subscribers.
Processes in place to protect network integrity

Regarding protection of network integrity, what do you do?

<table>
<thead>
<tr>
<th>Option</th>
<th>2006</th>
<th>2007</th>
</tr>
</thead>
<tbody>
<tr>
<td>We have a Business Contingency (BC) process</td>
<td>0%</td>
<td>10%</td>
</tr>
<tr>
<td>We have a Disaster Recovery (DR) process</td>
<td>0%</td>
<td>5%</td>
</tr>
<tr>
<td>We have a Risk management process</td>
<td>10%</td>
<td>10%</td>
</tr>
<tr>
<td>We regularly conduct BC/DR tests (at least yearly)</td>
<td>40%</td>
<td>60%</td>
</tr>
<tr>
<td>We do nothing, but we wish we could do more</td>
<td>50%</td>
<td>30%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

ENISA providers’ study 2007

- Slightly more than a third of the providers have both a Business Contingency plan (BC) and a Disaster Recovery plan (DR).
- Two-thirds of the providers have either a BC or a DR in place.
- However, 10% of the providers replied that they have no risk management process in place.
- Only 15% of ISPs undertake annual testing of their business continuity plans. A more careful examination of the data shows that 25% of ISPs which have implemented a BC or a DR test them at least once a year.

3.1.2 Trend analysis

The trend analysis provides a comparison between the data collected in 2006 and 2007.
- From an organisational point of view, some measures are implemented at a comparable level: publishing information on the web, providing security software for a fee, providing contact details for e-mail abuse. However, as the next graph shows, other measures are now much more widely implemented: providing training and awareness campaigns (a 200% increase), detailed guidance to subscribers (a 50% increase), providing free security software and contact details for security violations (a 33% increase).

Which of the following organisational measures do you take to secure your services?

<table>
<thead>
<tr>
<th>Measure</th>
<th>2006</th>
<th>2007</th>
</tr>
</thead>
<tbody>
<tr>
<td>We provide training or awareness campaigns</td>
<td>0%</td>
<td>15%</td>
</tr>
<tr>
<td>We provide written guidance for subscribers</td>
<td>0%</td>
<td>15%</td>
</tr>
<tr>
<td>We provide security software free of charge</td>
<td>0%</td>
<td>40%</td>
</tr>
<tr>
<td>We clear contact details for security violations</td>
<td>0%</td>
<td>40%</td>
</tr>
</tbody>
</table>

ENISA providers’ study 2007

- Regarding the methods that ISPs adopt to ensure an appropriate level of security, there are two interesting changes since last year. Firstly, there is a huge rise (from 38% to 65%) in the number following guidance contained in national legislation. Secondly, there is a notable reduction in the number following guidance contained in international standards, which has dropped from 46% to 35%.
- When a risk of a security breach arises in their network, more than two-thirds of ISPs inform their subscribers directly. This percentage has nearly doubled since last year, when only 38% of providers did so. The use of a customer portal for information also rocketed from 8% to 35%. Although last year no ISP replied that they reported to a National Regulatory Authority (NRA), this year ISPs from Greece and Finland confirmed that they do so.
- Almost all customers are now informed by their providers about the remedies they can take and even sometimes about the associated costs. There has been an increase from 54% to 87% in the notification of customers (see the graph below).

If the risk lies outside the scope of the measures you can take directly, then what do you do?

<table>
<thead>
<tr>
<th>Option</th>
<th>2006</th>
<th>2007</th>
</tr>
</thead>
<tbody>
<tr>
<td>We inform subscribers of any possible remedies they can take</td>
<td>0%</td>
<td>5%</td>
</tr>
<tr>
<td>We inform subscribers of any possible remedies they can take and the associated costs</td>
<td>0%</td>
<td>5%</td>
</tr>
<tr>
<td>We inform subscribers of the risk of not implementing countermeasures</td>
<td>0%</td>
<td>5%</td>
</tr>
<tr>
<td>We stop servicing non-compliant subscribers</td>
<td>0%</td>
<td>5%</td>
</tr>
</tbody>
</table>

ENISA providers’ study 2007

- Two other evolutions highlighted by the graph above are the huge increase in the notification of the risk of not implementing countermeasures (from 15% to 52%) and the number of ISPs which stop servicing non-compliant subscribers (from 8% to 39%).
- Compared with last year, the number of providers implementing a Disaster Recovery plan remains constant, at slightly above 50%. The number of providers with a Business Contingency plan in place increased from 46% to 56%. Annual testing of these plans is now undertaken by 25% of the providers; last year this figure was 0%. Having a risk management process in place is more common in 2007 (56%) than in 2006 (23%).

3.1.3 Recent developments

- Since California’s State Bill 1386, which made reporting of security breaches mandatory in 2003, many other US states have passed a similar law. As a result, there is more publicly available information about attempts to breach data privacy.

---

12 For more details about the ISO 27000 series, search for JTC1/SC27 at: [www.iso.org](http://www.iso.org)
• Providing information about security breaches to the public is not required by law in the EU. In the US this data helps raise awareness.13.

• Action taken at least at a national level has a greater impact on security and a lower impact on customer lost figures than action taken by a smaller group of providers. For instance, quarantining measures are mandatory in Finland and are applied by all providers. The effect of adopting measures nationwide means that providers do not lose customers for implementing security measures, as other providers have to do the same.

3.1.4 Comments
• The level of maintenance of reverse DNS is quite high.
• Partners (unlike staff and subscribers) only rarely receive written guidance from providers.
• Training and awareness campaigns are used by 43% of the providers. This represents important progress since last year and is welcomed by ENISA. Awareness helps prevent system compromise and is cost-efficient compared with handling support calls after the event.
• Large and small providers behave differently as far as methods of ensuring an appropriate level of security is concerned. While larger providers follow international standards, applying industry best practice and defining a Risk Management process, smaller providers prefer using Service Level Agreements (SLAs), following guidance contained in national legislation and taking into account the advice of the national computer security organisation of their country.
• The decrease in following international standards guidance is significant. This might be for a number of reasons including:
  • The increase in following national legislation guidance.
  • The high costs (time, resources, financial) needed to implement them.
  • The return on investment (ROI) of implementing standards is difficult to assess.
  • Resilience has emerged as a key issue and international standards do not address it yet.
  • As new standards in the ISO 27000 series are expected soon (27004 and 2700514) or have recently been released (27006), it could be that ISPs are waiting for more feedback before starting to implement them.
• It is interesting to note that, even if the general public is not particularly aware of the risks of security breaches encountered by ISPs, at least their own subscribers are informed.
• Stopping servicing non-compliant customers, a policy adopted by more than 30% of ISPs, is a starting point in the effort to limit botnets and improve the overall security of the Internet, especially if used in collaboration with quarantine systems which allow security updates. As a useful side-effect it also increases the awareness of end-users, thus benefiting the whole community.
• Risk management processes are still not widely used. One out of ten providers report having no risk management process in place at all and one third have no business continuity plan. Although these figures are also common in other industry sectors, providers would have been expected to have a higher level of implementation due to the nature of their critical business. Testing existing continuity plans is progressing, but percentages are still at a far from satisfactory level.

3.1.5 Advice & proposals
• Providers should be members of an association in order to increase their opportunities to share information and feedback, to acquire a common understanding and to develop and implement best practices.
• Standardisation bodies should make standards easier to implement and test.
• Providers should quarantine computers in their networks unless they are well protected (i.e. they have applied operating system patches and have recent anti-virus signatures).
• Providers should invest more resources in risk management and the testing of business continuity plans.
• The European Commission should make the reporting of security and privacy breaches mandatory.

3.2 Technical aspects
This chapter describes measures that providers take to secure their services, e.g. with filtering and traffic analysis.

3.2.1 Results from the survey
Technical measures to secure services

Comparison of filtering methods

- Basic Ingress Filtering
- Basic Egress Filtering
- Ingress Content Filter
- Egress Content Filter

ENISA providers’ study 2007

- All providers secure their services with basic ingress filters.
- In addition, 88% of all providers apply ingress content filters.
- Furthermore, nine out of ten providers have basic egress filtering and more than 70% of all providers implement egress content filters.
- 44% of all providers quarantine infected computers. The same proportion of providers use blackholing and sinkholing to secure their services.
- Not a single provider who replied to the survey has implemented DNSSEC.
- Four out of ten providers use traffic shaping as a security method.

13 See for example: Attrition data loss archive http://attrition.org/dataloss/
14 ISO 27004 Information security management measurements and ISO 27005 Information security risk management are under development.
15 Ingress filtering is applied to traffic coming from outside, whereas egress filtering is applied to traffic leaving the network.
3.2.2 Trend analysis

- Basic ingress filtering is now used by every provider. As of last year, 85% of all providers were implementing it.
- Other filtering methods, especially egress filtering, are much more widely used now than in 2006, according to a comparison with last year’s report. Usage almost doubled, from 46% to 92% for basic egress filtering and from 38% to 72% for egress content filters.
- Traffic shaping and the quarantining of infected computers remained at a similar level as in 2006.
- As in 2006, none of the providers reported that they had implemented DNSSEC.
- There has been a slight decrease in tracking complaints. In 2006 about 85% of all providers had implemented a tracking system; the figure now is 73%.
- On the other hand, there is an increasing trend in monitoring traffic peaks. The percentage of providers monitoring traffic rose from 62% to 73%.

3.2.3 Recent developments

- In its recent Opinion17 published in June 2007, the Article 29 Data Protection Working Party described and clarified the concept of personal data. The Opinion also contains advice for the application and interpretation of data protection rules in electronic communications.
- The IAB Unwanted traffic workshop18 reported that user complaints reveal only a small part (about 10% for DDoS attacks) of the problem of unwanted traffic.
- During the 5th eco anti-spam summit19, Richard Cox from Spamhaus20 asked registrars to prevent the usage of Fast Flux network (e.g. by limiting domain kiting21).

3.2.4 Comments

- The high increase in egress filtering (both basic and content methods) is very beneficial for the Internet community. Providers’ customers do not benefit directly from applying egress filtering. However, by doing so, providers are helping other providers’ operational teams. This is a very interesting development, demonstrating that providers are investing in the interest of the Internet community as a whole.
- Last year, providers relied mainly on complaints from customers or other providers to detect anomalies. It was a reactive process. This year the decrease in tracking complaints and the increase in monitoring traffic peaks could be seen as a move from purely reactive behaviour to the integration of more proactive initiatives.
- Monitoring traffic peaks and traffic anomaly detection are useful processes to identify security or spam problems at an earlier stage. They are costly solutions both from a software point of view and also because they require highly qualified personnel to implement and tune them. On the other hand, investing in such processes could decrease the costs of support call management when incidents occur. In addition, it could also enhance customers’ general feelings about the service.
- DNS is a very critical function for the majority of Internet activity. DNSSEC was created to improve the security of the existing DNS protocol. However, DNSSEC is not widely deployed. The reason for this lack of adoption should be analysed further.

3.2.5 Advice & Proposals

- ENISA should examine specifically the status of DNSSEC22. It is deployed in Sweden; Russia, Bulgaria and Brazil have signed their top-level domain TLD zones23. The survey uncovered no other implementations elsewhere.
- Providers can enhance their network security by monitoring traffic peaks and implementing traffic anomaly detection.

---

16 Wikipedia definition: Spamtraps are usually e-mail addresses that are created not for common communication, but rather to lure spam. More details at: http://en.wikipedia.org/wiki/Spamtrap
18 For more details about the workshop, see RFC 4948 at: www.ietf.org/rfc/rfc4948.txt
19 The 5th eco anti-spam summit: www.eco.de/5.dask
20 Spambase tracks Internet spammers: www.spamhaus.org/
22 For more details on DNSSEC, see RFCs 4033, 4034 and 4035, available at: www.ietf.org/
23 More information is available at: www.dnssec.net/
4 Anti-Spam Measures

During recent years, the amount of spam (measured both in quantity and bandwidth) has grown. Recent studies report that more than 90% of all e-mail traffic is considered spam. The amount of spam sent from EU countries is also increasing. At the same time, less spam reaches users' mailboxes, showing that providers have invested considerably in protecting the community from spammers in their own networks. However, it is always a competition between spammer and anti-spam filtering measures to find new methods to spread or block spam e-mail. In this chapter, ENISA describes the current methods and techniques used by providers to fight spam.

4.1 Organisational aspects

This chapter describes organisational measures that providers take to reduce spam, including their behaviour after identifying spam, and their techniques for handling abuse reports.

4.1.1 Results from the survey

According to ENISA’s survey, on average 8% of a providers’ helpdesk calls are related to spam.

Providing spam-filtering

- 90% of all providers offer spam-filtering methods free-of-charge on their network. Another 7% offer such services for an extra fee. The remaining 3% of providers admitted they do not offer spam-filtering methods and stated they wish they could do more.
- One out of six providers offers free spam-filtering software for their clients. In addition, the same number of participants provides this software for an additional fee.

Consequences after receiving spam

- Almost half of all providers contact an ISP directly when receiving spam from it.
- 68% of all providers filter either SMTP or the entire IP traffic of another provider when they identify that spam has originated from that provider.
- 29% of all providers undertake this filtering immediately; 39% allow the spam source time to try to solve the problem before blocking traffic.
- Two-thirds of all providers use blocking filters at IP level; the remaining one third filters at SMTP level.
- Only 7% of all participants report to their NRA when detecting spam from another ISP. One participant stated that he also reports to the NRA of the ISP who is sending spam.
- No ISP tries to pursue legal actions directly.
- A sixth of all providers said that there is not much they can do.

Analysing spam

- About 60% of all providers respond to complaints from other ISPs about receiving spam.
- 30% choose an automated spam detection method; 63% of all providers respond to complaints from their subscribers.
- 15% of the participants do not analyse where spam comes from.

Processing of abuse reports

- About 73% of all participants process abuse reports manually.
- The forthcoming standard ARF for e-mail feedback reports is used by a minority of 8% of providers.
- A reasonable proportion (19%) process abuse reports using a system developed in-house.

24 For more information on ARF (Abuse Report Format), see: http://mipassoc.org/arf/
• Although providers use automated reporting formats, considerable manual work usually has to be done too. Almost half of the providers using automated methods also process abuse reports manually. Vice versa, more than half the providers using automated methods do not process them manually.

• Some of the larger providers who replied to the survey implement feedback loops\textsuperscript{25}; none of the smaller providers does so.

Conflicts between ISP obligations and the use of spam filters

<table>
<thead>
<tr>
<th>Is there conflict between ISP obligations and the use of spam filters?</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="Image" alt="Conflicts between ISP obligations and the use of spam filters" /></td>
</tr>
<tr>
<td>ENISA providers' study 2007</td>
</tr>
</tbody>
</table>

One third of participants saw a conflict between the ISPs’ obligations to deliver messages/protect privacy and the use of spam filters that block messages.

Reasons mentioned include:

• “Suppression of UBE\textsuperscript{26} bounces is a difficult choice.”

• Conflicts between false positive and false negative rate in respect of the needs of subscribers for a zero false positive rate.

• “We believe giving customers choice in how to use anti-spam is the best way to overcome this. We do not want to make the decision for them, but deploy the best technologies and let them implement them per e-mail box.”

• “National data security law” is perceived as a conflict.

4.1.2 Trend analysis

• The ratio of providers seeing conflicts between their obligations and the use of spam filters has decreased since last year, from 62% to 35%, following, for example, clarifications in Opinion 119 of the Article 29 Working Party, which ENISA highlighted in its 2006 report.

• Reporting spam incidents to the NRAs is not very popular yet. The ratio of providers reporting to NRAs remained at the single-figure level.

• Handling abuse reports is in the ascendant. A majority of over 85% of all providers say that they process reports, and more than a quarter manage them via an automated method.

• The practice of contacting an ISP when receiving spam from it dropped from more than 60% in 2006; now less than half of the providers are still doing so.

• Analysing where spam comes from is a falling trend. Whereas last year every provider reacted to requests from foreign ISPs claiming to have received spam, this year more than a third admit that they do not process these requests. Reacting to automatically monitored spam levels decreased from 46% to 30%.

4.1.3 Recent developments

• SpotSpam is a project supported by the European Commission which is intended to facilitate legal action against spammers at the international level. The project (which includes pilot software) was completed in September 2007. The results were presented during the eco anti-spam summit\textsuperscript{27}.

• Signal Spam\textsuperscript{28}, launched in May 2007, is a new French initiative, providing Best Practices for users, bulk e-mail senders and service providers in order to reduce spam.

• By August 2007, Spamcop.net, a proprietary collector and redirector of spam complaints, had forwarded about 362 million spam reports to providers, giving them information about numerous abuse cases.

• MAAGW published a Best Common Practices (BCP) document\textsuperscript{29} for e-mail senders, with recommendations on how best to send bulk e-mails.

• “Domain tasting” is a method used by spammers in order to register domains for a short time without paying for them. ICANN, which is responsible for the assignment of domain names, has started to collect information on domain tasting\textsuperscript{30}.

4.1.4 Comments

• Providers usually filter incoming spam messages, but less than a third of them are proactive and analyse the origin of spam. Accordingly, providers spend more time on filtering than on spam elimination. On the one hand, they have a good chance of eliminating spam on their network. On the other, providers might despair at analysing spam when there is nothing they can do about it. Spam is an international problem and intercontinental contacts between providers are complicated. Different laws, time zones and languages make communications complex and inefficient. Forthcoming services such as SpotSpam\textsuperscript{31} will help to mitigate this problem by acting as an intermediary.

• The abuse management of providers could still be improved. Although all providers process reports about abusive behaviour from their networks, for the most part they manage them manually. The lack of available tools for abuse report management is probably the main reason. ARF is a candidate for a forthcoming standard for abuse reporting and is becoming increasingly well known since it was first announced in 2005. It might help to automate the process for larger providers. However, processing abuse reports properly will always require additional manual work.

---

25 A feedback loop is a system to collect user feedback on e-mail tagged as spam.
26 UBE means unsolicited bulk e-mails.
27 The content of the 5th German Anti-Spam Summit organised by eco is available at: www.eco.de/5.dask
29 The latest version of the document is at: www.maaag.org/about/MAAAG_Sender_BCP/
30 ICANN have published an official request at: www.icann.org/announcements/announcement-2-10aug07.htm
31 The SpotSpam project: www.spotspam.net/
• The obligations of providers and the satisfaction of customers are sometimes seen as conflicting. Providers protect their customers against spam, but cannot avoid mistakes such as false positives (judging a legitimate e-mail as illegitimate). Giving the customers the choice whether and how aggressively they want to be protected from spam seems to be a good way to handle this issue.

• The SpotSpam project aims to collect and share information about spam. From a technical point of view it is now ready and the legal framework is in place. Providers can now join the project and send in information.

4.1.5 Advice & Proposals

• Providers should start reporting to NRAs or to a trusted third party on a voluntary basis (e.g. SpotSpam), using a set of agreed metrics.
• Standardisation bodies should establish a standard for the handling of automated abuse reports.
• Member States and NRAs should encourage or require the reporting of spam waves.
• ENISA should follow the developments of the SpotSpam and Signal Spam projects.
• The larger providers should consider providing feedback loops and increasing the quality of legitimate bulk mailings.
• ICANN should aspire to a solution for domain tasting, since this technique is often used by spammers.

4.2 Technical aspects

This chapter describes the measures that providers take to reduce spam, including preventive anti-spam measures and spam-filtering methods. The effectiveness of these methods will also be discussed.

4.2.1 Results from the survey

Sender authentication

A majority of 81% of providers uses SMTP AUTH as their authentication method.
Less than a fifth of all providers use POP3 before SMTP to ensure an authenticated sender.
Nearly 40% of all providers offer secure SMTP via TLS.
Sender ID Framework (SIDF) and DKIM are used by a very small percentage (5%).

Spam-filtering measures

Blacklisting (82%) and content filters (75%) are the most widely used anti-spam measures.
Only four methods (greylisting and sender authentication, in addition to the ones mentioned above) are used in more than 50% of all cases.
On average, providers combine 4.7 different anti-spam methods.
A very small group of providers uses unknown outsourced technologies.
More than half of the providers implementing a blacklist use it without consulting an additional whitelist.
Some providers offer sender authentication data (SPF records, DKIM signatures...), but do not use sender authentication for spam-filtering.
A sixth of the providers use frequency analysis to determine spam.

Effectiveness of anti-spam measures

To collect feedback on the effectiveness of anti-spam measures, ENISA asked the providers to indicate their percentage of aborted connections due to blacklisting, unknown recipients or greylisting, as well as the percentage of accepted connections via whitelisting and of e-mails with a virus or with spam detected via content-based mechanisms. The following diagram explains in more detail where the data comes from:
To interpret the results, the first of the charts below focuses on the left side of the diagram above, covering all SMTP connections received by the providers’ mail servers. The second chart below takes into account the treatment of accepted e-mail.

All SMTP connections

- 70% of all SMTP connections are blocked via blacklisting.
- Whitelisting is used to accept 2.2% of all connections.
- Greylisting, which blocks 1.6% of all connections, is often used after a connection has passed blacklist filters.
- Almost every sixth SMTP dialogue can be cancelled due to an unknown recipient.
- As a result of this, one out of eight connections is not blocked at SMTP level and leads to an entire SMTP dialogue delivering the e-mail.

Accepted e-mails

- A very small percentage (0.6%) of all submitted e-mail is filtered by a virus scan.
- 46% of all submitted e-mail is filtered out via other filters, which are mainly content filters.
- The remaining e-mail delivered to users’ mailboxes (HAM) represents only 6% of the overall e-mail traffic! (The 6% is calculated with the formula 54% (HAM) of the previous non-blocked 12% e-mail.)

Preventative measures

- Almost every second provider blocks [manages] access to port 25 from all hosts on its network, prohibiting the sending of spam without proper authentication.
- Message Submission for Mail on port 587 is provided by less than a quarter of all participants.
- Only half of all providers which block port 25 offer themselves Message Submission (on port 587).

Reacting to outgoing spam

- A majority of 62% of all providers add subscribers to a blacklist if they repeatedly send spam.
- 10% of the providers put good subscribers on a whitelist.
- The remaining 28% of providers have no reactive technical measure for subscribers sending spam.

4.2.2 Trend analysis

- SMTP authentication is becoming more popular. The number of providers implementing this measure has increased from 62% in 2006 to 81%.
- The use of SMTP TLS rose from 23% last year to 38% in 2007.
- More and more providers are using Lightweight MTA authentication protocols. It appears that providers prefer SPF [48%] and Reverse-MX [33%] to Microsoft’s Sender ID [5%].
- The standardised signature-based authentication DKIM is not widely used (5%). However, some providers stated that they plan to implement DKIM.
- Reactions to outgoing spam are not improving. However, proactive methods, such as managing port 25, are proving a promising tool in the fight against spam sent by customers.
4.2.3 Recent developments

- Image spam has evolved, disguising the content of an e-mail in various ways. In the second quarter of 2007, spam first occurred using PDF or MS Excel files for transport. Other formats are conceivable. In addition, spammers tend to obfuscate text in an e-mail.

- Commtouch\(^\text{32}\) calculated that 35% of world-wide spam is image spam. Due to their larger file sizes, image spam comprises more than 70% of the entire traffic wasted by spam.

- Spam has been translated into non-English languages including French and German in order to overcome the linguistic barriers of the recipients and escape from filters.

- ICANN is aware of the domain tasting problem and has developed an issues report\(^\text{33}\) about this topic. It initiated a discussion in September 2007 about whether a policy development process should be launched.

- In 2004 the IETF working group MARID\(^\text{34}\) stopped trying to define a standard for sender authentication methods. Many drafts had been published, including SPF and Sender ID Framework, but agreement on which method to choose could not be reached. In May 2007, with DKIM, the first e-mail authentication method became an IETF standard (RFC 4871\(^\text{35}\)) and succeeded the draft of Domain Keys.

- A paper\(^\text{36}\) from Georgia University mentioned spam from IP addresses that were hijacked via BGP.

- Spam sent from European countries is increasing. Spamhaus.org now lists four European countries in their top 10 of the worst spamming countries\(^\text{37}\) (in 2006 Europe had only one entry). Sophos\(^\text{38}\) has calculated that Europe is now the worst spamming continent with 35% of all spam originating within its borders.

- Research on blacklisting\(^\text{39}\) has shown similarities between blacklists. An intersection matrix shows overlaps between entries on different lists. Methods to measure the false positive rates of blacklists have also been developed.

4.2.4 Comments

- Spammers tend to send more spam from European countries. The increasing use of botnets in order to send spam allows spammers to send messages from countries with high Internet penetration. In 2006, blacklist vendor Spamhaus\(^\text{40}\) listed only one country from the EU in the top 10 of the worst countries for generating spam (the UK). As of August 2007 four EU countries (the UK, Germany, France and The Netherlands) featured in this not very flattering list. Managing port 25, in particular, is a very efficient countermeasure and already almost half of the providers enforce this technical limitation. ENISA hopes to see progress in this trend with other providers also managing port 25 soon.

- Providers still invest more in protecting subscribers from incoming spam than in protecting other networks from outgoing spam. Whereas 97% of all providers offer spam-filtering for inbound traffic, less than 50% limit the volume of outbound mail or manage port 25. This is probably the result of a financial decision. Subscribers would be dissatisfied without spam-filtering in their inbox. They tend not to notice the increasing quality of service if providers implement outbound spam filters. However, providers should also take into account other positive aspects of filtering outgoing e-mail such as developing a good reputation as a clean provider. This would help prevent their e-mail being filtered by other providers and avoid the risk of having their legitimate mail blocked.

- Only 6% of all e-mail traffic reaches user mailboxes. And of this 6% some is still spam e-mail. Strangely, even if spam is growing in quantity, size and bandwidth, which remains a huge problem for providers, it attracts less media and public attention than a few years ago, because less and less spam actually arrives in users’ mailboxes.

- Blacklisting and content filtering are the most frequently used anti-spam methods. The results of the study demonstrate that implementation of about five different methods is common practice.

- Implementing best practices\(^\text{41}\) on anti-spam measures will help providers improve their installations against spam.

4.2.5 Advice & Proposals

- Providers should review their anti-spam installations for the common practices reviewed in this survey.

- Providers should compare the effectiveness of their anti-spam installations with the results of this study, in order to identify further improvements.

- ENISA will organise a workshop in order to discuss existing and new anti-spam installations with relevant stakeholders. The information gathered within the workshop will be used as input for ENISA’s future Work Programme.

- Providers should consider managing TCP port 25 in order to minimise spam originating from Europe.

---

33 The charter of the working group is published at: www.ietf.org/html.charters/OLD/marid-charter.html
34 The DKIM RFC (4871) is available at: http://tools.ietf.org/rfc/rfc4871.txt
35 The paper is available at: www.cc.gatech.edu/~feamster/publications/p396-ramachandran.pdf
36 See www.spamhaus.org/statistics/countries.lasso for the most blacklisted countries.
37 See www.spamhaus.org/statistics/countries.lasso for the entire list.
38 ETIS best practices documents: www.etis.org/
39 RIPE Good Practice for combating Unsolicited Bulk Email: www.ripe.net/docs/spam.html
40 MAAWG best practices documents: www.maawg.org/about/publishedDocuments
41 ENISA’s future Work Programme.
5 Outlook

In recent years, spam sent from EU countries has been increasing. ENISA would like to encourage the European community to act together in order to reverse this trend. ENISA is confident that providers applying best practices would reduce the amount of spam sent from their infrastructures. ENISA would also like to encourage the exchange of information between stakeholders, by inviting providers to join providers’ associations and working groups, to attend conferences and to share their techniques to combat and limit spam.

This study and the discussions with providers show that there is a lack of information regarding the effectiveness of current and future anti-spam measures and their compatibility with existing privacy regulations. To help raise awareness in this field, ENISA invites key European stakeholders to debate these issues at a workshop. Invited speakers will include representatives of the European Commission, regulators, ISP providers, anti-spam software vendors, research institutions and privacy experts. The workshop will be held within a European track of the Inbox-Outbox event, in London, UK, on 27th and 28th November 2007. Providers are welcome to attend the European track free of charge. The same programme is offered on both days, so that providers may choose to attend either the first day or the second. A report on the topics discussed will be prepared and published on the ENISA website.

The ENISA Work Programme 2008 includes the theme “resilience in electronic communications” in which the Agency is requested to implement a study on how providers create, improve and maintain the resilience of their infrastructures. This will allow an extension of this survey, moving from anti-spam and security measures to resilience.

42 MAAWG best practices documents: www.maawg.org/about/publishedDocuments, ETIS best practices in anti-spam: www.etis.org/, RIPE Good Practice for combating Unsolicited Bulk Email: www.ripe.net/docs/spam.html
43 Inbox-Outbox November 2007 event includes a European track: www.inbox-outbox.com/
6 Appendix

6.1 List of recommendations

The recommendations below are based on the analysis of facts and trends from the study. The recommendations are sorted by the targets who should implement them.

Advice & proposals to providers

- **Providers** should be members of an association in order to increase their opportunities to share information and feedback, to acquire a common understanding and to develop and implement best practices.

- **Providers** should consider managing TCP port 25 in order to minimise spam originating from Europe.

- **Providers** should quarantine computers in their networks unless they are well protected (i.e. they have applied OS patches and have recent anti-virus signatures).

- **Providers** should invest more resources in risk management and the testing of business continuity plans.

- **Providers** can enhance their network security by monitoring traffic peaks and implementing traffic anomaly detection.

- **Providers** should start reporting to NRAs or to a trusted third party on a voluntary basis (e.g. SpotSpam), using a set of agreed metrics.

- **The larger providers** should consider providing feedback loops and increasing the quality of legitimate bulk mailings.

- **Providers** should review their anti-spam installations for the common practices reviewed in this survey.

- **Providers** should compare the effectiveness of their anti-spam installations with the results of this study, in order to identify further improvements.

Advice & proposals to the European Commission

- The **European Commission** should make the reporting of security and privacy breaches mandatory.

Advice & proposals to the Member States

- **Member States and NRAs** should encourage or require the reporting of spam waves.

Advice & proposals to other organisations

- **Standardisation bodies** should make standards easier to implement and test.

- **Standardisation bodies** should establish a standard for the handling of automated abuse reports.

- **ICANN** should aspire to a solution for domain tasting, since this technique is often used by spammers.

Advice & proposals for ENISA

- **ENISA** should examine specifically the status of DNSSEC. It is deployed in Sweden; Russia, Bulgaria and Brazil have signed their TLD zones. The survey uncovered no other implementations elsewhere.

- **ENISA** should follow the developments of the SpotSpam and Signal Spam projects.

- **ENISA** will organise a workshop in order to discuss existing and new anti-spam installations with relevant stakeholders. The information gathered within the workshop will be used as input for ENISA’s future Work Programme.

---

44 For more details on DNSSEC, see RFCs 4033, 4034 and 4035 available at: www.ietf.org/

45 More information is available at: www.dnssec.net/
6.2 Questionnaire

Study on Spam and Security measures

May 2007

Please note: You can find explanations for the terms followed by an asterisk* at the end of this document. Questions have multiple choices allowed; please submit answers even if you don’t reply to all questions.

About your organization

Name of your organisation

Country

Contact name

Email

Phone

Are you ☐ an ISP*   or/and ☐ an ESP*   or/and ☐ a Telco*?

Security

1. Please order the following list of threats from most concerning (1) to least concerning (8) for your organisation:
   - Act of nature beyond control
   - BGP Hijack*
   - DNS attacks
   - DoS*/DDoS*
   - Social Engineering/Spying
   - Spam
   - Viruses
   - Worms

2. Which of the following organizational measures do you take to secure your services?
   - We provide regular information on information security to our subscribers by …
     - ☐ … publishing information on our web site
     - ☐ … sending physical mail
     - ☐ … sending email
   - We provide detailed written guidance for
     - ☐ … staff
     - ☐ … partners
     - ☐ … subscribers ☐ … including a policy defining permitted/prohibited uses of the messaging services
   - We provide security software for users
     - ☐ … free of charge
     - ☐ … for a fee
   - We provide clear contact details
     - ☐ … for email abuse
     - ☐ … for security violations
   - ☐ We provide security support via Hotline/Helpdesk
   - ☐ We provide remote technical assistance (i.e. with access to the device)
   - ☐ We maintain up-to-date reverse DNS records
   - ☐ We provide training or awareness campaigns
   - ☐ We inform subscribers about the legal consequences of sending spam
   - ☐ We forbid spamming in Terms & Conditions
   - ☐ Other (please specify):
3. Which of the following technical measures do you take to secure your services?
   - Basic filtering (e.g. spoofed IP address) in ...
     - [ ] Ingress
     - [ ] Egress
   - Content filtering (e.g. anti-viruses) in ...
     - [ ] Ingress
     - [ ] Egress
     - [ ] Quarantining an infected / malicious PC
     - [ ] Traffic Shaping / Throttling
     - [ ] Blackholing/Sinkholing
     - [ ] DNSSEC (RFC 4033-4035)
     - [ ] Other (please specify):

4. What measures do you take to become aware of security or spam problems?
   - [ ] We track complaints
   - [ ] We deploy real-time traffic anomaly and/or signature-based detection
   - [ ] We deploy spamtraps
   - [ ] We monitor for traffic peaks
   - [ ] We subscribe to security intelligence services
   - [ ] Others (please specify)

5. How do you ensure an appropriate level of security? Please choose your three most appropriate options:
   - [ ] We follow guidance in international standards
   - [ ] We follow industry best practice
   - [ ] We define a Risk Management process
   - [ ] We define a Service Level Agreement (SLA)
   - [ ] We follow guidance in national legislation
   - [ ] We follow the advice of the national computer security organization of our country
   - [ ] We define an appropriate level in our Security Policy
   - [ ] We do what is necessary based on our internal risk assessments
   - [ ] No guidance or any measures needed

6. When a particular risk of a security breach arises in your network, what do you do?
   - [ ] We inform subscribers directly (i.e. individually)
   - [ ] We inform subscribers via a customer portal (to which only subscribers have access)
   - [ ] We issue reports to the public (e.g. with a press release, on our public website)
   - [ ] We report to the NRA
   - [ ] We decide whether and how subscribers should be informed

7. If the risk lies outside the scope of the measures you can take directly, then what do you do?
   - [ ] We inform subscribers of any possible remedies that they can take
   - [ ] We inform subscribers of any possible remedies that they can take and the associated costs
   - [ ] We inform subscribers of the risk of not implementing counter measures
   - [ ] We stop servicing non-compliant subscribers

8. Regarding protection of network integrity, what do you do?
   - [ ] We have a Business Contingency (BC) process
   - [ ] We have a Disaster Recovery (DR) process
   - [ ] We have a Risk management process
   - [ ] We regularly conduct BC/DR tests (at least yearly)
Study on Spam and Security measures

Security

☐ We do nothing, but we wish we could do more
☐ Others (please specify)

SPAM

9. Which of the following measures do you take to prevent your subscribers from sending unsolicited communications (spam)?

☐ We use a blocking list system:
  ☐ We put a subscriber on a blacklist* if the subscriber repeatedly sends spam
  ☐ We put on a whitelist* all subscribers who do not send spam
  ☐ We use a greylist* system

☐ We block access to port 25 from all hosts on our network other than those that are explicitly authorized to perform SMTP relay functions
☐ We provide Email Submission services on port 587 (as described in RFC 4409)
☐ We limit high outbound mail volumes
☐ We perform outbound virus scanning
☐ Other (please specify)

10. Which of the following measures do you take to protect your subscribers from receiving unsolicited communications (spam)?

☐ We offer spam-filtering on our network (e.g. by subscribing to black/white-lists, see question 11) ...
  ☐ ... free-of-charge  ☐ ... for an additional fee

☐ We offer spam-filtering software that subscribers can install on their computers ...
  ☐ ... free-of-charge  ☐ ... for an additional fee

☐ We do nothing, but we wish we could do more
☐ Other (please specify)

11. Which of the following spam-filtering measures do you take on your network?

☐ Blacklisting* (e.g. DNSBL)
☐ Whitelisting* (e.g. DNSWL or CSA*)
☐ Greylisting*
☐ Sender authentication*
☐ Checksum analysis (e.g. DCC*)
☐ Blacklisting of URIs (e.g. URIDNSBL)
☐ Content filtering* (e.g. rule-based or statistical)
☐ Reputation system*
☐ Slowing down the senders connection
☐ Frequency analysis of connection problems
☐ Outsourced system (technology unknown)
☐ Other (please specify)

12. Which of the following sender authentication mechanisms do you implement?

☐ SMTP AUTH (RFC 2554)
☐ POP3 before SMTP
☐ Sender ID Framework (SIFD*)
☐ DomainKeys Identified Mail (DKIM*)
☐ SMTP TLS (RFC 3207)
☐ Reverse-MX
☐ Sender Policy Framework (SPF*)
☐ Other (please specify)

13. When do you analyze where spam comes from?

☐ On request from ISPs who received spam from our network
☐ When an automatically monitored spam level reaches a certain threshold
☐ Following complaints from our subscribers
☐ We do not analyze where spam comes from
☐ Other (please specify)

14. What sort of measures do you take if you detect spam coming from another ISP?
Study on Spam and Security measures

15. Could you provide us the following information about your anti-spam system? [See graphical explanation]
   a) Percentage of aborted connections due to **blacklisting** (in relation to all SMTP connections): %
   b) Percentage of aborted connections due to **unknown recipients** (in relation to all SMTP connections): %
   c) Percentage of aborted connections due to **greylisting** (in relation to all SMTP connections): %
   d) Percentage of accepted connections due to **whitelisting** (in relation to all SMTP connections): %
   e) Percentage of as virus infected filtered emails (in relation to accepted emails): %
   f) Percentage of as spam detected filtered emails (in relation to accepted emails): %

16. Do you think that there is a conflict between ISP obligations of delivering messages/protection of privacy and the use of spam filters that block some messages?
   □ No  □ Yes, please specify:

17. Do you plan to install or implement an anti-spam method in the next six months?
   □ No  □ Yes, please specify:

18. How do you process abuse reports?
   □ They are processed manually
   □ We use the ARF® standard reporting format
   □ We provide feedback loops to other organisations
   □ We use another reporting format or automated tools/method, please specify:

**Miscellaneous**

19. If one or several questions did not offer appropriate answer options, please use this space to explain. Please also indicate the number of the question.

20. Do you think that a workshop on the matter of this study before the end of 2007 would be valuable for you? □ yes □ no
   If yes, what would be areas that should be covered:
   □ Discuss measures of providers regarding spam measures
   □ Discuss measures of providers regarding security measures
   □ Laws and legacy problems regarding spam
   □ Laws and legacy problems regarding security
   □ Presentation of study results
   □ Presentation from security and spam filtering vendors
Study on Spam and Security measures

- Presentation of new methods from security and spam filtering research
- Others (please specify)

21. Could you provide us with the following information that will increase the quality of the survey results?

How many email boxes do you manage?  
How many email messages do you transport per day?  
Could you indicate the percentage of your helpdesk calls that concern spam?  
How many persons are fully dedicated security staffs?  
What is your annual budget in the area of security?  

---

1 We know that this information is highly sensitive information. ENISA will use it advisedly and won’t publish it with identifiable relationships to you. Please consider that this data will highly increase the quality of the survey results.

2 Same as above
--- Glossary of the questionnaire ---

**Explanation of terms**

This list illustrates ENISA’s understanding of some more specialized terms that are used in the context of this study. Definitions by external parties (e.g. Wikipedia) have been checked and sometimes adjusted by ENISA.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARF</td>
<td>Abuse Reporting Format, see <a href="http://mipassoc.org/art/">http://mipassoc.org/art/</a></td>
</tr>
<tr>
<td>BC(P)</td>
<td>Business Continuity Planning (BCP) is a methodology used to create a plan for how an organization will resume partially or completely interrupted critical function(s) within a predetermined time after a disaster or disruption. BCP may be a part of a larger organizational effort to reduce operational risk associated with poor information security controls, and thus has a number of overlaps with the practice of risk management. – Source: Wikipedia</td>
</tr>
<tr>
<td>BGP Hijack</td>
<td>BGP hijacking is the illegitimate taking over of groups of IP addresses by corrupting Internet routing tables. – Source: Wikipedia</td>
</tr>
<tr>
<td>Blackholing / SINKholing</td>
<td>Blackholing or sinkholing: This approach blocks all traffic and diverts it to a black hole, where it is discarded. The downside is that all traffic is discarded - both good and bad - and the targeted business is taken off-line. Similarly, packet-filtering and rate-limiting measures simply shut everything down, denying access to legitimate users. – Source: ComputerWorld</td>
</tr>
<tr>
<td>Blacklist</td>
<td>A blacklist is a list or register of entities who, for one reason or another, are being denied a particular privilege, service, or mobility. – Source: Wikipedia</td>
</tr>
<tr>
<td>Certified Senders Alliance (CSA)</td>
<td>Bulk mailers who send advertising material with the recipient’s permission (permission marketing) are already complaining that a substantial part of requested messages such as newsletters no longer reach the recipient due to mail filtering. Bulk mailers counteract this presently by negotiating with internet service providers to be added to their internal white list. This is the reason for the creation of a white list of bulk mailers that is centrally managed and for the setup of a standardized procedure that can consistently offer high quality and can manage complaints effectively. – Source: <a href="http://www.eco.de/servlet/PB/menu/1779020/II/index.html">http://www.eco.de/servlet/PB/menu/1779020/II/index.html</a></td>
</tr>
<tr>
<td>Content Filtering</td>
<td>Content filtering is the most commonly used group of methods to filter for security problems (e.g. viruses). Content filters act either on the content, the information contained in the mail body, or on the mail headers (like “Subject:”) to either classify, accept or reject a mail. – Source: Wikipedia/ENISA</td>
</tr>
<tr>
<td>DCC</td>
<td>The idea of the DCC is that if mail recipients could compare the mail they receive, they could recognize unsolicited bulk mail. A DCC server totals reports of checksums of messages from clients and answers queries about the total counts for checksums of mail messages. A DCC client reports the checksums for a mail message to a server and is told the total number of recipients of mail with each checksum. If one of the totals is higher than a threshold set by the client and according to local whitelists the message is unsolicited, the DCC client can log, discard, or reject the message. – Source: <a href="http://www.rybolite.com/anti-spam/dcc/">http://www.rybolite.com/anti-spam/dcc/</a></td>
</tr>
<tr>
<td>DDoS</td>
<td>A distributed denial of service attack (DDoS) occurs when multiple compromised systems flood the bandwidth or resources of a targeted system, usually one or more web servers. – Source: Wikipedia</td>
</tr>
<tr>
<td>DNSSEC</td>
<td>DNSSEC (short for DNS Security Extensions) adds security to the Domain Name System (DNS) used on Internet Protocol networks. It is a set of extensions to DNS, which provide origin authentication of DNS data, data integrity, and authenticated denial of existence (i.e. authenticated non-existence reply). DNSSEC was designed to protect the Internet from certain attacks such as DNS cache poisoning. All answers in DNSSEC are digitally signed. By checking the signature, a DNS resolver is able to check if the information is identical (correct and complete) to the info on the authoritative DNS server. – Source: Wikipedia, based on RFC 4033-4035</td>
</tr>
<tr>
<td>DomainsKeys Identified Mail (DKIM)</td>
<td>DKIM provides a method for validating an identity that is associated with a message, during the time it is transferred over the Internet. That identity then can be held accountable for the message. In most cases the signing MTA acts on behalf of the sender by inserting a DKIM-Signature header, and the verifying MTA on behalf of the receiver, validating the signature by retrieving a sender's public key through the DNS. – Source: Wikipedia, <a href="http://www.dkim.org">http://www.dkim.org</a></td>
</tr>
<tr>
<td>DoS</td>
<td>A denial-of-service (DoS) attack is an attempt to make a computer resource unavailable to its intended users. – Source: Wikipedia</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Authority as defined by article 28 of EU Directive 95/46/EC.</td>
</tr>
<tr>
<td>DR(P)</td>
<td>Disaster recovery is a plan for a business to restart operations after a disaster; this is especially evident in information technology; with most large computer systems containing software to limit data loss and to aid data recovery. – Source: Wikipedia</td>
</tr>
<tr>
<td>Egress Filtering</td>
<td>Egress filtering is the process of filtering packets from going from the inside to the outside. – Source: ENISA’s own definition</td>
</tr>
<tr>
<td>Electronic communication network</td>
<td>Electronic communications network means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed. – Source: EU Directive 2002/21/EC</td>
</tr>
<tr>
<td>Electronic Communication service</td>
<td>Electronic communications service means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks. – Source: EU Directive 2002/21/EC</td>
</tr>
<tr>
<td>ESP</td>
<td>Email service provider.</td>
</tr>
<tr>
<td>Greylist</td>
<td>A mail transfer agent which uses greylisting will &quot;temporarily reject&quot; any email from a sender it does not recognize. If the mail is legitimate, the originating server will try again to send it later, at which time the destination will accept it. If the mail originates from a spammer, the spammer will probably not resend it. – Source: Wikipedia, shortened</td>
</tr>
<tr>
<td>Ingress Filtering</td>
<td>Ingress filtering is the process of filtering of packets from outside the network. – Source: Wikipedia shortened</td>
</tr>
<tr>
<td>ISP</td>
<td>An Internet service provider (ISP, also called Internet access provider) is a business or organization that offers users’ access to the Internet and related services. – Source: Wikipedia</td>
</tr>
<tr>
<td>Ministry</td>
<td>Ministry (e.g. telecommunications, or transport, or other)</td>
</tr>
<tr>
<td>NRA</td>
<td>National Regulatory Authority (e.g. for Telecommunication)</td>
</tr>
<tr>
<td>Public communication network</td>
<td>Public communications network means an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services. – EU Directive 2002/21/EC</td>
</tr>
<tr>
<td>Quarantining a computer</td>
<td>Quarantining a computer means isolating a computer into a special network until it has reached a certain security level. The computer is offered to install updates for anti-virus signature files or install software patches. – Source: ENISA’s own definition</td>
</tr>
<tr>
<td>Real-time anomaly detection</td>
<td>Anomaly detection tries to discover malicious behavior by comparing current behavior to learned normal models of behavior. An anomaly detection approach usually consists of two phases: a training phase which defines what is normal and a working phase which compare new data to the learned model. – Source: Long Fei (Purdue University)</td>
</tr>
<tr>
<td>Remote technical assistance</td>
<td>Technical assistance done remotely, using a phone line and/or an Internet connection. It gives access to the device in question, enabling remote input and output. The user requests such assistance and gives his consent to remote access prior to any action. – Source: ENISA’s own definition</td>
</tr>
<tr>
<td>Reputation system</td>
<td>A reputation system is a type of collaborative filtering algorithm which attempts to determine ratings for a collection of entities, given a collection of opinions that those entities hold about each other. In detail, these systems can be used to exchange characteristics of spammers (e.g. IP, domain). – Source: Wikipedia, ENISA</td>
</tr>
<tr>
<td>Sender ID</td>
<td>Sender ID is an anti-spam proposal from the MARID IETF working group that joined Sender Policy Framework (SPF) and Caller ID. – Source: Wikipedia</td>
</tr>
<tr>
<td>Sender Policy Framework (SPF)</td>
<td>Sender Policy Framework (SPF) is an extension to Simple Mail Transfer Protocol (SMTP), the standard Internet protocol for transmitting email. SPF makes it easier to counter most forged &quot;From&quot; addresses in e-mail, and thus helps to counter email spam. – Source: Wikipedia</td>
</tr>
<tr>
<td>SMTP Authentication</td>
<td>SMTP authentication allows a requested authentication mechanism, which performs an authentication protocol exchange to authenticate and identify the user. The authentication mechanism can be for example ESMTP AUTH LOGIN / PLAIN, TLS, Kerberos, GSSAPI. – Source: RFCs 2554, RFC 2222, ENISA</td>
</tr>
<tr>
<td>Spamtraps</td>
<td>Spamtraps are usually e-mail addresses that are created not for communication, but rather to lure spam. Since no e-mail is solicited by the owner of this spamtrap e-mail address, any e-mail messages sent to this address are</td>
</tr>
<tr>
<td><strong>Teleo</strong></td>
<td>A telephone company (or telco) provides telecommunications services such as telephony and data communications. With the advent of cellular telephony, telcos now include wireless carriers. – Source: Wikipedia</td>
</tr>
<tr>
<td><strong>Traffic Shaping</strong></td>
<td>Traffic shaping is an attempt to control computer network traffic in order to optimize or guarantee performance, latency, and/or bandwidth. Traffic shaping deals with concepts of classification, queue disciplines, enforcing policies, congestion management, quality of service (QoS), and fairness. Traffic shaping provides a mechanism to control the volume of traffic being sent into a network (bandwidth throttling), and the rate at which the traffic is being sent (rate limiting). For this reason, traffic shaping schemes need to be implemented at the network edges to control the traffic entering the network. It also may be necessary to identify traffic flows at the ingress point (the point at which traffic enters the network) with a granularity that allows the traffic-shaping control mechanism to separate traffic into individual flows and shape them differently. – Source: Wikipedia</td>
</tr>
<tr>
<td><strong>Whitelist</strong></td>
<td>A whitelist is a list of accepted items or persons in a set. This list is inclusionary, confirming that the item being analyzed is acceptable. – Source: Wikipedia</td>
</tr>
</tbody>
</table>
Description of question 15

ENISA is aware of the complexity of this question. However, with the results of this question an overview of the efficiency of the different kinds of spam filtering can be provided. We look forward to receive this data from many participants and would be glad to get your data.

ENISA purposely didn’t mention a timeframe for the data and is pleased to obtain as recent data as possible. Please notice the two different relations between the absolute value of SMTP connections (email envelope analysis) and accepted emails (email DATA analysis).

In the first part (email envelope analysis), please provide information about percentages of blocked connections during transmitting the email envelop within the SMTP dialog (up to DATA statement).

\[
\text{% of connections ready for DATA delivery} = 100\% - a) - b) - c)
\]

In the second part (email analysis), please provide information about percentages of filtered emails due to the email analysis, i.e. measures during or after the DATA delivery of the email.

\[
\text{% of ham emails} = 100\% - e) - f)
\]
6.3 Additional links

ENISA dedicated page on European providers’ security and anti-spam measures:

ENISA Surveys 2006 – Survey on Security and Anti-spam measures taken by Electronic Communications Service Providers:

Contact Network of Spam Authorities (CNSA):

www.oecd-antispam.org/

ITU Survey on Anti-Spam legislation worldwide:

APWG Phishing Activity Trends Report (June 2007):

Symantec’s Internet Threat Report 1Q2007:
www.symantec.com/enterprise/threatreport/index.jsp

Spam Statistics:
- Spamhaus – www.spamhaus.org/statistics/countries.lasso

E-mail reputation systems:
- Lashback – www.lashback.com/
Authors:
Pascal Manzano, Expert in Security Policies, ENISA
Christian Rossow, Expert in Anti-spam, 
Institute for Internet-Security, if(is)

The authors would like to acknowledge the document review and useful comments received from Carsten Casper, Evangelos Ouzounis and Alain Esterle during the writing of this study.

For further information about this report:
pascal.manzano@enisa.europa.eu

Legal Notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless it is stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of-the-art and it might be updated from time to time.

Third party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic mechanical, photocopying, recording, or otherwise without the prior written permission of ENISA, or as expressly permitted by Law or under terms agreed with the appropriate rights organisations. Source must be acknowledged at all times. Enquiries for reproduction can be sent to the contact address quoted in this publication.
