Global Information Assurance Certification Paper

Name: Niklas Andersson
GSEC Practical Version: 1.4b
2002-11-18

Title:

Deploying a Network Abuse Team – Case Study

Abstract
This document describes a situation I was confronted with during the end of year 2000.
I was hired to set up a Network Abuse team at a new Broadband Internet Service Provider in Sweden. The company was providing Ethernet to the home at 10Mbit full duplex to each customer.

A Network Abuse Team is a function at an ISP (Internet Service Provider) that handles customers that doesn't comply with the set-up rules and policies that basically all ISPs have, or that breaks the law by the use of their Internet connection.

The goal of this document is to share my experience of deploying this type of function and how you can avoid some pitfalls that I fell into.

This document is mainly written for ISPs, however it may very well be useful for deploying a similar function at other sites providing Internet access to a large number of people such as large corporations, schools and governments.

Before
Every ISP should have an e-mail address that is used to report abuse of the Internet connection. The de-facto standard is abuse@isp.com

Before this team was established the ISP in question had a lot of problems with customers doing their best to utilize their Internet connection in all kinds of mysterious ways. The abuse mailbox was flooded with mail from angry customers and other people around the world who in one way or another had been posed by some kind of Network Abuse. There were basically two types of mail:

- Cases where the source of the Network Abuse was one of our customers.
- Cases where the target of the Network Abuse was one of our customers.

There were a lot of different issues reported. These were the different categories:

Denial Of Service Attacks – Attacks with different types of tools for the purpose of either crashing the target or making sure it couldn't communicate on the Internet. Some of the techniques used were: Smurf attacks, Land attacks, SYN-Flooding.

Portscan – Scans of the open TCP/IP ports of a computer, most of the times a preparation to gain knowledge of the computer for the purpose of either hacking or to see if the host is infected with a Trojan such as Netbus, Subseven etc.

Hacking – Attempts to hack a computer.

SPAM – Sending unsolicited mail.

Netiquette violations – Different types of Netiquette violations mainly on chat channels such as threats, foul language etc.

Fraud – Trying to lure people to giving up their credit card numbers. Customers using their connections for commercial use – violation of our end-user agreement

Virus / Trojans – People spreading Viruses and Trojans on purpose or by mistake.

Copyright Violations – People spreading Copyright protected software.

Breaking the Law – This was the worst kind of Network Abuse. People trading Child Pornography, serious threats on chat channels, successful hacking etc.

At this time we had approximately 30.000 customers, we received about 100 reports of Network Abuse by e-mail every week.

A typical report to the team could look like this:

-----Start Example Report-----

From: Johan Doe [mailto:john@doe.com]
Sent: den 26 februari 2001 23:28
To: abuse@isp.com
Subject: Security attempt from 10.0.XXX.XXX

ref 11584, 11580, 11473, 11528

Our network was recently subjected to an FTP port scan (tcp port 21) from Your IP address 10.0.XXX.XXX, presumably in an attempt to find FTP -accessible Systems in our network in order to attempt commonly known security exploits.

Further such attacks will dictate that we block ALL network traffic from Your networks.

Please identify the cause of this and put an immediate stop to all such activities. Attached are our logs of this incident, times are in Pacific USA Daylight time.

Thank you,

John Doe Email: johan@doe.com
Director of Information Technology
Companyname, City, Country

```
Date/Time(-0800)Action Pro Source IP   (Src Port)  Dest IP (Dest port)
-------------- ------ --- ------------ -----     ------------ ----
Feb 26 14:01:25 denied tcp  10.0.XXX.XXX(1076) -> 192.168.X.X(21)
Feb 26 14:01:25 denied tcp  10.0.XXX.XXX(1242) -> 192.168.X.X(21)
Feb 26 14:01:27 denied tcp  10.0.XXX.XXX(1365) -> 192.168.X.X(21)
Feb 26 14:01:28 denied tcp  10.0.XXX.XXX(1130) -> 192.168.X.X(21)
Feb 26 14:01:29 denied tcp  10.0.XXX.XXX(1266) -> 192.168.X.X(21)
Feb 26 14:01:34 denied tcp  10.0.XXX.XXX(1085) -> 192.168.X.X(21)
Feb 26 14:01:34 denied tcp  10.0.XXX.XXX(1245) -> 192.168.X.X(21)
Feb 26 14:01:36 denied tcp  10.0.XXX.XXX(1356) -> 192.168.X.X(21)
```

-----End Example Report-----

Problems Before

One of the problems before we started off was the quality of the reports, we could get mail where the customer had been kind enough to enlighten us of: what had happened, source IP-address of the attacker but not the time of the event – which makes it all useless since we used DHCP (Dynamic Host Configuration Protocol) to provide IP-Addresses to the customers.

Another big problem was that the company didn't have reliable informa tion on what customer had the IP-address in question at the time of the Network Abuse.

Our entries in RIPE (Réseaux IP Européens) were another problem. This is the database where the information about the owner of IP-Addresses in Europe is stored. The problem was that at the time we registered the IP-Addresses.

However the biggest issue was that we didn't have any procedures of how to handle and prioritise these reports.

The situation we had at hand was not looking good, if we had chosen to neglect this we would risk several things such as, bad publicity, other ISP: s could ban our IP-Address range, our mail servers could be blacklisted on services such as MAPS (Mail Abuse Prevention System) and ORDB (Open Relay DataBase)

However the biggest issue was th at Swedish law obliges an ISP to be able to help the Police with information about who had the specified IP-address at a certain time.

During

Hiring Staff

My work started off by hiring people; my first idea was to hire people with a lot of network security skills, technicians who had extensive knowledge of protocols, hacking techniques, mail servers etc. I thought that it takes one to know one…

This proved to be not exactly the case, a lot of time is consumed by talking to customers by the phone, writi ng e-mails, registering cases - this is not exactly a technicians dream. I learned this the hard way by employing a skilled technician; he got bored and quitted within 6 months.
In my opinion the ideal person to work at a Network Abuse team is a person w ith excellent communication skills, knowledge of the law, basic technical skills and very accurate.

Security around the team

I realized that this team would be handling a lot of sensitive information, such as Police Reports, Abuse reports of customers tr ading Child Pornography and so on. Therefore I made sure from the beginning that the Abuse Team would be the only ones who could access this information both in digital and physical way. These were the measures I took:

1. Placed the team in an office with l imited access only to them.
2. Installed a safe for sensitive documents.
3. Limited access rights on the fileserver to only them, making sure to remove the administrator's access.
4. Limited access in the case handling system making sure that the cases created by the team couldn't be read by anyone else.
5. Limited access in the mail server, allowing only the team to read the abuse mailbox.
6. Instructed the switchboard operators to never give out the team's personal/cell phone numbers.

System support

To be able to run this type of organisation we needed some different types of systems/tools. These were the ones I found out to be necessary:

1. Mail – Any mail client is good, we chose Outlook, because of its ability to file incoming mails in folders, allow multiple users on the same mailbox and the advanced search functions.

2. Tracking tools – This is used to track down the customer that had the specified IP-Address at the given time, we had the luxury of having our DHCP software developed in-house, so modifying it to fit our needs was not a problem.
   A word of advise, make sure that the time is running correctly on this system preferably by setting it by NTP (Network Time Protocol) otherwise you could end up with sending a warning or shutting down a customer who had the IP - address before or after the one who really did the deed.

3. Case Handling Tool - To be able to register and track the incoming cases we used a tool called ARS Remedy, this tool was already used in the organisation by the Support and Customer Care departments. ARS Remedy is a very powerful case-handling tool with lots of functionality such as case tracking, escalation, notification, time tracking. This system is probably too powerful for this type of operation, but since we had it we might as well use it. If yo u chose

another system make sure that the system is capable of the following:

a. Assigning a unique case number, this is very useful when you start getting a lot of cases. It's also very useful to include as a reference when you send out a Letter or a mail t o a customer (more on this later on), thereby making it a lot easier if the customer calls you and want to discuss the matter.
b. Search function
c. Different user access levels, as mentioned before, you should limit the access to allow only the personnel workin g in the team to see the cases.

4. Search tools on the Internet – When we received a report with another source IP-address than ours we just forwarded it to the registered owner of the address. There are several ways to find out who the owner is of an IP -address, one of the easiest ways are to search at one of the following databases http://www.ripe.net/ripencc/pub -services/db/whois/whois.html (Europe) http://www.apnic.net/apnic -bin/whois.pl (Asia) http://www.arin.net/whois/index.html (US) or a great collection of them all at http://www.geektools.com/cgi -bin/proxy.cgi

Fighting it

Now we got the necessary system support, personnel, and security around the team. This was the time to start to take action, so our biggest question was how to stop people from abusing their Internet connection? We could always shut down the users account? The problem with this is that the sales department wouldn't be too happy if we started to shut down every customer that did a portscan.

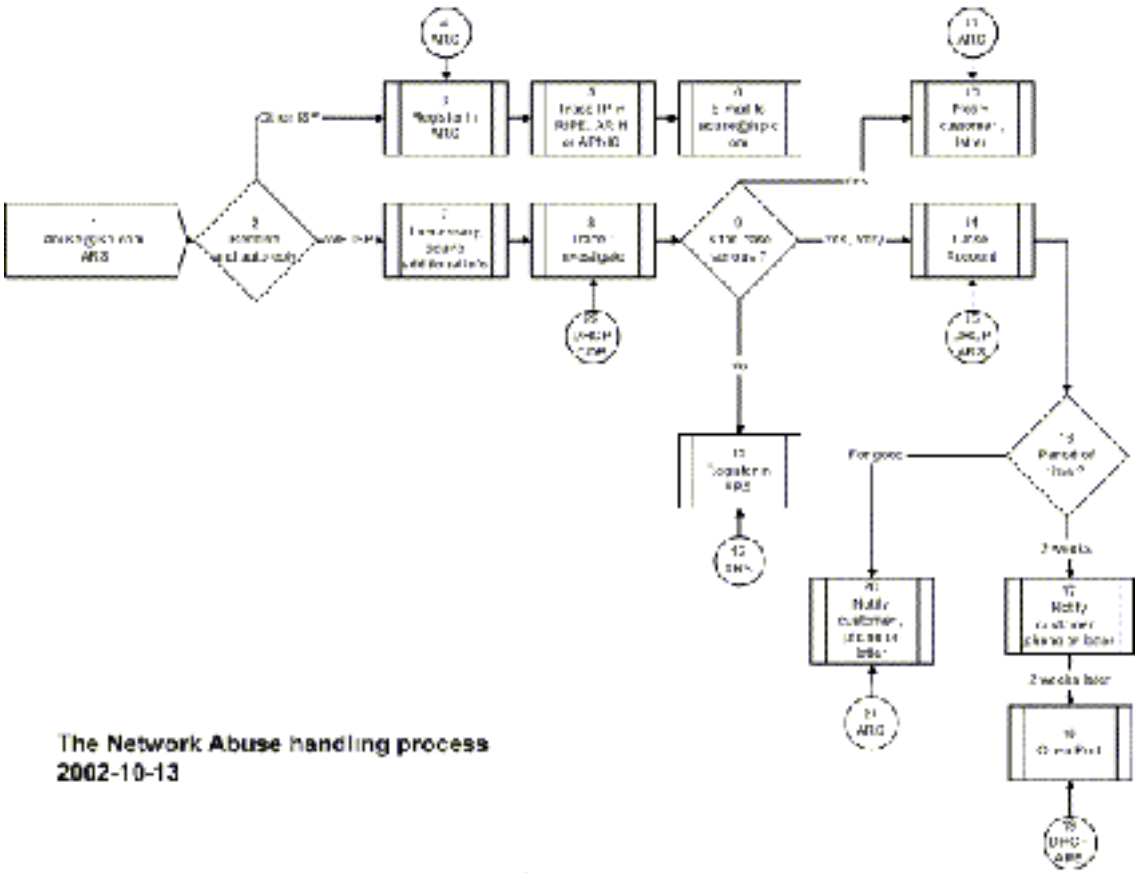
We tried different approaches, first we tried to send E-mail to the person in question. This was not working out because some of the times the person didn't use the registered e-mail; Web-based e-mail like Hotmail, Yahoo etc. is big nowadays. If however the person intended got the e -mail, it was easy to just delete it and forget about it. Basically e -mail just doesn't have enough teeth in it.

After this we tried to call the person in question, this was far too time -consuming.

We finally started to send out normal letters, this gave an interesting ef fect:
The typical person who was misusing their Internet connection was approximately 15 years and still living with their parents. An unmarked envelope addressed to the person who signed up for the connection was almost always read by one of the parents, thereby creating a momentum in the household – especially if a lawyer formulates the letter. (Examples later on)

Workflow

After trying some different approaches we finally decided how we should work. This is an explanation of the workflow that we use ri ght now, it may not suite everyone, but it might be helpful when you are creating your own.



The Network Abuse handling process
2002-10-13

Explanation of the workflow:

(Step 1) The report arrives from different sources to the team by E -mail abuse@isp.com

(Step 2) The mail is received and an auto reply is sent back, the technician checks if the source of the abuse is from us or from another ISP. This is a quick check since the technician knows our IP address range.

(Step 3) The source was from another ISP. Th e technician registers the case in ARS our case handling system *(Step 4)*, enclosing the received mail.

(Step 5) The IP-Address is traced using RIPE, ARIN or APNIC or http://www.geektools.com/cgi -bin/proxy.cgi

(Step 6) The case is forwarded by e -mail to the ISP that has the IP -Address in question.

(Step 7) If necessary, acquire additional information.

(Step 8) Trace and investigate, in this step the customer is tracked down, using the DHCP software and our customer database (CDB) *(Step 22)*.

(Step 9) A decision is made if the case is serious or not.

(Step 10) The case is serious but not to the degree that we should shut down the customer. We send out a warning by letter to the customer.

(Step 11) Update the case in ARS

(Step 12, 13) The case is not serious. Update the case in ARS.

(Step 14) The case is very serious. The customer is disconnected (using our DHCP system) and the case is updated in ARS *(Step 15)*

(Step 16) A decision is made if the disconnection is for good or just for a period of time (normally two weeks)

(Step 17) The customer is disconnected for two weeks, a notification is sent by letter or in some cases by phone.

(Step 18) After the set time has expired, the customer is connected again, and the case is updated in ARS *(Step 19)*

(Step 20) The customer is disconnected for good and the case is updated in ARS *(Step 21)*

Documentation

Network Abuse Policy

We realized that we would need some documentation to support our work. First of all we needed a policy that stated what was okay and what was not while using our connection to the Internet. This policy is called “Network Abuse Policy”.
Make sure to publish the Network Abuse Policy on an easy to find location such as your homepage or portal. Another good idea is to include a copy of the policy when you send out a Warning Letter.
See appendix A for a sample Network Abuse Policy.

Reply Mail

As mentioned before, a lot of the incoming cases were incomplete in one way or another, therefore we created a reply mail that we send back to everyone who sends in a case on abuse@isp.com Another reason to do this is to notify the person that we have received the case and that we are working on it. This tends to have a calming effect and avoids some of the phone calls placed by people asking about what is happening with their case.
See appendix A for a sample reply mail.

Warning Letter

This is the letter we send out to customers that has conducted a Network Abuse.

See appendix A for a sample Warning letter.

Prioritising the Cases

Setting the priority of the different cases can be tricky; we needed to consider the Law, the company's reputation, the safety of our customers and the company's earnings. For these reasons it can be complicated to give an exact recommendation.

For example: in the beginning we considered a Portscan to be a quite serious offence, we named it "Preparation for Computer Intrusion" which it very well could be. However, since we n ormally gave one warning then shut down the customer – a lot of customers were shut down…. It didn't take long before the sales department called us up and asked why we shut down the customers that they had been working hard to get in the first place.

The cases at our site that always gets the highest priority are:

- Denial of service attacks
  Due to its nature, this type of case could be fatal if someone on the Internet is attacked with a denial of service attack.
- Police inquiries
  Information from us may be crucial for an on-going investigation.
- Child Pornography

Proactive measures

Frequently Asked Questions

After a while when we had talked to a lot of customers, we started seeing a pattern of questions emerging. Therefore we set up a FAQ (Frequently Asked Questions) on our customer portal. This is where we try to answer the most common questions such as:

- How do I protect myself when I'm surfing the Internet?
- Am I allowed to set up an FTP (File Transfer Protocol) server?
- What is Spam mail?

Here we also recommended a Software Firewall and an Antivirus Software. Another recommendation that we use a lot is how to protect against specific threats such as Code Red and Nimda.

Probes

We had quite a lot of problem when Code Red struck; it spread like wildfire in our network, most of the time the customers weren't even aware of that their computers were infected. Therefore we set up a Probe, we did this by setting up a computer with Linux and Snort (Network Intrusion Detection) installed, this way we could see t he IP-addresses that were trying to infect the probe in the Snort -log. After this we traced the IP-addresses and informed the customer that he/she was infected. This was much appreciated.

Test lab

We received a lot of firewall logs, since all the softwa re firewalls generate different log outputs we needed to learn what to look for. Therefore we set up a test lab with three computers connected to each other by a switch, after this we installed a software firewall on one of the computers and a wide collect ion of hacking tools and port scanners on the other one. Then we started simulating attacks from the "hacking" computer and watched and learned the firewall logs on the other one. If you decide to do this, make sure that your lab is NOT connected to the co mpany network. Another tip is to create Ghost -Images of the lab computers; they tend to crash after a while since the hacking tools are often poorly written. A third tip is to ask the vendors of the software firewalls for free copies, if you explain what y ou will use them for they usually send you a copy (hoping that you will recommend it in the future)

After

After a while we started noticing a slight decrease in the amount of reports that was coming in to the team, this was most likely due to the fact that the word started spreading on the Internet telling that the ISP in question now had a working Network Abuse Department that didn't tolerate Network Abuse. We actually saw a few examples of this on our customer discussion forum.

The big benefit is to have a well-documented structured way to work. This was well proven when the Nimda-worm struck; we could quickly post a recommendation on our customer portal that described the worm and how to protect against it.

The problems we had before with incomplet e reports is not a big problem anymore, the key-solution for this is the Reply Mail that the person receives when sending a mail to abuse@isp.com (see Appendix A) Another big help with this problem is to publish recom mendations and FAQ (Frequently Asked Questions) on the homepage, where you explain why you need that particular information.

Nowadays we have reliable information of what customer has an IP -address at a given time. The problem we had with this before was due to a lack of documentation, this is now corrected.

We still receive quite a lot of Network Abuse cases. The difference now is that we have the capability, procedures and knowledge that are needed to handle this "downside" of Internet. The organisation it satisfied and we have received encouragement and appreciation from our management, the Swedish Police and our customers.

It took me about 6-8 months to get the team working properly with all the personnel and procedures in place.

Appendix A

Sample Reply Mail

---------- START of sample Reply Mail ----------
This is an automatic reply to confirm that your message has been received by SAMPLE_ISP Abuse & Security.

Your report must always include all relevant information. Log file from firewa ll or mail, IP-addresses, date and time (time zone) etc, so we are able to investigate your report. If you are reporting a netiquette violation, please don't forget to include a mail header or a log file, which we need to trace the incident.

SAMPLE_ISP ta kes all reported abuse complaints seriously, and will handle them in accordance with the User Service Agreement and Acceptable Use Policy, in a timely and efficient manner.

SAMPLE_ISP is dedicated to ensuring that its service is used in a manner that is consistent with the above policies.

Reports will be handled according to incoming date and we normally don't report back.

Best Regards
SAMPLE_ISP
Network Abuse & Security
Abuse@isp.com <<mailto:abuse@isp.com>>

---------- END of sample Reply Mai l ----------

Sample Warning Letter

---------- START of Sample Warning Letter ----------
[Name and Address of the customer]

Reference number:

This is a letter from the Network Abuse Department at SAMPLE_ISP
The function of the team is to prevent Network Abuse in SAMPLE_ISPs network.
It has come to our knowledge that someone connected to the Internet from your connection and your subscription, has been using the connection in a way that is not allowed according to SAMPLE_ISPs General Terms for private users.

The Network Abuse was of the following type:

Copyright violation

Copyright violation or un -allowed distribution of Copyright protected material, is according to Swedish law punishable and SAMPLE_ISP takes this type of violations very serious.

SAMPLE_ISP has received a report from [Universal Studios, Motion Pictures Associates etc] regarding Copyright violation:

[Include report from Universal Studios, Motion Pictures Associates etc]

Why this is of interest for you:

According to the General Terms for private users that has been signed by you, you are solely responsible for the actions that are taken from the Broadband connection in your home.
According to paragraph XX in the General Terms for private users, SAMPLE_ISP can immediately shut down the connection if a Network Abuse takes place from your Broadband connection.

If this is repeated SAMPLE_ISP may use its rights to terminate your subscription prematurely.
This would mean that the Broadband connection and the subscription are c losed without further notice.

For SAMPLE_ISP it is of outermost importance to protect our customer's security and integrity, we believe that this will in the end lead to a safer and more secure Internet for all of us.

If you would like to contact us rega rding this, send an e -mail to abuse@isp.com
Please provide the reference number above.

Regards

SAMPLE_ISP

---------- END of Sample Warning Letter ----------

Sample Network Abuse Policy

---------- START of sample Network Abuse Policy ----------

Sample Network Abuse Policy

Purpose of this policy
SAMPLE_ISP's purpose of this policy is to define what we consider as network abuse and what actions we may take to stop it.

Interpretation
Generally, conduct that violates Swedish law, reg ulation, or the accepted norms of the Internet community, whether or not specifically mentioned in this Policy, is prohibited. In addition to the legal issues, SAMPLE_ISP can in this policy impose further restrictions.
SAMPLE_ISP reserves the right at all times to disallow activities that damage its commercial reputation and goodwill.

General Security
Any "denial of service" attacks, any attempt to break authentication or security measures, or any unauthorized attempt to gain access to any other account, h ost or network is prohibited.

E-mail

1. Customer may not send unsolicited, commercial e -mail to any other customer account that has not specifically requested such information or that causes complaints from the recipients of such unsolicited e -mail. SAMPLE_ISP's services may not be used to send unsolicited advertising messages to other network Customers. Customer may not flood/Spam newsgroups with commercial or non-commercial postings.
2. Customers may not continue to send commercial e -mail to a recipient if recipient has requested that Customer discontinue such communication. Any use of SAMPLE_ISP's network for the composition, distribution, or collection of bulk e-mail, abusive e-mail, or any form of unsolicited, commercial e -mail is strictly prohibited.
3. SAMPLE_ISP prohibits the transmission of e -mail to recipients that is harassing, insulting, threatening, abusive or hateful.
4. The forwarding or propagation of chain letters of any type is prohibited.
5. "Mail-bombing" (i.e. flooding a Customer site with large o r numerous e-mail messages) is strictly prohibited.
6. Customers may not forge header information.
7. SAMPLE_ISP prohibits the use of Customer's account, or network connection, to collect replies of messages sent from any other provider that violate the rules of this Policy or those of the originating provider.

NEWS

1. SAMPLE_ISP may provide Customers with uncensored news feed. SAMPLE_ISP does not control newsgroup content nor is SAMPLE_ISP responsible for postings by SAMPLE_ISP's customers.
2. It is the responsib ility of those persons who post messages to determine a newsgroup's etiquette. Message posters are expected to submit messages relevant to the newsgroup's topic and not submit the same message to large numbers of forums or newsgroups.
3. Customers are prohib ited from forging header information and from posting chain letters of any type.
4. Customers may not cancel or supersede a posting of a message other than their own unless they serve as newsgroup moderators in the performance of their on-line responsibiliti es.

IRC (Internet Relay Chat)
Using programs that interfere with others' use, or running an IRC robot, on any IRC server is prohibited. When logged into any IRC server, users are expected to comply with the rules and policies established by the server's administrator.

Copyright Property
Using SAMPLE_ISP's connection to commit, or assist any violation of copyright law is prohibited.

Virus
Any use of SAMPLE_ISP's network for the composition, distribution, or collection of Virus or Trojan type programs is prohibited.

Publishing of Illegal Material
Publishing of any material that violates this policy, is offensive or that violates Swedish law is prohibited.

Consequences of Violation
Violation of this Policy by a SAMPLE_ISP customer may result in tempora ry suspension or permanent termination of service, at SAMPLE_ISP's exclusive decision.

Modification
This policy is maintained and updated by [Name].
This document may be updated without notice.

REPORTING AND ENFORCEMENT:
If you are aware of a potential v iolation of this Policy, direct information to abuse@isp.com

---------- End of sample Network Abuse Policy ----------

References:

MAPS – Mail Abuse Prevention System
http://work-rss.mail-abuse.org/rss/

ORDB – Open Relay Database
http://www.ordb.org/

Abuse.net contact database - Network Abuse Clearinghouse
http://www.abuse.net/lookup.phtml

Carnegie Mellon University Thomas A. Longstaff, James T. Ellis, Shawn V. Hernan, Howard F. Lipson, Robert D. McMillan, Linda Hutz Pesante, Derek Simmel "Security of the Internet" 1997
http://www.cert.org/encyc_article/tocencyc.html

Sally Hambridge RFC1855 “Netiquette Guidelines” October 1995
http://www.ietf.org/rfc/rfc1855.txt

Ripe Network Coordination Centre “R ipe Whois Database”
http://www.ripe.net/ripencc/pub -services/db/whois/whois.html

Asia Pacific Network Information Centre “Apnic Whois Database”
http://www.apnic.net/apnic -bin/whois.pl

American Registry for Internet Numbers “Arin Whois Database”
http://www.arin.net/whois/index.html

CenterGate Research Group “Geektools Whois Proxy”
http://www.geektools.com/cgi -bin/proxy.cgi

North Atlantic Internet inc. “Acceptable Use Policy”
http://www.naii.net/aup.html