

SECURITY THREATS AND TRENDS

MARCH 2007

SECODE AB

Secode helps companies and organizations gain insight, competence and thereby control over their operations from a complete IT security perspective. We deliver proactive and perpetual vigilance within two areas: 24/7 Managed Security Services and Security Consulting.

The Company was originally founded in 1986 as System Sikkerhet A/S, in Arendal, Norway. In year 2000, Secode AB was founded in Sweden and started its 24/7 Managed Security Services and Security Consulting. The two companies merged in January 2004, thereby forging the leading Digital Security Company in the Nordic region. In March 2006 the Finnish IT-security company Netsol OY (founded in 1996) was merged into Secode. From the first of January 2007 Secode has established sales-offices in both Denmark and the Netherlands and delivers IT-security services to customers in these countries as well. Secode helps many customers in private and public sectors, from seven different locations, using close to 85 security specialists. These specialists have long experience from building large computer networks and/or up-to-date IT security competence. Secode AB today has more than 100 employees.

All this together makes Secode the leading Northern European Digital Security Company within Managed Security Services combined with IT-Security Consultancy Services.

SUMMARY

The total number of reconnaissance attacks has shown a slight decrease during February. This may be due to the fact that February is a short month, and we may come to the conclusion that the traffic level has been pretty stable.

Focus of the Month takes a closer at the vulnerable society.

TABLE OF CONTENTS

1. INTRODUCTION	3
2. THREAT LEVEL	4
RECONNAISSANCE ATTACKS FEBRUARY 2006	4
TYPE OF RECONNAISSANCE ATTACKS	5
RECONNAISSANCE ATTACKS PR COUNTRY	6
INTERNET WORMS AND SPAM	7
3. ALERT STATISTIC	8
HANDLED ALERTS	8
REPORTED INCIDENTS	9
4. FOCUS OF THE MONTH – THE VULNERABLE SOCIETY	10
HISTORY	10
PRESENT DAY	11
OUR BIGGEST THREATS	11
SOURCES	12

1. INTRODUCTION

This report is based on three main parts; Treat level, Alert Statistic and Focus of the Month.

Threat level is a presentation of what threats organizations are exposed to through their Internet connection. In this threat evaluation, reconnaissance attacks from the Internet against customers of Secode are analyzed and presented.

Alert Statistic is based on alerts from Secode's IDS and IPS tools. An alert appear when a sensor recognizes network traffic that fit the implemented signatures/filters, and in these cases alerts will be transferred to Secode SOC (Security Operation Center). All alerts, both false and genuine, are manually handles by analysts at Secode.

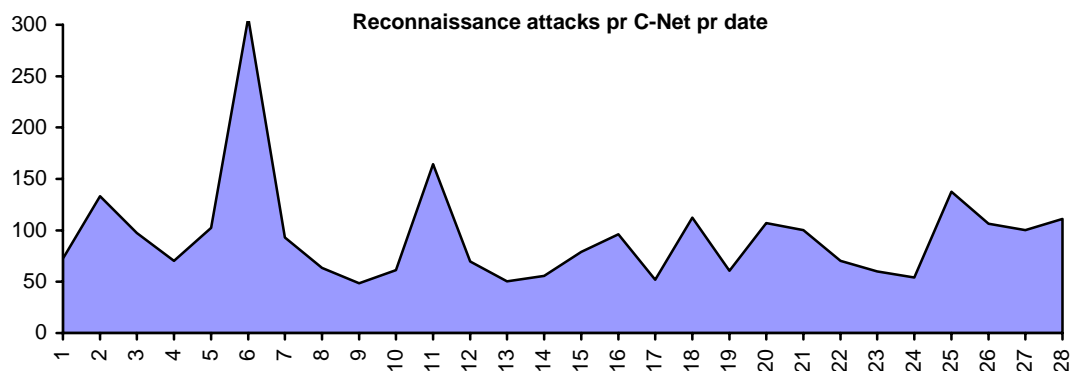
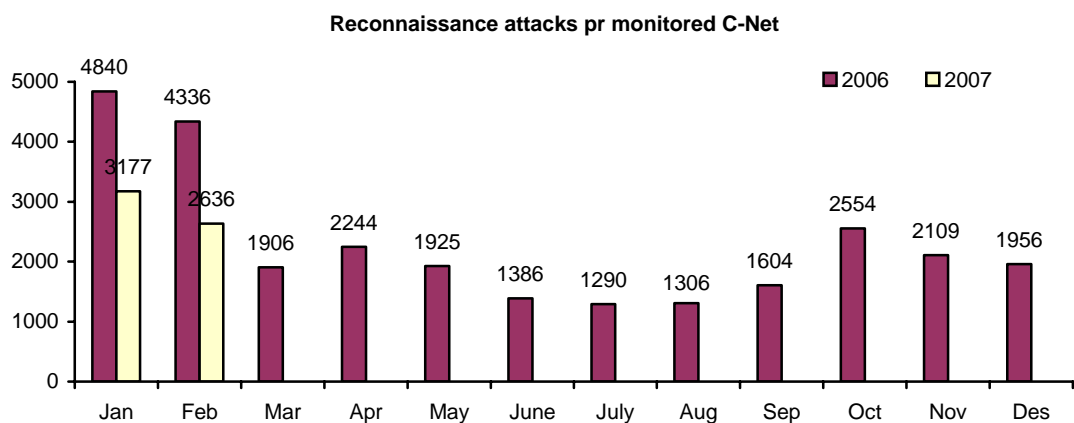
Focus of the Month is an article that focuses on relevant topics within IT Security. This might be topics discussed in media, incidents that can influence the threat level, or changes in the attack pattern from the Internet.

2. THREAT LEVEL

Due to high activity level, Internet worms and spamming are handled in a separate subchapter; "Internet worms and Spam", and are excluded from the other charts in this chapter.

RECONNAISSANCE ATTACKS FEBRUARY 2006

The statistics below gives an overview of the average number of reconnaissance attacks per network under surveillance. However, the activity level may vary from one network area to another. Despite these variations in the total activity level, we (mostly) register the same kind of attacks in different network areas.



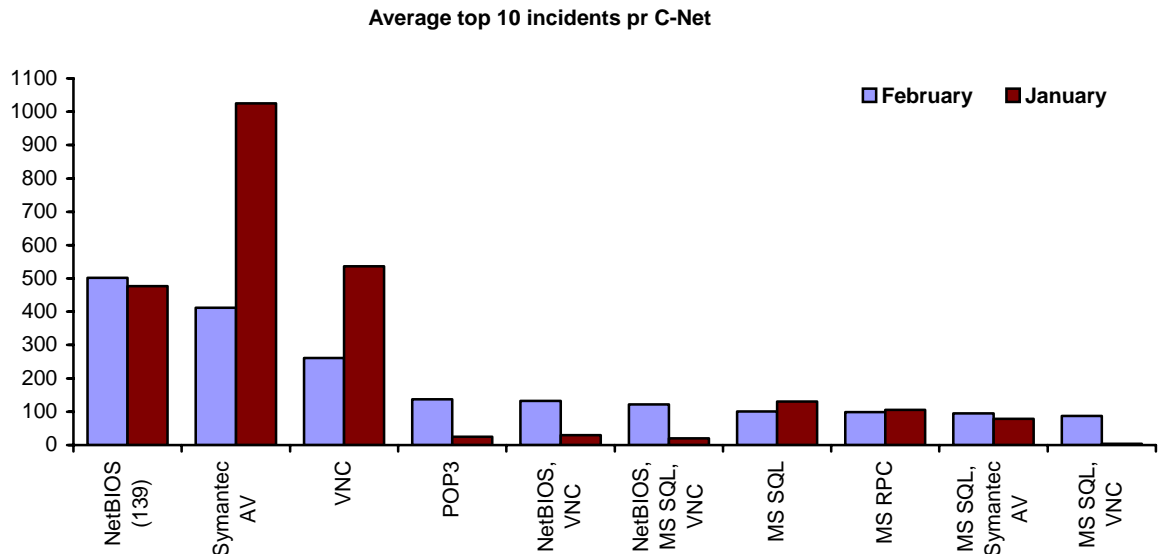
The total number of reconnaissance attacks has shown a slight decrease during February. This may, however, be explained by the fact that February is a short month. It is therefore very likely that the numbers of attacks are pretty stable.

This month the traffic towards SSC-Agent (port 2967) is starting to reduce to a normal level. There are still searches against this service, but we see a clear reduction.

There are no special attacks causing the peek around the 6th of February.

TYPE OF RECONNAISSANCE ATTACKS

The diagram below contains a summary of the most common reconnaissance attacks during the last two months, whether it is scans for one single service or combined scans for several services.



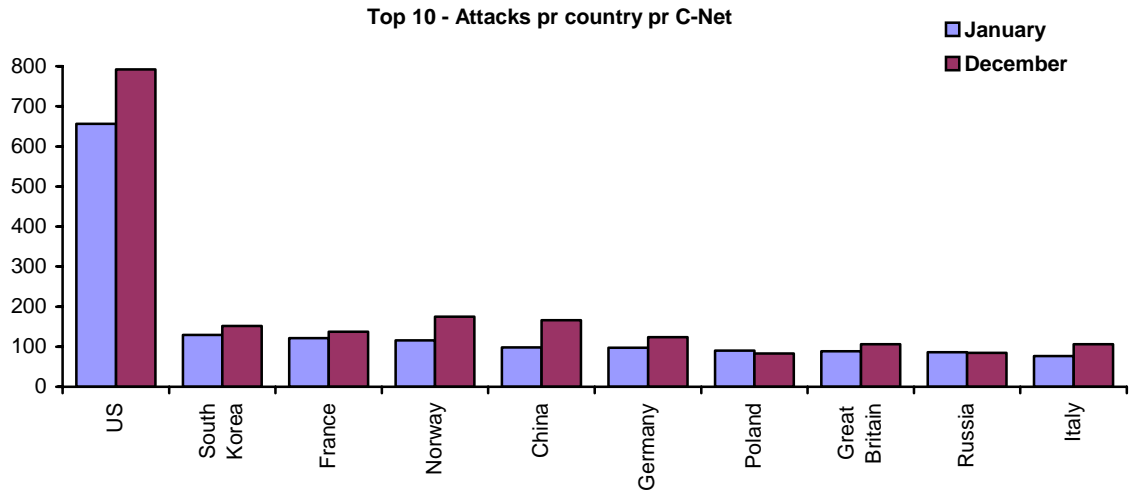
As previously mentioned, searches against port 2967 (SSC-Agent or Symantec AV) decreased heavily this month, and once again NetBIOS entered the top of the list. Searches against VNC have also decreased this month, but searches against VNC combined with other services increase quite a lot. Searches against POP3 are among the top of the list this period. This is due to three exploits on services using this port. The three exploits were one Axigen eMail exploit and two IMAP exploits.

In January vi had lots of searches towards port 2968, which we have not seen so much of this period. There are no big surprises on the top 10 list this period, as we have seen many times before.

All services have been at the top 10 list before.

RECONNAISSANCE ATTACKS PR COUNTRY

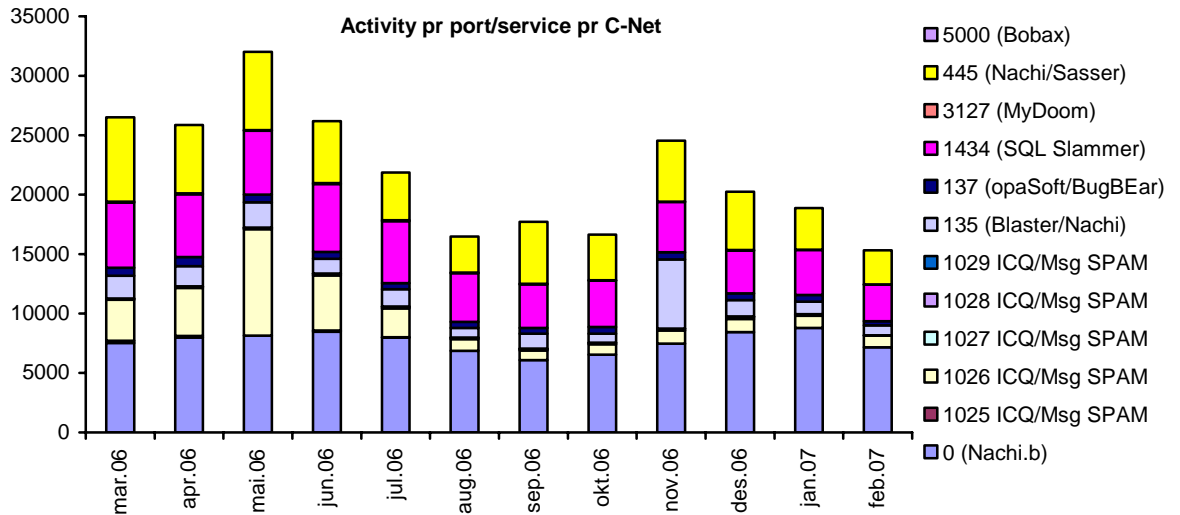
The malicious activity in the statistic below is mainly automated attacks, which comes from infected computers (e.g. Internet worms or viruses). This means that most of the attacks are not directly aimed, but are rather a secondary effect.



As in prior periods the US is the most aggressive source behind reconnaissance attacks, this month followed by South Korea and France. In this period there have been registered a decrease from most of the countries, which is most likely due to the decrease of searches against port 2967. These searches were basically the reason behind the general increase last week. It may also be due to the fact that February is a shorter month.

INTERNET WORMS AND SPAM

Because of a high level of activity against certain services, this traffic is presented in a separate statistics. This applies for those services which are most frequently targeted by Internet worms and spamming attempts.



The number of worms is still decreasing slightly this month. It is mostly traffic at port 0, 1434 and 445 which is decreasing, while the other categories remain stable. It is hard to pinpoint if this is due to a real decrease in traffic or if it is due to the short period we have put behind us.

3. ALERT STATISTIC

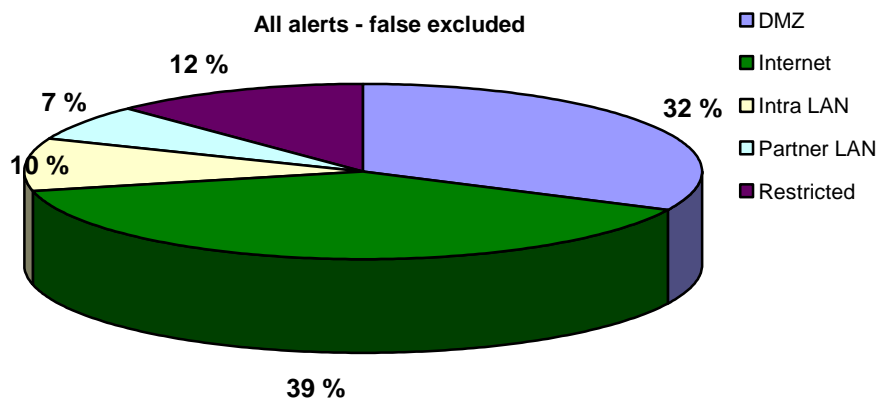
This chapter gives a summary of alerts from IDS/IPS sensors. These alerts are all analyzed by Secode SOC. The statistics shows the distribution of alerts per net segment that are under surveillance.

HANDLED ALERTS

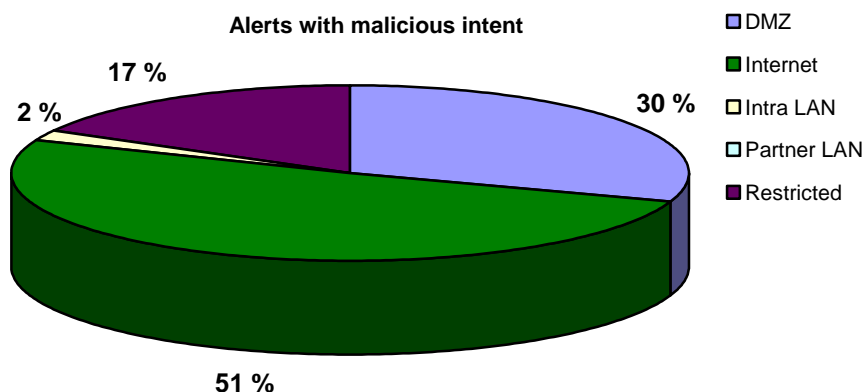
The statistics below shows handled alerts distributed at the different network segments where Secode's measuring points are placed.

The network segments are divided into the following:

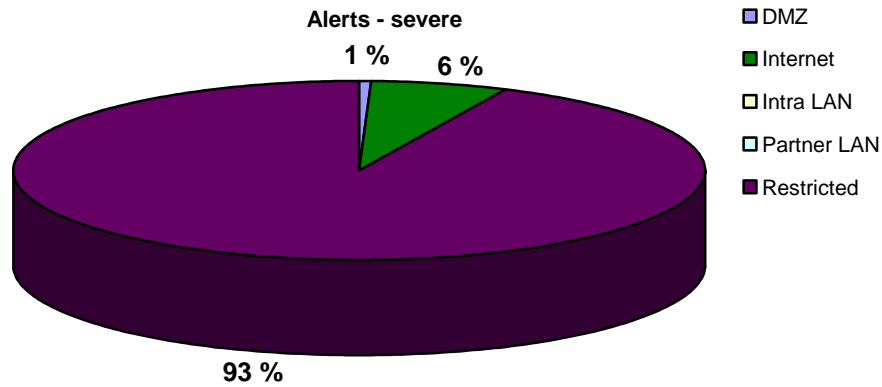
- Internet: the measuring point is located outside the firewall on a network exposed to the Internet
- DMZ: the measuring point is placed inside the network and monitors traffic against services that are exposed to Internet or other unsafe, external networks
- Intra LAN: the measuring point is placed inside the network and monitors traffic between clients, servers and other network equipment
- Partner LAN: the measuring point is located in an environment that is used for communication towards external partners. The partner LAN is without Internet access
- Restricted LAN: the measuring point are located in a limited environment with a very well defined traffic pattern and without Internet access



The diagram above shows the distribution for all genuine alerts.



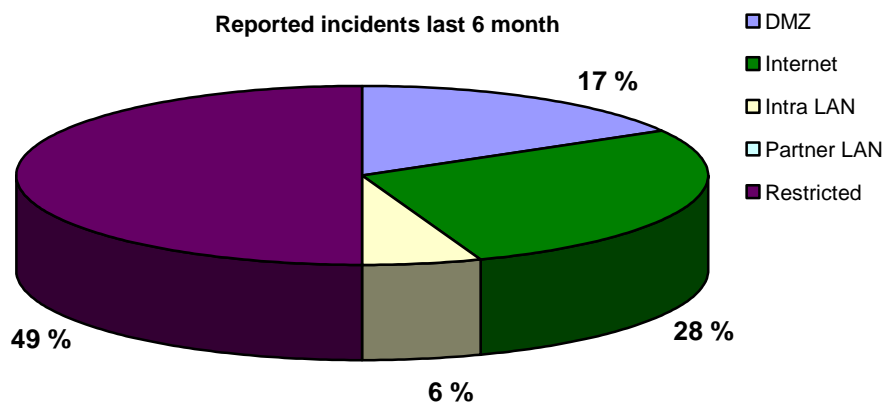
The diagram above shows the distribution for all alerts caused by activity with malicious intent, without the customer necessary being vulnerable.



The diagram above shows the distribution of all alerts caused by activity with malicious intent, and where the customer might be vulnerable or compromised.

REPORTED INCIDENTS

The statistic below shows distribution of incidents reported to customers of Secode the last 6 months.



4. FOCUS OF THE MONTH – THE VULNERABLE SOCIETY

This month's focus will analyze how the society makes itself more and more vulnerable, and how this makes cyberterror and other threats to computers and other technical machinery more severe than ever before. Even though we are very vulnerable through our network and computer uses, the most vulnerable part of society is indeed the electrical network. However, I am not an electrician, so I will not discuss that part of the aspect in this article.

HISTORY

To understand how vulnerable we now are, we have to look at the history. Keep in mind that I am not an historian either, so this is pretty abstract.

About 100 years ago, they could not in their wildest imagination predict how society is build today. Electricity was not a normal part of the everyday life, it was not possible to get electricity out to all. The telephone was only for the few, some had never heard about it, and the idea of the telephone being mobile was radical. Handwriting was still the main way of getting words on paper, even though the typewriter had been available in some sort for a while.

The society at that point was not at all as vulnerable as today. They did not rely on electricity, because many did not have any. Most industries were still based on power from steam, horsepower, and manpower and so on. Their communications was mostly by postal services or it may be by telegram. The society was "slow". You could not work as fast as today, because you could not get your products out any faster than a horse managed to carry it. In short, you relied on yourself and not everybody else.

50 years later the electricity was in use at most industrial factories, and the telephone was in use for long distance calls. Cordless phones were not far from being introduced. Typewriters were the main way of getting words on paper in several businesses. And at this point a machine doing calculations had been introduced already, in 1943. This "calculator", which is considered the first electronic computer, occupied about 1800 square feet (60 square meters) and weighed almost 50 tons. About ten years later the first IBM computer was introduced, the IBM 701.

In the fifties and sixties we started to make ourselves more vulnerable, by making ourselves dependent on other parts of society. For instance, it was most unlikely to have one steam-engine or similar power source in every industrial hall. Instead there was a power plant nearby giving several industrial halls energy to power their machinery, or their machinery was powered by gasoline. This made the factories dependent on power deliveries. Communication started to be done more by phone, which made them dependent on the telecommunication company. Deliveries were made mostly by car and trucks, which made them dependent on gasoline and road development.

10 years ago we started to really see the blooming of our modern society. Everything that needed power was given it by electricity or gasoline. We started to use mobile phone more. The telephone at home was still in use, but needed to give room for Internet over the telephone lines. The typewriter was more or less replaced by a personal computer at every workplace, and the personal computer started to make a big entrance into people's homes. We had started to make the society technical.

PRESENT DAY

Today we are more technically dependent than ever before. There are many buildings and houses that have only electricity as a heating source, including hospitals and nursing homes. We do not know how to travel from A to B anymore without car, plane or other motor vehicle, because the distances are too big. Actually many stores are placed at somewhat decentralized locations, only available by car. We rarely use cash, we use credit cards instead. Most of our banking is done by Internet, several banks does not even have a physical location available for there customers. Every cash register is now connected to Internet so the transaction is registered at a server at once. Some stores do not have their product prized in store, only on a server available by Internet.

Our technical dependence is growing bigger everyday. Even building constructors, plumbers, carpenters and so on are dependent on technology today. Everything, and I mean everything, will be handicapped by loosing the ability to connect to the Internet.

To make it easier to understand how dependent we are, let's do a mind experiment. It is an ordinary day in your life as an employee at an insurance company. You start your day as any other day, by having some breakfast, taking your car to work and start working. Let's say that you are working with some kind of insurance analysis. After a couple of hours you start having problems with your computer, and soon it becomes known that a computer virus is starting to spread throughout the network. All server connections are being closed from the different workstations. At this point you are not allowed to do much more then work at the files that are not infected, and all files you need to do your work is located on a fileserver. You contact the IT-department at your company to find out how long you have to wait, and get the understanding that you can not enter the server until the next day. You decide to go home early. At the way home you stop at a gas-station to get some gas for your car, but they are not able to accept credit cards due to a computer error. You do not have cash but are pretty sure that you can get home with the gas you have. On the way home you stop at the store trying to buy some dinner, but they can't accept card either because their Internet connection is down, so you leave the store with nothing to eat.

This is only one example of how a day may become for one person. Just imagine how it would be if 10 000 were affected by something like that. Or let's say that the infrastructure for Internet and telephone is destroyed in a whole city. What would happen then? This is not that likely, but we have made our lives more dependent on the technological infrastructure and less dependent on nature and what that may give us.

OUR BIGGEST THREATS

There are many threats that may leave part of society hurting. I will not even try to cover all here. The most common attacks that are deployed towards computers are all capable to bring a firm or a bigger part of the society down on their knees. Here is a short description of some of them:

Cyberterror

This is most likely the most dangerous kind of attack. The attackers behind a cyberterror attack are not attacking to make money, but to pursuit a goal that are political, religious or ideological. The definition of cyberterrorism is wide, and all destruction of digital property may be an act of terrorism if it is done with the intent to pursuit a goal as described above. In other words, spam, virus, cross-site scripting and so on may be used as an act of cyberterror.

Cyberterror support is a relatively new definition that includes "unlawful use of information systems by terrorists which is intended, by itself, to have a coercive effect on a target audience. Cyberterror support augments or enhances other terrorist acts."

Cyberterror may be small acts, like cross-site scripting, or something severe, like interrupting an airplane instrument and making it crash.

Spam

Spam is something that everyone that have an e-mail account have become used to. But except for the annoyance of having spam entering your computer at all times, many people do not see any problems with it. Actually this has become one of our biggest problems today. As our e-mail servers is literary spammed with unwanted e-mails, our e-mail servers and spam filters are having troubles with keeping up. As our mail servers are filled with spam it causes problems for other e-mails to pass through. In other words, spam makes communication more difficult.

Virus

Viruses has reduced to a minor threat during the last couple of years, as many antivirus companies have become better at developing signatures at a short amount of time. However, if a virus is capable of spreading fast and are "lucky" to get pass the antivirus software, a virus may do some serious damage. Several computers may be infected in almost no time, and this will leave a company hurting.

Trojans

A Trojan is a synonym for backdoor. If there is a backdoor in a system, almost anybody with some knowledge about computers and the backdoor may enter it, and make some serious damage. There is a huge number of Trojans arising every day all over the world. That makes it difficult to stop this problem.

Hackers

There a still some hackers out there, dedicating their lives to make it difficult for companies, or selling company information to others. Dependent on the malicious intent from the hacker this may be damaging for a small part of the society or for a bigger part.

Cross-Site Scripting and Phishing

Redirecting websites to other sites with malicious intent has become more and more of a problem. Phishing sites are used to get personal information from users of a banking system or similar and cross-site scripting are mostly used to get a statement out to users. Cross-Site scripting is often used to cyberterror.

There are many more aspects, and I may give examples for every part of it, but the conclusion is that as we make ourselves more dependent on technical systems, the threats are growing bigger and stronger.

SOURCES

Computer Hope.com:

<http://www.computerhope.com/history/194060.htm>

Wikipedia - Telephone

<http://en.wikipedia.org/wiki/Telephone>

IBM 701

http://www-03.ibm.com/ibm/history/exhibits/701/701_1415bx01.html

Cyberterror – Prospects and Implications

<http://www.nps.navy.mil/ctiw/files/Cyberterror%20Prospects%20and%20Implications.pdf>