Internet filtering and how it affects security, efficiency and thriving in Norwegian companies

Joachim Deisz

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2005

The MSc programme in Information Security
is run in cooperation with the Royal Institute
of Technology (KTH) in Stockholm.

Institutt for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Preface

The work with this thesis started last autumn, when I desperately tried to conceive an idea for a topic worth investigating. At the time I was using a computer in a company network which had an Internet filter installed, and for some reason I was often blocked when I tried to enter websites related to computer security and hacking. I asked myself why this happened, and if the employees in that company felt as frustrated as I did. And so the idea for this thesis was born.

Since then, the work has progressed by fits and starts. As must be expected, I encountered some snags along the way, and at one point actually started looking for alternative topics. Due to what I now believe was a misunderstanding, I got the impression that my project would be rejected because it focused too much on the sociological aspects of information security, an aspect that I for one believe is crucial. I was also a little disappointed with the filter vendors, who was reluctant to contribute in any way, or who never delivered what they promised. Apart from this, the project has been an enjoyable and instructive experience.

I would like to thank the good people of the participating companies and organisations for their time and effort. You know I cannot publish your names, so I have to express my gratitude without giving you formal credit in this report. Thanks for all your help; I could not have done this without you.

I would also like to thank Frode Volden for his assistance with the statistical analysis; Henning Gravnås for excellent opposition; my friends and family for letting me use your connections and resources; and Ingvild for her support and advice through my ups and downs. Last but not least, I shall thank my teaching supervisor Slobodan Petrovic for helpful hints and ideas, and for boosting my effort.

Abstract

In this thesis it has been investigated if and how Internet filtering can contribute to security in networks, and if filtering affects thriving and efficiency in organisations. It has been used a mix of qualitative and quantitative methods, mainly making a theoretical fundament supported by experiments and surveys. The project has provided knowledge about filtering techniques to assure that the reader understands the following discussion and argumentation.

Investments in Internet filtering and other content control mechanisms are expected to increase significantly in the future. What the filtering companies think about their own products is well known, but few objective, systematic investigations and quantifications of filter's contribution to security are done. Also, little is done to find out how an organisation reacts to "babysitting-ware". Traditional security measures like firewalls and antivirus software are directed towards external threats, whereas Internet filters are aimed against internal behaviour. Software or policies that influence on personal freedom and obstruct the workflow may have adverse effects on thriving as well as efficiency, although the filter vendors claim the opposite. This thesis provides answers on how filtering provides protection from some Internet based threats, while it disqualify filters as a countermeasure against e.g. phishing and most malware. We have also surveyed Norwegian companies to see how filtering affects job satisfaction and efficiency, and the conclusion is that filtering in fact is threatening both.

Keywords for this thesis are Internet filtering, work efficiency, electronic monitoring, Internet surfing habits and job satisfaction.

Sammendrag (Abstract in Norwegian)

I dette prosjektet har vi undersøkt hvordan internettfiltrering kan bidra til øket sikkerhet i nettverk, og hvordan internettsensur påvirker organisasjonen sosialt. Vi har valgt en blanding av kvalitativ og kvantitativ metode, der vi stort sett har laget et teoretisk grunnlag for konklusjoner og støttet disse med kvantitative eksperimenter. Vi har gitt en innføring i de tekniske aspekter ved filtrering slik at alle lesere skal ha gode forutsetninger for å forstå diskusjonen og konklusjonene.

Det er ventet at investeringene i Internettfiltre vil øke betydelig i årene fremover. Vi vet en del om hva produsentene av slike filtre mener om sine egne produkter, men mener det mangler en objektiv gjennomgang av hvordan filtre kan bidra til sikkerhet i nettverk. I tillegg er det etter vår mening gjort lite for å finne ut hvordan ”barnevaktprogramvare” påvirker organisasjoner. Mens kjente sikkerhetsprodukter som brannmurer og antivirusprogramvare er hovedsakelig rettet mot angrep utenfra er Internettfiltre hovedsakelig et mottiltak mot uønsket intern adferd. Programvare eller retningslinjer som begrenser personlig frihet kan ha negativ innvirkning på både effektivitet og trivsel, i motsetning til hva filterprodusenter generelt hevder. Denne studien viser at filtre kan ha en gunstig effekt i forhold til enkelte Internettbaserte trusler, men at de ikke beskytter mot for eksempel ondsinnet programvare eller phishing. Rapporten konkluderer også med at Internettfiltre kan redusere både effektivitet og trivsel i organisasjoner.

Table of contents

List of figures

List of tables

1 Introduction

We know that security may be in conflict with efficiency, personal freedom and flexibility, but also that at the same time those goals cannot be achieved without a certain level of security. Decision makers and those responsible for IT-security will always try to balance the need for security against other goals of the organization. This analysis of cost-effectiveness permeates the decision-making process when new security measures are considered or existing solutions are evaluated. After all, the main motivation for improving security often is to secure profits.

To make the best decision it is imperative to collect all relevant facts. Relevant facts in this context may be potential threats to security, the expected contribution to security, and costs connected with the implementation. Actual cost is more than procurement, licenses, and other easy quantifiable variables; there are abstract costs to be considered as well. Changes in efficiency, distrustfulness towards the motivation of implementing a measure, and reduced employee satisfaction are among factors that can tip the scale when a security measure is considered. However, there is little knowledge on these abstract factors compared to the easily accessible monetary costs, even though they may have an influence on the profitability of the investment. Also, the benefits of any security measure are vigorously advocated by vendors and security consultants, so the basis for a decision may be skewed.

The purpose of this thesis is to assess some of the abstract factors in connection with installation of an Internet filter, and to give a sober evaluation of the benefits of this security measure. This will hopefully provide to a more complete foundation for decisions.

1.1 Reading guide

Before we continue we shall give a short introduction to the chapters of this report. This guide will make it easier for the reader to navigate through the chapters and locate areas of special interest.

Chapter 1 consists of an introduction to this report, an introduction to the area of interest, the motivation for this thesis and a presentation of the research questions that will be answered by our research.

Chapter 2 introduces the reader to previous work done in areas related to our research questions.

Chapter 3 gives a technical introduction to Internet filtering. The chapter provides “nice-to-know“ information, but may be skipped by readers who feel updated on filtering technology.

Chapter 4 explains and describes the research methods that are chosen for our research. We also discuss ethical questions and possible implications of our experiments.

Chapter 5 gives a more detailed explanation to the methodology of questionnaires, and describes our survey and some experiments we carried out in connection with our research.

Chapter 6 contains a qualitative assessment of Internet filters that will form the basis for later experiments.

Chapter 7 presents the results of experiments and the survey. The results are interpreted and discussed.

Chapter 8 presents the conclusions of our research.

Chapter 9 discusses areas of our research that should be refined or explored further, and proposes ideas for further research.

Chapter 10 lists work and resources we have quoted or referred to in the report.

1.2 Background

The Internet and other computer networks are increasingly more important channels of communication and information dissemination. In 2004, 84% of Norwegian companies were connected to the Internet [SSB1]. This survey included a selection of all companies with more than 10 employees, which means that industries where few of the employees normally spend time in offices – for example transport, craft industries, fisheries and so on – probably drag the numbers down. In finance, engineering, public administration and other "indoor trades", the share of companies and employees with access to the Internet might be closer to 100%.

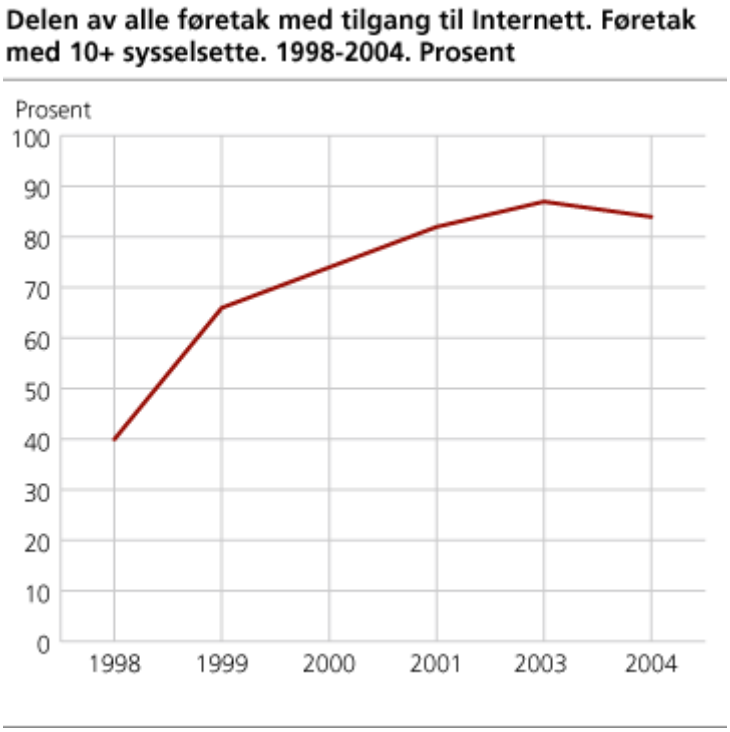

Figure 1 - Companies with access to the Internet [SSB1]

The number of threats on the Internet is also increasing. According to IBM Global Business Security Index [IBM, 2004] 28,327 new viruses were discovered in 2004. This is an increase of 25% from 2003, raising the number of known viruses to 112,438. In the same period phishing[1] increased with a staggering 5000% [IBM, 2004]. Traditionally, viruses and other malicious software (malware) have been hiding in attachments in e-mails, and the receiver had to do something actively - like opening a file or running a program – to get infected. IBM states that those days are over as hackers have discovered new vectors of attack, such as malicious code embedded in JPEG and BMP pictures [IBM, 2004]. The unlucky user can get infected with viruses or Spyware[2] just by visiting a website with hacked or intentionally prepared images. Today, attackers focus less on servers – which are often very well protected – and more on clients. The clients are now powerful machines, and often connected to

[1] E-mails containing a link to a fraudulent Web site, for example asking the receiver to give away their username and password to a site for "maintenance reasons"

[2] Software that covertly gathers user information through the user's Internet connection without his or her knowledge

the Internet via a broadband connection, thus an attacker can gain access to considerable resources without beating heavily defended servers [Telenor, 2004].

We have several means of detecting, containing and deleting malware. Antivirus software detects and deletes known viruses and other malware in computers; e-mail cleaners detect and delete known viruses in e-mail; firewalls can stop excessive traffic generated by worms; and intrusion detection systems (IDS) can detect traffic generated by unknown viruses not killed off by antivirus software. But these are all "fire-extinguishers"; they cannot protect the systems before they are exposed to the threat. Also, virus protection in general can only remove known malware. New and metamorphic[3] viruses cannot be recognized before the antivirus companies update the software, and the viruses therefore have a window of opportunity to infect computers and bring IT-systems down. Even a stateful firewall cannot stop a user from deliberately but unwittingly initiating a download of a picture, a media file or a webpage.

"Internet filtering is software that identifies, categorizes[4] and manages Internet content" (IDC). The software is usually situated on a server between the workstations and the firewall, and filters traffic to and from the Internet. To learn more about this, read Chapter 3 Technical Aspects. Internet filtering is sometimes called "web filtering", "URL filtering" or "Employee Internet Management (EIM)". We shall use all these terms in this report to improve the rhythm of the language and make the thesis easier to read.

Internet filtering is a relatively uncommon technology in Norwegian companies and organisations, but if we follow the international trend as predicted by IDC, investments in such technology will have an annual growth of 23% in the period 2002-2007 [InSe, 2003]. This means that restrictions on web surfing will be introduced to a number of Norwegian employees in the next few years.

1.3 Research problem

Some security mechanisms - like firewalls, e-mail cleaners, antivirus software, and intrusion detection systems - fight infections or prevent them from spreading. Internet filters on the other hand, can prevent users from ever coming in contact with the source of malware - for example an untrustworthy website - and stop unwitting users from getting infected in the first place. This is clearly an advantage, as many security measures only protects against known attacks, but it seems we do not know enough about how a pre-emptive mechanism will add to security, and which classes of attacks can be avoided. It is also possible that Internet filtering contributes to security in other ways than preventing infections, and this should be investigated further.

Apart from Internet filters, the security measures listed above are installed to protect the companies and the employees from external attacks or threats. They are therefore presumably not likely to raise internal controversy. Internet filters, on the other hand, are directed towards unwanted internal behaviour as well as to prevent certain threats. Employees may feel that this is in direct conflict with their personal freedom. We suppose that most people do not like to be under surveillance or to have new rules imposed on them, and then the implementation of a new security policy or a new security product may decrease employee satisfaction and motivation. If this were the case, we would be interested in more knowledge about how Internet filtering affects thriving and work morale.

[3] Code that change itself a little for every new generation

[4] The process of analysing the content of the webpage and deciding on the nature of that page. Pages of a similar nature are put in the same category or class of pages. Examples of categories can be "Adult content" and "News".

The hypothesis that form basis for this thesis is that employees would prefer to have unobstructed access to the Internet and as much privacy and as little surveillance as possible. We suppose that some employees are actually obstructed by the Internet filter, and perhaps experiences decreased efficiency because of this. We also assume Internet filters can add significantly to security. We shall try to provide more knowledge on these subjects with this thesis.

1.4 Justification, motivation and benefits

For all security requirements, one should perform a cost/benefit analysis. In some cases, this cost/benefit analysis can be limited to the direct economical costs of procurement, implementation and management, weighed against the potential losses if a security incident should occur and the probability of that happening. But most often, costs are not only the investment costs but also the indirect costs on performance and user friendliness [Ølnes, 1995].

Some researchers believe high employee satisfaction has a positive influence on stress, learning abilities, absence due to sickness and company turnover [Luthans, p. 129-130], and we therefore believe it will be interesting to establish if filtering has adverse effect on thriving. This survey should provide a broader understanding of how Norwegian employees react to Internet filtering. Hopefully we shall also be able to find out if and how much filtering adds to security and efficiency. Together, these facts will be useful to companies who consider installing an Internet filter and want to know both the positive and the potentially negative effects of that investment. This knowledge can also help direct scarce funds for security to the security measures that give most security for the money.

We believe that IT-management, Internet filter vendors and HES[5] departments are most likely to benefit from this survey.

1.5 Research questions

1.5.1 What impact will the filter have on work-efficiency?

One of the most important selling points of the filter vendors is that Internet filtering reduces cyberslacking and increases employee efficiency. As stated above, Internet filtering may have an influence on satisfaction, and thereby efficiency. But we have a more technical issue to address as well; will an Internet filter make employees use the network less for non-work related tasks so that Internet filtering can be said to improve availability. If employees spend less time surfing the web and do not download streaming media or large media files because of a filter, this increases the bandwidth available for business related use of the network. Another aspect is the *time* spent on private tasks on the Internet. This is not directly related to security, but it can certainly be an important aspect when a company wants to know if their security investment is worth the money. In that respect this is a natural part of the thesis.

Efficiency is more than the absence of slacking. In Chapter 3, we shall see that Internet filters are riddled with false positives, which in this case means that webpages the employees need may be blocked. The Internet is a powerful tool in research, trading, communication etc., so some employees or companies might actually experience decreased efficiency if they are deprived of access to this resource.

[5] Health, Environment, Security

1.5.2 What is the attitude towards Internet filtering among Norwegian workers?

To see the whole picture of Internet filtering related costs it is vital to find the possible downsides and drawbacks of the system. Examples of drawbacks are decreased job-satisfaction and distrust between employees and employer. Filtering may at the same time have a positive effect on thriving at work, for example because employees enjoy a porn-free environment or an increased feeling of safety.

By assessing their attitude towards Internet filtering we shall establish if there is any reason to believe users also experience reduced thriving at work because of the filter.

The feeling of being monitored is also of importance here. Broad research has concluded that monitoring at the workplace impairs efficiency and thriving and enhances stress, especially with those who do creative or difficult tasks [AT], [Aiello, 1993]. Aiello and Svec [Svec, 1993] claim that computer monitoring impairs complex task performance, and go as far as to recommend that monitoring should never be used. Chalykoff and Kochan [Chal, 1989] have argued that employees' satisfaction with computer-aided monitoring has a large impact on overall job satisfaction. Most of this research discusses performance monitoring - not Internet filtering specifically - so the results cannot be transferred directly to this thesis. But if we take all this into consideration, it seems likely that Internet filtering can have adverse affects on work-morale if the employees look upon it as a surveillance-system.

1.5.3 What impact does Internet filtering have on security?

We want to know if security increases significantly when an Internet filter is installed. Most of the general research that has been done on Internet filtering seems to have been carried out by the Internet filter vendors themselves, or on behalf of the vendors. The results of such research are questionable, simply because the researchers have a strong interest in the outcome. A thorough analysis of the system and the attacks it protects against has as far as we know not been provided, even though this is absolutely necessary to do a cost benefit assessment. We shall provide such an analysis, and use it as a platform to show how filtering can improve security in networks.

1.6 Summary of claimed contributions

This research will contribute in three areas: (1) the thesis will give a quantification of how filtering affects work-efficiency; (2) the thesis will give new knowledge on the attitudes towards and views on Internet filtering in Norway; (3) we shall provide a quantitative assessment of Internet filters' contribution to security in networks based on a qualitative analysis.

Together, these results will provide a broader understanding of how this particular security measure affects an organization.

2 Previous Work

In this section we shall present previous work that can help us answer the three research questions asked in Section 1.5, or that will contribute to the research.

Internet filtering appears to be an area of less interest to researchers than for example virus-control or firewalls. This may be because Internet filtering is a relatively new area of security, not really evolving before the Internet spread wide enough to constitute a profitable market. For example, the alleged market leader [SecLab, 2004] Websense was founded as late as 1994. Most of the previous research we have found is from the year 2000 or later, although R.P. Weber wrote "Basic content analysis" as early as before 1990.

2.1 What influence will the filter have on work-efficiency?

Much work is done in this area, but unfortunately most of it is done by the companies that produce Internet filters. Whitepapers [web@work, 2004], [Davies, 2001] and [SecuComp, 2005] all conclude that cyberslacking[6] is a major problem in most companies, and that Internet filtering will improve efficiency significantly. [Young and Case, 2004] bases their work on statistics showing that 37% of American workers surf the Internet constantly at the job, and that more than a half of them often use the Internet for private purposes at work.

Even though these surveys may have reached correct some conclusions, we feel that the question should be investigated in an independent survey like in our research.

2.2 What is the attitude towards Internet filtering among Norwegian workers?

We have not found any research specifically targeting Norwegian workers, but some research is done in other countries. Attitudes can vary much from country to country, but research done on other cultures may still provide some answers or support our research.

[Witty, 2004] sought to find how Australians felt about restrictions on private use of e-mail and Internet in the workplace, and in which cases filtering would be appropriate. The respondents were mainly collected via discussion-groups on the Internet and Australian websites, so the survey does not claim to represent the mean of the population. Both qualitative and quantitative data were collected. Some of the more interesting findings of the survey were that:

- 62% of the respondents meant that offensive material on the Internet should be banned in the workplace, but only 37% wanted their employer to use Internet filtering to do this.
- Those who spent the most and the least time on browsing were the strongest antagonists of filtering.
- Employees in networks without filter were more sceptical towards filtering than employees who used a filtered network.
- The respondents widely accepted that some categories of websites were blocked. 61% felt that offensive material should be blocked, but only 3% wanted to block entertainment and news.

[6] Wasting work time on private browsing, chat etc.

Witty's work can perhaps provide an explanation to some of the findings in our survey, and be a useful reference in our thesis.

Another useful piece of work is [Panina, 2004], which suggests that cross-national institutional differences lead to different management systems in different countries. Cross-national dissimilarities in institutional environments are likely to create management control practices that will vary from country to country. Employee-oriented management practices specifically are prone to effects of national institutions because strength of labour unions and national labour regulations vary widely. Thus, electronic productivity monitoring is particularly sensitive to nationally idiosyncratic institutional pressures. A monitoring scheme – for example an Internet filter - that works perfectly in one country or system may be controversial somewhere else.

Panina and Aiello operate with five dimensions that affect the acceptance of electronic monitoring among workers:

- Individualism/Collectivism
- Uncertainty Avoidance
- Power Distance
- Masculinity/Femininity
- Confucian Dynamism

From the work of Panina and Aiello we can derive that Norway is a fairly individualistic, feminine country with generally low power-distance. Thus, Norwegian workers should be more likely to accept electronic monitoring if the purpose is personal development or improvement of the quality of life at work, and if it measures group level performance rather than individual behaviour. Employee-participation in the implementation of electronic monitoring is also believed to diminish opposition against it. The paper cites European research which shows that monitoring is now more accepted due to an increased understanding of its importance to security and efficiency, so the opinion on monitoring might change.

In our survey, we ask the employees what motivation they believe the employer had to install filters. If there is significant correlation between the answers to that question and other trends in the statistics of the survey we have conducted, Aiello's and Paninas' work may offer an explanation.

2.3 What impact does Internet filtering have on security?

[Neumann, 1989] proposes a general classification of various computer misuse techniques and is meant to cover all possible attacks that exists or may be invented in the future. The classes should be viewed as conceptual; they were developed back in the eighties when some of today's threats against IT-systems were not thought of. The classes still apply, since new attacks fit into these superior categories. Neumann's classification will form the basis for our theoretical work on security provided by Internet filters in Chapter 6. We will discuss possible attacks belonging in each class, and if Internet filtering can provide protection against them.

We have not found much work about security provided by Internet filters, at least not work we find trustworthy. It seems most of the work done in this area is of the white paper nature. For example, [Winproxy, 2005] suggests that Internet filters can prevent both spyware installation and communication, but does not cite experiments or research to support their claims. [Websense] claims that Internet filtering will "reduce bandwidth consumption significantly" and that a filter may save the company from spending unnecessarily large funds on their network connection.

Some work are done concerning Internet filters meant for schools, private homes, libraries etc. [Resnick et al, 2002] found that restrictive filters were only a little more effective at blocking pornography than liberal filters, but that they decreased the availability of non-pornographic websites.

Our thesis concentrates on filtering solutions for corporate networks, so that work will not be used here.

3 Technical aspects

In this section we shall describe the techniques and technology used in Internet filtering. We feel that this is important to understand the discussions and argumentation in chapters 6 and 7, especially the parts about false positives and updating of the filter database. If the reader already has a good understanding of Internet filtering, this section may be skipped.

3.1 How sites are categorised

A number of techniques and clues are used by Internet filter producers to identify the nature of a website. The following list of such techniques is not exhaustive, but it covers the most important areas of categorisation.

Keyword analysis: One way to determine which kind of website we are dealing with is to consider the text or language on the pages. Certain words and phrases are believed to be specific to a genre, for example pornographic and gambling sites. The earliest filters used "unintelligent" keyword filtering, resulting in numerous false positives. A ban on the word "sex" would for example block pages of educational or medical nature.

Most Internet filters divide web pages into many categories of content, for instance SurfControl has 147, ranging from "Religious" to "Violence". While it is easy to establish that a webpage containing the text "18+ WARNING this website contains adult material!" is of a pornographic character, using text to distinguish for example between the categories "Abortion - pro life" and "Abortion – pro choice" (Websense) can be very difficult. To find the finer nuances in a chosen text, Bayesian filtering can be used. Simply put, Bayesian filtering is the process of utilizing a specific statistical method called Bayesian to classify documents into categories [Bolstad, 2004]. Particular words have a known probability of occurring in webpages of a certain category. This probability is derived from historical statistics as well as the current situation, and new words can be added to the list. The more words in the text we can attribute to the specific category, the more likely that the webpage itself belongs to it. For example, the word "beaver" can be used in many contexts, but put together with the words "dam", "stream" and "timber" it is probably used about animals, not a beard or the female sex.

Support vector machines (SVM) can also be used for statistical analysis of text. A vector machine is a set of algorithms designed to classify a set of values (e.g. a text). The algorithms are supposed to "learn" by viewing several examples of input-output (text and category), and then create or approximate a function that can be used to classify new inputs (text) [Taylor, 2000].

The Internet is global; there are websites from all parts of the world. This means that keyword filtering algorithms must understand several languages. Luckily, almost all Internet sites are in one of the 30 top languages, with English as the far most popular. The statistics varies a little, but the general picture is that 99% of all webpages are written in one of the 30 most common languages, and that the top five languages (English, Japanese, German, Chinese and French) cover 90% of the Internet pages [Vila]. The market leaders in Internet filtering all claim to analyse multiple languages when they categorise sites, but the number of languages differs a lot. Websense tells us that they have categorised sites in more than 50 languages, but they do not specifically say that text analysis is used. SurfControl claims to have sites in more than 70 languages in 200 countries in their database, so in practise it should not be possible to avoid text analysis by choosing an obscure language for a website.

Optical Character Recognition (OCR): Text on Internet pages is usually written characters, each character uniquely identified by ASCII or Unicode. This text can be read and processed digitally. But sometimes the text is in the form of symbols or pictures instead, for instance when a document is scanned, and these pictures cannot be read as easily, even though a human reader would not see any difference from normal text. One needs a pattern recognition system to translate the images into machine-edible text. A good OCR system recognizes text in graphics and images, analyses coloured type or transparent text on any background, and are capable of interpreting a variety of fonts, rotations etc.

OCR can also do *Logo and Object Recognition*; to search for logos, symbols and other graphical elements in photos. The identification of a logo can ease the categorisation of a site, for example a VISA- or MasterCard-logo indicates that the site may be a Webshop of some sort.

Image analysis: "Image analysis is the extraction of useful information from images; mainly from digital images by means of digital image processing techniques. Image analysis tasks can be as simple as reading bar coded tags or as sophisticated as identifying a person by its face" (Wikipedia.org).

A human would instantly recognize and even categorise the content of an image, but it is not feasible to manually analyse the millions and millions of pictures found on the Internet. ISS have more than one billion images in their database, according [Issfaq, 2004], and surely that shows that computers must be used for analysis. If one person categorised one picture pr second, all day, all year, he/she would spend 31 years to analyse 1 billion pictures.

It is beyond the scope of this thesis to explain digital image analysis in detail; we shall simply concentrate on how the technology is used in categorisation of Internet sites to better understand how filtering works.

Face recognition: Recognizes faces (although seldom able to identify known individuals), which is useful when categorising pictures; say separate animals or cars from humans.

Pornography and Recognition of Nudity: By analysing the qualities of human skin and skin tones, it is possible to identify nudism or pornography. This is of course very helpful because one of the most important categories to rule out is "adult content". The reasons for this will be discussed later in the report.

Digital Fingerprint: Images is not always proprietary to a certain webpage, they can sometimes be found on several sites. When images or data are analysed, they are characterized and labelled for later identification on the Internet, intranets or in e-mail messages.

Similarity comparison: To make it easier to label an image, it can be compared to already categorised images. A strong resemblance indicates that the image is of the same category.

URL and linkage analysis: The content of a site can be harmless in and of itself, but if it is a portal for other, perhaps malicious sites, it should be categorised thereafter. If the filtering system knows the nature of the sites that the page links to, it can fit the page into the right genre.

Some filters also analyse the URL of the site itself. This is controversial, as the URL can be misleading. Let's look at an example; www.whitehouse.com is a site with adult material, www.whitehouse.org is a humorous site, www.whitehouse.net is a political protest site, www.whitehouse.gov is the official site

of The Whitehouse, and finally; www.thewhitehouse.com is the homepage of a real estate agent. These sites should all go in different categories, but their URL's are almost identical.

A URL is one thing, IP-addresses something else. Some Internet filters, for example ISS Proventia®, keep track of the IP-addresses as well as the URLs. It is trivial to change the URL of a site to attempt to trick the Internet filters, so a filter that blocks IP-addresses would seem to have an advantage. However, this advantage has its downside; it is entirely possible that several Internet sites share the same IP-address. Also, many sites have dynamic IP-addresses, which means that blocking a certain IP-address can be futile, and even do damage to an innocent third party.

Manual inspection: The major players in the filtering market do not leave it all to the machines. Both Websense and SurfControl claim that staff manually categorises new sites after an initial classification by the tools described above. SurfControl claims to update their database with up to 45.000 sites every week [SurfControl]. They also admit to have less than 70 researchers, which means that each and every one of them has to categorise at least 130 sites pr day. Websense and ISS Proventia are no different. There are several organisations that oppose Internet filtering for various reasons. Some of these doubt that manual inspection is used as much as the filter companies claim, and refer to a number of wrong categorisations to make their point: It is impossible to categorise the enormous number of new and altered sites manually [Censorware, 2005].

3.2 False positives

False positives are a problem with many security measures. Internet filtering is no exception, according to several organisations and researchers. [Finkelstein, 2003] and [Peacefire] list numerous sites that they claim are put in the wrong category by Internet filters like WebSense. There are two main reasons web sites are put in the wrong category. The first reason is that automated categorisation misinterprets the content of a site and labels it wrong. This could be discovered and fixed by manual inspection, but apparently this does not always happen. [Finkelstein], [Peacefire] and [Tien, 2001] all conclude that it is impossible to inspect all new and altered webpages manually, even though some filtering companies claim that this is done. The second reason for wrong categorisation is that the moral standards may vary from country to country. A webpage that is deemed unmoral in the US may not raise controversy in Norway. [Miner, 1998] gives several examples of this and of cases where filtering companies choose to block web sites they do not approve of.

3.3 How websites are picked for categorisation:

Existing database*:* The content of websites is subject to change. Sometimes the change is so substantial that the site should be re-categorised, perhaps because a domain name is sold to someone else, a change in policy or a change in business (e.g. an informational site that starts to sell products as well). Websense, SurfControl and ISS Proventia claim to have between 8 and 20 million websites in their databases, so we understand that monitoring all of these sites for signs of a substantial change in content must be a pretty hefty challenge.

New visited URLs: All the major filter technologies utilize automatic customer feedback. Every time a user tries to connect to a site that is not in the filter database, the URL is sent to the vendor for analysis and classification. The categorised URL is then added to the local database at the next update, usually the day after. Depending on the local configuration, this either means that the site is blocked until it is categorised (unless it belongs to a blocked category), or that the site is accessible at least until next update. However, as will be shown in Section 6.2, we have reasons to doubt that automatic customer feedback always work as intended.

Webcrawlers: A webcrawler or webspider is a program that automatically and systematically browses the Internet and registers new sites and pages. With a basis in the filtering database, it visits known sites and registers all hyperlinks on those pages. Unknown hyperlinks are then added to a list of sites or pages to be categorised, and the program "crawls" on through the web.

Customer submission: Customers and those interested can submit URLs to unknown pages for categorisation on the filtering companies' homepages, and with some vendors even propose a categorisation.

3.4 Filtering in practise:

What is filtered: This depends on local configuration and the completeness of the filter that is installed. All major Internet filters can block access via http or ftp to predetermined URLs, and most of them can also block Instant Messaging (IM), streaming media and peer-to-peer (P2P)[7] connections. Transfers of specific file types such as mp3, .exe, .mpg etc. can be stopped independently of source to increase protection against malware or excessive bandwidth use. The filter can be configured to block different categories depending on time of day, user group, a user specific time quota and/or a number of bytes, depending on what the management wants to achieve with the Internet filter.

How the content is filtered: As stated before, the main filtering happens when a request to connect to a site is made. The requested URL is looked up in the filter database, and correspondingly allowed or blocked. If the URL is unknown, the request is blocked or allowed depending on local configuration. While it is possible to block certain file types or -extensions, there is no "on the fly" categorisation of unknown web sites or the downloaded pages. The categorisation of webpages takes place centrally with the filter vendor, and the local databases are updated on a daily basis.

[7] Peer-to-peer: P2P programs make it possible to browse and download the content of others disks in the network. Users can also choose to share some of their own files for downloading. However, history has shown that P2P software can have security holes that let crafty users browse the entire content of a disk, not just the shared files. P2P programs are often bundled with advertising software and spyware that introduces new security-holes. In addition, this networking application would open up a hole in the company's firewall.

Topology: The model in Figure 2 is collected from Secure Computing's Smartfilter [SecuComp], but the topology is the same for all major filter systems. The content filtering software rests on a shared or dedicated server connected to the firewall or a proxy. All http, ftp, and related traffic flow via this server.

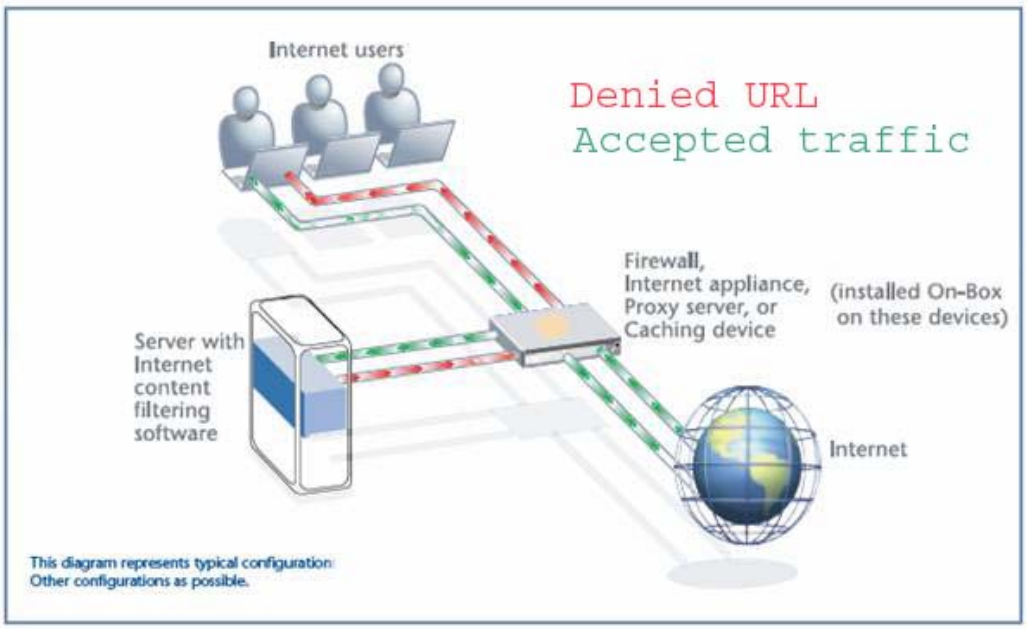

Figure 2 - Filter system topology, based on [SecuComp, 2005]

Outgoing requests for http, https or ftp connections, instant messaging (IM) and P2P networking are evaluated and blocked or permitted according to the filter database and the local configuration. If for example someone tries to access an URL in the "block"-list, the request is stopped, and a block-message is displayed in the browser window instead of the wanted webpage. The content of this message can be tailored to the organisations needs, and e.g. include a referral to the company's web policy. If the request is for a site that's not in the block-list, the filter is completely transparent to the user.

3.5 Products used in experiments in this thesis

Websense [Websense] and SurfControl [SurfControl] are by far the biggest in the corporate market. Together, they hold more than 40% of the market (October 2004, measured by revenue), with the next competitor (Secure Computing) at 9.2% [IDC, 2004]. As Figure 4 shows, there is a heap of very small brands that combined control 40% of the business and the author does not pretend to have a full overview over the myriad of products in the trade. [Timber, 2000] gives a summary of 36 different filtering technologies, and they even miss relatively large brands, like ISS Proventia, Symantec and McAfee, indicating that the list is far from complete.

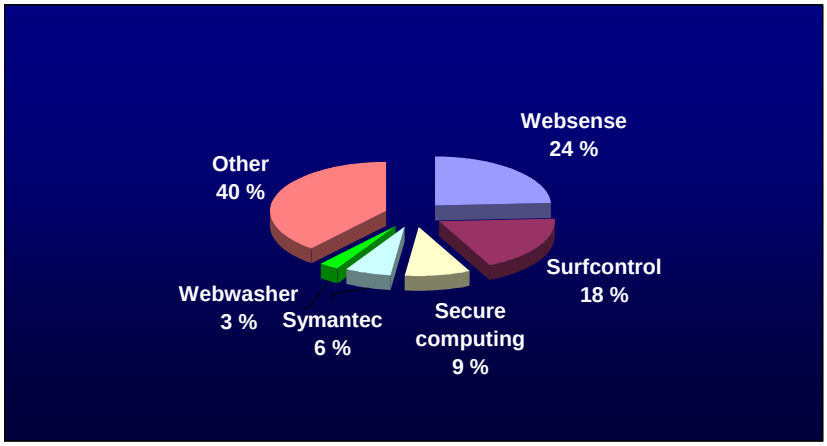

Figure 3 - Internet filtering market shares

It should be noted that only some of the filters in [Timber, 2000] are meant for the corporate market; most of them are products for home PCs. ContentProtect, Cybersitter, Netnanny, McAfee PC, Norton PC and SurfPatrol, to mention a few, are all competitors in the parental-control segment of the filtering market. These filters are installed directly on the workstation, and typically divide the Internet sites into fewer categories than the enterprise versions. Most of the parental control filters rely more heavily on on-the-fly dynamic content recognition than a comprehensive database of websites. Filters for home use will not be a part of this survey.

SurfControl: Offers web filtering in addition to e-mail filtering, instant message filtering and threat protection, and holds 18.5% share of the market for these products combined [InSe, 2003]. They provide filtering tools for Windows, Linux, Novell and Checkpoint, and claim to be compatible with virtually any topology of routers and switches. Their URL list is divided into 47 categories and 145 subtopics allowing for detailed filtering. Sites from 200 countries and in 70 languages are evaluated in the list. The filter can be configured to block all pages that have not already been categorised in the filter database. The web filter report can generate statistics on how the company uses the Internet, at what time of day the most of the traffic is generated, etc.

Websense: the alleged market leader in web filtering software had a 24.2% market share in 2003 [InSe, 2003]. The Websense Enterprise suite analyses and reports on employee Internet use, blocks unwanted content and optimizes use of IT resources, including bandwidth and desktop resources. Their URL database is organized into 90 categories, and contains approximately 8.5 million websites, published in more than 50 languages. Websense have developed solutions tailored for different industries, like education, healthcare and manufacturing.

This chapter has provided a walk-through of the technical aspects of Internet filtering that covers what we believe are most important to understand the rest of this report. We shall now move on to methods used in the survey.

4 Choice of methods

In this chapter we will describe the methods we preferred for our research. We start with a general introduction to research, and continue with the choices we made to investigate each of the research questions described in Section 1.5. We have conducted a survey that provides answers to all three questions, and therefore decided to describe the survey and the benefits of this approach in Chapter 5.

4.1 Introduction to research techniques

This thesis searches for answers in several fields. Attitude measurement, theoretical analysis of a system and quantification of efficiency requires diverse approaches to the study.

In [Creswell, 2003], three approaches to scientific research are identified:

- The quantitative approach: To analyse quantifiable information through the collection of data from experiments, surveys (e.g. questionnaires) and other measurements. The data can for example be used to find cause and effect of a variable or to test a theory through manipulation and observation.

- The qualitative approach: New knowledge is primarily developed from constructivist (i.e. socially and historically constructed meanings with an intent of developing a theory or pattern) or participatory perspectives. Theories are derived from knowledge gathered through observation, case studies and grounded theory.

- The mixed methods approach: Collecting and analysing data from both quantitative and qualitative approaches in a single study. Both numeric and text information are collected so that the final database represents both quantitative and qualitative information. Knowledge claims are based on pragmatic grounds as for instance consequence-oriented or problem-centred.

In this project, we have used the mixed methods approach to research. We have done a qualitative evaluation of the theoretical security-contribution of Internet filters which forms the basis for quantitative experiments. We have also used the quantitative approach when we conducted a survey to collect data to base our conclusions on. The results and conclusions are thus of both a qualitative and quantitative nature.

4.2 What impact will the filter have on work-efficiency?

In Chapter 1, we said that we would assess the amount of cyberslacking and the private (mis-)use of company networks as measures of efficiency. In addition, we want to know if filtering decreases work-efficiency by restricting access to necessary Internet resources. To find answers, we do not need to quantify efficiency as such; we only need a relative measure to see if there are differences between employees in companies with and without filters. To measure the use of Internet in an organisation, we could either monitor the network or ask the users about their habits. Monitoring would unarguably produce the most accurate results, but that approach has both ethical and legal implications as well as practical disadvantages. We instead decided to ask the users themselves through an anonymous questionnaire distributed to employees in companies with and without Internet filtering. The respondents may not have given accurate information about how and how much they use the Internet,

but we assume that erratic answers will be evenly distributed between the users. Thus, the potential relative differences between users in filtered and unfiltered networks should be observable.

The questionnaire is part of the survey described in Chapter 5.

4.3 What is the attitude towards Internet filtering among Norwegian workers?

Measuring attitudes is not a straightforward task. Attitudes are related to personal values and social conformity, and there may be a gap between the "politically correct" attitudes we express and our true feelings [Fowler, Mangione 1990]. A survey that tries to measure attitude towards sensitive issues like work morale, pornography and surveillance, must take this into consideration and strive to give the respondents a feeling of anonymity and security. We decided to do this part of the survey with a questionnaire utilizing the Likert scale [Likert]. The Likert-procedure is to produce a number of statements, and then ask the respondents not only whether or not they agree with the statements, but also to rate their view from "strongly agree" to "strongly disagree" on a scale with 5 or 7 levels. An example of a statement in this context is "what I do on the Internet while I am at work is nobody else's business".

[Oppenheim, 1996] emphasises some points when constructing statements:

- Avoid ambiguity
- Redundancy can be useful
- Order matters

We strived to show the utmost scrutiny when we designed the statements in the survey. Statements should not be ambiguous or impossible to relate to. The statement "I used to browse a lot at work, but after the Internet filter was installed, I work more" in an early edition of the questionnaire was omitted because the statement implies that the respondent worked in the company before a filter was installed. Another weakness of the statement is that it is really two statements in one; "I used to browse a lot" and "after the Internet filter was installed, I work more". Would the respondent feel that it was an ambiguous statement? Other ambiguities can spur from e.g. double negatives, or simply clumsy wording.

According to [Oppenheim, 1996], it is a good idea to have several statements related to each attitude. Conformity between the responses to these statements increases reliability, while no correspondence indicates that the respondent gives arbitrary answers or that the questionnaire is poorly constructed. The order of the questions also matters. If one needs to ask the respondent questions that can be offensive, this should be done as late as possible in the questionnaire unless the provocation is a calculated part of the investigation. It is also wise not to ask for personal information until the end of the form to avoid distorting the feeling of anonymity. Open-ended questions can be a good supplement to the forced-choice variant. Most of us have participated in a survey at some point in our lives, and been frustrated because it did not ask us exactly the right questions. It can also be frustrating when none of the presented answers correspond fully with our opinion. Open-ended questions give the respondents a chance to express their views, or to nuance their answers.

The survey is described more closely in Chapter 5.

4.4 What impact does Internet filtering have on security?

To answer this question accurately one should be monitoring a controlled environment over a period of time, or analyzing the statistics of a very large number of networks to find tendencies that can be attributed to Internet filtering. Such a large-scale experiment would require time and resources of a magnitude that is not available in this study, but we believe to find sufficient data by using a mixed method approach.

We performed a theoretical analysis of the expected security-benefits of Internet filtering. The analysis was based on the acknowledged "Classes of techniques for computer misuse" [Neumann, 1989] and included which attacks or classes of misuse techniques Internet filtering may or may not prevent or render harmless. In connection with the analysis we did a literature study especially targeting white papers and technical specifications of different Internet filters. We also searched for knowledge about attacks and malicious technology to support the theoretical analysis.

The classification forms the basis for experiments and discussion. A weakness of such an analysis alone would be that the provided results were not supported by empirical data from experiments. We therefore developed metrics (see Section 6.2) to confirm the theoretical results, and carried out experiments (see Section 5.2) to provide data for those metrics. With this approach we believe it is possible to pinpoint the areas where Internet filters can add to security regardless of which other security measures are implemented in any given IT environment, and test if the reality and theory correlates.

There are many ways to gather data and get results in research like ours. We have prioritised to keep the data collection simple and use methods that require small technical resources, and believe we have succeeded with this without compromising validity or reliability. Closer descriptions of survey and experiments as well as discussion of validity and reliability are presented in Chapter 5.

5 Survey and experiments

In this chapter we describe the survey and some experiments that have been carried out in connection with our research. We discuss the validity and reliability of the data, and present our thoughts on potential ethical implications of our work.

5.1 The survey

The survey was carried out in the form of a questionnaire that measured the respondents' opinions and experiences on different aspects of Internet filtering. To collect information with a questionnaire has many advantages [Oppenheim, 1996]:

- Low cost of data collection
- Low cont of processing
- Avoidance of interviewer bias
- Privacy, when carried out anonymously.

There are also disadvantages, mainly concerning response rates and the potential for misunderstandings between respondents and the author. To address these problems we made a test group assess the questionnaire and point out sentences or questions that could be misunderstood. The test group consisted of students with little or no knowledge of IT-security systems, and two experienced researchers. The final version of the form was tested to be sure it did not take too long to read and answer.

To avoid low response rates proved to be a bit more troublesome. We wanted to distribute the questionnaires randomly to employees in different organizations or companies with an Internet filter installed, and employees in organizations without Internet filtering. The first problem was to find companies with filters, because most IT-managers and filter-vendors are reluctant to surrender any information regarding IT-security measures. Potential companies with filters were found only after wide use of personal contacts. Next, very few organisations saw the point in spending time and resources on participating in a survey. We had a goal of 200 respondents, but had to settle for less. A number of 104 respondents overall should still be sufficient to give useful results, but few respondents may in some cases yield low significance or uncertain data.

The questionnaire itself consisted of three parts. Part one enquired of the respondents how much and for what purposes they used the Internet. Part two included the Likert-test and some additional questions about why the employees thought the filter was installed. Part three asked for demographics. Part one and three were identical for the participants in both filtered and unfiltered companies, while part two was adapted to the respective groups. The questionnaires and an explanation to how we quantified the answers are included in Appendix A.

The answers have been subject to statistical analysis with SPSS 13.0 [SPSS] to reveal trends and tendencies in the groups of respondents, and amongst the results we found was how the employees in organizations with and without Internet filtering differs in their use of the Internet. This work will tell us more about the potential dangers which unfiltered browsing allows for (and filtering stops), and if filtering improves availability by the release of bandwidth.

Participating companies

We asked a total of 24 companies and organisations to participate in our survey. An initial enquiry was made via telephone and/or e-mail, and followed up with more e-mails until the company had accepted

or declined. The e-mail contained a copy of the questionnaire, and assured the company of complete anonymity for both the respondents and the company itself. In Section 3.5 we described the two filter-products that would be used for our experiments. It would have been ideal if all the participating companies used those very products, but we cannot guarantee that this is the case. Two companies confirmed that they used SurfControl, while only one used WebSense. The last two companies decided against revealing any information about their filter solutions.

The sampling of respondents was not truly random. In some companies or organisations, all employees that were present on the day the questionnaire was distributed, responded. We assume that who were and who were not present on the day of the survey was completely incidental, so we have no reason to believe that the population was skewed in those cases. In other companies, employees were picked at random from all departments, but only those who could spare the time participated. In these cases, there is a possibility that the respondents for some reason were more motivated to state their opinion than the average employee in that company, and that this could mean that the sample was not representative. However, the respondents were not told what the theme of the questionnaire they would be answering was prior to the survey, so we believe that this will not affect the results significantly. Table 1 presents a summary of companies asked, and their response to our enquiry.

Trade	Asked	Yes	No
Finance	3	1	2
IT/Telecom	8	2	6
Education	2	2	0
Public services	4	2	2
Engineering	3	2	1
Healthcare	2	0	2
Other	2	1	1
Sum	**24**	**10**	**14**

Table 1 – Summary of companies asked to participate in the survey

Interviews with IT-personnel

In connection with the survey we talked with IT-personnel in the companies that had filter installed in the network. We did not interview them formally, but rather discussed Internet filtering on a general basis and in relation to their company. Because of the informal nature of these conversations, we shall not present the outcome among the results of this thesis, but we shall still bring some of the statements into consideration in Chapter 6 and in the discussion.

5.2 Experiments

We have carried out a number of experiments with the Internet filters Websense and SurfControl. The experiments all utilised the *URL-testers* of the respective filtering companies. A URL-tester is a web-application that allows you to type in the address to a web page and checks that address against its own database of web addresses. The application then returns the category of the web page, or tells you that the page is unknown to the filter. The URL-tester utilise the very same database that is installed in their customers' networks (please see Appendix D). The URL-testers are found at http://mtas.surfcontrol.com/mtas/MTAS.asp and http://ww2.websense.com/global/en/SupportAndKB/SiteLookup/

When we tested URLs, it was to see either *if* it was categorised or in *what* category it was put. Because the filter-databases delete "dead" URLs from its entries, we took care to check the availability of every page before we tested the URL. We also made sure the web addresses or IP-addresses were spelled correctly. The experiments with URL-testers were carried out to gather data for the metrics described in Chapter 6.

In connection with the analysis of the responses to the questionnaire, we decided to carry out an experiment that we had not planned in advance. It seemed that the filters we tested did not perform well with Norwegian webpages, so we utilised the URL-testers on a number of Norwegian URLs. Perhaps it is not common to expand the number of experiments this way, but in this case we felt that it was natural to examine the question more closely. The experiment and the results of it are presented in Section 7.2.

5.3 Ethical considerations

Some of the experiments in this project meant that we had to visit websites of a rather dubious character, for example porn-sites, hacker-sites and phishing-sites. We know that this would enhance the risk of malware-infections, and that it could jeopardise the security in the internal network. We took all possible precautions to prevent malware from infecting and spreading from the tested websites. The test-PC was set up with Symantec Antivirus [Symantec], Tiny personal firewall [Tiny] and Ad-Aware Plus [Ad-Aware] in addition to the security measures in the network itself. We encountered several attempts to install malware on the computer. Among these were three trojans[8], two backdoors[9] and plenty of spyware. The attacks were repelled by the anti-malware programs, but we suppose there is a theoretical chance that something slipped through. So far, we have no indications that this was the case.

In the questionnaire, we asked the respondents some personal questions about their Internet surfing habits. It was imperative that they felt confident that all information was treated and stored in a way that ensured their anonymity and prevented tracking. The forms were distributed together with an unmarked envelope to put the answers in. In some companies the form was distributed via e-mail and printed out by the respondents themselves. In those cases, the participants were requested to put the answer in an envelope, or to fold and staple it together in a way that prevented anyone from reading it without breaking the seal. We did not receive any forms or envelopes that appeared to be tampered with.

Even though the forms were anonymous, it could still be possible to identify some of the respondents in a few cases. Age, profession and gender are sometimes enough to single out a person in a small group, but since the individual results will not be published or given back to the employers who probably could identify some of the respondents from the data, we feel that anonymity is maintained. However, we have still included all the answers in Appendix B. To decrease the possibility of someone identifying individual respondents, we have omitted the data about company, gender and department. We have found some correlations between age, company and other variables, and shall comment these in Chapter 7. We admit that it can be controversial to exclude some of the data in the score sheet, but we feel that the promised anonymity of the respondents must be heeded.

[8] A Trojan horse is a program with an overt (documented or known) effect and a covert (undocumented or unexpected) effect

[9] A backdoor is a method of bypassing normal authentication or obtaining remote access to a computer, while intended to remain hidden to casual inspection. The backdoor may take the form of an installed program (e.g., Back Orifice) or could be a modification to a legitimate program.

6 Security provided by Internet filters

In this chapter we shall explore Internet filters' theoretical contribution to security. The theoretical work will help crystallise the areas where Internet filters may contribute to security, and thus limit the number of experiments needed later. The general idea is that we must know what to look for before we start looking.

We start with giving an overview of [Neumann, 1989], and then analyze each of the proposed classes in turn. We cannot analyse every possible vulnerability or attack related to information security in this thesis, but we will discuss all subjects of relevance to filtering. We will also consider claims made in whitepapers and marketing information from the producers of Internet filters of what filtering can protect against when we pick the threats to concentrate on.

Table 2 describes the classes of computer misuse developed by [Neumann].

Class	**Description**
C1 External misuse • Visual Spying • Misrepresentation Physical scavenging	Generally non-technological and unobserved, physically separate from computer and communication facilities, for example visual spying, dumpster-diving[10] etc
C2 Hardware misuse • Logical scavenging • Eavesdropping • Interference • Physical attack • Physical removal	Physical access normally needed. Eavesdropping, interference, examining stolen media, theft, sabotage etc
C3 Masquerading • Impersonation • Piggybacking attacks • Spoofing attacks • Networking attacks	Impersonation, playback and spoofing attacks, creating bogus systems, usurping communication lines etc
C4 Pest Programs • Trojan horse attacks • Logic bombs • Malevolent worms • Virus attacks	Planting and arming malicious software such as worms, virus, spyware, trojans etc
C5 Bypasses • Trapdoor attacks • Authorization attacks	Utilizing existing flaws, buffer overflows etc, password cracking.
C6 Active misuse of resources • Basic active misuse • Incremental attacks • Denials of service	Misuse of (apparently) conferred authority that alters the system or its data.
C7 Passive misuse of resources • Browsing • Inference, aggregation • Covert channels	Misuse of (apparently) conferred reading authority.
C8 Misuse resulting from inaction	For example failure to avert a potential problem in a timely fashion, or an error of omission etc.
C9 Use as an indirect aid in committing other misuse	a) As a tool in planning computer misuse etc. b) As a tool in planning criminal/unethical activity.

Table 2 - Classes of computer misuse, Neumann and Parker [Neumann, 1989]

[10] Searching through discarded material looking for otherwise unavailable information. Businesses and individuals frequently discard information including printouts with passwords, credit card numbers, business planning and so on; determined divers can recover some of this.

6.1 Theoretical contribution of Internet filters

We will now discuss the attacks that falls into the classes of computer misuse and if and how Internet filters can prevent or control those attacks.

In those cases where it is obvious that filtering cannot affect the security level, the respective class will be discussed briefly. When we are in doubt - or when we believe that filters can contribute to security in theory - the discussion will be more exhaustive. We will present how we think filters can prevent and/or mitigate attacks where applicable, and near the end of the chapter we shall propose metrics that will be used to support or defy our theoretical findings. The results of the experiments are presented and discussed in Chapter 7.

Class C1 External misuse:
This class comprises attacks that are executed without any access to the computer system, such as *social engineering*, *dumpster diving*, visual spying etc. There is little reason to believe that Internet filtering could prevent or limit any such attack, since computer systems are not involved. One could argue that Internet browsing habits can be recorded and used as a basis for extortion, and that Internet filtering could prevent that browsing and thereby the reason for being extorted, but the author finds this far fetched and does not want to pursuit the subject further.

A more reasonable argument can be produced for physical misrepresentation, i.e. to breach physical security by deceiving guards or co-workers, for example with a fake ID-card. The information needed to make a fake ID-card can be extracted via a trojan or on the basis of clues left behind on the Internet, but this is a consequence of matters that will be discussed under the category “Pest programs”.

Class C2 Hardware misuse:

- Logical scavenging – Examining stolen media
- Eavesdropping – Intercepting electronic or other data
- Interference – Jamming, electronic or otherwise
- Physical attack – Damaging or modifying equipment, power
- Physical removal – Removing equipment and storage media

Again, these are attacks in the physical domain. Internet filtering products are software that cannot prevent physical theft or electronic interference. Furthermore, Internet filters have no cryptographic capabilities either, so it will not limit the impact of physical theft of media. Internet filters can, as a result of protection in other areas have a positive influence on the nature of stolen media, e.g. that a stolen disk does not contain child pornography.

We have decided to put excessive bandwidth use into this class. We could also have placed it in the class C6 - Active misuse of resources, but since bandwidth is a physical resource, we feel that it belongs here. If employees use the corporate network excessively for non-work related tasks, like downloading streaming media or sharing files through a P2P-network, this can be said to be hardware misuse. As previously stated, several studies conclude that employees spend a lot of their work time on the Internet, and this traffic “steals bandwidth” in the network. We also know that streaming media can be a strain on networks, and according to [TNS, 2005] more than 200.000 Norwegians listen to radio via Internet every day.

Prevention: One of the alleged key advantages of Internet filtering is the possibility to block access to streaming media, file downloads and excessive use of the Internet. But if the filter is not configured to block these activities, it will not help much.

Class C3 Masquerading

- Impersonation – Using false identities external to computer systems
- Piggybacking attacks – Usurping communication lines, workstations
- Spoofing attacks – Using playback, creating bogus nodes and systems
- Networking attacks – Masking physical whereabouts or routing

Impersonation: An impostor could deceive unsuspecting users and make them install a program, e.g. by posing as an IT-service man and asking them to install a "safety-patch" from a disk. Internet filters could not directly prevent this from happening, but if the program that was installed was a spy-program, the filter could prevent it from connecting to an external source.

Spoofing: As stated in the introduction, *Phishing attacks* are on the increase. A Phishing attack is really a spoof, a bogus website set up to look like a trusted site. A common spoof is to make webpages that look exactly like the home page of a bank or other financial institution, and direct unsuspecting users to it. The page often asks for registration or re-entering of account number, credit card number, pin-codes and other information needed to empty the banc account of the victim, or charge his credit card. There are two ways of directing users to the spoofed website. The most common is via a *Phishing*-mail. The victim receives an e-mail, apparently from his bank, his credit card company or somewhere else he has an account that can be bleed. He is urged to click a link or follow an URL to a webpage where he must update his customer information or something similar. The URL often looks legit, but the visible URL may not be the actual address he is sent to. A recent example is a scam directed towards Norwegian VISA customers. The customers were asked to click the link http://www.visa.com/security/index.php to be sent to a page where they could reconfirm their account information. The address they were really sent to was "http://safevisa.ueuo.com/index.php", a page that looked exactly like an official VISA-page, with links to the legitimate site and authentic logos. Unfortunately, all registered information was undoubtedly used to swindle the victims of the scam. A more complex approach is DNS cache poisoning, which simply put is to deceive a DNS-server and make it return the wrong IP-address when a specific URL is enquired about. The "new" IP-address leads to a spoofed site, just like the example above.

Prevention: Internet filters can prevent users from connecting to the spoofed sites. In the example with e-mail-Phishing above, the visible link differed from the actual link. A user might not see this, but the filter would. If the real link were to a blocked site, the connection would be stopped, and the user prevented from giving away information. Hopefully, he would also see a block-page that said that he just tried to visit a fraudulent site. Most Internet filters have dedicated a category to Phishing and frauds, so they should protect against this threat. In fact, Websense claims that "Websense Enterprise 'Phishing and other Frauds' Web Filtering Category Protects Organizations against Advanced Internet Scams" [Websense2]. In the case of DNS cache poisoning, Internet filters that register and filter IP-addresses can stop the scam. When the DNS server returns the wrong IP to the browser, the outgoing http-request is assessed and the IP address looked up in the database. The site will be blocked if the IP address is blocked.

Not all phishing-frauds send information to a website that can be blocked. Sometimes the receiver is just a mailbox, or a hijacked, otherwise legitimate, site.

Piggybacking attacks: When a workstation is used for a DDoS-attack (Distributed Denial of Service), as a host for Phishing-attacks or as a relay for sending spam mail, this can be said to be Piggybacking attacks. The attacker takes control over the workstation, for example with the help of malware, and turns it into a bot[11]. Botnets can comprise a collection of cracked machines running programs (usually referred to as worms, Trojan horses, or backdoors) under a common command and control infrastructure (Wikipedia.org [Wiki]). The number of BOT-applications rose significantly in 2004, and is expected to rise further in 2005 [SecLab, 2004]

Prevention: Internet filters can prevent infections with malware via some attack vectors. This is explained in more detail in class C4 - Pest Programs.

Mitigation: If a workstation is turned into a mailbot, an Internet filter that checks SMTP can stop all traffic on port 25 (SMTP) that is not going to the company mail server. Very few, if any, Internet filters check SMTP, and of course, a firewall or a mail-filter could do this just as well.

Workstations that are enslaved and used in a DDoS attack will typically send heaps of HTTP or ICMP requests to the targeted server. Internet filters could stop these requests from leaving the corporate network, and so cripple the attack. We find it a bit unlikely that the servers normally targeted by a DDoS attack would be of a nature that is likely to be in a block-list, since these servers often belongs to businesses or governmental organisations. We therefore doubt that an Internet filter would help in this situation. Once the attack was started and the malicious traffic detected, both a firewall and an Internet filter alike could be configured to stop traffic to the attacked server.

Class C4 Pest Programs *Setting up opportunities for further misuse*

- Trojan horse attacks – Implanting malicious code, sending letter bombs
- Logic bombs – Setting time- or event-bombs (a form of a Trojan horse)
- Malevolent worms – Acquiring distributed resources
- Virus attacks – Attaching to programs and replicating

Trojan horse: "A Trojan horse is a program with an overt (documented or known) effect and a covert (undocumented or unexpected) effect" [Bishop]. Although many (most?) programs have unexpected effects, we here think about malicious programs that are disguised as, or hidden in, legitimate software. A trojan can be a virus, a worm, spyware, keyloggers etc. In this section trojans, viruses, worms, spyware etc. will be treated as a whole; Malware.

How to get infected: The most common way to get infected is to open an attachment in an e-mail, to download a program from an http- or an ftp-server, or to visit an infected website where the Trojan horse may hide in the form of a Java applet, JavaScript, ActiveX control, or other form of executable content. It is believed that some sites are more likely to distribute malware than other. Jonathan Read (CISSP) with Anti-trojan.org [Anti-Trojan] states that free porn sites should be avoided at all costs. "There normally is a reason these are free and more often then not it is because you end up infected with a porn dialer."[12] Read also advises against visiting warez-sites (pirated software), as most of them are crawling with spyware. A small survey by eBlocs [eblocs, 2004] concluded that 98% of porn sites install spyware of some sort, and 15% install a porn dialer. The reader should notice that this survey

[11] A bot (short for "robot") is a program that operates as an agent for a user or another program or simulates a human activity (whatis.com)

[12] A program that hijacks modems and then dials high-cost sex-lines

only checked 100 sites, and that eBlocs have a financial interest in this research as they sell URL-filters. Anyway, it seems likely that the essence in this is correct. Porn sites often install spyware.

Ordinary, arbitrary websites can also be a distribution point of malware. The Nimda worm [Symantec 2] is a good example of this. When Nimda runs on a workstation, it generates random IP-addresses and tries to connect to web servers. When a server is found, it is hacked and infected, and the worm goes in to a second stage. The web pages are modified to infect visitors on the page, exploiting a programming error in certain versions of Internet Explorer. The users do not necessarily need to click on any attachment to be infected, the programming error allows the malware to be executed automatically as the web page (or mail body) is viewed. This is called a *drive-by installation* [Winproxy, 2005].

Prevention: Internet filtering can prevent or reduce the number of infections via some of these attack vectors. First of all, Internet filtering can prevent a user from downloading programs unless they are specifically approved, such as an update or a patch. (Of course, a trusted patch or update can be infected as well, for example due to a spoofed server or a manipulated compiler [Bishop, 2003, p. 615], but this is not the point here.) Internet filters can stop executable files like .exe, .vbs, .com and .bat in an http or ftp transfer, or even over channels like IM and P2P.

“Pest-2-peer” programs have a reputation for spreading malware both in P2P-transfers and in the P2P software itself. An example: In 2002, a trojan named "W32.Dlder.Trojan" was included in the installation-files of several P2P-programs (BearShare, LimeWire, Kazaa and Grokster). The installer was hidden in a legitimate CyDoor-application (advertising software), and was installed when users set up the file-sharing applications. After installation, the trojan downloaded a file named "Explorer.exe" from a website, 2001-007.com, and installed the program into a user's system folder. The two-part trojan then created a start-up key for the Explorer.exe file. During next system restart, the Explorer.exe file would be activated. From that point on, the Trojan could connect to the 2001-007.com website on a regular basis and reports the user's ID and all URLs visited [Delio, 2002]. 19 of the top 50 viruses and worms encountered in the spring and summer of 2003 used P2P and IM applications—a 400% increase over all of 2002 [Symantec3, 2003]

Internet filters can prevent users from connecting to P2P sites and networks. This means that the users are prevented from downloading the program via the company network, but they could still install it from a disk if they have the privilege to install programs. The filter would further prevent them from downloading content from other P2P users and thereby clog a potential stream of malware. There are many viruses that are specifically designed to spread in P2P networks, e.g. the worm Win32.Worm.Duload [Bullguard, 2002], but the main problem is that there is nothing to prevent malevolent user to place malicious software in the files they share with others. And for some reason it seems many file sharers are less picky about the .exe files they download from strangers on their own initiative than the files they receive in e-mails.

Porn sites, gaming sites, warez-sites and other categories that often contain spyware can be blocked. These sites are often easy to recognise, and uncontroversial to block [Witty, 2004], so Internet filters could deliver a major contribution to avoiding drive-by installation of malware

Mitigation: Once a malicious program is installed, it can do anything the user has access or rights to do; Delete files, sending information out of the network, download and install other malware etc. This means that the malware’s freedom to manoeuvre is limited if the users’ rights are decreased. To communicate with the outside world, the trojan must have an open communication channel. Any port could be used, but in practise that would be ineffective. Most LANs are protected by a firewall, and if

properly configured it could block all communication on ports that are not in use by trusted applications in the network. This is why a trojan would rather use a port that is already open, and perhaps also exploit the program that is dedicated to that port. There are many examples of malware that utilize communicating programs like mIRC, P2P, IE, etc to spread or to get files and information through a firewall. An Internet filter could inhibit the malware in several ways.

If a keylogger or some other spyware tried to contact a remote host via an http or ftp request, the filter would block the traffic if it went to a site that was in the block-list. The same holds for worms and virus that try to spread this way. If the users cannot communicate through the filter, neither can the malware.

Some malware is known to download more malware. The "Download.Trojan" attempts to connect to a specific http or ftp server and download other Trojans or malware. An Internet filter could both stop the outgoing connection to the malicious site (if it is in the block-list) and stop the download of executable files. We should notice that even a stateful firewall might not stop this transaction, because the contact is initiated from the inside by what appears to be a legitimate user.

Class C5 Bypasses *Avoiding authentication and authority*

- Trapdoor attacks – Utilizing existing flaws
- Authorization attacks – Password cracking, hacking tokens

Trapdoor attacks, password attacks, and the like can be accomplished with the help of different trojans - for example a keylogger – installed on a workstation. How Internet filtering can affect the possible success of such an attack is discussed under Class 4 (and will not be repeated here). Different vectors of attack, like exhaustive trial-and-error attacks, derivation of passwords, guessing of passwords etc will not be affected by an Internet filter, because these filters stop information from getting out through specific channels, they do not repel attacks from the outside.

Class C6 Active misuse of resources *Writing, using, with apparent authorization*

- Basic active misuse – Creating, modifying, using denying service, entering false or misleading data
- Incremental attacks – Using salami attacks[13]
- Denials of service – Perpetrating saturation attacks

Salami attacks: A salami attack contains many small transactions that together make an impact, for example a slow port scanning that is below the detection threshold of an IDS.

Prevention: IDS may not recognise small leakages from workstations, but Internet filtering will stop all outgoing traffic over http, ftp and other protocols it's supposed to filter, regardless of the amount of data. This is of course provided that the receiver of the information is in the block-list. The subject of spyware is already discussed.

[13] A salami attack is a series of minor computer crimes that together results in a larger crime. Typically, this type of crime is hard to detect and trace. For example, a fraud activity in a bank where an employee steals a small amount of funds from several accounts can be considered a salami attack [Wiki].

DoS-attacks: If a company network falls victim to a DoS-attack, an Internet filter would probably not help. Even if some of the networks' own workstations were part of the attack, it is unlikely that an Internet filter would block access to internal resources over http or ftp. The incoming external requests that were part of the attack would not be affected by a filter that only blocks outgoing requests.

Class C7 Passive misuse of resources *Reading, with apparent authorization*

- Browsing – Making random or selective searches
- Inference, aggregation – Exploiting database inferences and traffic analysis
- Covert channels – Exploiting covert channels or other data leakage

Filters can stop outgoing connections on some protocols, not incoming hacking attempts. It holds no capabilities of access-control either, so we expect that filters cannot at all contribute to security in this class.

Class C8 Misuse resulting from inaction *Wilfully failing to perform expected duties, or committing errors of omission*

There are many websites with political or ideological content that may influence an employee to be inactive or even reluctant to do his duty. To block such sites may of course have a preventive effect on anarchy, but the author feels that this is too far-fetched to be a part of this study, and leaves the question to the sociologists.

Class C9 Use as an indirect aid in committing other misuse *Preparing for subsequent misuses, as in off-line pre-encryptive matching, factoring large numbers to obtain private keys, autodialer scanning*

This class collects all cases where a computer is used to prepare for subsequent misuse of other systems, e.g. fraud. One way to prepare for malicious acts is to gather background information on vulnerabilities, hacks and exploits on the Internet. There are several sites dedicated to malicious hackers, spreading tools and knowledge that can be used to attack IT-systems. It is widely believed that insider intrusion is a considerable threat, and indeed the "2003 Computer Crime and Security Survey," compiled by the Computer Security Institute and the FBI, found that 62 percent of respondents reported a security incident involving an insider [FBI]. A disturbing fact is that most programs made for attacking other systems also contain embedded malware in the form of spyware, trojans etc. If someone downloaded a script to do some innocent spying on the guy in the neighbour cubicle, this could also open the network to external hackers.

Prevention: Internet filters can block access to sites dedicated to hacking and malicious activity. Most filters have an own category for these sites, partly to block sites that can be used to attack the filters themselves. Users can of course get this information through other networks or a private Internet connection, but at least the potential malware is not downloaded to a corporate computer, and the corporate network is not used for malicious activity.

6.2 Target areas of experiments

We have seen that Internet filtering can contribute to security in some areas. We will concentrate on the classes C2 Hardware misuse, C3 Masquerading, and C4 Pest programs in our experiments. We will

now propose a number of metrics that can be used to find out if filters really affect security in those classes. The metrics are based on [NIST], but we have decided to include reliability and validity of the metrics in the tables below.

Class C2 Hardware misuse:

Metric ID	C21 Bandwidth use
Indicator	Used bandwidth per employee
Description	Will filtered networks experience less user-generated traffic than non-filtered?
Measurement	Will filtered users put less strain on the local network than non-filtered?
Experiment	Conduct a survey by measuring the use of Internet for private reasons among employees with and without Internet filter, and check for differences between the behaviour of the two groups.
Metric	Expected traffic generated based on standard values for browsing, file transfers and streaming media in kb pr person. Proposed values for bandwidth use: Browsing 64kb/s, IM 10kb/s, P2P 200kb/s, Streaming media 160kb/s.
Formula	C21 = (kb/s per non-filtered user / kb/s per filtered user).
Reliability	Main sources of error: Inaccurate data from respondents (if the data is derived from the users themselves), difficult to assess the bandwidth used in file transfers.
Validity	Good. The unnecessary strain users put on networks can be traced back to these activities.

Table 3 - Metric C21 - Bandwidth use

We used the survey described in Section 5.1 to gather data for this metric. The results are presented in Chapter 7.

C3 Masquerading:

Metric ID	C31 Phishing
Indicator	Categorisation of URL
Description	Will the filter recognise a fraudulent website?
Measurement	Can filters prevent a user to connect to a fraudulent website by following the URL provided in a scam-mail? How wide is the “window of opportunity”?
Experiment	Find fresh phishing-mails and test the URLs of the fraudulent sites in the URL-testers of an Internet filter.
Metric	Percentage of successful categorisations
Formula	C31= ((number of successful categorisations/total number of categorisations)*100)
Reliability	Need a large number of attacks to get good reliability. Important to measure fresh attacks to make sure the fraud-site is not closed by the ISP, and to measure as much of the window of opportunity as possible
Validity	Good, as the URL-testers utilise the same database as the full-scale filter solutions (See Appendix D). The success of the filter relies on correct categorisation of the pages. Measured performance does not necessarily predict future performance.

Table 4 - Metric C31 Phishing

We performed this experiment with URL-testers (see Section 5.2) throughout the project period to gather a sufficient number of Phishing sites. Details of the experiment and the results are presented in Chapter 7.

C4 Pest programs – Prevent infections

Metric ID	C41 Pest programs
Indicator	Number of infections
Description	Are the computers of employees in unfiltered networks more often infected with malware?
Measurement	Will filters' alleged ability to steer users away from infectious web sites reduce the number of malware infections on their computers?
Experiment	Ask users in filtered and unfiltered networks about how often their computers are infected with malware
Metric	Difference in average number of infections per year
Formula	Average # of infections in filtered networks / Average # of infections in filtered networks
Reliability	Depends on the companies' ability to discover malware. Results may be affected by other security measures in the network, e.g. antivirus software. With a large number of companies, this source of error will be less significant.
Validity	Good.

Table 5 – Metric C41 Pest programs

We used the survey described in Section 5.1 to gather data for this metric. The results are presented in Chapter 7.

We would also like to test if Internet filters can prevent e.g. spyware from communicating with an external host, but will leave this to further research as we have access to neither spyware nor the technical test environment such experiments would require.

7 Results and discussion

In this chapter, the results of the survey will be presented along with the results of the experiments. We shall interpret the results and discuss their possible implications. Section 7.1 presents some general information about the survey, and demographic circumstances that may have affected the results. After that, we discuss our findings related to efficiency, thriving and security.

7.1 General observations and demographics

A total of 104 persons responded on the query, 56 respondents in companies without filtering and 48 respondents in companies with filtering. Of these, 46 were women and 55 were men (see Figure 4), while three respondents did not state their sex and are therefore omitted from queries involving gender-differences. The distribution of gender corresponds with the general gender distribution in the Norwegian workforce [SSB2].

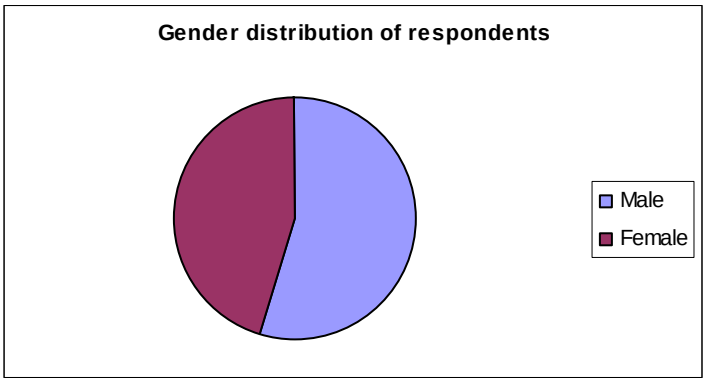

Figure 4 - Gender distribution of respondents

The respondents were not evenly distributed between companies with and without filter, as shown in Figure 5. There is an overweight of men in companies with filter, and an overweight of women in the other companies. The survey revealed a connection between gender and the use of Internet, so this imbalance will affect some of the measurements. From Table 6, we can read that there is a correlation between gender and Internet use; men tend to use the Internet more than women. Knowing that the genders of the respondents are not evenly distributed in the companies, we shall take this correlation into consideration when we discuss the results below.

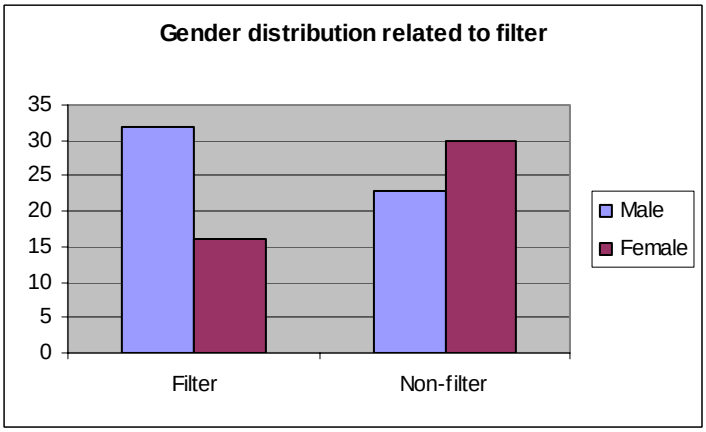

Figure 5 - Gender and filtering

Question	Gender	No of answers	Mean	Std. Deviation	Std. Error Mean
1c	Male	55	0,31	0,858	0,116
	Female	46	0,15	0,470	0,069
1e	Male	55	1,20	1,095	0,148
	Female	46	0,91	0,725	0,107

Table 6 - Relation between gender and Internet use

Explanation to Table 6:

- Question: Refers to the question number in the survey. 1c – "How much do you use instant messaging per day in average?" and 1e – "How much do you use the Internet for private purposes per day in average?". Please see Appendix A
- Gender: Male or female
- No of answers: Simply the number of respondents that stated their gender
- Mean: The mean value of the answers for that question and group. If the number is multiplied with 15, we get the number of minutes spent on that particular task.
- Std. Deviation: Standard deviation (Norwegian: "Standardavvik")
- Std. Error Mean: Standard error of the mean (Norwegian: "Feilleddets standardavvik")

The youngest respondent was a 22 year old woman, the oldest a 64 year old man. The age-distribution of the respondents is fairly compliant with that of the work force in general, but with a slight underrepresentation of the group 55+ [SSB3]. 6 respondents would not tell us their age, and are omitted from queries involving age. The age distribution is shown in Figure 6.

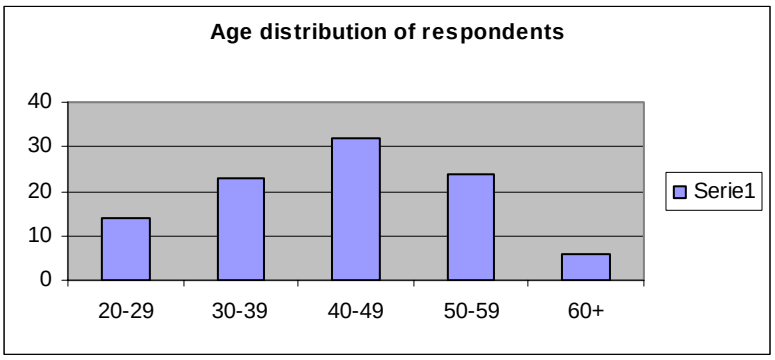

Figure 6 - Age of respondents in the survey

As shown in Figure 7, the average age of respondents in companies without filtering was significantly higher than that of companies with filtering. Concerned that this variance could influence the results, we investigated possible correlation between age and other variables. As we can see in Tables 7, 8 and 9, there is a strong correlation between age and the use of Internet; the youngest people in the group use the Internet far more than the oldest. Knowing that the average age of the respondents is higher in the companies without Internet filtering, we shall take this correlation into consideration in the discussion.

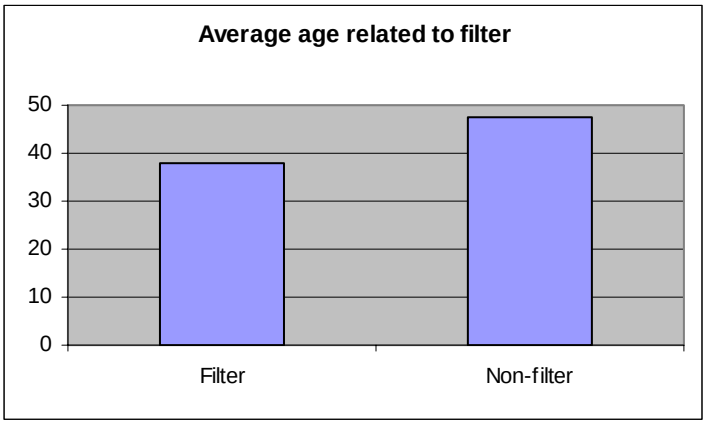

Figure 7 - Average age related to filtering

1c	Mean	N	Std. Deviation	ANOVASig.
0	44,21	84	10,025	
1	32,29	7	9,250	
2	41,67	6	11,219	0,015
5	30,00	1	.	
Total	43,06	98	10,450	

Table 7 - Chat related to age

1d	Mean	N	Std. Deviation	ANOVA Sig
0	59,00	2	1,414	
1	47,00	38	9,831	
2	41,57	23	8,173	
4	41,05	20	10,704	0,001
6	35,89	9	10,240	
10	34,40	5	10,714	
Total	43,05	97	10,503	

Table 8 - Internet use related to age

1e	Mean	N	Std. Deviation	ANOVA Sig.
0	47,20	20	10,247	
1	42,80	64	10,679	
2	40,11	9	7,817	0,109
4	37,25	4	5,909	
6	27,00	1	.	
Total	43,06	98	10,450	

Table 9 - Private Internet use related to age

Explanation to the tables:

- 1c, 1d and 1e refers to the respective questions in the questionnaire. 1c – "How much do you use instant messaging per day in average?", 1d – "How much do you use the Internet per day in average?" and 1e – "How much do you use the Internet for private purposes per day in average?". Please see Appendix A
- Mean: Average age of the respondents that answered "0", "1", "2" etc
- N: Number of respondents that answered "0", "1", "2" etc
- Std. Deviation: Described above.
- ANOVA Sig.: The ANOVA significance is the statistical significance of the correlation between "Mean" and "N". The lower the number is, the stronger is the correlation.

As we discussed in the introduction, typical "indoor-professions" have a very high degree of employees with Internet access. It is therefore not surprising that so many of the respondents work in administration. In fact, more than a half of the participants claim to do administrative work, while the rest is distributed evenly between "Technical/development", "Sales", "IT" and "Other". This distribution is shown in Figure 8. We expected a difference in habits and attitudes amongst the professional groups, but no such variance was found in the statistics, not even for the IT-professionals.

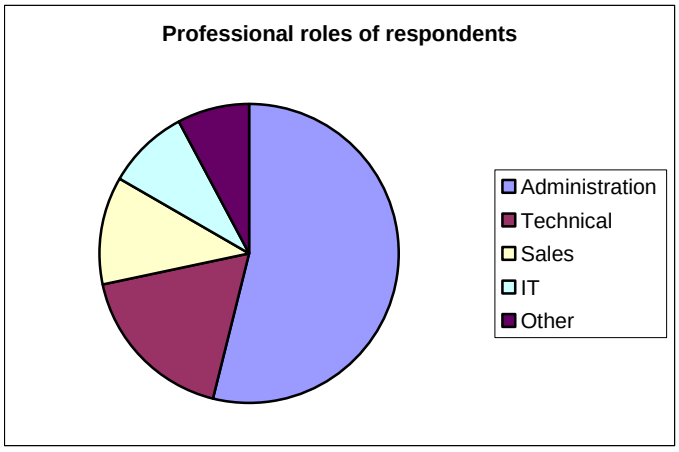

Figure 8 – Respondents by line of work

The general observations above will be taken into consideration in the coming discussion of the results related to our research questions as validity and reliability can be weakened by a skewed population.

7.2 Efficiency

There are two aspects of efficiency in this survey. 1: How much time is spent on private matters on the Internet? 2: What is the respondents view on their own efficiency regarding the constraints of the filter?

The first question is answered with the questions 1c ("How much do you use instant messaging per day in average?") and 1e ("How much do you use the Internet for private purposes per day in average?") in the questionnaire. If Internet filtering reduces cyberslacking, one would expect a difference in the average time between filtered and unfiltered employees claimed to spend on private surfing or

chatting. File sharing and listening to streaming radio does not necessarily demand the employees' attention, and this activity is therefore omitted here.

As we can deduce from Table 10, there are no big differences between the groups in the time spent on private tasks. There is a tendency that filtered employees spend *more* time on private surfing though, but this is more probably caused by other factors. In the previous section we saw that the filtered companies had an overweight of men, and that the average age was 8.6 years younger than in the non-filtered companies. The results in tables 6-9 above make it seem likely that the differences in Internet use between filtered and unfiltered employees in the survey are coincidental, and not caused by the restricting capabilities of the filter.

Question	Filter	No of answers	Mean	Std. Deviation	Std. Error Mean
1c	No	56	0,07	0,375	0,050
	Yes	48	0,42	0,919	0,133
1e	No	56	0,96	0,934	0,125
	Yes	48	1,17	0,953	0,138

Table 10 - Private Internet use related to filtering

We should also notice that the time spent on private surfing is quite low. The average employee spends 15 minutes per day on private tasks on the Internet, and this stand in contrast to the findings of [web@work, 2004], [Davies, 2001], [SecuComp, 2005] and [Young and Case, 2004] cited in Section 2.1, which all found much higher values.

That the groups have the same Internet surfing habits is perhaps not surprising; even those companies that filter their employees' Internet browsing usually allow access to news. And sure enough; our survey showed that 72.3% of the respondents visit news-sites weekly or daily (45.7%). "Leisure and sports" is less popular; 21.1% visit such websites on a weekly or daily basis. Websites belonging to one of the 8 remaining categories in question 1f of the survey (see Appendix A) are rarely or never visited. It seems likely that news-sites account for most of the private Internet traffic on corporate networks, and as long as these sites are not blocked, a filter will generally not affect cyberslacking. This is further supported by the fact that filter strictness - the number of categories blocked – gives no significant effect on time spent on private browsing.

In the questionnaire, we also asked the respondents in companies with a filter installed if they would visit the Internet more often if the filter was not present. Only one person did slightly agree with this, 10.7% did not know, and the rest slightly or strongly disagreed. This does not prove anything, but it is interesting as the trend is confirmed by the other findings in the survey.

The second question we want to answer is "what is the respondents view on their own efficiency regarding the constraints of the filter?". We try to find the answer to this with questions 1g (in your opinion, does private use of the network make you less efficient at work?) and statements 2a2, 2a5, 2a8 and 2a12 which all enquire if the respondents are blocked by the filter while working (see Appendix A, or two paragraphs down).

Only 3 respondents (2.9%) felt that private Internet surfing made them much less efficient at work. Interestingly, none of them used the Internet for private purposes, and one of them never used the Internet at all. 13.2% stated that private surfing made the a little less efficient, while the majority of 83.7% meant that it had no effect on their efficiency or even made them more efficient. Perhaps they

mean this because they only read news etc. during a lunch break or when they have nothing else to do. One could of course argue that few employees would admit that they waste their working time, and that asking the employees themselves could never produce a correct result. We agree with this, but these answers also indicate that most employees do not feel that there is a need to filter Internet access to improve efficiency, and that may affect thriving as pointed out by [Panina] in Section 2.2.

The respondents are not uniform in their answers to the questions asking if the filters hinder them in their work. The four statements they should give their opinion on were (translated from Norwegian):

1. The filter sometimes hinders my work (2a2)
2. The filter never blocks pages I need (2a5)
3. I feel that the filter makes me less efficient (2a8)
4. I am rarely or never blocked by the filter (2a12)

Almost all respondents had a meaning about these statements (they did not use the "do not know alternative"). Our general impression is that half of the respondents feel hindered while the other half does not, and this brings the mean close to 3 (middle alternative). There seems to be a clear overrepresentation of employees in technical roles among those who oppose the filter, while those working in administration feel less hindered. We should also notice that there are significant differences between the companies, probably because of different configuration of the filters or other reasons we are unaware of. There is greater support for statement 1 than for statement 3, the latter being more specific about efficiency. Nevertheless more than a third agrees with number 3, and claim that the filter is such an annoyance that it makes them less efficient in their jobs. There was also an open-ended question about efficiency, and several of the respondents used this opportunity to complain about the filter. A woman in administration was annoyed by the filter because she was blocked whenever she tried to book airline tickets for her colleagues, and therefore had to do the job by phone or fax. An employee in techs claimed that he had to take his work home and use his private network to accomplish certain parts of his job. Many respondents felt that too many web pages were being blocked, and that they did not understand how those pages could be harmful. As has been pointed out in Section 3.2, filters are far from flawless, and several studies have shown that all filters wrongfully block a lot of websites due to erroneous categorisation [Finkelstein, 2003], [Peacefire].

One of the IT-managers that were interviewed in connection with the project explained that security was not – and should not be – regarded as a democratic process in the company. Nobody liked to be obstructed or to have their personal freedom limited, but it was sometimes necessary to implement security measures, according to this IT-professional. Finding the perfect balance between user friendliness and security is a constant challenge for management and IT-staff. We can easily imagine that those responsible for IT-security feel that the importance and impact of their work is not recognised in the organisation, and that complaints usually come from people who do not see the whole picture. In this case, at least a third of the respondents feel that filtering decreases efficiency because the filter blocks websites they need. One can ask oneself what the outcome would be if it were documents or programs the employees could not access. Would this criticism be ignored, or would someone have to fix the problem immediately or else find himself a new employer?

Curious about the statements from employees and IT-managers, we decided to test a number of Norwegian URLs to see how the two market leading filters performed. The test and its results are presented in Section 7.4.1.

More research is needed to establish if the filters really pose a threat to efficiency or if annoyed employees just use this survey to give strategic support to their complaints about the annoying filters.

Judged from the results of this research however, there is little doubt that web filters decrease rather than increase efficiency at the workplace.

7.3 Attitudes – thriving and feeling of surveillance

7.3.1 Thriving

Does filtering have any effect on job satisfaction or thriving at work? We asked the respondents to state their opinion on the following (Translated from Norwegian):

1. Internet filtering makes the workplace a nicer place for the employees (2a1)
2. I'm often annoyed with the filter (2a3)
3. My colleagues rarely express any disliking towards the filter (2a9)
4. I like my work more after the filter was installed (2a14)

Almost a half of the respondents ticked the "Do not know" alternative on statement 4. After a closer look it's easy to see that the statement is poorly constructed, as it assumes that the filter was installed after the respondent started in the company. Those who started their career in the companies after the filter was installed cannot have an opinion on this matter.
The histograms below are graphic representations of the responses on statement 1-4, where low values (to the left) indicate negative attitude towards the filter and vice versa.

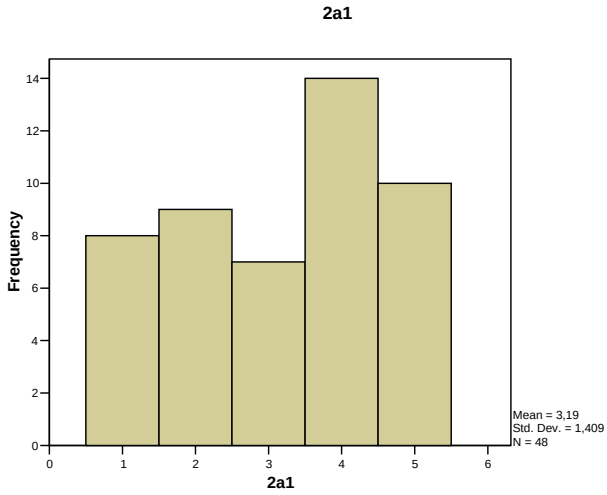

Figure 9 – Internet filtering makes the workplace a nicer place for the employees Agree -> Disagree

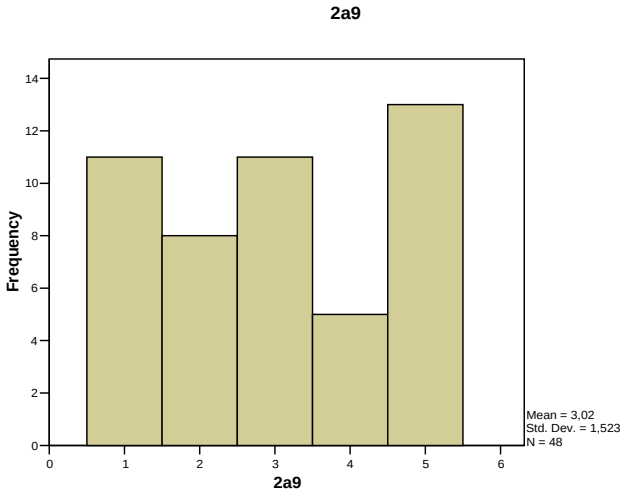

Figure 11 - My colleagues rarely express any disliking toward the filter, Agree -> Disagree

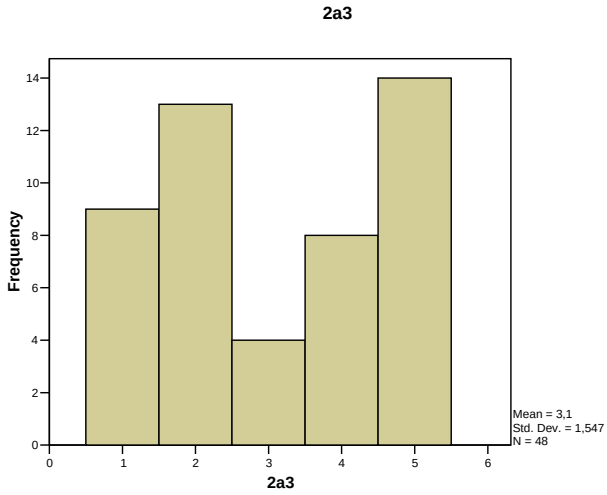

Figure 10 – I'm often annoyed with the filter Disagree -> Agree

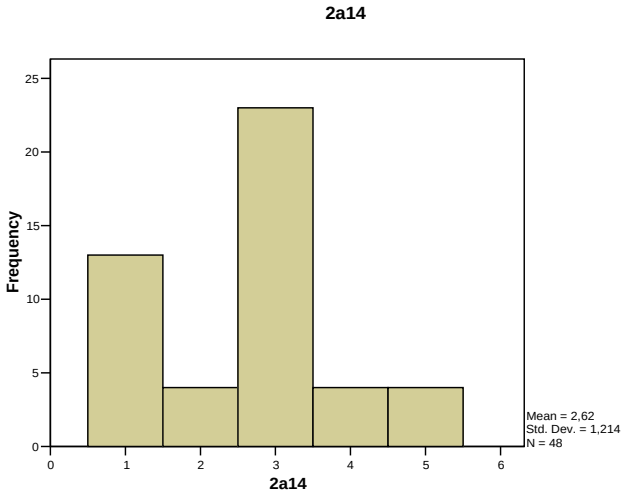

Figure 12 – I like my work more after the filter was installed Agree -> Disagree

As we can see from the histograms, it is difficult to draw conclusions from these statistics alone. The respondents are evenly distributed in their opinions, and the mean value for all statements is very close to 3 (except for 2a14). This spread in opinion also makes for poor significance because of the relatively few respondents. We get a much better understanding of the results if we look at the individual statistics for each company. Almost all the votes for the values to the extreme left are cast by respondents in the same company. A large number of the employees in this company also feel less efficient because of the filter, and this may explain why they are so annoyed by the filtering. The connection is hardly coincidental.

The fact that Internet filtering irritates some users comes as no surprise. It is much more interesting that so many feel that filtering *increases* thriving in the workplace, that it is in fact better to work in a company with filtering. This means that it is possible to install a filter without reducing job satisfaction, and even use it to increase thriving. Why are the employees in one company so much more negative to filtering than those in the other companies? This survey was not designed to give an exact answer to that question, but it indicates that the configuration of the filter - more specific the number of categories filtered and the strictness of the filter - plays a large role. [Witty] showed that some categories of websites are controversial to block, while others are not (e.g. porn), and according to our survey, there is no evidence that filtering affects efficiency in a positive way, rather the opposite. Taking this into account together with the fact that several respondents feel that too many pages are filtered for reasons they do not understand, it is tempting to advice all companies to configure their filters to block only uncontroversial sites - or sites that are believed to threaten security - namely porn, gambling, violence, racism, hacking etc. There is no point in filtering sites to reduce cyberslacking as this does not seem to be a problem in Norwegian companies anyway, and strict filters seems to be a nuance to the employees. We shall discuss this further in the summary. For now we conclude that filtering in and off itself do not reduce job satisfaction, but that it may if it obstructs the employees in ways they do not understand or agree with.

7.3.2 Surveillance

Surveillance or monitoring can not only be illegal or unethical; it can also have adverse effects on job satisfaction, morale and creativity, and increase stress [Luthans].

We made the following statements and asked the respondents whether they agreed or not.

1. How I use the Internet while I am at work is a private matter (2a4x)
2. I feel monitored at work because of the filter (2a10)
3. Censoring the Internet is always wrong (2a15)
4. In addition to these statements, we also asked if the filter was installed to monitor the employees (2b1).

The results in Figures 13-16 tell us that most of the respondents support Internet control in principle. 80% of the employees recognise that they cannot do whatever they want on the company network and that censoring the Internet is not always wrong. Still, almost one third of the respondents feel that they are monitored at work, at least to some extent, and 75% believe that surveillance of the employees is one of the reasons why the company installed a filter. Perhaps this distrust indicates that the employer or IT-department have not informed the employees sufficiently about the purpose of the filter.

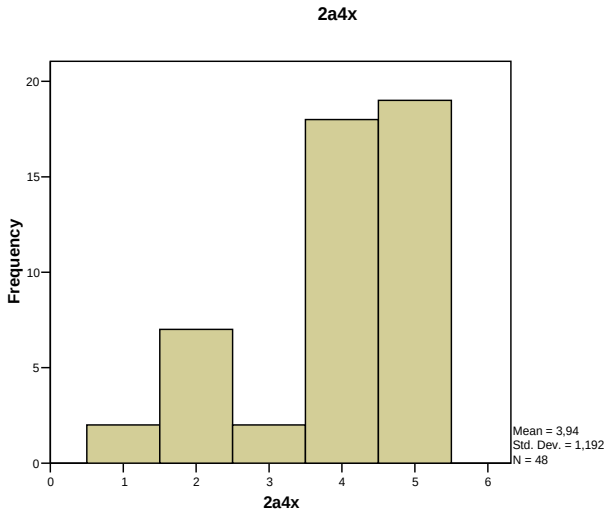

Figure 13 – How I use the Internet while I am at work is a private matter, Agree -> Disagree

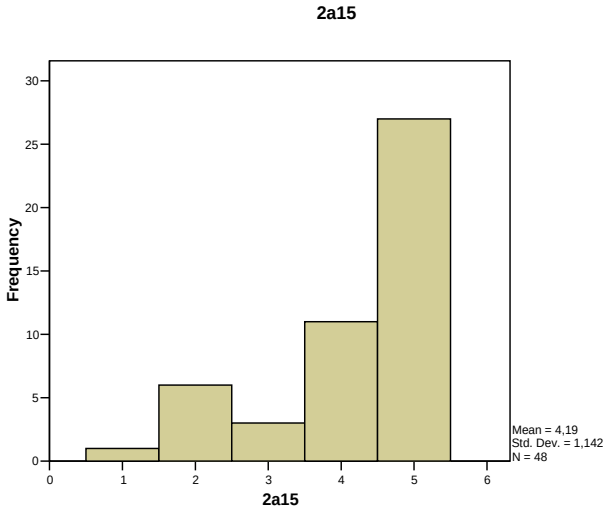

Figure 15 – Censoring the Internet is always wrong, Agree -> Disagree

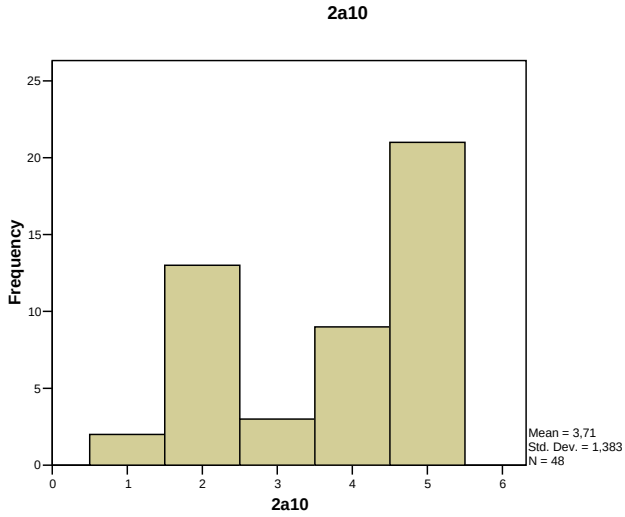

Figure 14 – I feel monitored at work because of the filter, Agree -> Disagree

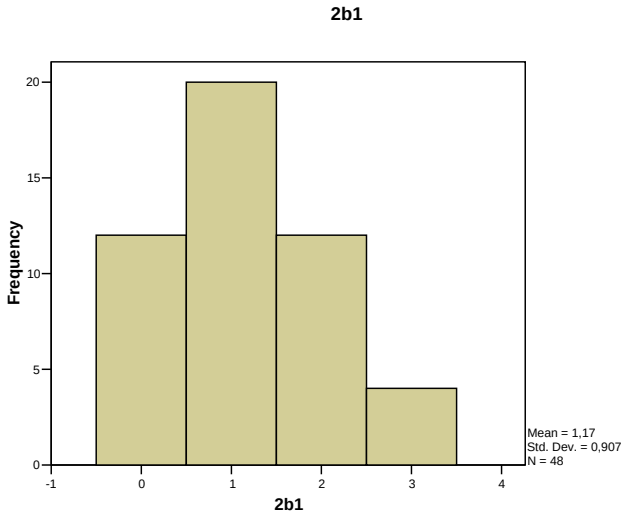

Figure 16 – The filter is installed to monitor the employees, Not important -> Very important

From the statistics we can find a connection between the feeling of being monitored and the time spent on the Internet (or vice versa). The strongest connection is between job-related use of the Internet and monitoring. In Figure 17, a high score indicates that the respondent feels monitored. One way to interpret this is that those who use the Internet very little are seldom exposed to the filter, and therefore do not feel monitored. Those who do not care about the filter or its monitoring capabilities use the Internet a lot. The middle group consists of users who spend some time on the Internet, but have feeling of being under surveillance. This last group would perhaps alter behaviour if the filter was

removed, using the Internet more. We find it difficult to say if that would be beneficial for the company or not.

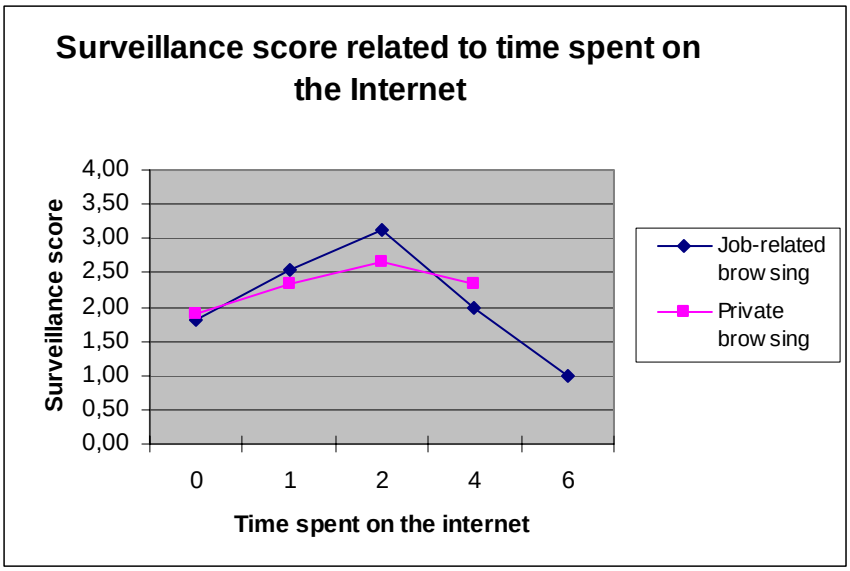

Figure 17 – Perceived degree of monitoring in relation to time spent on the Internet.

It seems that the respondents are divided in their opinions on surveillance and thriving. We find it likely that many more would accept filtering and be less suspicious about the managements' motivation for installing it if they were given more information about it. We say this based on the impression these results have given, and admit that there are no definite results in this survey that supports our belief.

7.4 Security

In Chapter 6, we found that filtering may contribute to security in classes 2, 3, and 4 of [Neumann, 1989]. Filtering might also have some effect in other classes, but we have not found it worthwhile to explore this further. In this section we present and discuss the results from several metrics as well as more results from the survey. The results are presented in the order of the classes of computer misuse. We start by presenting the general experiment testing for false categorisations of Norwegian URLs, as promised in Section 7.2.

7.4.1 Categorisation of Norwegian websites.

We tested a total of 190 addresses; most collected from well known search-engines like Google and Kvasir. The category "Top 52" contains the 52 most popular Norwegian websites according to the statistics of TNS Gallup [TNS, 2005]. Each webpage was inspected and categorised before we entered them into the URL-testers of Websense and SurfControl, respectively. The URL-testers utilise the same database as the real filters, so this test tells us how the filters perform in reality. If the filter categorised the page in a way that was clearly wrong (e.g. "Entertainment" instead of "Adult"), or that would increase the possibility that the page would be blocked, we called it a "wrong". If the page was categorised correctly, or in a fashion that was unlikely to affect the chance of blocking (e.g. "Business" instead of "Finance"), the categorisation was deemed correct. If the webpage was not in the filter database, it was marked "N/A". The results were unimpressive.

As Table 11 shows, there are significant differences in performance between the two filters. It seems that Websense has a more comprehensive database, but also a higher rate of error than SurfControl. Companies who have configured the filter to "Block if not categorised" will experience severely reduced availability when they need access to Norwegian pages. We recon that "Business", "Finance" and "Travel" are used for work-related tasks by many employees, but the filtering of those categories has a very low accuracy. We found that SurfControl may block as many as 85% (not categorised + wrongly categorised) of the pages in "Business". This will improve if the "Block if not categorised"-option is avoided, but then another problem will arise; Failure to block pages that should not be accessed by the employees. We assume that most companies would want to block the categories "Adult", "Games", "Chat" and "Gambling" to reduce the risk of malware-infection and cyberslacking. The filters we tested here, however, will allow almost one in three sites with games or adult content, and two out of three chat-rooms.

	Websense			SurfControl		
	Correct	Wrong	N/A	Correct	Wrong	N/A
Top 52	82,7	9,6	7,7	51,9	5,8	42,3
Travel	85,7	4,8	9,5	38,1	0,0	61,9
Business	50,0	14,3	35,7	14,3	7,1	78,6
Finance	77,3	0,0	22,7	27,3	0,0	72,7
Chat	33,3	33,3	33,3	33,3	33,3	33,3
Adult	67,6	10,8	21,6	73,0	8,1	18,9
News	85,7	4,8	9,5	61,9	0	38,1
Games	66,7	25,0	8,3	50,0	33,3	16,7
Gambling	100,0	0,0	0,0	42,9	0,0	57,1
Other	64,3	21,4	14,3	42,9	11,9	45,2
Overall Performance	**72,1**	**11,1**	**16,8**	**46,8**	**7,9**	**45,3**

Table 11 - Success rate of Internet filters categorising Norwegian webpages

The test gives rise to more doubts. First of all: Both filters claim that their databases will be updated the first time a user visit an uncategorised website. The author seriously doubts that www.dagbladet.no and www.aftenposten.no - which are two of the major Norwegian newspapers - have never been visited by a single user of Websense. Still those sites are not categorised. SurfControl on their side have not heard about www.telenormobil.no or www.brreg.no, to mention a few. Second: Both filters categorise both commercial airliners and typical charter airliners as "Travel", even though charter airliners are used almost solely for recreational travel. If the filters aim to reduce cyberslacking without obstructing business, it could be a good idea to diversify that category. We are sure that this is just one of many examples of logical errors in the categories.

7.4.2 Classes of computer misuse

Class C2 Hardware misuse:

Will filtering reduce unnecessary use of bandwidth? With 'Unnecessary', we mean private use of corporate network resources, such as private web browsing, listening to Internet radio and utilising instant messaging services or peer-to-peer file sharing. The questionnaire measures the use of all these resource-wasters, but since the measuring method is far from unbiased, the results can be questioned. However, we assume that inaccurate reporting is evenly distributed among the filtered and the unfiltered respondents.

Based on the assumption that the users will choose the best possible quality on the media they download, we have used these standard values when we measure bandwidth use:

Private browsing: 64 kb/s
Internet radio: 160 kb/s
Instant messaging: 10 kb/s
P2P: 200 kb/s

The "weighed sum" in Table 12 is calculated from how much a service is used, and how much bandwidth that service requires. Example: Browsing: 1.17 * 64 = 74.9

	Filtered	Unfiltered	Weight
Browsing	1.17	0.96	64
Radio	0.27	0.65	160
IM	0.42	0.07	10
P2P	0.00	0.00	200
Weighed sum	122.3	166.1	

Table 12 – Results: Metric C21 Bandwidth use

From Table 12, we see that filtering reduces bandwidth use with approximately (100 - (122/166)*100=) 26%. This is a substantial reduction, and could make a real difference in network costs. Unfortunately, there are great uncertainties related with the measurements, and the significance of the results is not good enough to draw a decisive conclusion, especially for Internet radio. With a standard mean error of 0.27/0.21 for Internet radio, there is a possibility that there is no or little difference between filtered and unfiltered users when it comes to radio listening. The low accuracy of the measurements forces us to conclude that even though there is a tendency, we cannot prove any bandwidth saving with Internet filtering. This does not correlate with the results in [Websense] cited in Section 2.3, and with the general claim of the filtering industry that Internet filters reduce strain on corporate networks.

Class C3 Masquerading

Metric C31 – Phishing: We used the URL testers of the two market leaders in Internet filtering, Websense and SurfControl, to see how new phishing sites were categorised. We got the URLs to test from www.antiphishing.org, the APWG discussion group, journalists and contacts in financial institutions. To be used for testing, we demanded that the sites should be:

- Working (the sites are often closed by the ISP's when the fraud is discovered, and then the URL database may very well be correct if it categorises the page as "Not categorised" or "Network error" or similar)
- New (a database of historic attacks exists on the Internet, but those phishing sites are usually closed down)
- Linked to in a genuine phishing mail widely distributed
- Aiming to steal information that could be used to access accounts, corporate networks etc.

This was ensured by reviewing a copy of the phishing mail, and by checking each phishing-site manually immediately before using the URL testers. New attacks happen every day, but only a few of them are reported in a way that makes them available to us. For this reason, the testing took place over

a prolonged period of time, from the 8th of April and up to the presentation of the thesis. In this period we tested 18 URLs, and discarded ca. 40 because the phishing-sites were already closed down. If the URL was not recognised and categorised as "Phishing and fraudulent sites" within one day after the phishing-mail was distributed, the filter failed to protect against that fraud.

Victimised company	Tested	SurfControl	Websense
Paypal	8th of April	**Yes**	No
Comcast	8th of April	No	**Yes**
Huntington Bank	8th of April	No	No
Charter one bank	8th of April	No[14]	**Yes**
VISA	8th of April	No	No
Planters bank	12th of April	No	No[15]
eBay	18th of April	No	No
Associated Bank	18th of April	No	No
Bank Of America	20th of April	No	No
Regions Bank	21st of April	No	No
Citizens Bank	26th of April	No	No
Marshall & Ilsley Bank	27th of April	No	No
Paypal	30th of April	**Yes**	**Yes**
South Trust Bank	2nd of May	No	No
VISA	19th of May	No	No
Paypal	23rd of May	**Yes**	No
Paypal	23rd of May	No	No
NCUA	26th of May	No	No
Percent correct		**16.7%**	**16.7%**

Table 13 – Results: Metric C 31 Successful categorisation of phishing sites

A success rate of 16.7% is low, but perhaps it is no big surprise. Fraud-sites like this are usually closed down very quickly after the bank or other financial institution the phish tries to exploit informs the ISP in question. Also, several of the phishing-mails we reviewed informed their "customers" that they only had 24 hours to provide requested information or to complete the needed "account update". During this very short time span, the producers of the filter must identify the fraudulent site, update the central filter database, and distribute this update to its customers. If the filter will make a difference, all this must be accomplished before the site is closed down, and this is apparently too ambitious. After all, how could the filter-companies discover a phishing-attempt quicker than the victims of that fraud?

Although we have insufficient data to draw strong conclusions, we are certain that Internet filters will not protect against phishing attacks in more than a few, isolated cases. The very nature of phishing; its swiftness and variability, render filters powerless. This conclusion is the opposite of what is claimed in [Websense2], cited in Section 6.1.

We believe that these results can be transferred to another class of misuse, namely C3. Metric C32 – Piggybacking: "Will the filter stop a DDoS-attack from a local host?" If a filter should be able to stop an attack like this, it would have to know the target of the attack and block all traffic to that server. The

[14] The site was categorised as "Adult/sexually explicit", and would probably have been blocked since most companies configure their filter to block pornographic sites.

[15] The site was still available April 18.th, but by then the categorisation was corrected.

time-span of a DDoS-attack is even shorter than that of a phishing fraud. According to Manik Bambha at the University of Southern California [Manik, 2004], 90% of all DDoS-attacks last less than one hour, which is obviously too short time to detect the attack and distribute an update. It is also likely that a network administrator would see this massive outgoing traffic and set a stop to it.

Class C4 Pest Programs *Setting up opportunities for further misuse*
We have not performed any experiments to support our theories for this class. We can still draw some conclusions with basis in the metric C31 – Phishing.

Malware prevention: Filters can and should block access to sites that are known to spread malware like spyware or trojans. However, we have seen that malware can spread to unprotected servers that then become carriers of infection. This means that a server that was safe and clean yesterday can be hazardous today, so filters must update the entire database every day to be sure that they do not allow malicious sites. Even if that was possible, there would still be a window of opportunity of 24 hours to spread an infection after the daily check was made. We believe that filtering will reduce the chance of malware infection through drive-by install, but more research is needed to quantify this reduction.

Spyware mitigation: “Can URL-filters prevent spyware or similar applications from connecting to a remote host?” If the remote host is new or unknown, filters will not increase the security. But spyware are active for a much longer period than fraudulent sites or DDoS-attacks are, so filters have a fair chance of stopping traffic to well-known sites. Just how much this will enhance security should be quantified through further research.
We have seen that Internet filters do not contribute to security in the way the producers and vendors claim. In Chapter 6, we identified several areas where filters could possibly contribute to security, but our theories on this have been rejected by the results of our experiments. With this, we conclude the chapter and continue to summary and conclusion.

8 Summary and conclusions

We have seen how Internet filtering can contribute to security and we have supported our theoretical deductions with experiments. It is clear from this work that Internet filtering can add to security in a few areas, for example when it comes to misuse of bandwidth. Filtering reduces the strain on company networks if it is configured to stop streaming media and file sharing. We do not, however, believe that it protects against phishing, leakage of information, outgoing DDoS-attacks or malware. There is no significant difference in the number of malware infections in computers filtered and unfiltered networks, and this may be because there are no differences in how the employees use the Internet.

Filtering decreases rather than increases the employees' efficiency. We have not found anything that support the filter-producers claims that filtering reduces private browsing, instant messaging or file sharing, or that cyberslacking is a problem in Norwegian companies. We find it likely that strict configuration of the filter will obstruct work-related use of the Internet and frustrate the employees, without giving any advantages. This is also supported by [Resnick]. The two most common filters lack a comprehensive database of Norwegian websites, and both will block innocent sites and/or allow pornographic or other malicious sites through the filter. We strongly recommend that IT-managers avoid the configuration-option "Block if not categorised", as it will block up to 50% of Norwegian websites.

Norwegian workers agree that the corporate network should never be misused, and they generally do not perceive filtering as monitoring or surveillance. Their thriving seems not to be affected by filtering unless the filter is too strict, and the attitude towards filtering is very much the same among the workers in both filtered and unfiltered networks.

9 Further research

The data that constitute the basis for our conclusions are not as comprehensive as we would prefer. A survey of a larger scale should be carried out to support our research and remove any doubts we might have. Metrics that can answer decisively if Internet filters offer any protection against outgoing DDoS-attacks and information-leakage from spyware and Trojans should be developed by the eager and well-equipped scientist who wants to contribute to a deeper understanding of security in filtering.

It has been argued that some companies install Internet filters to avoid the negative publicity that could follow if their employees where caught browsing dubious websites. This is not explored in this thesis, but would be an interesting question to investigate. There is nothing in our research that indicates that such a strategy would work since none of the respondents admitted to having visited controversial websites, but a broader survey might clarify this.

The sociological implications of Internet filtering are intertwined with the technical challenges. Our research could inspire researchers in other fields, for example organisational psychology, to investigate how Internet filtering affects an organisation and if organisations react differently to filtering. It is likely that some organisations more than others have success in implementing security measures without diminishing employee motivation or seeding mistrust. It would be interesting and useful to the security community to know more about success factors for smooth implementation.

It would also be interesting to see if filters could be rendered completely powerless by the use of redirects, dynamic addressing, some sort of UDP-encapsulation or other techniques that avoid filtering altogether. Internet filtering blocks one of the largest e-industries – pornography - effectively from corporate networks. This means that there probably is funding available to those who find a way to circumvent filtering.

10 References

Ad-Aware: Homepage of Ad-Aware software company http://www.lavasoft.com/

Aiello: J. R. Aiello: "Computer-based work monitoring: Electronic surveillance and its effects", 2003. *Journal of Applied Social Psychology*, 23**:** 499-507.

AT: The Norwegian Labour Inspection, citing an Icelandic survey by Gudbjorg Linda Rafnsdottir et al., Institute of Occupational Health, Reykjavik Iceland.
http://www.arbeidstilsynet.no/publikasjoner/arbeidervern/art78.html

Anti Trojan: Homepage of the organisation Anti-Trojan
http://www.anti-trojan.org/

Bishop: Matt Bishop: "Computer Security – Art and Science".
ISBN 0-201-44099-7 Addison-Wesley 2003

Bolstad: William M. Bolstad: "Introduction to Bayesian Statistics".
ISBN: 0-471-27020-2, or see http://www.bayesian.org/ for other resources.

Bullguard: Homepage of Bullguard antivirus company
http://www.bullguard.com/virus/96.aspx

Censorware: The Censorware project: http://www.censorware.net

Chal: J. Chalykoff and T.A. Kochan: "Computer-aided monitoring: its influence on employee job satisfaction and turnover", 1989. Personnel Psychology, 42**:** 807-834.

Creswell: John W. Creswell: "Research Design. Qualitative, Quantitative, and Mixed Methods Approaches".
ISBN 0-7619-2442-6 Second Edition, SAGE Publications 2003

Davies: R.A. Davies: "Cyberslacking: Internet abuse in the workplace", 2001. Electronic version found at http://www.liebertonline.com (Membership required)

Delio: Michelle Delio, "What They Know Could Hurt You", Wired News 2002
http://wired-vig.wired.com/news/privacy/0,1848,49430,00.html

eblocs "Online Identity Theft – How it Happens and How To Stop it " Electronic version found at http://www.eblocs.com/pornscams.html

FBI: FBI: "2003 Computer Crime and Security Survey".
http://www.symantec.com/region/in/smallbiz/library/insider.html

Finkelstein: Seth Finkelsteins homepage. http://www.sethf.com/anticensorware/

Fowler: F. Fowler, T. Mangione: "Standardized survey interviewing. Minimizing interviewer-related error", 1990
ISBN: 0-8039-3093-3, SAGE Publications Inc.

IBM: IBM: "Global Business Security Index 2004". http://www1.ibm.com/services/us/index.wss/rs/imc/a1008866?cntxtId=a1000400

IDC: International Data Group: "Worldwide Leader in Web Filtering Expands into Web Security". http://www.idc.com/getdoc.jsp?containerId=32218

InSe: PricewaterhouseCoopers: "Information Security: A strategic guide for business". ISBN: 1-891865-11-0

Issfaq: ISS: "Proventia Filter Database FAQ": http://www.iss.net/support/documentation/docs.php?product=39&family=13

Young & Case: Kimberly Young and Carl Case: "Internet Abuse in the Workplace: New Trends in Risk Management", CYBERPSYCHOLOGY & BEHAVIOR Volume 7, Number 1, 2004

Likert: A.N. Oppenheim: "Questionnaire design, interviewing and attitude measurement", ISBN 1 85567 043 7 New edition 1996. Pinter Publishers.

Luthans: Fred Luthans: "Organisational Behaviour", 1995. ISBN 0-07-113466-2 McGraw-Hill

Manik: Manik Bambha, University of Southern California: "DDOS". Electronic version of lecture found at http://netweb.usc.edu/cs558/Slides/manik.ppt

Miner: Barbara Miner: "Internet Filtering: Beware the Cyber Censors" 1998. Electronic version found at http://www.rethinkingschools.org/archive/12_04/net.shtml

NEU: P. G. Neumann and D. B. Parker: "A summary of computer misuse techniques". In Proceedings of the 12th National Computer Security Conference, pages 396–407, Baltimore, Maryland, USA, Oct. 10–13, 1989.

NIST: Standard for information security and metrics. http://www.nist.no

Oppenheim: A. N. Oppenheim: *Questionnaire design, interviewing and attitude measurement* Pinter Publishers 1996 ISBN 1-85567-043-7

Panina: John Aiello and d. Panina: "Acceptance of electronic monitoring and its consequences in different cultural contexts". Electronic version: http://www.rci.rutgers.edu/~jraiello/electrocult.doc

Peacefire: Homepage of the organisation Peacefire. http://www.peacefire.org/

Resnick et al: Paul Resnick, Caroline Richardson, Derek Hansen, Holly Derry and Victoria Rideout: "Does pornography-blocking software block access to health information on the Internet?", 2002. http://jama.ama-assn.org/cgi/content/abstract/288/22/2887

SecLab: Security Labs: “Security trends report 2004. “ http://www.websensesecuritylabs.com/resource/WebsenseSecurityLabs20042H_Report.pdf

SecuComp: Secure Computing: “Secure Computing filtering overview” http://www.securecomputing.com/index.cfm?skey=274

SPSS: Homepage of SPSS software company, producer of software for statistical analysis. http://www.spss.com/spss/

SSB1: Statistisk Sentralbyrå: ”Delen av alle føretak med tilgang til Internett, etter mengd sysselsette, næringsområde og fylke. 1998-2004. Prosent” Statistics found at http://statbank.ssb.no/statistikkbanken

SSB2 Statistisk Sentralbyrå: ”Tabell 03781: Sysselsatte, etter alder og kjønn” Statistics found at http://statbank.ssb.no/statistikkbanken

SSB3 Statistisk Sentralbyrå: ” Tabell: 03780: Personer i arbeidsstyrken, etter alder og kjønn”. Statistics found at http://statbank.ssb.no/statistikkbanken

Statistics: Homepage of StatSoft Software Company http://www.statsoftinc.com/textbook/glosfra.html

SurfControl: Homepage of Internet filter company SurfControl http://www.surfcontrol.com

Svec: C. M. Svec and J. R. Aiello: “Computer monitoring of work performance: Extending the social facilitation framework to electronic presence”. *Journal of Applied Social Psychology*, 23**:** 537-548.

Symantec: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=155

Symantec2: Definition and threat assessment of Nimda.A: http://www.sarc.com/avcenter/venc/data/w32.nimda.a@mm.html

Symantec3: Symantec: “Internet Security Threat Report, October 2003” http://enterprisesecurity.symantec.com/content.cfm?articleid=1539

Taylor: Nello Cristianini, John Shawe-Taylor: An Introduction to Support Vector Machines and Other Kernel-based Learning Methods Cambridge University Press. ISBN: 0-521-78019-5

Telenor: Telenor: ”IT sikkerhet - Trender og utvikling i 2004”http://www.telenor.no/bedrift/sikkerhet/news_show.php?news_id=35

Tien: Lee Tien: ”Blacklisting Bytes”, 2001. Electronic version found at: http://www7.nationalacademies.org/itas/whitepaper_1.html

Timber: Homepage of Timberline Technology: “Internet filter overview“ http://www.timberlinetechnologies.com/products/contentfilt.html

Tiny: Homepage of Tiny Software Company. http://www.tinysoftware.com/

TNS: TNS Gallup: "Statistics for March 2005 in cooperation with Mediebedriftenes Landsforening". Electronic version found at http://www.mediebedriftene.no/index.asp?id=26378&open=26378

Vila: www.tripod.com: "Website language stats" http://members.tripod.com/vstevens/papyrus/2001/pn010417.htm Statistics also available at http://www.uis.unesco.org

Web@work: Harris Interactive on behalf of Websense: "Web@work", 2004. http://ww2.websense.com/global/en/PressRoom/MediaCenter/Research/webatwork/webatwork2004.pdf

Websense: Homepage of Websense Internet filtering company. http://www.websense.com

Websense2: Websense press release: "PR_06 21 04_phishing_FINAL.pdf". http://ww2.websense.com/docs/misc/WebsensePressKit.zip

Wiki: Internet based encyclopedia. http://www.wikipedia.org

Winproxy: Bluecoat Security: "Preventing Spyware Infestation", 2003 www.winproxy.com/mktg/whitepapers/winproxy-Spyware-wp-v3.pdf

Witty: Monica T. Witty, Queens University Belfast: "Should Filtering Software be utilised in the Workplace?", 2004. Electronic version: http://www.surveillance-and-society.org/articles2(1)/filtering.pdf

Ølnes: Pål Spilling and Jon Ølnes: "Race common functional specification h 211 security of service management". http://citeseer.ist.psu.edu/329942.html, June 1995.

Appendix A - Questionnaires

The questionnaires are quoted in Norwegian only because we are afraid that a translation would not convey the meaning of the questions accurately.

Common part of questionnaire:

”God formiddag.

Datasikkerhet og beskyttelse mot trusler på internett er mye omtalt i media for tiden.
Denne spørreundersøkelsen er en del av et forskningsprosjekt ved Høgskolen i Gjøvik som skal se på hva slags tanker norske arbeidstakere har om sikkerhet og bruk av internett.

Besvarelsen din er helt anonym. Opplysningene du oppgir vil utelukkende bli brukt til å lage et statistisk grunnlag for videre analyse. Skjemaene blir samlet inn og oppbevart på en måte som gjør det umulig å spore en besvarelse tilbake til en bestemt person. Undersøkelsen har ingen tilknytning til bedriften du jobber i utover at den har sagt seg villig til å delta, og ingen personlige data du gir fra deg vil bli gitt videre til din arbeidsgiver.

Det vil ta ca **5 min** å fullføre skjemaet. Vennligst sett ring rundt det svaralternativet som passer deg best.”

DEL 1 - Alle spørsmål gjelder bruk av internett på arbeidsplassen:

1a. Når du er på jobb, hører du på radio via internett? (snitt pr. dag)

(Aldri 0-15 min 15-30 min 30-60 min 1-2 timer over 2 timer)

1b. Laster du ned film eller musikk via fildelingsprogrammer? (f.eks. Kazaa, Grokster, Morpheus, Direct Connect etc) Snitt pr dag

(Aldri 0-15 min 15-30 min 30-60 min 1-2 timer over 2 timer)

1c. Bruker du Instant Messaging-programmer som MSN, mIRC og ICQ på jobben? (gjennomsnittlig "pratetid" pr dag)

(Aldri 0-10 min 10-20 min 20-40 min 40-60 min over 1 time)

1d. I løpet av en vanlig arbeidsdag, hvor mye bruker du internett aktivt (leser/surfer)?

(Aldri 1-15 min 15-30 min 30-60 min 1-2 timer over 2 timer)

1e. Hvor mye av denne tiden gjelder private formål (f.eks. nyheter og netthandel)?

(Ingenting 1-15 min 15-30 min 30-60 min 1-2 timer over 2 timer)

1f. Hvilke typer internettsider har du besøkt via bedriftens nettverk, og hvor ofte?

	aldri	årlig	månedlig	ukentlig	daglig
Nyheter og media					
Sport/fritid/reise					
Nettbutikker					
Spill					
Dating/kontaktannonser					
Pornografi/erotikk					
Gambling/casino					
Nettsider om hacking					
Humor					
Jobbsøk					

1g. Hvis du av og til bruker internett til private formål når du er på jobb, føler du at dette gjør deg mer eller mindre effektiv på jobben?

Mye mindre effektiv litt mindre ingen betydning mer effektiv mye mer effektiv

1h. Har du noensinne hatt datavirus på PC'en din?

Vet ikke aldri årlig månedlig ukentlig daglig

1i. Har du noensinne hatt spyware på PC'en din? (Spyware er fremmede programmer som overvåker deg og din bruk av PC'en uten at du merker det, og må vanligvis fjernes av et eget anti-spionprogram som for eksempel "adAware")

Vet ikke aldri årlig månedlig ukentlig daglig

2c. Er der andre årsaker du mener ligger til grunn?

Svar:

2d. Har bedriften din regler for bruk av internett?

Ja Nei Vet ikke

Evt. Kommentar:

3. Har du ellers synspunkter som kan være av interesse i denne sammenhengen?

Svar:

Del 4 – Demografiske opplysninger
Til slutt ville vi sette pris på om du fylte ut opplysningene under. Disse vil gjøre det lettere for oss å forstå resultatene fra undersøkelsen.

Kjønn: Mann Kvinne

Alder:

Arbeidsområde: Administrasjon Teknisk/utvikling Salg IT Annet

Brett nå arket til A5-format og stift hjørnene slik at kun forsiden er synlig for den som samler det inn, eller legg skjemaet i en lukket konvolutt.

Tusen takk for at du tok deg tid til å delta! Ha en god dag videre!

Internettfilter: Vanlige merker er WebSense, SurfControl, Symantec, Proventia etc., men bedriften kan godt ha et filter fra en annen leverandør eller et egenutviklet filter. Du merker at du har et filter hvis du får beskjed om at en nettside du prøvde å gå inn på er blokkert, men så lenge du bare besøker sider som er tillatt er filteret "usynlig". Filteret kan også sperre for nedlasting av film og musikk, radio over internett, chatte-programmer og lignende.

Part two, users in filtered networks:

DEL 2

Et *internettfilter* (**IF**) er et program eller et system som hindrer deg i å gå inn på bestemte nettsteder/websites når du bruker internett på arbeidsplassen. Det er arbeidsgiveren eller IT-avdelingen (evt. i samarbeid med resten av de ansatte) som stiller inn hva slags sider man får besøke, og hvilke som blir blokkert. For mer informasjon om hva et IF er, se siste side.

Vi vil her komme med noen påstander som er relatert til internettfilter i større eller mindre grad, og vi vil gjerne vite i hvilken grad du er enig i disse påstandene. Vennligst sett kryss for det alternativet som passer best for deg: Helt enig – litt enig – vet ikke/likegyldig – litt uenig – helt uenig

	Helt enig	Litt enig	Vet ikke	Litt uenig	Helt uenig
1. IF gjør arbeidsplassen mer trivelig for de ansatte					
2. Filteret hindrer meg av og til i arbeidet					
3. Jeg irriterer meg ofte over filteret					
4. Hva jeg gjør på internett i arbeidstiden er en privatsak					
5. Filteret blokkerer aldri nettsider jeg trenger					
6. Jeg synes ikke det er galt om noen omgår filteret					
7. Det er greit at arbeidsgiver overvåker vår bruk av internett					
8. Jeg føler jeg blir mindre effektiv pga filteret					
9. Mine kolleger uttrykker sjelden misnøye med IF					
10. Jeg føler meg overvåket på arbeidsplassen pga filteret					
11. Jeg ville surfet mye mer på internett i arbeidstiden hvis vi ikke hadde filter					
12. Jeg blir sjelden eller aldri blokkert av filteret					
13. Ledelsen har tatt fra oss et frynsegode ved å installere filter					
14. Jeg trives bedre på jobben etter at filteret ble installert					
15. All sensur av internett er galt					
16. At de installerte filter viser at ledelsen ikke stoler på oss					

2b. Hvor viktig tror du disse grunnene er for at din bedrift har installert et filter (Svært viktig - uviktig)?

	Svært viktig	Viktig	Litt viktig	Uviktig
1. Overvåke hvordan ansatte bruker Internett				
2. Øke vår effektivitet				
3. Frigjøre nettressurser ved at vi bruker datanettet mindre				
4. Øke sikkerheten i bedriften				
5. Hindre at ansatte laster ned kopibeskyttet materiale				
6. Hindre at ansatte besøker nettsteder som er uforenlig med bedriftens profil (for eksempel pornografiske nettsteder)				

Part two, users in unfiltered networks:

DEL 2

Et *internettfilter* (**IF**) er (…) informasjon om hva et IF er, se siste side.

Vi vil her komme med noen påstander som er relatert til internettfilter i større eller mindre grad, og vi vil gjerne vite i hvilken grad du er enig i disse påstandene. Vennligst sett kryss for det alternativet som passer best for deg: Helt enig – litt enig – vet ikke/likegyldig – litt uenig – helt uenig

	Helt enig	Litt enig	Vet ikke	Litt uenig	Helt uenig
1. Et IF ville gjort det triveligere på arbeidsplassen					
2. Et IF vil være til hinder i arbeidet mitt					
3. Jeg tror jeg ville blitt irritert av et IF					
4. Hva jeg gjør på internett i arbeidstiden er en privatsak					
5. Jeg har kolleger som ofte ser porno på internett					
6. Jeg vil ikke at arbeidsgiveren min skal installere et IF					
7. Det er greit om arbeidsgiver overvåker vår bruk av internett					
8. Jeg tror jeg ville blitt mer effektiv med et IF					
9. Jeg føler meg støtt av at kolleger ser porno på internett					
10. Jeg ville følt meg overvåket på arbeidsplassen med et IF					
11. Mange av mine kolleger ville fått gjort mer om bedriften hadde begrenset tilgangen til internett					
12. All sensur av internett er galt					
13. Jeg mener at arbeidsgiver er i sin fulle rett til å regulere de ansattes bruk av internett i arbeidstiden					
14. Jeg ville trives bedre på jobben om IF ble innført					
15. Jeg tror ikke mine kolleger ville reagert negativt på et IF					
16. Installasjon av et IF er et utrykk for mistillit fra ledelsen					

2b. Hvor viktig tror du disse grunnene er for noen bedrifter installerer et filter (Svært viktig - uviktig)?

	Svært viktig	Viktig	Litt viktig	Uviktig
1. Overvåke hvordan ansatte bruker Internett				
2. Øke ansattes effektivitet				
3. Frigjøre nettressurser ved at ansatte bruker datanettet mindre				
4. Øke sikkerheten i bedriften				
5. Hindre at ansatte laster ned kopibeskyttet materiale				
6. Hindre at ansatte besøker nettsteder som er uforenlig med bedriftens profil (for eksempel pornografiske nettsteder)				

How we quantified the answers, Part 1:

Question 1a, 1b, 1d and 1e: Each quarter of an hour counted one point, so that "15-30 min" gave 2 points and "1-2 timer" gave the mean value of 4 quarters and 8 quarters; 6 points.

Question 1c: Each 10 minute period counted 1 point.

Question 1f: From left to right 0, 1, 2, 3, 4

Question 1g: -2, -1, 0, 1, 2

Question 1h, 1i: From left to right 0, 1, 2, 3, 4

How we quantified the answers, Part 2:

Part two consists of a number of statements that the respondents agree or disagree with. Some of the questions are negative to filtering, some are positive. To get a consistent score we decided that attitudes in favour of filtering were close to 5 while attitudes in opposition to filtering were closer to 1. This means that "Strongly agree" may give 1 or 5 points depending on the question.

2a, companies with filter:

Statement 1, 5, 7, 9, 11, 12, 14 from left to right 5, 4, 3, 2, 1
Statement 2, 3, 4, 6, 8, 10, 13, 15, 16 from left to right 1, 2, 3, 4, 5

2a, companies without filter:

Statement 1, 5, 7, 8, 9, 11, 13, 14, 15 from left to right 5, 4, 3, 2, 1
Statement 2, 3, 4, 6, 10, 12, 16 from left to right 1, 2, 3, 4, 5

2b, all companies:

From left to right 3, 2, 1, 0

Appendix B - The score sheet

The following pages contain the raw data from the questionnaires. The readers should note that the questions that are answered in posts 2a1 – 2b6 differs between filtered end non-filtered employees.

Some data are omitted to assure the anonymity of the respondents. This applies to company, gender and department.

Explanation to some posts:

Fr = Company (Data excluded)
Fi = Filter (0/1 = No/Yes)
41 = Gender (Data excluded)
42 = Age
43 = Department (Data excluded)

A blank space means that the question was not answered.

ID	Fr	Fl	1a	1b	1c	1d	1e	1f1	1f2	1f3	1f4	1f5	1f6	1f7	1f8	1f9	1f10	1g	1h	1i	2a1	2a2	2a3	2a4x	2a5	2a6	2a7x	2a8	2a9	2a10	2a11	2a12	2a13	2a14	2a15	2a16
1	X	1	0	0	0	4	2	4	2	3	2	0	0	0	3	3	1	0	1	1	1	1	1	4	1	2	1	1	1	2	3	2	2	1	2	2
2	X	1	0	0	0	2	0	4	0	0	0	0	0	0	0	0	0	1	0	0	2	5	1	5	1	1	5	1	1	5	1	1	2	1	5	1
3	X	1	0	0	0	4	1	3	3	0	0	0	0	0	0	0	0	1		1	1	1	1	5	1	2	2	1	1	2	1	2	4	1	5	1
4	X	1	0	0	0	4	1	2	1	3	0	0	0	1	2	1	0	1	0	3	1	1	3	2	1	1	4	2	2	4	2	1	3	1	4	3
5	X	1	0	0	0	1	0	1	0	2	0	0	0	0	0	0	0	-1	0	0	2	1	2	4	1	2	2	2	2	2	1	1	3	2	5	2
6	x	1	0	0	0	6	2	4	2	2	1	0	0	0	1	1	1	0	1	2	1	2	2	2	1	2	2	2	1	4	2	2	2	1	4	4
7	X	1	0	0	0	4	1	3	2	0	0	0	0	0	0	0	1	1	0		1	1	1	4	1	3	5	1	5	2	1	1	4	1	4	2
8	X	1	0	0	0	4	2	4	3	3	0	0	0	0	0	0	0	0	1	1	5	2	2	4	4	2	5	5	3	5	1	2	5	4	2	2
9	X	1	0	0	0	2	1	4	2	0	0	0	0	0	0	0	0	1	0	0	2	2	2	4	2	2	3	3	2	2	1	2	2	3	5	2
10	X	1	0	0	0	2	2	3	2	2	0	0	0	0	0	0	3	0	0	1	4	2	2	4	2	4	4	4	2	2	2	4	4	3	5	2
11	X	1	0	0	0	1	0	1	3	0	0	0	0	0	0	0	0	0	0		1	1	2	5	1	2	4	2	1	4	2	2	5	1	5	2
12	x	1	0	0	0	6	4	4	4	2	0	0	0	0	0	2	0	-1	1	1	1	1	1	5	1	1	1	1	1	1	2	1	1	1	5	1
13	X	1	0	0	0	2	1	3	1	0	0	0	0	0	0	1	1	1	1	1	2	1	1	4	1	1	4	1	1	1	1	1	5	1	5	3
14	X	1	0	0	0	1	1	4	0	0	0	0	0	0	0	0	0	0	0	0	2	2	3	5	4	4	2	4	2	4	1	4	4	3	5	4
15	X	1	0	0	0	1	1	2	2	0	0	0	0	0	0	0	0	0		0	3	4	4	2	3	3	4	2	3	5	1	3	5	3	4	5
16	X	1	0	0	0	4	1	3	1	3	0	0	0	0	0	0	2	-1	0	2	2	1	1	5	1	1	1	1	1	2	1	2	5	1	5	2
17	X	1	0	0	0	4	1	2	2	2	0	0	0	0	0	0	0	0	0	2	1	1	1	5	2	5	1	2	1	3	1	4	5	1	4	3
18	x	1	0	0	0	2	0	3	0	0	0	0	0	0	0	0	0	0			4	3	5	5	4	5	5	5	3	5	3	4	5	3	5	5
19	X	0	0	0	0	1	0	4	3	0	0	0	0	0	0	1	2	0	0	0	5	5	4	4	3	4	4	3	1	4	2	4	4	4	4	2
20	X	0	0	0	0	4	1	4	4	1	0	0	0	0	0	0	0	0	0	0	1	5	5	5	5	5	5	1	5	5	1	5	5	5	1	5
21	X	0	0	0	0	1	0	3	0	0	0	0	0	0	0	0	0	0			3	4	5	2	5	5	5	1	5	2	4	1	1	1	2	3
22	X	0	0	0	0	1	1	2	2	1	0	0	0	0	0	1	0	1	0	0	4	5	4	5	3	4	1	1	1	2	4	5	2	4	4	4
23	X	0	0	0	0	1	1	2	2	0	0	0	0	0	0	0	0	0	1	0	2	4	4	4	5	2	2	3	5	2	2	3	2	2	2	2
24	X	0	0	0	0	1	0	2	0	0	0	0	0	0	0	0	0	0	0	0	3	3	1	5	5	1	5	1	1	1	2	5	2	2	3	3
25	X	0	0	0	0	6	4	4	2	2	0	0	0	0	0	0	0	1	0	0	3	3	1	4	3	1	4	2	3	2	3	2	5	2	3	4
26	X	0	4	0	0	6	6	4	4	1	2	0	0	0	0	3	3	-1	0		1	3	1	4	5	2	2	3	3	4	3	4	1	2	2	2
27	X	0	0	0	0	1	1	3	0	0	0	0	0	0	0	0	0	0			1	5	5	4	3	3	4	3	3	3	3	2	5	3	3	2
28	X	0	0	0	0	1	1	4	0	0	0	0	0	0	0	0	0	0			3	5	3	2	3	2	5	3	3	3	3	2	4	3	3	2
29	x	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	5	5	5	5	5	5	3	5	5	3	3	3	1	3	2

30	X	0	0	0	0	1	1	3	2	0	0	0	0	0	0	0	0	-1	0		3	4	4	5	3	2	2	2	3	2	4	4	4	3	3	2
31	X	0	0	0	0	2	1	4	1	2	0	0	0	0	0	0	0	0	0	0	3	2	1	2	5	1	4	2	1	2	3	1	4	1	2	2
32	X	0	0	0	2	2	1	4	2	0	0	0	0	0	0	0	0	-1	2	2	5	5	5	2	3	2	1	3	3	3	1	3	4	3	3	2
33	X	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	2	0			3	3	2	3	3	2	3	2	2	3	4	4	1	4	5	2
34	X	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-2			3	5	3	5	3	2	4	3	1	3	3	5	4	3	3	2
35	x	0	0	0	0	1	1	3	2	0	0	0	0	0	0	0	2	0	0	0	3	5	5	5	5	5	3	3	3	5	3	5	5	3	3	2
36	X	0	1	0	0	2	1	2	1	0	0	0	0	0	0	0	2	0	0		3	3	3	5	5	2	2	3	1	2	4	2	1	3	3	2
37	X	0	0	0	0	1	1	3	0	0	0	0	0	0	0	0	0	0	0		3	3	3	5	5	5	2	1	5	5	1	2	5	3	3	2
38	X	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	5	5	4	5	5	3	3	2	5	3	2	5	3	3	2
39	X	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0			3	5	5	5	5	5	5	1	5	5	1	1	3	1	5	2
40	X	0	0	0	0	2	1	4	2	0	0	0	0	0	0	0	0	0	1		2	5	3	2	5	3	1	1	5	2	1	2	2	2	3	2
41	x	0	0	0	0	1	1	4	3	2	0	0	0	0	0	2	1	0	0		2	5	2	4	5	3	1	1	2	2	3	4	2	1	4	2
42	X	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	1	0		0	3	5	5	5	5	5	4	3	4	5	1	4	5	3	5	2
43	X	0	1	0	0	4	1	3	2	2	0	1	0	0	0	2	2	-1	0		4	5	2	5	5	1	4	2	1	4	2	4	5	1	2	2
44	X	0	10	0	0	6	1	2	2	1	0	0	0	0	0	2	1	0	1	0	4	4	4	4	5	3	5	3	1	2	4	3	4	2	3	2
45	X	0	4	0	0	1	1	4	0	0	0	0	0	0	0	0	0	1																		2
46	X	0	0	0	0	10	2	4	3	0	0	0	0	0	0	0	2	0	1		5	5	3	5	5	3	2	2	1	4	1	5	5	4	3	2
47	x	0	0	0	0	1	1	3	0	0	0	0	0	0	0	0	0	0	0		2	3	2	4	3	2	1	1	1	1	3	2	4	1	2	2
48	X	0	0	0	0	2	0	1	1	0	0	0	0	0	0	0	0	-2	1		3	3	3	5	3	3	5	3	1	3	5	3	5	3	3	2
49	X	0	4	0	2	10	1	3	2	2	0	0	0	0	0	1	1	0	1		1	2	1	2	5	2	2	1	3	2	1	4	2	1	2	2
50	X	0	0	0	0	2	1	3	3	0	0	0	0	0	0	0	0	0	1		3	5	3	5	3	4	2	3	1	2	3	1	4	3	4	2
51	X	0	0	0	0	1	1	4	2	1	0	0	0	0	0	1	1	1	1		3	5	3	5	3	3	4	3	2	5	3	2	5	2	3	2
52	X	0	10	0	0	1	1	2	2	0	0	0	0	1	0	0	0	0	1		3	5	5	4	3	5	4	1	1	5	4	1	4	3	3	2
53	x	0	0	0	0	1	1	4	1	0	0	0	0	0	0	0	0	0			3	3	3	3	3	3	2	3	3	2	3	4	4	3	3	2
54	X	0	2	1	0	6	2	3	1	1	0	0	0	0	0	1	1	1	1	2	3	2	2	4	3	2	5	2	3	4	4	4	4	2	2	2
55	X	0	0	0	0	4	1	3	0	0	0	0	0	0	0	2	3	-1	1	0	2	4	3	4	5	3	1	1	1	2	4	5	4	1	2	2
56	X	0	0	0	0	2	1	3	2	2	0	0	0	0	0	0	2	0	1		1	1	1	2	5	1	1	2	3	1	1	3	2	1	1	2
57	X	1	0	0	2	2	2	2	2	2	0	0	0	0	0	2	2	0	1	0	5	2	2	4	3	4	4	3	4	2	2	4	4	4	2	4
58	X	1	1	0	1	2	1	4	3	2	1	0	0	0	1	2	1	0	1	2	4	1	4	2		1	4	1	2	4	1	2	5	3	5	4
59	x	1	0	0	2	2	1	3	3	1	0	0	0	0	0	1	0	0	0	0	5	5	5	5	5	5	2	5	5	5	1	5	5	5	5	5

60	X	1	0	0	1	1	1	4	0	0	0	0	0	0	0	0	0	-1	0		5	5	5	2	5	5	1	5	5	5	1	5	5	5	5	5
61	X	1	0	0	0	4	1	4	2	2	0	0	0	0	0	0	2	0			4	5	5	5	5	5	1	5	5	3	1	5	5	3	5	4
62	X	1	0	0	0	2	1	3	2	1	0	0	0	0	2	2	1	0	0	2	3	1	2	4	1	5	2	2	2	2	3	4	3	2	3	2
63	X	1	0	0	0	1	0	2	0	0	0	0	0	0	0	1	0	1			2	1	4	5	1	5	5	2	4	4	1	1	5	4	5	2
64	X	1	0	0	0	4	1	4	1	1	0	0	0	0	1	2	2	1	1	2	2	1	2	3	2	5	1	2	3	4	4	2	3	3	4	3
65	x	1	0	0	0	1	0	4	0	0	0	0	0	0	0	0	0	1	0		5	5	5	4	3	5	2	1	5	5	1	5	5	5	5	5
66	X	1	1	0	2	2	1	3	3	2	2	0	0	0	0	3	0	0	0	0	5	3	1	3	5	3	5	3	3	3	3	5	3	3	1	3
67	X	1	0	0	2	2	2	4	2	1	1	0	0	0	0	2	1	0	0	1	5	5	5	5	5	5	5	5	1	5	2	2	5	2	4	4
68	X	1	0	0	5	6	4	4	2	2	2	0	0	0	2	2	2	0	0		3	3	2	4	4	5	4	4	4	5	1	4	5	3	2	5
69	X	1	0	0	0	1	1	2	1	1	0	0	0	0	2	0	1	0	0	0	4	3	5	5	5	5	4	4	4	5	2	5	5	3	4	4
70	X	0	0	0	0	1	1	4	0	0	0	0	0	0	0	0	0	0	1		3	5	5	1	5	5	1	1	5	5	1	3	5	1	5	1
71	x	0	0	0	0	2	1	4	2	0	0	0	0	0	0	0	1	0	1		3	5	5	3	5	5	5	1	1	5	1	5	5	3	4	5
72	X	0	0	0	0	1	0	3	2	0	0	0	0	0	0	0	0	0	1		5	5	5	4	3	2	4	1	3	5	4	3	5	5	2	5
73	X	0	0	0	0	2	1	4	3	1	0	0	0	0	0	0	2	0			3	3	3	5	5	3	4	1	2	4	1	5	4	1	5	4
74	X	0	0	0	0	1	1	4	3	2	0	0	0	0	0	0	0	-1	0		3	5	2	5	3	2	2	1	1	2	5	1	5	3	4	4
75	X	0	0	0	0	2	1	4	2	0	3	0	0	0	0	0	0	0	1		3	3	3	4	3	4	2	1	3	2	1	4	2	1	3	3
76	X	1	0	0	1		1	4	0	4	1	0	0	0	0	1	1	0	0		2	5	5	5	5	5	4	5	5	5	1	5	5	3	5	2
77	x	1	0	0	1	4	1	4	2	1	0	0	0	0	0	1	1	0	1	0	3	3	2	4	4	4	2	4	5	2	1	2	2	3	4	2
78	X	1	0	0	1	6	1	4	2	1	0	0	0	0	0	0	3	1	0	0	5	5	4	4	5	5	5	5	3	5	1	5	5	5	5	5
79	X	1	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	-2			5	5	5	5	5	3	5	5	5	5	1	5	5	3	5	5
80	X	1	0	0	0	4	2	4	3	3	0	2	0	0	0	0	0	0	1	2	4	2	2	4	2	5	1	5	2	2	1	5	5	2	5	2
81	X	1	1	0	1	10	1	4	3	4	1	0	0	0	0	2	2	-1		0	4	5	5	5	5	5	2	5	1	5	1	1	5	1	5	5
82	X	1	0	0	0	10	1	4	0	1	0	0	0	0	0	1	0	0	0		4	5	4	5	5	3	5	5	5	5	1	2	5	3	5	1
83	x	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0		3	5	3	5	3	3	4	3	3	3	3	5	5	3	5	5
84	X	0	0	0	0	1	1	2	2	0	0	0	0	0	0	0	0	0	1		3	3	1	2	5	2	2	3	1	1	3	2	4	3	3	2
85	X	1	0	0	0	1	1	3	1	0	0	0	0	0	0	0	2	0		2	4	5	3	4	5	5	5	5	3	5	1	5	4	3	3	4
86	X	1	0	0	0	2	1	4	2	0	1	0	0	0	0	0	1	0			3	5	5	2	5	4	4	5	5	5	1	5	3	1	3	4
87	X	1	0	0	1	1	0	1	1	0	0	0	0	0	0	0	1	0			4	5	5	4	5	5	4	5	5	5	1	5	5	3	5	5
88	X	1	0	0	0	2	1	3	1	1	0	0	0	0	0	0	2	0	0	0	4	2	4	5	4	2	4	5	3	4	1	5	4	3	4	4
89	x	1	0	0	0	10	2	4	4	2	1	0	0	0	0	3	4	1			4	4	2	1	5	5	5	5	5	5	1	4	4	4	5	1

90	X	1	0	0	0	1	1	4	4	0	0	0	0	0	0	0	4	2			5	5	5	5	5	5	1	5	3	5	1	5	5	3	5	1
91	X	1	0	0	0	6	4	4	4	3	0	0	0	0	0	2	0	0	0		4	5	5	4	5	5	5	5	5	5	1	5	5	3	2	5
92	X	1	0	0	0	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0	3	3	3	4	5	5	4	3	3	2	1	3	3	3	5	2
93	X	1	10	0	0	1	1	4	0	3	0	0	0	0	0	3	3	2	0	0	4	3	4	1	3	2	4	5	4	2	1	5	4	3	4	2
94	X	1	0	0	0	1	1	3	1	0	0	0	0	0	0	0	3	0	0	0	3	3	4	2	4	4	2	3	3	4	3	5	2	3	2	2
95	x	0	0	0	0	3	1	2	3	0	0	0	0	0	0	1	0	1			1	3	2	4	5	1	2	1	3	1	2	2	2	1	3	2
96	X	0	0	0	0	3	1	2	1	2	0	0	0	0	0	0	2	0	1	1	3	3	3	2	5	3	4	3	1	3	2	4	2	3	3	3
97	X	0	0	0	0	2	1	4	3	3	0	0	0	0	0	0	0	-1			2	4	2	4	3	3	1	2	3	4	3	2	4	2	4	2
98	X	0	1	0	0	3	1	4	3	0	0	0	0	0	0	0	0	-1	0		1	1	1	5	5	1	5	1	1	5	1	5	5	1	1	1
99	X	0	0	0	0	3	1	4	1	0	0	0	0	0	0	2	0	1	0		3	5	2	5	5	5	5	1	1	5	1	5	5	1	4	5
100	X	0	0	0	0	3	1	4	2	0	0	0	0	0	0	0	1	1	0		3	3	2	4	3	4	4	3	3	2	3	4	4	3	3	2
101	x	0	0	0	0	3	1	3	4	0	0	0	0	0	0	2	0	0	0		2	4	3	4	5	2	5	1	2	2	1	5	4	1	4	2
102	X	0	0	0	0	3	0	1	1	1	0	0	0	0	0	0	0	0	1	0	3	5	5	5	3	5	3	3	3	5	3	5	5	3	3	5
103	X	0	0	0	0	1	1	3	3	0	0	0	0	0	0	0	0	0	0		1	5	5	5	5	1	1	1	1	5	1	1	1	1	3	5
104	X	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0			1	5	5	5	3	5	5	3	1	5	3	5	5	3	5	5

ID	2b1	2b2	2b3	2b4	2b5	2b6	2c	2d	3	41	42	43
1	3	0	1	2	0	2	0	1	0	X		X
2	0	3	0	3	3	3	1	1	0	X	41	X
3	2	3	0	2	1	1	1	1	1	X	29	X
4	0	2	1	3	1	2	0	1	0	X	33	X
5	1	2	1	2	2	2	0	1	1	X	27	X
6	0	1	1	3	2	2	0	1	0	X	27	X
7	1	3	2	3	1	3	0	1	1	X	44	X
8	0	1	0	3	1	2	0	1	0	X	39	X
9	2	2	2	3	2	3	0	1	1	X	38	X
10	3	2	1	3	2	3	1	1	0	X	36	X
11	2	3	1	3	0	2	0	1	1	X	33	X
12	3	1	0	3	2	3	0	1	0	X	43	X
13	3	1	0	3	0	3	0	1	0	X	36	X
14	0	2	3	3	3	3	0	1	0	X	58	X
15	2	0	0	3	2	3	0	0	0	X	53	X
16	1	2	2	2	0	3	0	1	1	X	28	X
17	1	3	2	2	2	2	0	1	0	X	42	X
18	0	3	3	3	1	3	0	1	0	X	55	X
19	2	2	2	2	1	2	0	1	0	X	56	X
20	1	1	1	2	1	3	0	1	0	X	39	X
21	3	3	0	3	1	2	0	0	0	X	42	X
22	1	2	1	2	1	2	0	1	0	X	50	X
23	0	0	0	1	1	2	0	0	0	X		X
24	2	2	1	2	2	2	0	1	0	X	61	X
25	1	2	1	2	0	2	0	0	0	X	41	X
26	3	2	1	1	1	2	0	0	0	X	27	X
27	2	1	1	3	2	3	0	1	0	X	47	X
28	2	1	1	2	3	3	0	0	0	X	59	X
29	2	2	1	2	1	2	0	0	0	X	60	X
30	1	1	0	2	1	2	0	1	0	X	56	X
31	2	3	2	2	0	2	0	0	0	X	39	X
32	2	2	2	2	2	2	0	1	0	X	40	X
33	2	2	3	1	1		0	1	0	X	42	X
34	1	1	0	1	1	2	0	1	0	X	58	X
35	0	0	2	3	0	0	0	0	0	X	53	X
36	2	3	2	1	0	3	0	1	0	X	50	X
37	1	1	1	3	3	3	0	1	0	X	52	X
38	1	2	1	3	3	3	0	-1	0	X		X
39	1	1	1	1	1	1	0	0	0	X	51	X
40	2	1	1	1	1	3	0	1	0	X	47	X
41	1	2	2	3	2	2	0	1	0	X	50	X
42	1	2	2	3	2	2	0	1	0	X	43	X
43	1	3	3	3	2	2	0	-1	0	X	31	X
44	1	2	2	2	2	3	0	0	0	X	45	X
45							0	0	0	X	58	X
46	1	2	2	1	3	3	0	0	0	X	48	X
47	2	2	2	2	2	2	0	0	1	X	62	X
48	1	3	2	3	1	3	0	0	0	X	46	X
49	2	1	2	2	1	0	0	-1	0	X	26	X
50	1	2	0	2	3	3	0	0	1	X	42	X
51	2	1	2	1	3	1	0	0	0	X		X
52	1	0	1	3	2	3	0	0	0	X	40	X
53	2	3	2	3	2	3	0	0	0	X	45	X
54	0	1	2	3	0	2	0	1	1	X	53	X

55	1	3	2	3	2	3	0	-1	0	X	45	X
56	2	2	1	1	1	2	0	0	0	X	33	X
57	0	3	2	3	3	3	0	1	0	X	42	X
58	2	2	2	3	3	3	0	1	0	X	32	X
59	1	1	1	3	1	2	0	1	0	X	42	X
60	1	3	2	3	3	3	0	1	0	X	46	X
61	0	2	1	3	2	3	0	1	0	X	36	X
62	1	1	2	3	1	3	0	1	0	X	38	X
63	2	2	2	3	3	3	0	1	0	X	41	X
64	1	1	3	1	2	3	0	1	0	X	42	X
65	2	3	3	3	0	3	0	1	0	X	50	X
66	2	2	0	2	3	3	0	1	0	X	61	X
67	1	2	3	3	3	3	0	1	0	X	39	X
68	1	1	2	3	1	3	0	1	0	X	30	X
69	1	2	1	1	1	2	0	1	1	X	53	X
70	3	3	3	3	3	3	0	-1	0	X	52	X
71	0	0	0	3	2	1	0	1	0	X	44	X
72	0	2	2	3	1	2	0	-1	0	X	55	X
73	1	1	0	3	0	2	0	-1	0	X		X
74	0	3	1	3	0	2	0	-1	0	X	39	X
75	0	1	1	3	2	2	0	0	0	X	37	X
76	0	3	2	3	3	3	0	1	0	X	44	X
77	1	3	2	3	2	3	0	1	0	X	25	X
78	0	3	2	3	1	3	0	1	0	X	22	X
79	2	3	3	3	3	3	0	1	0	X	42	X
80	1	3	2	2	1	2	0	1	0	X	33	X
81	1	3	0	2	0	3	0	-1	0	X	28	X
82	1	3	2	3	3	3	0	1	0	X	26	X
83	2	2	2	2	2	2	0	0	0	X	41	X
84	2	2	0	1	3	3	0	-1	0	X	53	X
85	1	3	2	3	1	1	0	0	0	X		X
86	2	3	1	2	1	2	0	1	1	X	24	X
87	2	3	2	3	2	2	0	1	0	X	29	X
88	2	3	2	3	3	3	1	1	0	X	39	X
89	0	1	1	0	2	3	1	1	0	X	44	X
90	1	3	3	3	3	3	0	1	0	X	31	X
91	1	2	2	2	2	2	0	1	0	X	35	X
92	1	1	2	3	1	2	0	1	0	X	57	X
93	0	0	0	0	0	0	1	1	0	X	25	X
94	1	3	2	1	1	3	0	1	0	X	32	X
95	1	1	1	1	1	1	0	-1	0	X	62	X
96	2	1	0	1	2	2	0	0	0	X	47	X
97	2	1	0	2	1	1	0	0	0	X	55	X
98	0	1	1	3	0	3	0	-1	0	X	41	X
99	0	3	3	3	2	2	0	0	0	X	49	X
100	2	2	1	2	1	3	0	0	0	X	36	X
101	2	1	2	3	2	2	0	1	0	X	64	X
102	0	3	1	3	1	1	0	-1	1	X	56	X
103	2	0	0	0	0	3	0	-1	0	X	49	X
104	1	2	2	3	1	1	0	0	0	X	53	X

Appendix C - Mail to companies

God morgen,

Jeg ønsker å gjennomføre en spørreundersøkelse blant brukere av Websense. Undersøkelsen er en del av et prosjekt som skal finne sikkerhetsgevinster og avdekke svakheter i URL-filtere. Målet er å gi IT-ansvarlige og beslutningstakere et bredere grunnlag for kost/nytte-analyse av slike sikkerhetsprodukter.

Spørreundersøkelsen skal kartlegge surfevaner, bruk av P2P-programmer og strømmende media, og måle holdninger til sikkerhet og filtrering. Jeg vil ikke spørre om teknisk informasjon eller personlige opplysninger.

Bedriftens kostnad: Jeg ønsker å dele ut et spørreskjema til 10-30 av de ansatte. Det tar ca 5 minutter å fylle ut skjemaet, og jeg vil samle inn svarene senere på dagen. Belastningen blir altså et sted mellom 1 og 2,5 timeverk.

Hva bedriften kan få ut av det: Jeg vil kort tid etter undersøkelsen utarbeide statistikk for bedriften. Statistikken (altså for egen bedrift) med kommentarer vil bli gjort tilgjengelig for bedriften om ønskelig. De bedriftene som vil får også et eksemplar av den endelige rapporten.

Anonymitet: Bedriftens deltakelse i prosjektet er hemmelig. Ingen opplysninger som kan identifisere bedriften eller deltakerne vil bli offentliggjort eller oppgitt til veileder og medstudenter. Alle data blir anonymisert. Ingen av de opplysningene som samles inn kan brukes til å kartlegge IT-systemet eller sikkerhetstiltakene bedriften har.

Studiets hjemmeside: http://nislab.hig.no

Ha en god dag videre!

Mvh Joachim Deisz

Appendix D - Mail to filtercompanies

We wrote a mail to Websense customer service to be sure that their URL-tester used the same database as their customers do.

Mail to Websense:

"*Good afternoon,*
I'm writing a masters thesis titled "Security added by Webfilters", and one of the things I'm looking into is if URL-filters can prevent phishing. A possible practical approach is to check known fraudulent websites with the "Websense site lookup tool" to see how the site is categorized. Would this method give a correct picture of how Websense filters perform in reality in this matter? Is the database of the site lookup tool updated as often as "the real thing"?

The category "Network error", what does it mean? That the link or URL is dead, i.e. that the site is down?

Best regards
Joachim Deisz
http://nislab.hig.no"

Their reply written by Ronnie Manning:

"*Joachim,*
Hello... Yes, the Websense Site Lookup Tool is updated as often as our customer's products. And for the category "network error" that means that the site is not resolving to an IP.

Best,
Ronnie "

We also wrote a mail to the SurfControl customer service to be sure that their URL-tester was up to date as well.

Mail to SurfControl:

"*Good afternoon,*
I'm writing a masters thesis titled "Security added by Webfilters", and one of the things I'm looking into is if URL-filters can prevent phishing. A possible practical approach is to check known fraudulent websites with "SurfControl Filter Testing and Submissions" to see how the site is categorized. Would this method give a correct picture of how Surf Control filters perform in reality in this matter? Is the database of the site lookup tool updated as often as "the real thing"?

What happens if a link goes dead? What category will it be inserted into?

Best regards
Joachim Deisz
http://nislab.hig.no"

Their reply written by Carl Gottlieb:

"*That is correct,*

We have a central database of URL's and IP's along with an associated category (e.g. phishing) which is manually updating on a daily basis on the central location at Surfcontrol, with the clients' product downloading this daily list automatically on a daily basis. If a URL or IP goes dead, it will remain categorised until we find it centrally at Surfcontrol and remove it from our list.

The test a site lookup tool on the website is real time.
Hope that helps!

Appendix E – Complete testdata from Norwegian URLs

ID	URL	Kategori	Websense	J	N	X	Surfcontrol	J	N	X
1	www.vg.no	Nyheter	News	1			News	1		
2	www.msn.no	Nyheter	News	1			Searchengines	1		
3	www.dagbladet.no	Nyheter	N/A			1	News	1		
4	www.startsiden.no	Annet	Searchengines and portals	1			Searchengines	1		
5	www.tv2.no	Nyheter	News	1			News	1		
6	www.gulesider.no	Annet	Searchengines and portals	1			Searchengines	1		
7	www.aftenposten.no	Nyheter	N/A			1	News	1		
8	www.kvasir.no	Annet	Searchengines and portals	1			Searchengines	1		
9	www.finn.no	Annet	Webshop		1		Vechiles		1	
10	www.sol.no	Annet	Searchengines and portals	1			Searchengines	1		
11	www.nrk.no	Nyheter	News	1			News	1		
12	www.online.no	Portal	Hosting	1			Hosting Sites	1		
13	www.dnbnor.no	Finans	Financial Data and Services	1			Financial Data and Services	1		
14	www.dinside.no	Portal	Searchengines and portals	1			Hosting Sites	1		
15	www.eniro.no	Annet	Business		1		N/A			1
16	www.start.no	Onlinespill	Sports		1		Searchengines		1	
17	www.bt.no	Nyheter	News	1			News	1		
18	www.itavisen.no	Nyheter	Information Technology	1			Computing and Internet	1		
19	www.qxl.no	Annet	Internet auctions	1			Shopping	1		
20	www.telenormobil.no	Annet	Information Technology	1			N/A			1
21	www.tvnorge.no	Annet	Entertainment	1			Entertainment	1		
22	www.dn.no	Nyheter	Financial Data and Services	1			News	1		
23	www.hegnar.no	Finans	Financial Data and Services	1			Finance & Investment	1		
24	www.ba.no	Nyheter	News	1			News	1		
25	www.adressa.no	Nyheter	News	1			News	1		

26	www.hardware.no	Annet	Information Technology	1			Games		1	
27	www.digi.no	Annet	Information Technology	1			Computing and Internet	1		
28	www.aftenbladet.no	Nyheter	News	1			News	1		
29	www.tinde.no	Annet	Real Estate	1			N/A			1
30	www.n3sport.no	Annet	Sports	1			Sports	1		
31	www.inpoc.no	Annet	Information Technology	1			Computing and Internet	1		
32	www.bilnorge.no	Annet	N/A			1	Vechiles	1		
33	www.fedrelandsvennen.no	Nyheter	News	1			N/A			1
34	www.catch-gamer.no	Onlinespill	Games	1			N/A			1
35	www.dt.no	Nyheter	News	1			News	1		
36	www.internettkatalogen.no	Annet	Reference Materials	1			N/A			1
37	www.barnimagen.com	Annet	Society and Lifestyles	1			N/A			1
38	www.amobil.no	Annet	Business and Economy		1		N/A			1
39	www.f-b.no	Nyheter	News	1			N/A			1
40	www.haugesunds-avis.no	Nyheter	News	1			N/A			1
41	www.imarkedet.no	Finans	Financial Data and Services	1			N/A			1
42	www.oslobors.no	Finans	Financial Data and Services	1			N/A			1
43	www.akam.no	Nettbutikk	Shopping	1			N/A			1
44	www.dinbaby.com	Annet	Society and Lifestyles	1			N/A			1
45	www.tu.no	Nyheter	Business and Economy	1			N/A			1
46	www.propaganda-as.no	Nyheter	News	1			N/A			1
47	www.mozon.no	Helse	Health	1			N/A			1
48	www.agderposten.no	Nyheter	News	1			N/A			1
49	www.t-a.no	Nyheter	News	1			N/A			1
50	www.orapp.no	Finans	Financial Data and Services	1			N/A			1
51	www.ukeavisen.no	Nyheter	Education materials		1		N/A			1
52	www.itavisen.biz	Finans	N/A			1	N/A			1
53	http://www.6pack.no/	Portal	Searchengines and portals	1			N/A			1

54	http://www.1001spill.no/	Onlinespill	Games	1			Games	1		
55	http://www.123spill.no/	Onlinespill	Games	1			Games	1		
56	http://www.sol.no/spill/	Onlinespill	Games	1			Games	1		
57	http://www.vg.no/spill/?pf=pc	Onlinespill	News		1		News		1	
58	http://www.aftenspill.no/	Onlinespill	Games	1			Hobby and recreation		1	
59	http://www.dagbladet.no/spill/	Onlinespill	News	1			News		1	
60	http://elitespill.com/	Onlinespill	Games	1			N/A			1
61	http://www.rikstoto.no/	Pengespill	Gambling	1			Gambling	1		
62	http://www.freeplay.no/	Onlinespill	Games	1			Games	1		
63	http://www.jippii.no/jsp/index.jsp	Annet	Hosting		1		Downloads	1		
64	http://gamer.no/	Spill	Games	1			Games	1		
65	http://klovn.no/moro.htm	Onlinespill	Society and Lifestyles		1		Entertainment	1		
66	http://www.oddsnet.com/	Pengespill	Gambling	1			Gambling	1		
67	http://www.lotteritilsynet.no	Annet	Government	1			N/A			1
68	http://www.dvdstrax.com/no/	Nettbutikk	N/A			1	Shopping	1		
69	http://www.kondomeriet.no/?osadcampaign=infoside	Erotiske art.	Adult Content	1			Adult/Sexually Explicit	1		
70	http://www.over18.no/	Nakenhet	N/A			1	Adult/Sexually Explicit	1		
71	http://www.lommelegen.no/sex/	Annet	Society and Lifestyles	1			Health	1		
72	http://www.klara-klok.unginfo.no/	Annet	Society and Lifestyles	1			N/A			1
73	http://home.online.no/~pwarsla/index_sex.htm	Annet	Hosting		1		Hosting Sites		1	
74	http://www.inn-ut.com/	Erotiske art.	Adult Content	1			Adult/Sexually Explicit	1		
75	http://www.g-sexshop.com/	Erotiske art.	Sex	1			N/A			1
76	http://www.pincempire.com/	Porno	N/A			1	N/A			1
77	http://www.voksneleker.no/	Erotiske art.	Adult Content	1			Adult/Sexually Explicit	1		
78	http://www.sex-shoppen.no/	Erotiske art.	N/A			1	Adult/Sexually Explicit	1		
79	http://www.dotten.no/	Erotiske	N/A			1	Adult/Sexually Explicit	1		

		art.								
80	http://www.nytelse.no/	Erotiske art.	Adult Content	1			Adult/Sexually Explicit	1		
81	http://www.eva-shop.no/	Erotiske art.	N/A			1	Adult/Sexually Explicit	1		
82	http://www.bustys.no/?afID=249	Erotiske art.	Adult Content	1			Adult/Sexually Explicit	1		
83	http://www.kvinnenettet.no/	Annet	Society and Lifestyles	1			N/A			1
84	http://www.onlinemagasinet.no/	Nakenhet	N/A			1	Adult/Sexually Explicit	1		
85	http://www.helsenett.no/	Annet	Health	1			N/A			1
86	http://www.doktoronline.no	Annet	Health	1			Health	1		
87	http://www.rosenhaven.no/	Erotiske art.	N/A			1	Adult/Sexually Explicit	1		
88	http://www.menopause-info.no/website/	Annet	N/A			1	N/A			1
89	http://shop.erotikknett.no/	Erotiske art.	Adult Content	1			Adult/Sexually Explicit	1		
90	http://www.gimmestad-psykoterapi.no/	Annet	N/A			1	N/A			1
91	http://www.club4shop.no	Erotiske art.	Network Errors	1			Adult/Sexually Explicit	1		
92	http://www.testselv.no/	Annet	N/A			1	Health	1		
93	http://www.keycard.no/	Nettbutikk	Shopping	1			N/A			1
94	http://www.pentad.no/	Annet	N/A			1	N/A			1
95	http://www.letsbuzz.no/	Annet	Business	1			N/A			1
96	http://www.slafs.com/fyllamat/	Porno	Sex	1			N/A			1
97	http://www.erotikknett.no/	Nakenhet	Sex	1			Adult/Sexually Explicit	1		
98	http://www.fetishdivas.no/	Nakenhet	Sex	1			N/A			1
99	http://fuckforforest.com/	Porno	Sex	1			Adult/Sexually Explicit	1		
100	http://www.gaysir.no/	Annet	N/A			1	N/A			1
101	http://www.nattavisen.com/	Porno	Sex	1			N/A			1
102	http://www.norskefitter.com/	Porno	Sex	1			Adult/Sexually Explicit	1		
103	http://www.penest.no	Nakenhet	Entertainment		1		Adult/Sexually Explicit	1		

104	http://www.pornogrisen.com/	Porno	Sex	1			Adult/Sexually Explicit	1		
105	http://www.pornokongen.com/	Porno	Sex	1			N/A			1
106	http://www.sexnoveller.no/	Porno	Adult Content	1			Adult/Sexually Explicit	1		
107	http://www.swingersnorge.com/newweb/www/hvaskjer/	Annet	Sex		1		Adult/Sexually Explicit		1	
108	http://www.aktuellrapport.no/	Porno	Sex	1			N/A		1	
109	http://www.duo.no/	Porno	Sex	1			Adult/Sexually Explicit	1		
110	http://www.cupido.no/	Porno	Sex	1			Adult/Sexually Explicit	1		
111	http://member.lek.no/	Porno	Sex	1			N/A		1	
112	http://www.chat.no/	Chat	Adult Content		1		Adult/Sexually Explicit		1	
113	http://chat.eros.no/	Chat	Adult Content	1			Adult/Sexually Explicit	1		
114	http://www.lovechat.no/	Chat	Web Chat	1			N/A			1
115	http://snakk.no/	Chat	N/A			1	N/A			1
116	http://chat.spray.no/	Chat	N/A			1	Chat	1		
117	http://home.no.net/bdbergen/index.php	Porno	Information Technology		1		Hosting Sites		1	
118	http://www.bjornbeckysplayground.com/	Porno	N/A			1	N/A			1
119	http://home.no.net/hen74/	Porno	Information Technology		1		Adult/Sexually Explicit	1		
120	http://www.sandrawang.com	Porno	Sex	1			Adult/Sexually Explicit	1		
121	http://www.cmbweb.no/hacker.htm	Annet	Vechiles	1			N/A			1
122	http://www.dnt.no/	Annet	Health		1		N/A			1
123	http://www.vinmonopolet.no/	Annet	Alcohol and Tobacco	1			Alcohol and Tobacco	1		
124	http://www.pornolinker.no/autorank.html	Porno	Sex	1			Adult/Sexually Explicit	1		
125	http://www.gratisporno.no/	Blank	N/A	1			Adult/Sexually Explicit		1	
126	http://www.norgestopp50.no/sexerotikk.shtml	Porno	Sex	1			Adult/Sexually Explicit	1		
127	http://www.eskorte.net/	Prostitusjon	Sex	1			Adult/Sexually Explicit	1		
128	http://www.no1onthe.net/	Porno	Searchengines and portals		1		Adult/Sexually Explicit	1		
129	http://www.exact-reise.no/	Reiseliv	Travel	1			N/A			1
130	http://www.gotogate.no/	Reiseliv	Travel	1			N/A			1
131	http://www.boarding.no/link.asp?cat=18	Reiseliv	Travel	1			Travel	1		
132	http://www.berg-hansen.no/	Reiseliv	Travel	1			N/A			1
133	http://www.ior.no/	Reiseliv	Travel	1			N/A			1
134	http://www.altomreiser.no/selskap/213	Reiseliv	Travel	1			N/A			1

135	http://www.norient.no/	Reiseliv	Travel	1			N/A			1
136	http://www.tfds.no/	Reiseliv	Travel	1			Travel	1		
137	http://www.tvete.com/	Reiseliv	Entertainment		1		Travel	1		
138	http://www.travelnet.no/	Reiseliv	Travel	1			Travel	1		
139	http://www.arcticexpress.no/	Reiseliv	Travel	1			N/A			1
140	http://www.saga.solreiser.no/	Reiseliv	Travel	1			Travel	1		
141	http://www.osloreisesenter.no/	Reiseliv	Travel	1			N/A			1
142	http://www.kurs-konferanse.no/	Reiseliv	N/A			1	N/A			1
143	http://www.floroflyservice.no/	Reiseliv	N/A			1	N/A			1
144	http://www.ebookers.no/	Reiseliv	Travel	1			N/A			1
145	http://www.hopetravel.com/	Reiseliv	Travel	1			N/A			1
146	http://www.tivoli.no/	Pengespill	Gambling	1			N/A			1
147	http://www.bettingadvice.com/	Pengespill	Gambling	1			Gambling	1		
148	http://www.nettips.co.uk/	Pengespill	Message Boards and Clubs	1			N/A			1
149	http://www.oddsen.nu/	Pengespill	Message Boards and Clubs	1			N/A			1
150	http://www.caplex.net/web/frameset/main.asp	Annet	Searchengines and portals		1		N/A			1
151	http://odin.dep.no/odin/norsk/kontakt/epost/bn.html	Annet	Government	1			Government	1		
152	http://odin.dep.no/odin/norsk/tlf_epost/index-b-n-a.html	Annet	Government	1			Government	1		
153	http://www.ssb.no/	Annet	News		1		News		1	
154	http://www.siu.no/adresser.nsf/Adresser/	Annet	Education materials	1			Education	1		
155	http://www.norgesstorstebedrifter.no/	Bedriftsinfo	Information Technology		1		N/A			1
156	http://www.norbed.no/	Bedriftsinfo	N/A			1	N/A			1
157	http://www.firma-katalogen.com/	Bedriftsinfo	Reference Materials	1			Computing and Internet		1	
158	http://www.bedriftsguiden.no/	Bedriftsinfo	N/A			1	N/A			1
159	http://enter.tradefacta.com/no/index.html	Bedriftsinfo	N/A			1	N/A			1
160	http://www.nortrade.com/	Bedriftsinfo	Searchengines and portals	1			N/A			1
161	http://www.kompass.no/	Bedriftsinfo	Business and Economy	1			N/A			1
162	http://www.rosaindex.no/	Bedriftsinfo	Reference Materials	1			N/A			1
163	http://www.varslingslisten.no/	Bedriftsinfo	N/A			1	N/A			1

164	http://www.purehelp.com/	Bedriftsinfo	Information Technology		1		N/A			1
165	http://www.norgeskilden.no/	Bedriftsinfo	N/A			1	N/A			1
166	http://www.gulesider.no/gsi/index.jsp	Bedriftsinfo	Searchengines and portals	1			Searchengines	1		
167	http://www.dn.no/bedriftsbasen/	Bedriftsinfo	Financial Data and Services	1			News	1		
168	http://www3.brreg.no/	Bedriftsinfo	Government	1			N/A			1
169	http://www.tind.no/	Forsikring	N/A			1	N/A			1
170	http://www.osloassuranse.no/	Forsikring	Financial Data and Services	1			N/A			1
171	http://www.moretrygd.no/	Forsikring	N/A			1	N/A			1
172	http://www.gard.no	Forsikring	Financial Data and Services	1			N/A			1
173	http://www.factor.no/no/start.html	Forsikring	N/A			1	Finance & Investment	1		
174	http://vital.no/	Forsikring	Financial Data and Services	1			N/A			1
175	http://www.vesta.no/default_flash.asp	Forsikring	Financial Data and Services	1			N/A			1
176	http://www.trygghansa.no/	Forsikring	Financial Data and Services	1			N/A			1
177	http://www.terra.as/	Forsikring	Financial Data and Services	1			Finance & Investment	1		
178	http://www.storebrand.no/	Forsikring	Financial Data and Services	1			Finance & Investment	1		
179	http://www.sparebank1.no/forsikring	Forsikring	Financial Data and Services	1			Finance & Investment	1		
180	http://www.norskeliv.no/	Forsikring	Financial Data and Services	1			N/A			1
181	http://www.klp.no/	Forsikring	N/A			1	N/A			1
182	http://www.if.no/	Forsikring	Financial Data and Services	1			N/A			1
183	http://forsikring.gjensidigenor.no/	Forsikring	Financial Data and	1			N/A			1

			Services							
184	http://www.enter-forsikring.no/	Forsikring	Financial Data and Services	1			N/A			1
185	http://www.jippii.no/jsp/games/index.jsp	Onlinespill	N/A			1	Games	1		
186	http://v25.tippinga.com/	Pengespill	Gambling	1			N/A			1
187	https://www.lavprisfly.no/	Reiseliv	Travel	1			N/A			1
188	http://www.wideroe.no/	Reiseliv	Travel	1			Travel	1		
189	http://www.sasbraathens.no/	Reiseliv	Travel	1			Travel	1		
190	http://www.norwegian.no/	Reiseliv	Travel	1			Travel	1		

Appendix F – Complete data from Phishing-test

Date	Tested	Tid	Address	SC	OK	WS	OK
1.4.	8.4.	7	http://www.paypal-cgi.us/webscr.php?cmd=LogIn	Fraud	Yes	Errors	?
7.4.	8.4.	1	http://comcast-database.biz/	N/A	No	Fraud	Yes
30.3.	8.4.	9	http://dllconf.com:280	N/A	No	Errors	?
24.3.	8.4.	15	http://www.lbgirls.net/galleries/001/galler.htm	Adult	No	Fraud	Yes
8.4.	8.4.	0	http://safevisa.ueuo.com/index.php	N/A	No	N/A	No
3.4.	12.4.	9	http://www.unionplantersonlinebank.com/upib/index.html?=update	N/A	No	Fraud	Yes
18.4.	18.4.	0	http://www.security-validation-your-account.com/signin.ebay/ …. (Truncated)	N/A	No	N/A	No
14.4.	18.4.	4	http://202.3.144.4/SITE/index.php	N/A	No	N/A	No
19.4.	20.4.	1	http://www.bofalert.com/online/popup.php	N/A	No	N/A	No
21.4.	21.4.	0	http://www.profusenet.net/checksession.php	N/A	No	N/A	No
25.4.	26.4.	1	http://211.250.204.133/docs/zens/citizens-Survey.htm	N/A	No	N/A	No
27.4.	27.4.	0	http://www.marata.com.br/site/flash/cib.ibanking-services.com/cih/index.php	N/A	No	N/A	No
30.4.	30.4.	0	http://review-data.org/go.html	N/A	No	N/A	No
2.5.	2.5.	0	http://comannd.com:280/	N/A	No	N/A	No
19.5.	19.5.	0	http://www.atm-fdic.com/	N/A	No	N/A	No
20.5.	23.5.	3	http://203.115.22.179/.us/paypal.com/webscr/	Fraud	Yes	N/A	No
23.5.	23.5.	0	http://pamyweb.free.fr/abuse/logins.php	N/A	No	N/A	No
26.5.	27.5.	1	http://211.155.17.246/.n/index.htm	N/A	No	N/A	No