Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2004 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

December 2004

Security Services by ISPs, Real Value or Waste of Money?

Kai Inkinen
Helsinki University of Technology

Harri Toivanen
Helsinki University of Technology

Teemupekka Virtanen
Helsinki University of Technology

Security Services by ISPs, Real Value or Waste of Money?

Kai Inkinen, Harri Toivanen and Teemupekka Virtanen
Helsinki University of Technology
P.O.Box 5400, FIN-02015 HUT
{kai.inkinen, harri.toivonen, teemupekka.virtanen}@hut.fi

Abstract

The Internet is a hazardous environment for the unaware. Crackers, viruses and spam-floods are a nuisance that people using the Internet and the web have to deal with almost on daily basis. Finnish ISPs are trying to improve the situation by offering different security services for home-users. Prices of services vary, and users might feel confused whether the services are actually worth the money spent. In this paper we look at some common threats to home-users and see what Finnish and foreign ISPs have to offer as a counter-measure. We also look at the pricing of the products and make a comparison to similar free products available on the Internet. We find that that most of the services currently offer more than they cost. There is however a lot to improve on advertising, education and user awareness of the services.

Keywords: ISP, security service, firewall, spam, anti-virus

1. Introduction

The Internet used to be a network to connect universities with each other. The people using and operating the early Internet were highly skilled hackers who usually knew the systems inside out. Furthermore the whole network was based on trust. A good example of tools built under this kind of an assumption is the rsh-toolset, where the only access-control is based on the source IP-address and username, both of which are easy to spoof.

The same kind of thinking has been the common approach even very recently. Only in the last version of Windows targeted for home-users, namely XP, has there been some kind of privilege separation between the users. This feature has existed already in Windows NT4 and Win 2000 but these are targeted for companies, not home-users. Without separation the assumption is that everybody has got administrator privileges. Once a cracker can access the system, he can do whatever he chooses with it, ranging from reading mail to wiping out the entire hard drive. Separated privileges help a bit, but cannot completely fix the problem because ”upgrading” a normal account to an administrator account is pretty straightforward.
This problem does not exist only in the Windows-series, although one sometimes gets this picture; every OS is vulnerable if the wrong set of configurations has been applied.

The optimal way to improve security is through education. Users should know their system and the software that is used, be aware of what kinds of threats and vulnerabilities there are and enforce strict security policies. Strong passwords and always patching the system with all the latest security fixes is the minimum thing to do. Even this would not make break-ins impossible, but reduce both the risks and the consequences. Unfortunately, this utopia will probably never be achieved, so most users have to rely on simple security-tools provided by others.

In this article we look at what the Finnish ISPs are doing to enhance security for home users. We look at the different tools provided and whether price and quality meet at any point or by any one ISP. But, for the user to be able to protect himself, he has to know who or what are the

main threats. This is discussed in chapter 2, where we look at vulnerabilities caused by the actions of the users and by different technical failures. In chapter 3 we look closer at the Finnish ISPs and their security products. We summarize the services, evaluate and compare them to each other and to similar freeware software. Chapter 4 reviews the level of helpdesks, manuals and advertisements in the home security business.

2. Background on security

2.1 The average user - The human part of the vulnerability

An easy mistake to make when evaluating common security issues, especially for security experts, is to overestimate the knowledge and skills of the users. After the Internet-boom in the mid 90's almost everybody in Finland has got connected to the Internet. This has resulted in the fact that most users are no longer skilled hackers as they were in the childhood of the Internet. Many users are being on-line just for fun. They want to access popular web sites, read and send e-mail, chat with their friends, buy things easily in the comfort of their homes. This also means that the average skill-level of the users has rapidly decreased. Most users are probably familiar with terms like firewall or computer virus, but few really appreciate the full meaning of the terms.

The problem is twofold. As programs are getting easier to use the threshold to start using advanced features gets lower and more novice users get introduced to the networked world. The users have learned to demand both easy usability and rich features without having to read the manuals, and the vendors, especially Microsoft, have answered this demand. Their approach to the dilemma is to enable all features by default. Security is traded for easy usability, and customers learn to avoid software that is more secure, but also slightly harder to use. If this development can go on it will undoubtedly make the situation worse.[19]

One more big problem seems to be that people tend to trust one another too much, as different social engineering cases show. An example of one such case is from the computer engineering department of HUT. The research was made to see how successful social engineering is in gaining access to restricted resources. One part of the research was to send an e-mail message, supposedly from the system administrator, to trick students into answering with their password and username. The reply-to-address was even set to a different domain, but out of 140 mails sent, the researchers were still rewarded with 11 valid username-password pairs. [8] The author was also a target for this test, but at the time unable read or answer any e-mail, because of being in the army.

In this article we will focus on the issues from the viewpoint of the imaginary 'average user' who does not have the education or the awareness of security issues. What can a person without most of the required computer skills do to protect himself? The big question is whether the provided services help the users to protect themselves, and are they worth the money spent?

2.2 The most common technical vulnerabilities

Threats to the normal home-user's computer can be either remote or local. In this study we only consider remote threats. This is because local exploits are harder to defend against, but also harder to take advantage of. It would either require the attacker to already be e.g. a family member and have a valid account, or alternatively the attacker to break into the home to get physical access to the computer system. The first is an issue of trusting the users of the system and the second is about the physical security of the home. The assumption in this research is

that the legitimate users are on the inside, trying to use the home system in benign co-operation, while the threats come from the outside. In real life the case might be quite different, as e.g. inconsiderate teenagers exercising file-swapping can be considered a serious risk group. By ruling out attacks from the inside, we can get a restricted model to evaluate. There is quite little an ISP can do anyway, if the user forgets to lock the doors or invites the crackers to her home.

The threats to the networked computer are changing all the time. Crackers are constantly finding new vulnerabilities, while system-vendors are doing their best to react and patch them up. When systems get more complex, the advantage seems to shift more and more to the crackers, unless some major breakthroughs in software and security engineering occur. A list of the twenty most serious Internet vulnerabilities is maintained on the Internet by the SANS-institute and the FBI [25]. The list is maintained and updated regularly and gives an overview of current vulnerabilities.

Here's a short extract of the list of Windows vulnerabilities[25] as of 2003-10-22.
1.Internet Information Services (IIS)
2. Microsoft SQL Server (MSSQL)
3. Windows Authentication
4. Internet Explorer (IE)
5. Windows Remote Access Services
The list for Linux/Unix-vulnerabilities is quite similar [25], as of 2003-10-22.
1. BIND Domain Name System
2. Remote Procedure Calls (RPC)
3. Apache Web Server
4. General UNIX Authentication Accounts with No Passwords or Weak Passwords
5. Clear Text Services

The lists show that most serious threats seem to come from running unnecessary services. Few home-users should have the need to run DNS-, web- or database-servers. Administering complex servers like these require both lots of skill and time so these are best left to experts, especially if the user is inexperienced. This fact is easily blurred because installing servers has been made so easy, regardless of the OS being used, installing a full-scaled web-server takes just a few minutes and a few clicks of the mouse. The user does not need to learn to configure the servers, as default settings are provided. In the worst case the servers might even be pre-installed, and the user might not even know he is running a server. This might even cause problems for professional system administrators as discussed in [9].

The article researches the reason why the slapper-worm was able to spread in the '.fi'-domain. The worm spread through a known vulnerability in the OpenSSL-server. The vulnerability and a patch for it was published almost two weeks before the worm was first found but still the number of hosts in the .fi-domain that got infected by the first version of slapper, was as big as 94. The research showed that over 60 % of the administrators of the infected systems were either completely unaware of the whole OpenSSL installation or that the service was running. [9] It is easy to understand that many home users are running vulnerable systems, as even IT-professionals are not always able to protect their networks.

3. Security services for home-users

3.1 ISPs in Finland

The Finnish ISP market is dominated by a few big actors. We will take a closer look at Sonera, Elisa, dna Internet, HTV and Saunalahti because they control a big share of the market. We will also take a smaller actor into account, because their current market share enables them to take a bit different approach to the issue. An example of a smaller, non-commercial ISP is 'DNA Kotiverkkoyhdistys', 'KVY' later in this article, which is basically a society of private people. In order to have an Internet-connection provided by them, the user needs to join the society. He is also urged to take part in different maintenance activities for the service [12]. Other, not strictly commercial ways to get an Internet connection also exist. Many universities offer some kind of service for their staff and students. This activity is different in nature, so the universities can not be considered to be considered as ISPs, and are not taken into account in this research.

None of the ISPs have so far had any big advertisement campaigns for their security services. We think that this is going to change, as the prices for the services and the profit margins keep decreasing. The ISPs are bound to find new ways to get a competitive edge over their competitors and security services are a good place to start. The field has recently got more attention as Sonera has some serious problem with spam, and the Swen-virus. This incident will be more thoroughly discussed in chapter 3.2.4.

3.2 The offered security services

3.2.1 Firewalls

There exist two main categories of firewalls, software and hardware. The difference is that a software firewall runs as an application process on a multi-purpose computer, while a hardware firewall runs on dedicated hardware and software. A hardware firewall is potentially more secure, but is also much more expensive than a software firewall. Price is often the decisive factor for home-customers, so all the solutions provided by the ISPs are software-based. Most of the ISPs also have hardware solutions, but the prices are counted in hundreds of euros per month. These services are clearly targeted at companies and are in practice unavailable for home users, both in price and availability. [10]

It is quite surprising that none of the ISPs in the research offer some inexpensive ADSL-modem/hardware firewall combination. An ADSL-connection requires a modem to work and many of these also include either a hub or a switch. A hardware firewall could surely be integrated into the box without too much extra expense. For example the least expensive hardware firewall found at Verkkokauppa.com, the Linksys Instant Broadband EtherFast© Cable/DSL} costs only 85 euros(2003-11-12) [26].

Modern software firewalls are usually optimized for easy usability. They have default configurations that suit most homes, and with some effort they can be configured for special cases. The problem with software firewalls is that the underlying OS might contain bugs that compromise the security, although the firewall software works correctly. Bugs are not impossible in the dedicated software of the hardware firewalls, but the restricted functionality allows a simpler design which makes hardening much easier.

A firewall is something of a must-have nowadays, e.g. Linux and Windows XP contain built-in software firewalls. The firewall in XP is very easy to use, but quite restricted in functionality, and does not replace a properly configured ``real'' firewall. The Linux firewall, NetFilter is quite the opposite. It is mainly targeted for experienced users. The most important feature that the Windows XP firewall to our experience lacks is filtering of outgoing traffic, that the other

firewall products in our research support [5, 16, 24,28]. Outward filtering prevents unauthorized programs to contact the Internet and thus helps in protecting against different kinds of malware, like spyware and adware, which are discussed closer in chapter 3,2,5 and restrain the spreading of viruses, which are examined closer in chapter 3.2.2.

ISP	Software	Price	Date
Sonera [22]	F-Secure	4,99 euros/month	2003-10-12
Elisa [5]	F-Secure	5,89 euros/month[2,4]	2003-10-13
Welho, HTV [27]	F-Secure	6 euros/month[2]	2003-10-12
Saunalahti [20]	F-Secure	4 euros/month[1]	2003-10-12
DNA Internet [3]	No info found	3,99 euros/month[2]	2003-10-12
KVY [12]	No service	-	2003-10-22
Telia (Sweden) [24]	Norman Personal FW	30SEK/month (3,4e)	2003-10-14
Earthlink (USA) [4]	Zone Alarm Pro	US$49,95 (44e) [3]	2003-10-14

[1]Includes in some ADSL-connections by default [3]Includes 1 year of free support and updates
[2]Only available as packages with the Anti-virus software [4]One time setup-fee 8,34 euros charged

Table 1. Offered firewall services and prices

All the firewalls in this research are targeted for Windows-users. None of the bigger ISPs have any kind of service for Linux-hosts. This is most probably a financial decision, as the number of installed Linux OS:s is much smaller than the Windows install-base. Linux is also more or less considered to be an OS for hackers. Novice users are not commonly using Linux so Linux users are usually skilled enough in issues of network protocols and firewalls to be able to configure the built-in NetFilter firewall manually from the command-line. New distributions of Linux include different wizard features, so less experienced users should reach satisfactory results. It would still give much added value if all distributions would contain e.g. default statefull filtering rules, denying all incoming traffic. Considering these facts, very few Linux users are probably willing to pay for such a service. As more novice users switch to Linux this is most probably going to change.

In table 1 we have listed prices and the software that ISPs offer. All the Finnish ISPs have gone for the F-Secure Distributed firewall. One big reason for this must be that F-Secure offers a suite with both anti-virus software and a firewall. Another reason is probably that F-Secure is a Finnish company, which we feel is an appealing factor to the Finnish customers.

The question is whether the normal home-user actually needs a firewall, and is it worth to pay, say 5euros per month for it? There are many decent freeware firewalls available for Windows, like Zonealarm or BlackIce Defender and several others can be found on the Internet, e.g. at www.firewall-net.com. An experienced user could also configure a Linux-box as a stand-alone firewall. However, choosing a good product among all the free software firewalls on the Internet is not all that straightforward, especially if one does not have a wide experience about these kinds of products. If one buys a service, then the choice has already been made by the ISP.

A service by an ISP includes some kind of customer service. This enables the user to call a helpdesk for assistance in case of emergency. The prices and open-hours for the helpdesks are discussed closer in chapter 4. The main benefit in choosing a commercial firewall product over freeware software is the better usability and richer set of features. Usually free products are test

versions of the real products, with some artificial limitations. For example the free version of ZoneAlarm lacks password protection and the ad blocking that ZoneAlarm Pro includes [28]. There might also be versions of the commercial software with full functionality, but with a restricted time, like 30 days for the Elisa firewall service [5].

As a conclusion the firewall services can not be considered to be more than barely OK. The prices are quite high, 3-5 euros, if compared to the anti virus services and the speed of updates is not nearly as important with firewalls. The available freeware firewalls are also generally of a good quality. The user just has to remember to update the freeware product with regular intervals. However, the real threat to these services to our opinion comes from cheap hardware firewalls. The user can get a dedicated hardware firewall for less than 100euros and it also usually works as a 4-port switch, NAT-firewall and DHCP-server. Some firewalls, like the Linksys firewall have additional features like IPSec VPN (Virtual Private Network) so it is a formidable choice compared to most software firewalls.

3.2.2 Virus scanners

In the market of anti-virus software speed is of essence. The faster the user can update his virus database, the more secure the system is against viruses. Essentially, a virus-scanner is useless, if a new virus strikes before one has got the latest virus-definitions. This is quite different from the field of software firewalls, as a firewall is still useful even if it is not the very latest version. Completely new viruses or updates on old viruses are found on a weekly basis [15]. Because viruses are actually manufactured to fool scanners, they can usually avoid detection with an old database.

Many recent cases [2, 6, 9] have shown that modern viruses have been able to spread, even if the vulnerability through which the virus spread should have been patched. Because of the automatic spreading, even users who are normally careful with their mail can get their computer infected. The lesson to learn is that one should always apply the latest patches for all the software being used. The user should also regularly update the virus scanning software. This is where the ISPs can come in. The anti-virus software offered by the ISPs includes the base install and updates for the software. Regular updates are absolutely vital, as e.g. the McAfee recent viruses-list shows [15]. A couple of new viruses are found every week, so a one-week old virus-database is close to being completely useless.

ISP	Anti-virus software	Price euros/month	Date
Sonera [22]	F-Secure Anti Virus	3,49[1]	2003-10-12
Elisa [5]	F-Secure Anti Virus	5,89[2,3]	2003-10-13
Welho, HTV [27]	F-Secure Anti Virus	3,50	2003-10-12
Saunalahti [20]	Autom. Mail filtering	1	2003-10-12
Saunalahti [20]	F-Secure Anti Virus	3[1]	
DNA Internet [3]	No info found	3,99[2]	2003-10-12
KVY [12]	No service	-	2003-10-22
Telia (Sweden) [24]	F-Secure Anti Virus	30 SEK/month (3,4)	2003-10-14
Earthlink (USA) [4]	No service	-	2003-10-14

[1]Includes in some ADSL-connections by default
[2]Only available as packages with the firewall software
[3]One time setup-fee 8,34 euros charged

Table 2. Anti-virus services and prices

Like with the software firewalls all the reviewed products were targeted at MS Windows users. This is because Windows is by far the most popular target for virus writers. There have been some viruses and worms for Linux, e.g. one report in [18] and one in [9], but they have never got to spread properly, so they have never got any big media attention. These differences come partly from that the install-base of Linux is much smaller but also because the OS-architecture is different, so spreading is much harder.

All of the Finnish ISPs seem to rely on F-Secure Anti-Virus, for their virus-protection service. As already mentioned, one should not focus on the vendor too much. The update speed is much more important than the vendor. All the services offer the software and online updates to the virus-database. This means that when the computer is connected to the Internet, the scanner can check for updates automatically. The overhead the version control check causes is negligible compared to the benefits. The interval could and should be set to as little as ten minutes. This way the customer gets the update almost immediately when the ISP gets it from the vendor. If the computer should not be connected to the Internet when an update arrives, then it will be fetched the next time the computer sets up the network connection. This scheme doesn't guarantee that the host stays virus-free because new viruses spread so fast that the anti-virus companies might not have a chance to react in time. However, by being careful with mail, and regularly updating the OS the risk can be reduced significantly.

Lately the importance of anti-virus software has increased rapidly. No matter how experienced or careful the user is, he might still end up getting a virus. Spending a few euros per month on a virus-scanner probably compensates for the lost time, work and money that a virus infection might cause.

The prices of the anti-virus software have been set low by all the ISPs. Sonera and Saunalahti even include it in the price for some connection types. Considering the importance of the service, the low prices are a good thing. The price for an ADSL- or Cable Modem connection is round 50euros per month, so using the service increases the price with less than 10 %. Still it requires the customer to take the effort to order the product and install it. It would probably be best if the service was included in all packages by default. Experienced users who are positive that they do not want the service could be given the right to opt-out. This arrangement would to our opinion result in that more novice users would be protected. Inexperienced users are the group that needs the protection most dearly anyway. The general conclusion is that the offered services are well worth their price, especially when compared to either being without virus-protection or using a bad, although free tool.

3.2.3 Anti-virus for mail

Virus protection can be taken one step further. Incoming mail can be automatically filtered for viruses before accepting it on the mail server. This can actually save a lot of storage if a virus is spreading aggressively, because the infected mails don't need to be first saved and then removed only later by the user. Sonera was forced to take this approach after dire problems with their mail service [23]. The issue will be discussed closer in the next chapter.

Saunalahti is the only ISP in our research that offers automatic filtering of infected mail, as listed in table 2. The service checks all arriving mail and removes infected ones. A notice is sent to the user for every removed mail, so the user knows about the incident. The service does not include the virus-scanner software and cannot be used for normal virus protection. It cannot replace anti-virus software on the home computer, but the risk of getting infected by a mail-virus can be reduced significantly.

As already mentioned the service has the benefit that it keeps the mail-box free from virus-mail. In the normal case the user would have to check all the mails and the clean up the mailbox himself. The price for this service is quite modest, only 1euros/month, in 12 month periods.

The question again arises, whether such a service should not be a default service for all Internet connections and mail services. This arrangement would save resources for both the ISP and the user. As we discuss in the next chapter the cost for an ISP can be very high if several computers in their network get infected and take down the whole mail-service. The situation is hopefully improving as a new bill for a law concerning digital media has been proposed by the government. This bill and spam-removal will be discussed next.

3.2.4 Spam and mail filters

Unsolicited bulk email, commonly referred to as spam, is becoming a problem all the time. It was very recently (2003-10-13) announced that the Sonera mail-service has been a subject for large spam attacks that were generated by the Swen-virus [11]. Due to the large spam-floods Sonera mail-servers got listed in the Open Relay Database, ORDB, effectively enabling spam-messages. Mail sent from servers listed in the ORDB is automatically rejected in many domains.}, five days later. At this point the mail service was cut down so badly that in the worst case mails were delayed by up to five days. Sonera clarified the situation and got removed from the database later the same day [1]. The news had however, already spread to the media and resulted in a major setback in PR for the ISP.

The Sonera case was not closed until the middle of November (2003-11-14), when the ISP announced that the problem is fixed. The significant change was achieved, when Sonera started to automatically filter all the Swen virus mail (2003-10-24). The ISP was also forced to distribute their anti virus software to 300 customers that had the biggest problems with the virus-infection. On top of all this Sonera paid 3.2 millioneuros in compensations to their customers. [23]

Spam-protection is quite a new service and not all of the big ISPs in our research do yet have an anti-spam service. This is however bound to change, as new legislation is being planned in Finland. The bill *HE125/2003* states that ISPs should be allowed to filter and remove viruses and possibly spam from mail and P2P network traffic, even without explicit approval by the customer. According to the Minister of Transport and Communications, Leena Luhtanen, the bill should be interpreted so that such harsh means are allowed only if “it is obvious that the mail threatens the security or the functionality of the whole system” (free translation by the author).[7,21] With the users consent filtering can be applied also in less extreme cases.

As spam is becoming such a big problem, we are hoping that the interpretation of the law will not become too strict. The ISPs should to our opinion be given extensive rights to decide what kind of mail could be considered harmful. This might make separate spam removal services obsolete as ISPs could filter out spam automatically. This could mean great savings for the ISPs, when a lot of storage is saved by not letting spam and virus mails take up valuable (backed up) storage space.

Spam-removal is currently offered as a separate service only by Saunalahti, for 2 euros/month. The service promises something like 90 % success-rate. This rate will probably not improve very much, unless some major breakthroughs are made. The spammers have volume on their side. They can just keep trying with different keywords added or removed to avoid getting filtered out by known filter applications.

It is quite unfortunate that the other ISPs do not offer a similar service. We feel that there certainly would be demand for it. The need for spam-removal varies from person to person, as some gets hundreds of spam-messages per day, and others, like the author hardly ever gets pestered. Paying 2euros for the saved time is quite reasonable, if sorting spam otherwise would take several minutes per day. Hopefully this kind of service will be included by default in every Internet-connection in the future.

3.2.5 Uncontrolled threats

Malware could be roughly divided into three categories: Trojans, worms and viruses, although virus is often used as a synonym for all of these. A *Trojan* is a program that is installed with some other, often useful program. A *worm* (e.g. Slapper) is an independent, self-replicating program that does not need a host-program. Worms usually do not do any harm to the infected host, but are found because of massive resource consumption when replicating. A *virus* is a program that is installed with some other program or by reading a file. The virus replicates on the host and tries to spread to other hosts. A virus is usually programmed to do some harm, like trash the hard-drive or corrupt files.

Fortunately there is a cure against these kinds of pests. The most popular tool for this is the Lavasoft Ad-Aware program. It works much like a virus scanner and removes suspicious software after confirmation from the user [13]. The program is quite efficient and even a more experienced user often find several different dubious programs when running the scan.

The last threats we look at in this article are JavaScript and ActiveX-components. Most firewall products make filtering of these possible, but few people have the knowledge to activate the filtering. Most browsers can also be configured to disable active contents. The problem is then that some sites, like e.g. Windows Update, require either JavaScript or ActiveX to work correctly. Fortunately modern browsers allow one to configure restrictions on site-to-site basis, so trusted sites could get more privileges than unknown or untrusted ones.

ISP	Firewall	Anti-virus	FW+AV	Avail.	grade
Sonera	4,99	X(3,49) [2,4]	4,99 (7,49) [2,4]	-	3
Elisa	5,89[1,2]	5,89[1,2]	5,81[3]	+	2
Welho, HTV	6,00[2]	3,50	6,00	-	2,5
Saunalahti	4,00[3]	3,00[3]	6,50	+	4
Dna Internet	3,99[2]	3,99[2]	3,99	-	3

[1]One time setup-fee 8,34 euros charged
[2]Only available as packages with both services
[3]Extra licence 3,49
[4]Includes in some connections by default
[5]Graded from 0(worst) to 5(best)

Table 3. Summary and evaluation of services and prices. All prices are in euros/month. Column avail. Shows if service is available without an Internet connection from the ISP.

3.2.6 Discussion and evaluation

A thing that is not normally brought up anywhere is that the security services are separate services that the user should be able to buy from any ISP. It should not have to be the same ISP that is providing the Internet connection. This is the case however only with Saunalahti and Elisa, as they provide their services to anyone. Sonera, dna Internet and Welho provide their

services only for their own Internet customers. Getting this information was not at all easy. We found the information on the Saunalahti and dna sites. In the rest of the cases we were forced to call the helpdesks to get the information.

Table 3 shows the prices for the security services that are available to Finnish customers. We have given a grade to each service according to our own impression and opinion. Because all the ISPs in the table use the same vendor, we have not graded the software, but instead based the grading on the price and availability of the services. We have given most weight to the anti virus service and its price, because we feel that this is the most important service for an average user. The grade is lowered if the user can not get the firewall and the anti virus separately. The next criterion is the overall price of the services. Least weight is given to the separate firewall service, as the user can easily use some of the available freeware firewalls. We have also given some weight to the general impression like availability and customer-service to grade every service from 0(worst) to 5(best).

All the services in our research get an accepted grade. The Saunalahti service is the best one to our opinion, and it is available regardless of which ISP the customer uses. The other services are all quite the same and of an acceptable level. A special notice has to be made about the Sonera and the Saunalahti services, as they are already bundled with some of the connections by default. Table 3 makes comparing the services easy, but the general conclusion is that most users are probably best of with the service provided by his current ISP, because this make paying and administering the service easy.

4. Customer service and manuals

Customer service can have a big impact on the way we feel about different products. The computer market in general has quite a bad reputation in customer service, both for hardware and software retailers. To our experience most people who are active users of computers have experienced bad customer service, ranging from non-motivated shop-clerks to plain-out lies about the products or their availability. One big reason for this is in our opinion the fierce price-competition in the business.

The web makes it possible for the user to easily compare prices of different stores and ISPs world-wide. For example e.g. the MBnet Hintaseuranta-site contains most computer related products one could imagine available in Finland [14]. The shops and ISPs will have to cut down their profit margins in order to excel in such comparisons. Savings can e.g. be achieved by reducing the number of the staff. When buying groceries, it is easy to go to the next shop to get the product, but when discussing ISPs the issue is different. There is usually a considerable setup-fee, so switching to another ISP is not done very lightly.

All the ISPs, expect KVY, have some kind of helpdesk over the phone. To our experience these are usually very hard to reach. On several occasions, also while conducting this research, the author has been forced to wait for service in different helpdesk-queues for up to ten minutes. If the user has to pay 1.34euros for each minute, like with the Saunalahti helpdesk, this can become quite expensive. Fortunately Saunalahti has so informative web-pages that we did not need to call them at any occasion. The answering hours and prices of the different helpdesks are summarized in table 4.

The major problem with phone-helpdesks is that aiding people on computer related matters is really hard, especially if the users are inexperienced. Novice users searching for *Any Key* -might be fun as a joke, but to our experience not so hilarious when actually encountered in a

real situation. There are different remote assistance tools, e.g. Microsoft XP Professional contains one built-in remote admin tool that allows a remote administrator to take over the desktop of a computer. However, if the goal is to improve security, not decrease it, this is sounds like a very bad idea. For example Windows remote services were listed as fifth most serious vulnerability in SANS/FBI-list in chapter 2.2.

It could probably be arranged for a person hired by the ISP to do house-calls, but this is an all too expensive option. So in practice the average user still needs a computer-skilled friend or relative if something goes wrong.

ISP	Weekdays	Saturday	Sunday	Price
Sonera [22]	8-20	10-16:30	-	free
Elisa [5] [2]	7:30-20	9-17	-	0,2913
Welho, HTV [27]	8-20 (20-22) [3]	9-16 (16-22) [3]	- (9-22) [3]	0,2913
Saunalahti [20] [2]	8-21	10-18	-	1.37
DNA Internet [3]	9-22	10-16[2]	-	0,37
KVY [12]	-	-	-	-
Telia (Sweden) [24] [4]	8-21	9-17	-	Free
Earthlink (USA) [4]	24h	24h-	24h	Not listed

[1]All prices when called from mobile phone
[2]Separate fault notice line open 24h
[3]Fault notice line, open hours not listed
[4]Separate number when calling from abroad

Table 4. Answering hours and prices of helpdesk, checked 2003-11-15.

5. Conclusions

Most people would want to find the 'Holy Grail' of computer security: The one single measure or tool that would make the systems secure against any kind of attack or mistake. It is uncertain if this *silver bullet* ever existed and unfortunately things seem to rather be going in the opposite direction. As the systems get more complex, more bugs can creep in and stay unnoticed in both protocols and implementations. This is why general awareness of threats must improve.

Education is the best way to minimize potential hazards, but we have to face the fact that most people are not fascinated about computers as is, but instead consider them as tools for achieving some means. People don't seem to be comfortable with getting a lot of education and reading hundreds of pages of manuals to be able to get their work done. At the same time the cracker-community is taking full advantage of the potential of the Internet. The web is a great place to find information about vulnerabilities to exploit and ubiquitous networking offers the possibility to act out these malicious acts on computers anywhere in the world.

The widely spreading virus-infections lately have shown that everybody loses in the end, if problems are allowed to spread freely. This is why we think that ISPs should be more aggressive about the marketing of their services. If the customers don't know about the services, they cannot take them into use either. In our opinion it would be beneficial for ISPs to offer these services included by default to all broadband connections. This would increase the price of an Internet connection only with approximately 10 %. The potential savings are significant as discussed in chapter 3.2.4. People using OS:s for which the ISP cannot offer software, could opt-out and get the difference as discount on the price of the connection. Sonera and Saunalahti

have taken a step in the right direction and offer some of their services bundled with some ADSL-connections. This not only takes away the effort to find out about the products but also the perceived extra cost, because it comes embedded. These kinds of measures would both bring positive PR for the ISP and noticeably increase the security of everybody using the Internet.

6. References

List and order alphabetically (according to authors' or editors' last names) all bibliographical references in 12-point Times New Roman, single-spaced, at the end of your paper. References in text must be included in Reference section and vice versa. References in text should be of the format: (Jones et al. 1995; Smith 1996). Please follow the MIS Quarterly format for references.

References

Bobacka, Mikael; "Sonera dränks i skräppost", Hufvudstadsbladet page 10–10, daily newspaper in swedish, date 2003-10-18; 2003.

Carrera Ero; F-Secure Virus Descriptions : Sobig.F; virus information site from F-Secure; 2003. URL http://www.f-secure.fi/v-descs/sobig_f.shtml

dna nettiturva; security services by dna ISP; 2003. URL http://www.dnafinland.fi/yksityisille/liittymat_ja_palvelut

Earthlink; earthLink ISP extra services; 2003. URL http://www.earthlink.net/extras/

Elisa tietoturvapalvelut; security services for Elisa customers; 2003. URL http://www.elisa.fi/tietoturva

Erdelyi Gergely; F-Secure Virus Descriptions : Lovsan; virus information site from F-Secure; 2003. URL http://www.f-secure.fi/v-descs/msblast.shtml

GOVERNMENT OF FINLAND; Hallituksen esitys Eduskunnalle sähköisen viestinnän tietosuojalaiksi ja eräiksi siihen liittyviksi laeiksi; Bill HE125/2003, proposed by the Finnish government; 2003. URL http://www.eduskunta.fi/

Greenman Teddy, Pesonen Lauri; Social engineering, short summary; Helsinki University of Technology, TML lab research Study on social engineering, from the course T-110.452, 2000; 2000. URL http://www.tml.hut.fi/Studies/Tik-110.300/2000/Homeworks/soc.html

Heinonen Arsi, Virtanen Teemupekka, Addams-Moring Ronja; We are running what? - why the slapper worm was able to spread in finland; in 2nd European Conference on Information Warfare and Security (ed. BILL HUTCHINSON); page 339–348; Edith Cowan University, Perth, Australia, Australia; 2003.

Hämäläinen Pertti; Jarrua haittaohjelmille; Tietokonelehti page 64–69; article about the security services offered for companies; 2003.

Kalevan Sanomat; kalevan Sanomat, web news-archive; 2003. URL http://www.kaleva.fi

Kotiverkkoyhdistys dna; association providing Internet-connections; 2003. URL http://www.dna.fi

Lavasoft, protect your privacy; products for removing spy- and adware; 2003. URL http://www.lavasoftusa.com/

Mbnet hintaseuranta; price comparison site for computer-related products; 2003. URL http://www.mbnet.fi/hintaseuranta/

MCAFEE SECURITY; Mcafee: Description of newly discovered threats; list of recently discovered viruses and vulnerabilities; 2003. URL http://us.mcafee.com/virusInfo/default.asp?id=recentlyDiscovered

Netfilter/IPTables firewall project for Linux; firewall project, published under the GNU-license; 2003. URL http://www.iptables.org

Open Relay Database, ordb.org; database containing mail relays that allow sending spam; 2003. URL http://www.ordb.org

O'Reilly Linux Devcenter; O'reilly linux devcenter: Linux virus reported; 2001. URL http://linux.oreillynet.com/pub/a/linux/2001/09/18/insecurities.html

Robertson G., Vuori T.A; Virus infection - the "people problem"; in 2nd Australian Information Warefare and Security Conference; page 37–44; 2001.

Saunalahden tuotevalikoima; services for Internet-connections by Saunalahti; 2003. URL http://saunalahti.fi/internet/turva/prp.php

Takala Pauli; Sähköisen viestinnän tietosuojalaki eduskuntaan ensi viikolla; local daily newspaper from Turku, Finland; 2003. URL http://www.turunsanomat.fi/osasto/?ts=1,2,0,0,136157,2003-10-12

TeliaSonera; Sonera Mobile Phone operator and ISP; 2003. URL http://www.sonera.fi

TeliaSonera Press - Tiedotteet 2003-11-14; press releases by TeliaSonera; referenced 2003-11-17; 2003. URL http://www.sonera.fi/press

Telia Säkerhetstjänster; security services offered by TeliaSonera Sweden; 2003. URL http://www.telia.se

THE SANS INSTITUTE AND THE FBI ; The twenty most critical internet security vulnerabilities; updated list of the worst vulnerabilities on Linux andWindows; 2003. URL http://www.sans.org/top20/

Verkkokauppa.com; network store for buying computer related hardware and software; 2003. URL http://www.verkkokauppa.com

Welho tietoturvapalvelut; security services by Welho ISP; 2003. URL http://www.htv.fi/welho/default.asp?f=9&s=155

Zonelabs firewall; zoneLabs provides different firewall products; 2003. URL http://www.zonelabs.com/