Internet security incidents, a survey within Dutch organizations

Martin Caminada
Vrije Universiteit, Amsterdam
Faculteit der Wiskunde en Informatica
De Boelelaan 1081a
1081 HV Amsterdam
The Netherlands
martinc@cs.vu.nl

Reind van de Riet
Vrije Universiteit, Amsterdam
Faculteit der Wiskunde en informatica
De Boelelaan 1081a
1081 HV Amsterdam
The Netherlands
vdriet@cs.vu.nl

Arjen van Zanten
KPMG EDP Auditors
Burg. Rijnderslaan 10
1185 MC Amstelveen
The Netherlands
Vanzanten.Arjen@kpmg.nl

Leendert van Doorn
IBM T.J. Watson Research Center
30 Saw Mill River Road
Hawthorne, NY 10532
United States
leendert@watson.ibm.com

Abstract

This paper presents the main results of a survey held by de Vrije Universiteit and KPMG EDP Auditors, concerning Internet-related security incidents. The survey was held within Dutch organizations that are currently using the Internet. The first aim of the project was to determine the actual security risks of using the Internet. This requires insight in the percentage of companies experiencing Internet-related security incidents, the damage caused by the incidents, the way the affected companies deal with the incidents and a profile of the perpetrators. The second aim of the project was to determine the effectiveness of security measures. This was done by (1) analyzing the security incidents to find out in which way they could have been prevented and (2) determining possible correlations between security measures and (the absence of) security incidents.

Keywords

security incidents, computer crime, hackers, risk analysis, security measures

1. Introduction

With new organizations connecting to the Internet each month, Internet security has become an important topic. The fact that security is indeed a problem for many Internet-connected organizations is illustrated by a survey carried out by Dan Farmer. It was found that over 60% of 1700 inspected sensitive Websites, such as banks, credit unions, newspapers, and government agencies could be broken into or denied of all network functionality [Farm96].

Given the large number of vulnerable sites, an interesting question is which part of the Internet-connected organizations is actually experiencing Internet related security incidents. This question is relevant, as it provides insight in the actual risks of an Internet connection, but is also hard to answer, as research material is still relatively scarce. The few available studies, such as carried out at CERT/CC [How97] and Prowatch (a commercial security surveillance service) [Pro97], are frequently based upon a special subset of the Internet-connected organizations, such as those requesting assistance of CERT/CC or those having the security of their network surveyed by Prowatch. It is therefore difficult to determine the extent to which the results are representative. It was from this lack of knowledge that *KPMG EDP Auditors* together with *de Vrije Universiteit, Amsterdam* took the initiative to hold a survey within the Dutch organizations that are using the Internet.

The survey had several goals. First of all, it was to be determined what part of the Internet connected organizations is actually experiencing Internet related security incidents. To gain further insight in the extent of the problem, the second research goal was to determine the damage that is being caused by the incidents. The third research goal was to determine the measures that should be implemented to successfully defend against security incidents. This was done by analyzing both the cause of the incidents and the effectiveness of the security measures.

A condensed version of this paper, emphasizing the results only, has been submitted for the Webnet 98 conference.

2. Definitions

An *attack* is an attempt to violate the security of a computer system by trying to identify and/or exploit security vulnerabilities. If an attack succeeds, the resulting security violation is called an *incident*. This survey focuses on the following kinds of incidents:

- unauthorized access, meaning that someone on the Internet gained access to (parts of) the computer systems of a responding organization without being authorized to do so;
- denial of service, meaning that someone on the Internet managed to disrupt the information services provided by the computer systems of a responding organization;
- malicious code, such as viruses and Trojan horses, being spread by means of the Internet.

This research exclusively focuses on the attacks and incidents coming from the Internet. Although most attacks are launched on purpose, this need not always be the case. People sending e-mail attachments containing viruses, for example, do not need to be aware of this.

The researchers found it useful to maintain a clear distinction between the Internet site and the internal IT-infrastructure. The *Internet site* consists of the information services (such as WWW of FTP) offered to the Internet. The *internal IT-infrastructure* on the other hand, consists of the information services (possibly including Internet services such as e-mail or Web-access) offered to internal users. The main difference between the Internet site and the internal IT-infrastructure is that the users of the Internet site are located (externally) on the Internet, while the internal IT-infrastructure is being used exclusively by own employees. This implies that the internal IT-infrastructure usually contains the greater part of the business critical information. Therefore, incidents affecting the internal IT-infrastructure can have a higher impact than incidents affecting the Internet site.

3. About the survey

The survey has been carried out by sending questionnaires to 878 Dutch organizations that are currently using the Internet. The organizations were selected using the *whois*[*] information of the *nl*-domain. For each domain name the following information was available:

- the domain name itself (such as *kpmg.nl*);
- the name and address of the organization owning the domain;
- the name, phone number, and e-mail address of the administrative contact person. Because the administrative contact person is authorized to request changes in the registration of the domain, he is required to be an employee of the organization owning the domain;
- the name, phone number and e-mail address of one or more technical contact persons, which can be contacted in case of any technical problems;
- the domain name and IP-address of one or more name servers, which take care of the translation of domain names into IP-addresses;

Some organizations have their own dedicated name server, while others are registered exclusively at the name servers of one or more Internet providers. This is indicated by the name of the name server. For example: the domain *kpmg.nl* is being served by a name server called *stargate.kpmg.nl*. At a great number of other domains, the relation between the domain name and the name of its name server is not present; the name servers often carry the names of Dutch Internet providers, indicating that the management of these domains has been outsourced to an Internet provider. In order to receive as much information as possible about any attacks and incidents, organizations that manage their own Internet facilities (and can therefore provide information from their own experience instead of having to rely on information provided by their Internet provider) are obviously preferred. Therefore, it was decided to include only those organizations that have their own name server.

The questionnaires to organizations that are clients of KPMG were sent through the contactpersons at KPMG. Questionnaires to organizations having no established contacts with KPMG were sent to the administrative contact person. Of the latter group, some 10% came back as undeliverable by the postal system. In many cases this was because the administrative contact person had left the organization. This is quite remarkable, because the fact that the addressee is registered as the administrative contact person means that he has the ability to apply changes to the registration of the domain (for example: to terminate it), even after leaving the organization.

The surveyed organizations were given approximately one month to return the questionnaires. Eventually, 145 responses were received, thus obtaining a response of 17%. Compared to other surveys, this is not a bad result. A comparable survey carried out by the *Computer Security Institute* (CSI) in co-operation with the FBI, for example, obtained a response of 9% [CSI96].

[*] *Whois* is an Internet service that provides information about the registration of DNS domains.

4. Characteristics of the responding organizations

Before discussing the results of the survey, it is informative to provide an overview of the characteristics of the responding organizations:

- both small and large organizations (measured by their annual turnover, the number of employees as well as the number of IT-administrators) are represented;
- although several sectors are represented by the responding organizations, approximately one third of the population consists of Internet providers and the IT-sector. This is probably caused by the preference for organizations that manage their own Internet facilities;
- about one third of the population (99 organizations) has an Internet-site that is maintained by own employees. More than half (58%) of the organizations with an Internet site have their site for longer than one year;
- about one third of the population (98 organizations) has a permanent link between the Internet and their internal IT-infrastructure (often using a firewall);
- the responding companies have serious interests in (the security of) their Internet-facilities because:
  - 53% of the responding organizations with an Internet site uses it to generate income (at least $ 5.000 on annual base[†]) or to provide their customers with support for delivered products or services;
  - in two third of the organizations where the employees have one or more Internet facilities at their disposal, one or more facilities (mostly e-mail) were classified as *essential*, meaning that the loss of the facility would result in a immediate loss of productivity;
  - in three out of four organizations more than 75% of the employees have a workplace with computer facilities, which means that a potential security incident can affect a significant part of the organization.

The results as presented in the remainder of this paper are – unless mentioned otherwise – based upon the organizations that (1) have a permanent connection between the Internet and their internal IT-infrastructure, or (2) have an Internet site that is maintained by own employees. This is done in order to maintain a constant level of Internet-usage when comparing differences between groups of organizations.

5. Organizations reporting attacks

The surveyed organizations were asked whether they had experienced any attacks (succeeded or not) on their Internet site or internal IT-infrastructure. Based on the answers, Table 1 was compiled. The average period the organizations have been using the Internet is also included.

Table 1 – Percentage of organizations reporting attacks on their Internet site or internal IT-infrastructure (regardless of detection measures)

Environment	Percentage of organizations reporting attacks
Internet site	32% over 18 months (n=99)
internal IT-infrastructure	29% over 19 months (n=98)

An organization does not need to be aware that it was attacked. The real chance of attacks is therefore probably higher than indicated by Table 1. A more realistic estimate can be compiled by only including organizations that regularly check the contents of their audit trails to see if any attacks or incidents took place. The resulting data is set out in Table 2. It is quite surprising to see that these are considerably higher.

Table 2 – Percentage of organizations reporting attacks on their Internet site or internal IT-infrastructure (organizations that regularly check their logfiles)

Environment	Percentage of organizations reporting attacks
Internet site	45% over 17 months (n=51)
internal IT-environment	40% over 20 months (n=47)

To find out which sectors are especially attractive for attackers, Table 3 has been compiled. For each sector, the percentage of organizations that report attacks, is shown. Virus attacks are not included, as these do not need to be launched on purpose (the sender is not necessary aware he is contaminated).

[†] The amounts money mentioned in this paper have been calculated from Dutch guilders into US dollars at a rate of 1 guilder = ½ dollar

Table 3 – Attacks related to sectors

Sector	Percentage organizations reporting attacks
IT-sector	44% (n=25)
Internet provider	52% (n=23)
education	47% (n=15)
media	62% (n=13)
non-profit	11% (n=9)
all sectors	40% (n=119)

As can be seen in Table 3, the percentage of attacked organizations is fairly constant between different sectors. The only exceptions are the media and the non-profit sector. These are reporting more and fewer attacks, respectively. A possible explanation is that hacker ethic is to some extent keeping the perpetrators from attacking non-profit organizations (of which most of them, such as humanitarian organizations or environment activists have an idealistic mission). The media on the other hand are likely to be extra attractive, because of their high visibility and the potential publicity a successful attack would generate.

In Table 4, the percentage of attacked organizations are set out against the company size, measured in the annual turnover and the number of employees. A clear trend does not become visible; it must therefore be assumed that most attackers do not select their targets based on their size.

Table 4 – Attacks related to annual turnover

Annual turnover	Percentage organizations reporting attacks
less than ½ million dollar	47% (n=30)
between ½ and 5 million dollar	38% (n=34)
between 5 en 50 million dollar	42% (n=24)
50 million dollar or more	35% (n=20)
not specified	33% (n=9)

Table 5 – Attacks related to number of employees

Number of employees	Percentage of organizations reporting attacks
less than 20	46% (n=41)
between 20 and 200	29% (n=42)
between 200 and 1000	42% (n=24)
more than 1000	60% (n=10)

From the above tables it can be concluded that the use of an Internet site or the use of a connection between the Internet and the internal IT-infrastructure bears a great chance of attacks. This chance is present for practically any kind of organization, regardless of its size or the sector it operates in.

6. Organizations reporting incidents

The percentage of organizations experiencing incidents (successful attacks) has been calculated using the same procedure as with the percentage of organizations experiencing attacks.

Table 6 – Percentage of organizations reporting incidents on their Internet site or internal IT-infrastructure (regardless of detection measures)

Environment	Percentage of organizations reporting incidents
Internet site	12% over 18 months (n=99)
internal IT-infrastructure	10% over 19 months (n=98)

When organizations that do not regularly check the contents of their logfiles are excluded, the percentages change, as shown by Table 7.

Table 7 – Percentage of organizations reporting incidents on their Internet site or internal IT-infrastructure (organizations with regular logchecks)

Environment	Percentage of organizations reporting incidents
Internet site	18% over 17 months (n=51)
internal IT-environment	9% over 20 months (n=47)

The numbers presented in Table 6 and Table 7 should be seen as mean values. Organizations can strongly influence their individual risk by implementing the right security measures, as shown in section 8.

There is a remarkable difference in incident reports between the Internet providers and the organizations that have outsourced their Internet site to a provider. While providers are affected by security incidents with respect to their Internet site, the organizations that have outsourced the maintenance of their site do not seem to be aware of it. Although no evidence was available that the provider incidents indeed affected client sites, it is certainly advisable for organizations outsourcing the maintenance of their Internet site, to define clear procedures for reporting security incidents in the agreement with their provider.

Table 8 – Reported incidents by providers and clients of providers

Organizations	Percentage reporting incidents Internet site
providers	15% (n=34)
clients	0% (n=31)

Two of the organizations having security incidents were deploying electronic commerce activities. Both of them reported to have an Internet site that offers products or services that can be ordered on the Internet site. Payment could also be done by means of the Internet; one of the options was payment by credit card. The two organizations were hit by a break-in on the Internet site and a break-in on the internal IT-infrastructure, respectively. Although no indications were present that the intruders had actually seen or copied any credit card related information, the incidents illustrate that besides the protection of the payment information exchanged over the Internet, also sufficient attention should be paid to the protection of the computer systems themselves.

7. A closer look at the security incidents

In the following paragraphs the incidents concerning unauthorized access, denial of service and malicious code will be dealt with. The number of reported incidents (17, 4 and 9 for unauthorized access, denial of service and malicious code respectively) is, however, not sufficient to do a thorough statistical analysis. The discussion will, therefore, be limited to the most striking trends.

7.1 Unauthorized access

In seems that in most incidents of unauthorized access, the impact on the operations of the affected organization is limited. The number of affected systems is usually one (counting only the affected systems within the surveyed organization). None of the organizations reported missed revenue, nor did the perpetrator read or modify any business sensitive data such as the personnel database or the financial records. The relatively small impact may be related to the fact that most incidents affect only the Internet site, whereas the mission-critical information is usually located on the internal IT-infrastructure.

Despite the relatively limited impact on the operations of the organizations, the incidents can be very annoying. In roughly half the number of incidents, the perpetrator misused the hacked systems for spreading undesirable information (such as illegally copied software or altered Web pages) or for launching attacks against the computer systems of other organizations, which can be quite embarrassing for the affected organization. Furthermore, the system administrators spend on average half a week for each incident.

Ten out of the seventeen unauthorized access incidents were reported as enabled by bugs in software. From the name and version number of the concerning software, it was determined that five incidents were enabled by exploiting bugs that were well-known at the time the incident took place, and for which a patch was available. These incidents, therefore, are in fact enabled by not timely installing security patches. This may be related to the high workload of the responsible system administrators, as in three organizations that have become victim of incidents enabled by not timely installing patches, the pressure of work, as described by the system administrator, was high. In two cases it was even noticed that "the urgent tasks and requirements coming from the organization take so much time that there is frequently not enough time left for necessary (less visible) maintenance."

Six incidents have been discovered as a result of existing detection measures (four times this was a routine check-up of the logfiles). The majority (eight incidents), however, was detected more or less by coincidence; examples include unusual system behavior, tips by other organizations, or an excessive high (traffic related) bill from the Internet provider.

After the incidents were detected, only two organizations deliberately postponed removing the intruder, in order to attempt to trace and identify him. Of the organizations that immediately started to disconnect the intruder, a majority was still able to identify the perpetrator. Apparently, it is not always necessary to take extra risks in order to identify the perpetrator.

7.2 Denial of service

With three out of 145 organizations reporting denial of service incidents, it can be stated that these kinds of incidents are relatively scare, despite the fact that they can relatively easily be caused. Apart from being a nuisance, the incidents did not have any serious consequences, such as a significant loss of productivity or missed turnover.

7.3 Malicious code

Despite the current attention for the security problems in Java and ActiveX, no incidents with respect to active content were reported. The incidents concerning malicious code, as reported by nine organizations, were all related to MS Word macro viruses spread by e-mail. These viruses, however, can cause considerable damage. This was indicated by the fact that:

- usually several systems were infected (in one incident even up to 45);
- the system administrators spent much time on handling of the incidents (sometimes several days);
- there is a realistic chance of passing the viruses through to business relations, something that happened to two of the responding organizations.

The absence of a permanent Internet connection does by no means result in a decreased risk of receiving viruses. In fact, six out of nine organizations that have been affected by Internet-spread viruses were solely using dial-up connections.

7.4 About the perpetrators

Based on the actions the perpetrator undertakes when he has gained unauthorized access to a computer system, his objectives can to some extent be deduced.

From the incidents as reported by the responding organizations, it can be stated that most intruders are not really interested in reading or modifying business-critical data. The information that was read or modified usually consisted of data such as logfiles, network traffic, Webpages or system binaries. Not a single responding organization mentions incidents in which the perpetrator has read or modified any truly sensitive data, such as customer files or financial data.

The perpetrators are more interested in the network facilities. In approximately half of the unauthorized access incidents, the hacked computer systems were abused for activities like Website hacking, the distribution of illegally copied software, or for launching attacks against the computer systems of other organizations. In some cases the intruder was eavesdropping the network traffic. The fact that eavesdropping intruders were also reported by Internet providers means that it is certainly advisable to use strong encryption when sending sensitive data over the Internet.

Another indication that most perpetrators have few interest in gathering business critical data, is the fact that more intrusions are being reported with respect to the Internet site than with respect to the internal IT-infrastructure. Furthermore, among the organizations reporting unsuccessful unauthorized access attempts, more attacks are reported with respect to the Internet site than with respect to the internal IT-infrastructure.

One of the first priorities of an intruder after having launched a successful attack is to safeguard his access. In almost half of the incidents concerning unauthorized access, the perpetrator realised new means of access; such as by adding new accounts, installing Trojan horses or reading the password file.

Most intruders can probably better be described as joyriders than as vandals or criminals. They break into a system not to gain financial profit (the affected organizations rarely suspect any financial motives) but to fully enjoy the power of the computer system and it's network facilities.

The intruders do not necessarily possess a high level of expertise, as many of them make use of well-known techniques.

In only two incidents the intruders were prosecuted.

The above conclusions did not come as a surprise, as they are more or less consistent with the experience at the Vrije Universiteit concerning computer intrusions [vDoorn92].

7.5 Additional security measures

Organizations affected by attacks or incidents often take additional security measures:

- almost all organizations confronted with unauthorized access incidents implemented additional security measures. The reported measures often do not require a continuing effort nor any additional resources apart from a certain amount of man-hours of the system administrators;
- the few organizations affected by denial of service incidents all implemented measures to prevent further incidents;
- two thirds of the organizations that became victim of malicious code incidents improved their virus checking as a result of the incidents;
- among the organizations exclusively detecting unsuccessful attacks, about half of them implemented additional security measures.

It appears that most organizations are not fully aware of the risks of their Internet usage until the first attack or incident takes place. The chance of attacks is relatively high, up to 45% during 1½ year, so it makes sense to implement appropriate security measures before being confronted with the first attack.

8. Effectiveness of security measures

One of the goals of this research was to determine the effects of several types of security measures. The effects will be presented in the form of graphs such as Figure 1. In these graphs, the responding organizations are represented in the form of two vertical bars. The left bar contains the organizations that did not implement a certain type of security measure; the right bar represents the organizations that did. Both bars are subdivided into three parts:

- a part containing organizations at which the security failed at least once (i.e. organizations that report one or more attacks that broke through the security, causing incidents); these are represented by the lower part of the figure, labeled as *security failed*;
- a part containing organizations at which the security was successful in defending against all off the attacks (i.e. organizations that report one or more attacks, but no incidents).; these are represented by the upper part of the figure, labeled as *security successful*;
- a part containing organizations that detected neither attacks or incidents.; these are represented by the middle part of the figure, labeled as *nothing detected*.

Graphs in the form of Figure 1 are limited in the sense that they do not contain information about the attacks and incidents that went undetected. Therefore, the actual percentage or organizations having attacks or incidents can be greater than indicated.

One of the assumptions used when interpreting the graphs is that security measures do not affect the chance of being attacked. Organizations are assumed to face the same chance of attacks, regardless of the security measures implemented.

The effects of the security measures will be determined by examining two relations:

1. the extent to which the security measure contributes to the *prevention* of incidents. Does the measure show a decrease of *security failed*?
2. the extent to which the security measure contributes to the *detection* of attacks and incidents. Does the measure show an increase of *security successful* and *security failed*? Detection is considered to be important, as it enables organizations to respond in an early stage, therefore limiting the potential damage.

The survey aimed to determine the effect of four types of security measures:

1. technical measures, which are implemented at the technical layer (hardware/software). Because of the sheer diversity of the various technical security measures, it was decided to restrict the scope to one specific often implemented technical measure: the firewall;
2. organizational measures, which are meant to set security standards and procedures within the organization. Organizational measures are defined by the management, in the form of written documents or guidelines;
3. detection measures, which are meant to inform the organization about the effectiveness of its security. By comparing the reported attacks and incidents among groups with different detection measures, it is possible to get an impression of the extent to which attacks and incidents go unnoticed;
4. human factors; these include various factors that affect people's ability to pay sufficient attention to security issues.

The four kinds of security measures mentioned above will be discussed in the following four sections. Security measures taken as a result of security incidents are ignored.

8.1 Effectiveness firewall

Over the last few years, firewalls became an important technique to guard against the risks of an Internet connection. A firewall consists of one or more computer systems that are placed between the Internet and the internal IT-infrastructure.

These systems carefully watch the traffic that enters the firewall and only allow authorized traffic to pass. The firewall itself should of course be immune to penetration.

In the questionnaire, it was specifically asked for firewalls that use proxies or stateful inspection. A simple packet filter – such as available on many commercial router products – without additional firewall components (such as a bastion host, [Ches94]) is not regarded as a firewall.

Of the 98 organizations that have a permanent link between the Internet and their internal IT-infrastructure, 58 were using a firewall (in 41 cases implemented by a commercial firewall product). The remaining 40 organizations have a permanent Internet connection without using a firewall. Of the latter group, six have a restricted Internet connection (such as a TCP/IP – IPX connection). Four organizations did not specify the way they secured their Internet connection.

Figure 1 depicts the effects of a firewall upon the level of security.

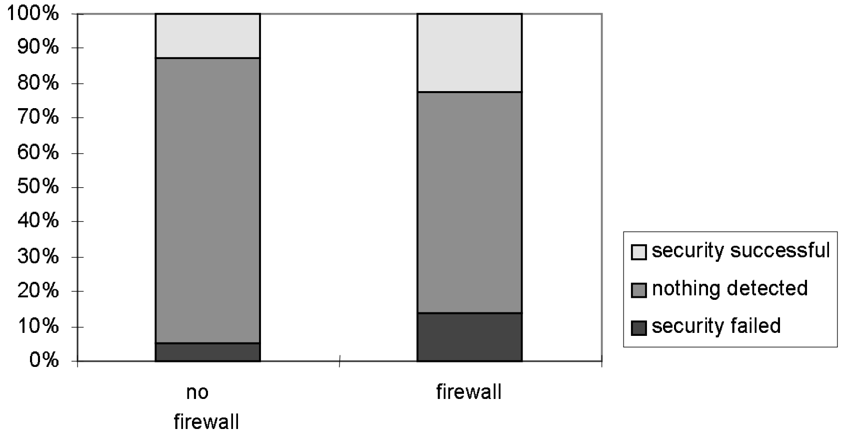

Figure 1 – Effects presence firewall

It is somewhat surprising to see that the presence of a firewall does not necessarily decrease the chance of security incidents. A possible explanation is that not all firewalls are of sufficient quality. In the survey, this was indicated by three findings:

- fifteen organizations (25% of those having a firewall) have a firewall which implements a *default permit* policy. This means that the firewall is instructed to pass all network services, except the services that are known to be dangerous and therefore explicitly disallowed. The main danger of such a policy is that the sheer number of information services makes it fairly easy to overlook a certain kind of dangerous network service. Furthermore, firewalls with a default permit policy will probably allow more services to pass than is strictly necessary. This implies an increased risk when new vulnerabilities are discovered. It is therefore strongly preferred to implement a *default deny* policy, which means blocking all traffic except the services that are explicitly allowed (and carefully evaluated) [Chap95];
- six organizations (10% of those having a firewall) have a firewall but at the same time allowed inbound remote logins to the internal IT-infrastructure without necessarily using encryption, one time passwords, or some other means of strong authentication. The danger of such a situation is that if an eavesdropper on the Internet manages to intercept the password, he can logon as a normal user [GaSp96];
- two organizations had their firewall installed by an external expert, without any kind of maintenance ever since.

Although the above criteria are only meant to provide a rough impression on the quality of the firewalls – a more thorough measurement would be to extensive to include in the questionnaire – it can nevertheless be stated that many firewalls do not appear to be functioning in an optimal secure way.

A second indication of the poor quality of the surveyed firewalls can be provided by examining the incidents that broke through a firewall. It was found that 5 incidents could be reduced to security holes in the firewall itself:

- in one case the services passed through the firewall were handled by software containing security holes;
- in the case of another incident the entire firewall (at least the security part of it) was out of service without the organization being aware of it;
- in the case of three incidents the firewall did not check on incoming e-mail, causing MS Word viruses to be able to reach the internal IT-infrastructure.

One other incident concerned a computer system reported as part of the internal IT-infrastructure but located outside of the firewall. The two remaining incidents were not being reported in enough details to determine the cause.

The insufficient quality of many firewalls is being confirmed by the people of KPMG that carry out penetration tests. They report that in one out of five cases they manage to break through the firewall. As the organizations that ask KPMG to do a penetration test often spend a more than average effort on security, it is likely that the total percentage of firewalls containing security vulnerabilities is more than 20%.

8.2 Organizational aspects of security

Organizational security measures are the security standards that are defined within an organization. These often come in the form of written documents in which the management states the required level of security, including the necessary steps to achieve this.

Organizational security measures are closely related with the field of risk analysis. As a result of this, adequate organizational measures vary between organizations that face different risks. It is therefore not feasible to judge the organizational measures upon their contents, without knowing the company-dependent risks. The questionnaire therefore exclusively asked if certain documents or standards are available, without making inquiries about their actual contents.

The organizational security measures this survey has focused on were selected using existing sets of security standards, such as the Code of Practice [Code93] and the OTB Studie Internet [OTBi97]. Using these standards, the following measures were selected to be part of the questionnaire:

- the presence of a written security policy. The security policy specifies the security requirements and the measures to achieve these requirements [Roos96];
- the explicit assignment of security responsibilities. The responsibilities can be included in the job descriptions, or be specified in a special security-related document (such as the information security policy);
- the inclusion of security requirements in *Service Level Agreement* (SLA's) or other kinds of written agreements between the users and the system administration. This measure is only relevant if such agreements are being used;
- explicit (written) attention to the risks of an Internet connection. This can be done by either defining the security requirements of the Internet-connection or by providing guidelines which computer systems can and cannot be linked to the Internet;
- the existence of user awareness measures;
- management involvement in the selection of services that are to be blocked or passed by the firewall;
- the presence of incident response procedures or guidelines.

Figure 2 depicts the effects of organizational security measures. The left-hand side contains the organizations with few measures, the right-hand side contains the organizations that defined many measures. The difference between few and many was defined in such a way that each side contains exactly 50% of the responding organizations.

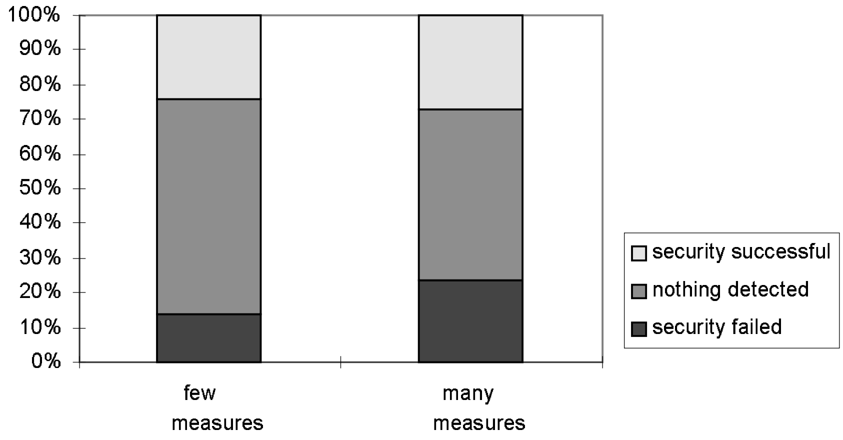

Figure 2 – Effects of organizational security measures

Figure 2 shows an increase of *security failed.* An improved detection can, however, not be concluded, as *security successful* stays at more or less the same level. Apparently, the actual level of security does not necessarily improve when many organizational security measures are present.

A possible explanation for the poor effectiveness of organizational measures is that these are meant to be translated to the operational level, as few intruders will be stopped by factors like security policies, job descriptions or user awareness measures by themselves. Only when the computer systems are free of security vulnerabilities, an attack can be successfully resisted. The organizational security measures are, therefore, only useful if they actually result in adequate operational security measures, most of which are related to the technical configuration of the computer systems.

In order to gain insight in the effects of the organizational measures on the implementation of operational procedures, the emphasis was laid on one specific operational procedure: a regular check of the system logfiles. Figure 3, Figure 4, and Figure 5 show to what extent the presence of an information security policy, the explicit assignment of security responsibilities, and explicit attention to the risks of an Internet connection actually contribute to a regular check-up of the logfiles (Figure 5 only shows the effects on the internal IT-environment, as its measure is not applicable to the Internet site)Figure 5 – Effects explicit attention to the risks of an Internet connection on regular checking of the logfiles. We have focused on these three organizational measures because the other ones were either too unlikely to result in an improved procedure for checking the logfiles (for example: user awareness measures) or were implemented too infrequently to derive statistical conclusions. The Y-axis represents the organizations performing regular logchecks.

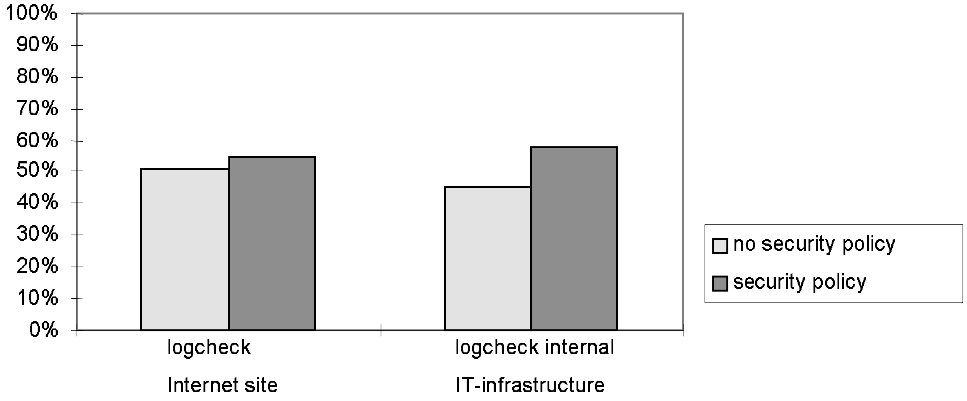

Figure 3 – Effect security policy on regular checking the logfiles

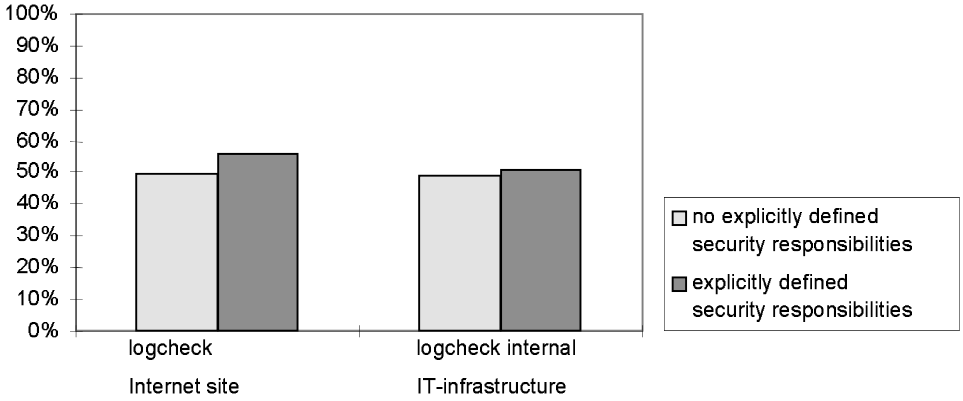

Figure 4 – Effect explicitly defined responsibilities on regular checking the logfiles

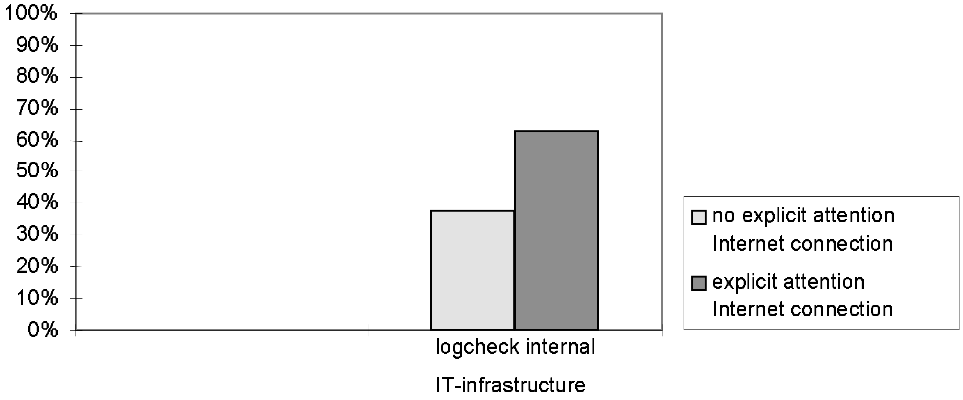

Figure 5 – Effects explicit attention to the risks of an Internet connection on regular checking of the logfiles

The above figures show that organizational security measures frequently do not significantly improve the checking of the logfiles. If this effect also appears at operational measures that are not included in the questionnaire, it can be concluded that the translation from organizational guidelines into operational (and technical) measures leaves a lot to be desired.

8.3 Auditing the security

An organization can use several means to gain insight in the effectiveness of its security. These vary from a simple software packet that scans for some well-known vulnerabilities, to a security expert conducting an audit. The measures included in the survey were selected to include both technical as organizational measures:

- the use of software (such as Tripwire) to detect attacks and/or incidents;
- the use of software (such as Satan) to detect security vulnerabilities;
- a regular check-up by an expert on information security; this check-up can either be a penetration test or an audit;
- the presence of guidelines or procedures for reporting incidents, in order to provide the management insight into the effectiveness of the security measures;
- the presence of a regular procedure for checking the logfiles.

These measures turn out to have a clear positive effect upon the detection of unsuccessful attacks; *security successful* increases 10% to 40%.

As a significant part of the incidents was detected by checking the logfiles, it makes sense to pay special attention to the effects of regularly checking the logfiles upon the detection of incidents.

The frequency with which the logfiles are inspected, however, is not the only factor that contributes to logfiles being an effective instrument to detect incidents. Intruders, for example, have been known to make alterations to the logfiles in order to wipe out the indications of their break-in. The quality of the logfiles as an instrument to detect incidents has therefore been measured by an index value based on three aspects:

- the amount of information being logged. Six different types of security relevant information were defined, each one contributing 1/6 index points;
- the frequency at which the logged information is evaluated. Daily, weekly, and monthly are rewarded with 1, 2/3, and 1/3 index point, respectively. Less frequently than one month gains 0 points;
- the way the audit trails are protected against modification by intruders. Making direct hardcopies or directly forwarding the information to an extra secure system gains 1 index point, making regular backups gains 2/3 index points. If no protective measures are taken, 1/3 point is assigned.

The items above work like a chain that is as strong as the weakest link. Therefore, the index is calculated as the minimum value of the individual items.

It is not feasible to define a clear boundary between adequate and inadequate logging. Therefore, in Figure 6, the median of the index values was taken as boundary value.

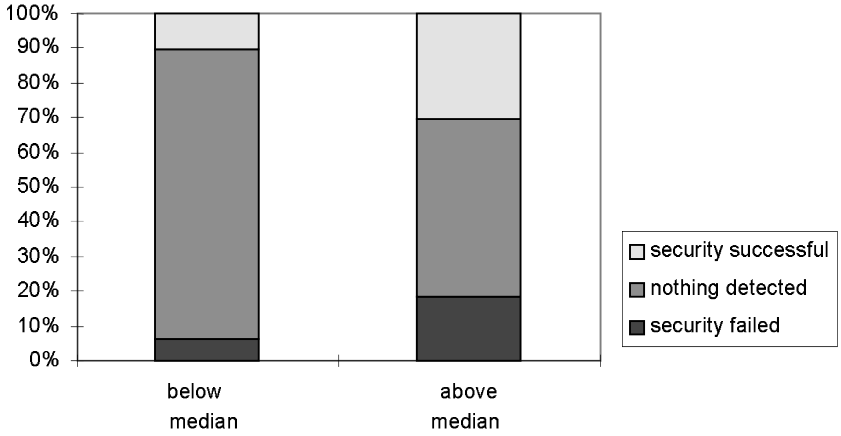

Figure 6 – Effects of checking logfiles of the Internet site

Figure 6 shows that organizations that have implemented a careful procedure for creating and inspecting the logfiles are more frequently reporting both attacks and incidents. It is therefore very likely that organizations without adequate detection measures are sometimes having incidents without being aware of it.

This presumption is confirmed by a closer inspection of the security incidents. It turns out that the "silent" attacks, where the perpetrator merely reads information without undertaking any further actions that might draw the attention on the incident, were exclusively reported by organizations that have implemented procedures for incident detection. Organizations that do not have regular security checks, on the other hand, were only reporting incidents with a relatively high visibility, such as where the perpetrator undertakes actions like Website hacking, attacks on other sites, or modification of system binaries.

Under the assumption that the chance of incidents does not depend upon the detection measures, it can be stated that approximately 10% of the organizations without a regular check-up on the logfiles are having incidents without being aware of it. This estimate is relatively modest compared what other researchers have found. For example, a test program by the *Defense Information Systems Agency* (DISA) found that 96% of the succeeded penetration tests carried out by DISA was not being detected [GAO96]. A research carried out by the *Air Force Information Warfare Center* (AFIWC) found that only 13% of the attacks was being reported [How97].

8.4 Human factors

Security is often said to depend upon people. It can therefore be expected that the level of security is improved if the people that are responsible for security – especially the system administrators – are well equipped for this task.

In order to put this assumption to the test, the survey included several measurements that provide an impression of the amount of knowledge, experience and workload of the system administrators, as well as the attention they pay to security.

8.4.1 Experience

It is only since the last few years that the Internet has been applied commercially on a wide scale. One of the implications is that many system administrators have relatively little experience with the administration of Internet services, as shown by Table 9

Table 9 – Experience system administrators with Internet

Experience	Number of system administrators
0 to 2 years	134
2 to 5 years	89
more than 5 years	34

Figure 7 depicts the effects of experienced system administrators on the level of security. An organization is said to have an experienced system administration if more than half of the system administrators have at least 2 years of experience. From Figure 7, it can be seen that organizations that have an experienced system administration not only manage to detect more security attacks, but are also able to prevent many of them from turning into incidents.

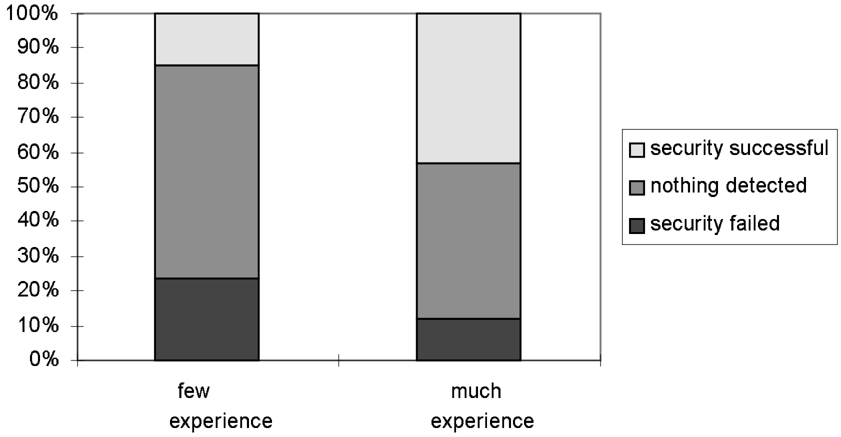

Figure 7 – Effects experience of system administrators

8.4.2 Membership of user groups

The amount of knowledge can strongly affect the quality of people's work. Unfortunately, it was not feasible to include in the survey a direct measurement of the amount of knowledge among the system administrators. Therefore, this information had to be measured in an indirect way, by focusing on the way the knowledge is kept up-to-date.

A very effective way to keep informed of new developments is to join a user group or other association of people that have a professional interest in IT. The members of a user group all have their specific expertise and are usually more than willing to share this knowledge with others.

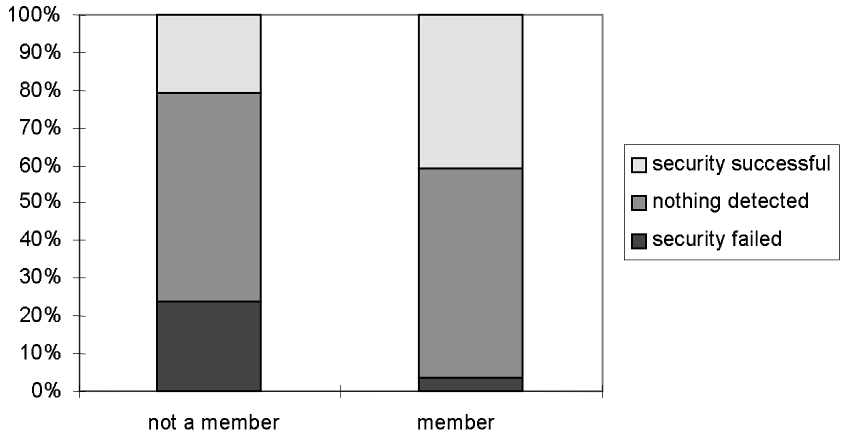

Figure 8 – Effects membership of user groups

Figure 8 shows a significant increase of *security successful*, together with a remarkable decrease of *security failed.* When assumed that both groups are under the same pressure of attacks, this implies that organizations where the system administrators are member of a user group are able to stop a significantly higher percentage of attacks.

One of the most likely reasons for the improved security is the people that join user groups; these clearly show a professional interest in keeping their knowledge up-to-date. The fact that in many cases the expenses are paid out of company funds is a clear indication that the employer finds it important to have a professional system administration, and is willing to make the necessary investments in its employees. A user group further offers easy access to several sources of information, such as presentations, books, magazines (often with discount) and informal contacts.

8.4.3 Workload

One of the questions the survey dealt with was the workload as experienced by the system administrators. The answers are set out in Table 10.

Table 10 – Workload as described by the system administration

Workload	Number of organizations
high	46
reasonable	53
low	15

One of the conclusions that can be drawn from Table 10 is that a considerable number of system administrators claim to have a high pressure of work. Of the group with a high workload, 30 system administrators specify that the urgent tasks and requests from the organization frequently take so much time that insufficient time is left for doing structural (and less visible) maintenance. Thirteen responding system administrators notice that overtime is regular, more than once a week on average.

In Figure 9, the effects of a high workload are specified. The organizations on the left-hand side have a system administration that describes their workload as high. Furthermore, they also indicate that overtime is regular, or that insufficient time is left for doing structural maintenance. The latter two conditions were added in order to make the criterion more objective. All the organization not meeting this criterion are depicted at the right-hand side.

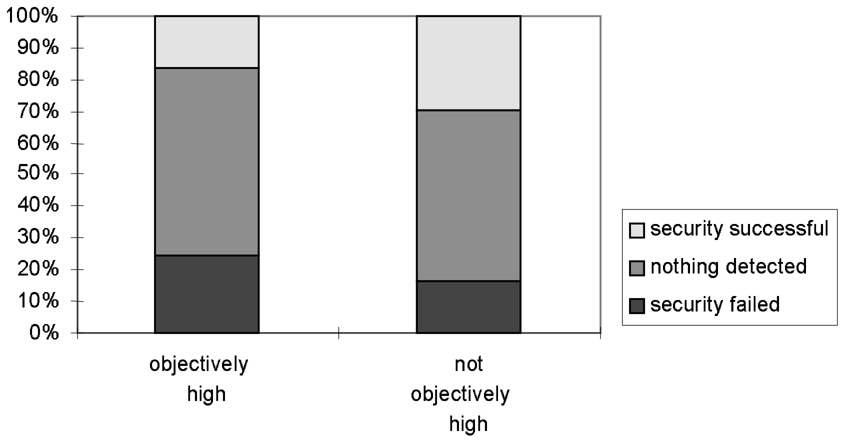

Figure 9 – Effects workload system administration

Figure 9 shows that the level of security is higher at organizations where the system administrators do not have a too high workload.

8.4.4 Applying patches

When new security vulnerabilities in software are discovered (something that frequently occurs), it is of vital interest that the software is replaced as soon as possible by a new version (a so called patch) in which the vulnerabilities have been fixed. Every day a known vulnerability has not been fixed, imposes a risk of incidents. A significant part of the responding organizations, however, does not apply patches within one month, as shown by Table 11.

Table 11 – Speed of installing patches

Applying patches	Number of organizations
within one day	30
within one week	23
within one month	9
frequently after longer than one month	15
no patches have been applied so far	35
not specified	3

The following reasons are given to postpone the installation of patches for longer than one month:

- the workload (mentioned five times);
- the small chance of the vulnerability being exploited, as perceived by the responding organization (mentioned six times);
- the risks of disrupting the systems by installing a patch, meaning that patches can only be applied when the systems are allowed to be out of order (mentioned nine times).

Figure 10 depicts the effects of regularly installing patches (at least once a month).

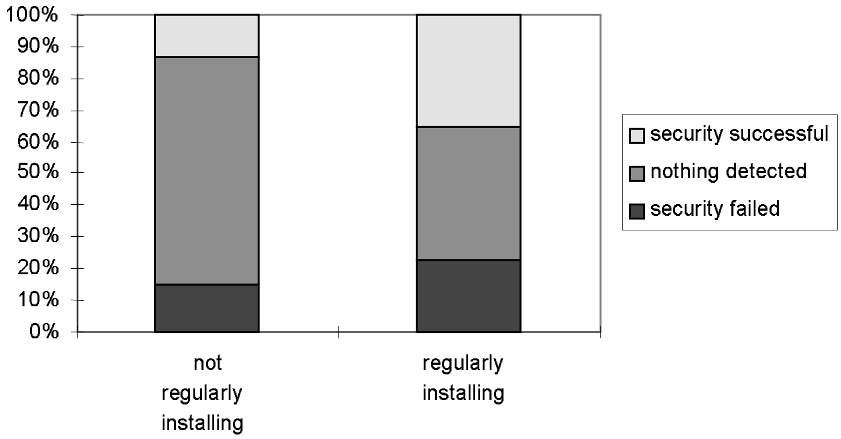

Figure 10 – Effects of regularly installing patches

Surprisingly, the percentage of organizations reporting incidents does not seem to drop if patches are regularly installed. It must however be noticed that four out of five organizations with incidents caused by not timely installing patches indicate that they do install patches on a regular base. Apparently, despite the attention being paid, it is quite easy to forget about installing a patch.

8.4.5 Other measures

There are two remaining measurements related to the quality of the system administration. These are their level of education and whether they make use of information sources with respect to security issues. Both measures show an increased detection of unsuccessful attacks. The percentage experiencing incidents, however, does not show a significant decrease.

9. Conclusions and recommendations

With up to 45% of the Internet connected organizations under attack, it can be stated that security is an essential requirement for anyone connecting to the Internet. Although this threat is present for practically every Internet connected organization (regardless its size or the sector it operates in), most organizations do not seem to be fully aware of it, as many measures are not implemented until the first attack or incident takes place.

Most security incidents seem to be affecting the Internet site instead of the internal IT-infrastructure, which causes the impact to be relatively low from a business point of view. This, however, does not mean that security is irrelevant, as in roughly half the number of incidents the intruder uses the systems in a way that can potentially embarrass the affected organization.

A significant part of the incidents concerning unauthorized access could have been prevented by timely installing security patches.

When considering malicious code, it appears that MS-Word viruses, spread by e-mail, are currently a far greater problem than Java or ActiveX. It is certainly advisable to have virus scanning on incoming e-mail, such as being offered by several commercial firewall products.

The mere presence of a firewall does not always provide adequate protection. Without careful planning, testing and maintenance, a firewall can provide a false sense of security.

The effect of security policies and other organizational security measures is somewhat disappointing, as not every policy results in the actual implementation of effective operational security measures. The security policy should state clear procedures for measuring the resulting operational measures.

The survey added further evidence to the fact that without adequate detection measures, only a small part of the incidents will be detected. Detection measures are an important aspect of security as they enable an organization to respond to incidents in an early stage.

Human factors have a clear influence on the security. Especially the level of knowledge, experience and the absence of a high workload among the system administrators have a positive effect on the security.

10. References

[Chap95] *Building Internet Firewalls*, D. Brent Chapman and Elizabeth D. Zwicky, O'Reilly & Associates, Inc. 1995

[Code93] *A code of Practice for Information Security Management*, British Standards Institution 1993

[CSI96] *1996 CSI/FBI Computer Crime and Security Survey*, Computer Security Institute and Federal Bureau of Investigation 1996

[Farm96] *Security Survey of Key Internet Hosts & Various Semi-Relevant Reflections.* Dan Farmer 1996

[GAO96] *Information Security: Computer attacks at Department of Defense Pose Increasing Risks*, government Accounting Office 1996

[GaSp96] *Practical UNIX and Internet security (2nd edition)*, Simson Garfinkel and Gene Spafford, O'Reilly & Associates, Inc. 1996

[How97] *An Analysis Of Security Incidents On The Internet 1989 – 1995*, John D. Howard, Carnegie Mellon University 1997

[OTBi97] *OTB studie Internet*, Overlegorgaan Technische Beveiligingsstandaarden 1997 (Dutch)

[Pro97] *Prowatch Secure Network Security Survey* 1997

[Roos96] *A Sense of Secureness, approaches to information security* (thesis). Edo Roos Lindgreen 1996

[vDoorn92] *Computer Break-ins: A Case Study*, Leendert van Doorn, Vrije Universiteit Amsterdam, NLUUG proceedings, October 1992