Internet Security Incidents, a Survey within Dutch Organisations

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

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

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

L. 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 Amsterdam and KPMG EDP Auditors, concerning Internet-related security incidents. The survey was held within Dutch organisations 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 right security measures in order to prevent security incidents. This was done by (1) analysing the security incidents to find out in which way they could be prevented and (2) trying to find correlations between certain security measures and (the absence of) security incidents.

1. Introduction

As more and more organisations are connecting to the Internet, security is becoming increasingly important. The fact that security is indeed a problem is illustrated by a survey carried out by Dan Farmer, showing that over 60% of 1700 inspected sensitive Websites, such as banks, credit unions, newspapers and government agencies, could be broken into or even destroyed [Farmer 1996].

Given the high number of vulnerable sites, an interesting question is which part of the organisations using the Internet is actually experiencing Internet related security incidents. The existing surveys that tried to answer this question, such as carried out by CERT/CC [Howard 1997] and Prowatch Secure (a commercial security surveillance service) [Prowatch 1997], are usually based upon a special subset of the Internet connected organisations, such as those requesting assistance from CERT/CC or those having their network security surveyed by Prowatch. It is therefore hard to determine to which extent the resulting figures are representative for the Internet as a whole. Furthermore, these surveys also provide little insight in the amount of damage caused by the incidents to the affected organisations.

A second question is what measures should be taken in order to prevent security incidents. Although many measures are being advised for the technical as well as the organisational part of security [Garfinkel & Spafford 1996] [Roos 1996], little is known about the effectiveness of these measures.

2. Definitions

An *incident* is a situation in which the security of a computer system has been violated. This survey focusses on the following kinds of incidents:

- unauthorised access, whereby someone on the Internet gained access to computer systems or information without being authorised to do so;
- denial of service, whereby someone on the Internet managed to disrupt the information services;
- malicious code, such as viruses and Trojan horses, being spread by means of the Internet.

An *attack* is an attempt to cause an incident by trying to identify and/or exploit security vulnerabilities.

A distinction is being made between the Internet site and the internal IT-infrastructure. The *Internet site* consists of the information services (such as WWW of FTP) that are being 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 differences 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 also means 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, a joint project between *de Vrije Universiteit Amsterdam* and *KPMG EDP Auditors*, was carried out by sending enquiries to 878 organisations that are currently using the Internet. The organisations were selected using the DNS information of the *.nl* domain, with a strong preference for organisations that have their own Internet system administration, as the questionnaires were to be filled in by the system administrators.

Eventually, 145 usable responses were received, obtaining a response-rate of approximately 17%. For a sensitive subject like computer security incidents, this is not a bad result. A similar survey, carried out by the *Computer Security Institute* (CSI) in co-operation with the FBI reached a response-rate of 9% [CSI 1996].

4. Characteristics of the Responding Organisations

The responding organisations can be described by the following characteristics:

- both small and large organisations (measured by annual turnover, number of employees and number of IT-administrators) are significantly represented;
- although several sectors are represented among the responding organisations, approximately one third of the population consists of Internet providers and the IT-sector. This is probably caused by the (earlier mentioned) preference for organisations that have their own Internet system administration;
- about one third of the population (99 organisations) has an Internet-site that is maintained by its own personnel. More than half (58%) of the organisations with an Internet site have their site for longer than one year, which is in principle long enough to be confronted with security incidents;
- about one third of the population (98 organisations) 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 organisations with an Internet site uses it as 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 organisations where the personnel has 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 organisations 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 organisation.

5. The Extent of the Problem

An estimate of the part of the Internet connected organisations that is attacked is hampered by the fact that organisations do not need to be aware that such attacks took place. The data of [Tab. 1] has therefore been calculated twice: once for all the organisations, regardless whether they have implemented adequate detection measures and once for the organisations that have at least implemented a minimal form of detection (a regular check of the log files). It is felt by the researchers that the latter group, although having a smaller size, provides a more realistic insight into the extent of the problem.

Environment	Percentage of organisations reporting attacks (regardless of detection measures)	Percentage of organisations reporting attacks (organisations with regular log-checks)
Internet site	32% over 18 months (n=99)	45% over 17 months (n=51)
Internal IT-infrastructure	29% over 19 months (n=98)	40% over 20 months (n=47)

Table 1: Percentage of organisations reporting attacks

A similar table can be set up with respect to the incidents (meaning attacks that have broken through the security measures), as done in [Tab. 2].

Environment	Percentage of organisations reporting incidents (regardless of detection measures)	Percentage of organisations reporting incidents (organisations with regular log-checks)
Internet site	12% over 18 months (n=99)	18% over 17 months (n=51)
Internal IT-environment	10% over 19 months (n=98)	9% over 20 months (n=47)

Table 2: Percentage of organisations reporting incidents

The percentages of attacks and incidents for the Internet site are based on organisations having an Internet site which is being maintained by their own personnel. The percentages of attacks and incidents for the internal IT-infrastructure are based on organisations having a permanent link (leased line) between the Internet and their internal IT-infrastructure.

6. Attacked Organisations

The attackers do not seem to be very selective when choosing their targets. The chance of an attack is relatively constant, regardless the size of the organisation or the sector it operates in.

The only exceptions are the media and the non-profit sector. These are reporting more, respectively fewer attacks. A possible explanation is that hacker ethic is to some extent keeping the perpetrators from attacking non-profit organisations (of which most of them, such as humanitarian organisations of the 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 amount of publicity a successful attack would generate.

7. Providers and Clients

Organistions	Percentage reporting incidents Internet site
Providers	15% (n=34)
Clients	0% (n=31)

Table 3: Reported incidents by providers and clients

There is a remarkable difference in incident reports between the Internet providers and the organisations that have outsourced the technical maintenance of their Internet site to a provider. While providers are affected by security incidents concerning their Internet site, the organisations that have outsourced the maintenance of their site do not seem to be aware of it. Although the cause of this situation could not be determined, it is certainly advisable for organisations outsourcing the maintenance of their Internet site, to define clear procedures for reporting incidents in the contract with their provider.

8. A Closer Look at the Security Incidents

In the following paragraphs the incidents concerning unauthorised access, denial of service and malicious code will be dealt with. The number of reported incidents (17, 4 and 9 for unauthorised 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.

8.1. Unauthorised Access

In seems that in most incidents considering unauthorised access, the impact on the operations of the affected organisation is limited. The number of affected systems is usually one (counting only the affected systems within the surveyed organisation). None of the organisations 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 organisations, the incidents can be very annoying. In roughly half of the incidents, the perpetrator misused the hacked systems for spreading undesirable information (such as illegally copied software or Website hacking) or for launching attacks against the computer systems of other organisations, which can be quite embarrassing for the affected organisation. Furthermore, the system administrators spend on average half a week for each incident.

Ten out of the seventeen unauthorised access incidents were reported as caused by bugs in software. From the name and version number of the concerning software, it was determined that five incidents were caused by bugs that were well known at the time the incident took place and for which a fix was available. These incidents, therefore, are in fact caused by not timely installing security fixes. This may be related to the high workload of the responsible system administrators, as in three organisations that have become victim of incidents caused by not timely installing fixes, 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 organisation take so much time that there is frequently not enough time left for necessary (less visible) maintenance."

8.2. Denial of Service

With three out of 145 organisations reporting denial of service incidents, it can be stated that these kinds of incidents are infrequent, 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.

8.3. 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 9 organisations, 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 with the 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 organisations.

8.4. About the Perpetrators

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

From the incidents as reported by the responding organisations, 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 like logfiles, network traffic, Webpages or system binaries. Not a single responding organisation mentions incidents whereby 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 unauthorised access incidents, the hacked computer systems were misused for activities like Website hacking, the distribution of illegally copied software or for launching attacks against the computer systems of other organisations. In some cases the intruder was eavesdropping the network traffic. The fact that eavesdropping intruders were also being 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 among the organisations reporting unsuccessful unauthorised 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 unauthorised 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 any financial profit (the affected organisations 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.

8.5. Additional Security Measures

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

- almost all organisations confronted with unauthorised access incidents have 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 organisations affected by denial of service incidents all have implemented measures to prevent further incidents;
- two thirds of the organisations that became victim of malicious code incidents improved their virus checking as a result of the incidents;
- among the organisations exclusively detecting unsuccessful attacks, about half have implemented additional security measures.

It appears that most organisations 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.

9. Effectiveness of Security Measures

The survey measured the effectiveness of several kinds of security measures: the presence of a firewall, security policies, the presence of security audits and the quality of the system administrators.

9.1. Effectiveness Firewall

A firewall is an often-used technique to establish a secure link between the Internet and the internal IT-infrastructure. In this survey it was measured to which extent the presence of a firewall actually contributes to the security of the internal IT-infrastructure. This was done by comparing the percentage of organisations experiencing security incidents on their internal IT-infrastructure for both the group of organisations with a firewall and the group of organisations not having a firewall.

Strangely enough, the percentage of companies experiencing Internet security incidents among the organisations having a firewall is not any less than among the organisations not having a firewall.

A possible explanation is that not all firewalls are of proper quality. This was indicated by the following findings:

- one out of four organisations reported that they have implemented a policy of allowing all services to pass through the firewall, other than a few services that are explicitly blocked. The main danger of such a *default permit* policy is that because of the great number and complexity of network services it is fairly easy to overlook a certain kind of dangerous network traffic. It is therefore advisable to allow only explicitly authorised network traffic, and block all other traffic [Chapman & Zwicky 1995];
- one out of ten organisations having a firewall offers the possibility of inbound logins without necessarily using encryption, one-time passwords or some other means of strong authentication. The danger of this situation is that if an eavesdropper manages to intercept the password, he can logon as a normal user [Garfinkel & Spafford 1996];
- at two organisations, the firewall had been installed by an external expert without any kind of maintenance ever since.

The above criteria are necessarily incomplete and could therefore only be used to get a rough impression of the quality of the firewalls, as a more thorough measurement would be too extensive to fit into the survey.

A second explanation for the poor effectiveness of the installed firewalls can be given by a closer examination of 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 organisation 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 be able to determine the cause.

The frequent poor quality of firewalls is being confirmed by the people of KPMG doing penetration tests. They report that in one out of five cases they manage to break through the firewall. As the organisations that ask KPMG to do a penetration test often spend a more than average effort to security, it is likely that the total percentage of organisations having security holes in their firewall is more than 20%.

9.2. Organisational Aspects of Security

The survey has tried to measure the effects of the following organisational security measures, taken from [BSI 1993] and [OTB 1997]:

- a written security policy;
- an explicit assignment of security related responsibilities;
- security clauses included in the *Service Level Agreement* (SLA's) if the organisation makes use of them;
- a written policy with respect to the risks of the Internet connection, if such a connection is present;
- user awareness measures;
- management involvement in the selection of services allowed to pass through the firewall;
- the existence of procedures and guidelines with respect to incident response.

To measure the effects of these organisational security measures, two groups of organisations were assembled: those having implemented many measures and those having implemented few. The difference between many and few was defined in such a way that both categories contain exactly 50% of the relevant responding organisations.

Surprisingly, the group of organisations that have implemented many organisational security measures does not have any fewer incidents than the other group. A possible explanation is that, in order to have an effective security, the organisational measures must be translated into operational procedures, as few intruders will be stopped by measures like security policies, job descriptions or user awareness sessions by itself. The organisational security procedures 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.

To measure the effects of the organisational measures on the implementation of operational procedures, the emphasis was laid on one specific operational procedure: a regular check of the system logfiles. For each organisational measure two groups of organisations were formed, those with and those without the measure. In most cases it was found that the group of organisations having implemented the organisational measure did not have a significantly higher percentage having implemented a regular logcheck than the group without the organisational measure. If this trend also appears at other operational security measures not included in the survey, than it can be stated that the effect or security policies and other organisational measures upon the quality of the operational procedures is frequently insufficient.

9.3. Auditing the Security

As a significant part of the incidents was detected by checking the logfiles, special attention was being paid to the effects of a regular audit on the logfiles. It turned out that the number of incidents reported with respect to the Internet site was significantly greater with the organisations performing regular logchecks (18% reported incidents) than with organisations that check the contents of their logfiles only if there is a direct reason to do so (6% reported incidents). If the organisations without adequate detection measures are under the same pressure of attacks as the organisations that do have adequate checks, then it can be assumed that the former group is having security incidents without being aware of it. This assumption is being confirmed by a further analysis of the reported 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 organisations that have implemented procedures for incident detection. Organisations 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.

If organisations without proper detection measures have the same chance of being (successfully) attacked as those that do have adequate detection measures, it can be inferred that approximately 12% of the former group is having Internet related security incidents without being aware of it.

If 18% of the organisations are having incidents, while only 6% of the organisations without adequate detection measures are aware that such incidents have taken place, then the latter group has managed to detect only one third of the incidents. This however, 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 [GAO 1996]. A research carried out by the *Air Force Information Warfare Center* (AFIWC) found that only 13% of the attacks was being reported [Howard 1997].

9.4. Quality of the System Administrators

Security often depends on people. The survey has tried to find out which human factors have a significant effect on the effectiveness of the security. The focus was on the system administrator, as he was the person filling in the questionnaire. From the information provided, it was inferred that the following factors are important when security is at stake:

- the level of knowledge. Because a direct measurement would be unfeasible, the level of knowledge could only be measured by indirect means. The level of knowledge has therefore been measured by asking whether or not the system administrators are members of a user group, as these are specifically aimed at the exchange of knowledge among their members;
- the level of experience with the administration of Internet services;
- the pressure of work. In 30% of the responding organisations the pressure of work of the system administrators is on such a high level that overtime is regular (more than once a week) or that the urgent tasks and requests coming from the organisation take so much time that insufficient time is left for doing

structural maintenance. In this situation it is up to the professionalism of the system administrators to – despite the high workload – pay enough attention to important things not immediately visible to the users, such as computer security. It is, however, the task of the management to structurally improve this situation.

10. Conclusions and Recommendations

With up to 45% of the Internet connected organisations under attack, it is safe to state that security is an essential requirement for anyone connecting to the Internet. Although this threat is present for practically every Internet connected organisation (regardless its size or the sector it operates in), most organisations do not seem to be fully aware of it.

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 organisation.

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

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 sole availability of a firewall does not always provide a proper protection. Without careful planning, testing and maintenance, a firewall can provide a false sense of security.

The effect of security policies and other organisational 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, however, an important aspect of security as they enable an organisation 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.

11. References

[Chapman & Zwicky 1996] *Building Internet Firewalls*, D. Brent Chapman and Elizabeth D. Zwicky, O'Reilly & Associates, Inc. 1995

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

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

[Farmer 1996] *Security Survey of Key Internet Hosts & Various Semi-Relevant Reflections.* Dan Farmer 1996 <http://www.trouble.org/survey/>

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

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

[Howard 1997] *An Analysis Of Security Incidents On The Internet 1989 – 1995*, John D. Howard, Carnegie Mellon University 1997 <http://www.cert.org/research/JHThesis>

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

[Prowatch 1997] *Prowatch Secure Network Security Survey* 1997

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