Federal Office
for Information Security

The IT-Security Situation in Germany in 2005

Contents

Table of figures

Preface

1 Preface

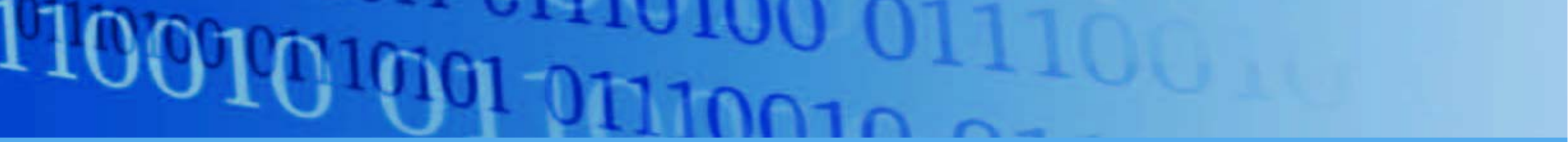
Both the economy and society depend upon safe information technologies because there are too many networked systems in the meantime, and there is too much dependence on smoothly functioning information technologies. IT-security is part and parcel of a nation's security and must, hence, be understood as a national task.

With its Federal Office for Information Security (BSI), Germany has a specialised agency that deals with all IT-security-related questions. The BSI’s objective is to guarantee the secure use of information and communication technologies in our society. To achieve this objective, it is necessary to record and analyse the current situation and to present it to the general public.

This report presents the current IT-security situation in Germany. It provides an overview of pending challenges. Furthermore, the report shows trends and makes it possible to categorise and evaluate them since one can only react adequately to a hazard if one is aware of exactly what the hazard is. We will only be able to utilise the advantages of the information technologies and their world-wide network systems without limitations if we succeed in protecting them, and hence ourselves, appropriately.

July 2005

Udo Helmbrecht, PhD
The President of the BSI



Introduction

2 Introduction

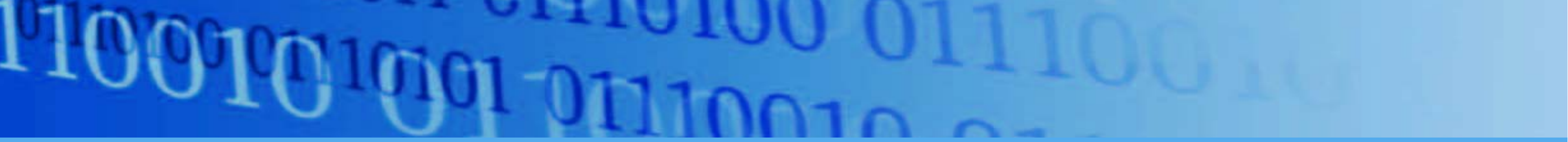
Information Technology (IT) has become the outstanding social factor of our time. Its world-wide application is on the rise, and so is our dependence on IT — and Germany is no exception to the rule either. Computers, mobile telephones, and the Internet have evolved into the basis of a mobile, knowledge- and networked-based information society.

The transformation in information technology has led to new types of threats. This becomes evident, for example, in malicious programs (malware). While computer viruses and worms used to be spread by exchanging infected disks, today they are spread via the Internet and E-mails. This new "proliferation" methodology increases the striking power of these "pests". Given the vast number of IT network systems, epidemics spread around the globe in no time at all, causing tremendous financial repercussions on society.

In this paper, the BSI reports on the IT-security situation in Germany. The description of current technological security gaps and threats clearly shows which dangers related to the use of IT have to be currently taken into consideration. In addition, the report shows in which direction the threats are evolving and which precautionary measures have to be taken to avert future threats as well.

These explanations clearly show that all social groups have a special safeguarding obligation. In order to realise adequate IT-security, the administration, the economy, and the citizens as well have to consider this subject as having great importance for them. Since each group uses information technology differently, their respective IT-security-related requirements differ from one another. This report shows comprehensive tasks, specific to each target group, which guarantee safe and reliable IT.

The report summarises insights gained from our own surveys as well as from other expert contacts. These insights are complemented and verified by studies that were carried out by various IT-security companies.



IT-Security Awareness and IT-Security Competence in Society

3 IT-Security Awareness and IT-security Competence in Society

IT-security awareness comprises several areas: Knowledge about the significance of IT-security is part of it as well as an understanding of the corresponding IT-security level and one's own responsibilities. It is only when both are present that one can speak of sound IT-security competence.

Studies show that there is hardly any IT-security competence present in the various groups of society. Despite the fact that citizens are increasingly more dependent on information technology — be it in the workplace, be it for digital money transfers, in communications or in E-Commerce — only a few people place the necessary emphasis on safe information technology in practice. The same applies to the economy and to the State. In companies, security is often only taken seriously after damage has been done. And that even though, today, economic success and competitiveness are determined decisively by properly functioning information technologies. Similarly, reliable IT forms the basis of everyday administrative procedures. Nevertheless, an adequate security awareness is still missing here as well.

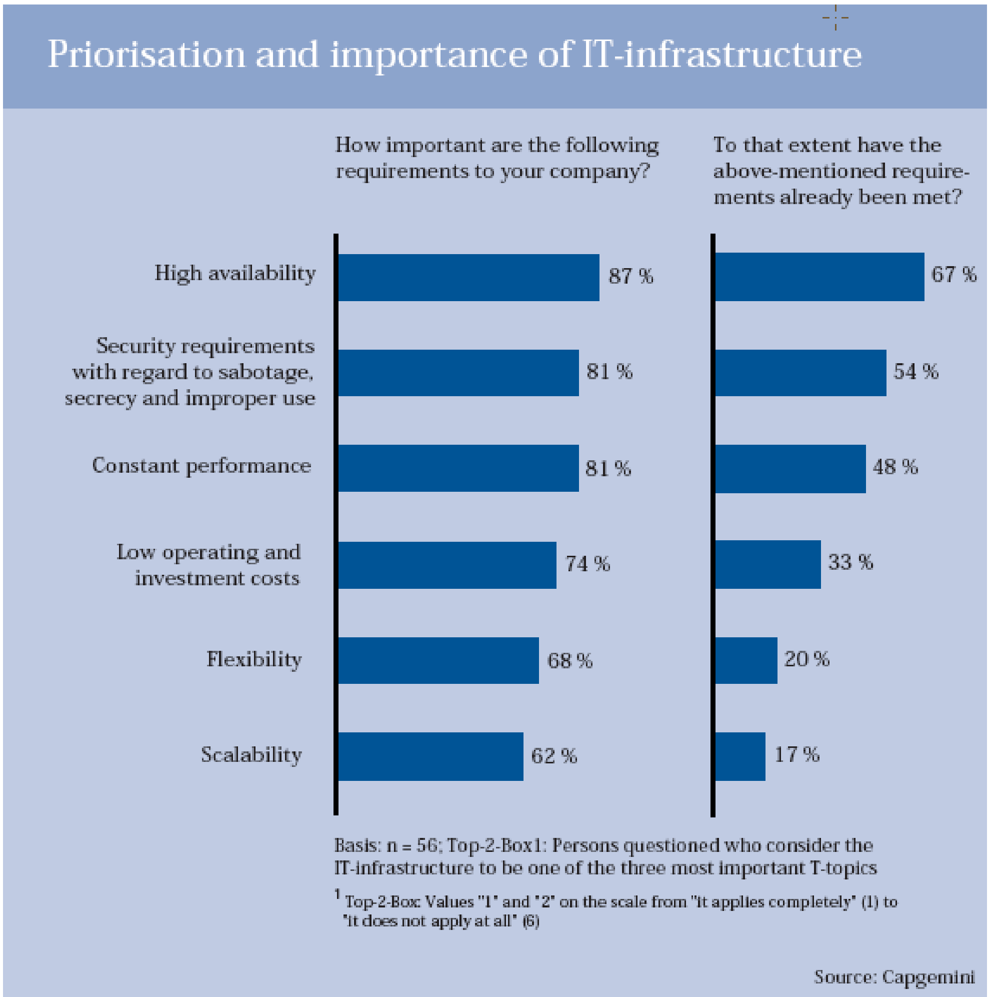
3.1 The General Public

In their own estimate, German Internet users have good specialised IT knowledge. According to a representative survey of the BSI, about 50 percent of them have good and even very good knowledge [2]. Only one person in ten says that he or she has little or no specialised knowledge. Similarly, the population is well informed about possible attacks that exist in connection with the Internet. About 90 percent of the population are aware of the fact that their own computers could be misused by third parties and seven out of ten users know that sender addresses in E-mails can be counterfeited [2].

Despite these seemingly positive results, the survey also shows that the topic "IT-security" is of secondary importance in practice. Four out of ten users do not use any anti-virus programs and only half of them use a Firewall. Only one out of two secures data on a regular basis. Users are also negligent in protecting their systems by installing current security updates for their operating systems and applications. Only one third of the users regularly install updates to close security gaps. Four out of five users update their anti-virus software once a month, one out of three, once a week.

3.2 The Economy

IT-security is one of the most important issues for IT administrators in the economy. Eighty-three percent of them rate this topic as first or second item on their priority list [7]. In Germany, about 89 percent of all IT administrators believe that the economy is at risk due to insufficient IT-security. Questioned about how they perceive the security situation in their own organisation, however, only about 25 percent indicated that they were subject to an acute threat [3]. For the majority, the propagation of malware absolutely poses the greatest danger to the IT-security of their own company. However, the human factor — i.e. error and negligence of their own personnel — also plays a significant role in keeping their IT-security at a high-level [9]. Furthermore, there is the expansion of traditional in-house company networks through the introduction of mobile computers such as notebooks or PDAs, through networking home-based and tele-workplaces as well as wireless transmission technologies such as WLAN. These areas pose a significant new risk in the eyes of many IT-security officers.



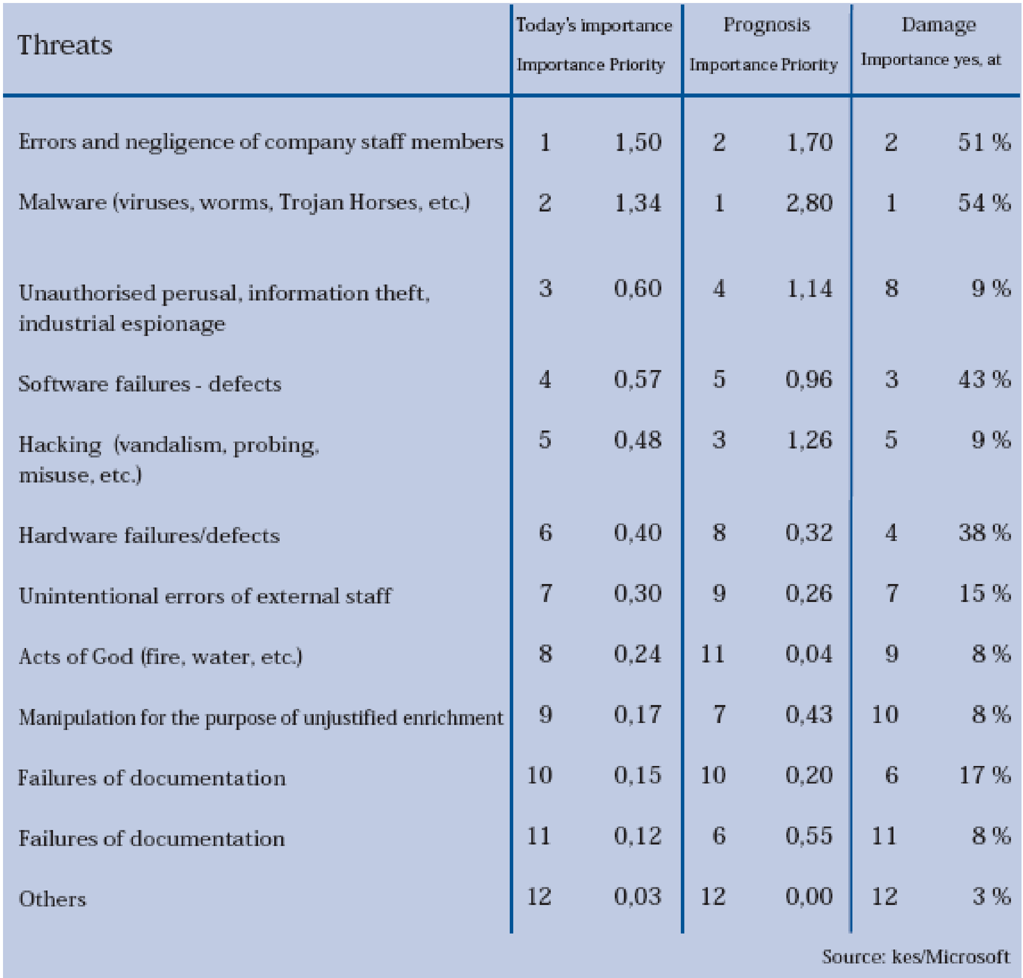
Basis: n = 56; Top-2-Box1: Persons questioned who consider the IT-infrastructure to be one of the three most important T-topics

[1] Top-2-Box: Values "1" and "2" on the scale from "It applies completely" (1) to "it does not apply at all" (6)

Source: Capgemini

Figure 1: Priorisation and importance of IT-infrastructures in German companies [7]

Although IT-security challenges are known, there are impediments to the development and implementation of corresponding security concepts. Studies show that only fifty percent of all IT administrators have outlined a written strategy about information security [11]. Insufficient financial resources are also named among the hindrances. Despite a growing threat potential, only 39 percent of all German companies provided a higher budget for IT-security in 2004 than in the year before; in 40 percent of the cases, the budget remained the same [12].



Threats	Today's importance		Prognosis		Damage	
	Importance	Priority	Importance	Priority	Importance	yes, at
Errors and negligence of company staff members	1	1,50	2	1,70	2	51 %
Malware (viruses, worms, Trojan Horses, etc.)	2	1,34	1	2,80	1	54 %
Unauthorised perusal, information theft, industrial espionage	3	0,60	4	1,14	8	9 %
Software failures - defects	4	0,57	5	0,96	3	43 %
Hacking (vandalism, probing, misuse, etc.)	5	0,48	3	1,26	5	9 %
Hardware failures/defects	6	0,40	8	0,32	4	38 %
Unintentional errors of external staff	7	0,30	9	0,26	7	15 %
Acts of God (fire, water, etc.)	8	0,24	11	0,04	9	8 %
Manipulation for the purpose of unjustified enrichment	9	0,17	7	0,43	10	8 %
Failures of documentation	10	0,15	10	0,20	6	17 %
Failures of documentation	11	0,12	6	0,55	11	8 %
Others	12	0,03	12	0,00	12	3 %

Source: kes/Microsoft

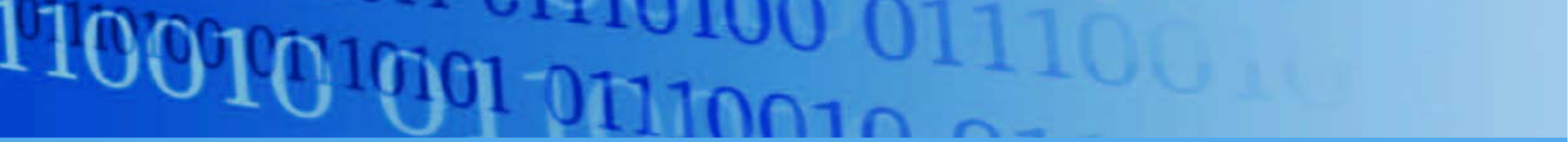
Figure 2: Significance of the different danger zones for German companies [9]

Small- and medium-sized companies (SMCs) mainly focus on the growing threat of malware. By comparison, other threats such as hacker attacks and Spam mails, on the other hand, only play a small role [3].

3.3 The Administration

Some administrative decision-makers are not yet sufficiently sensitive to IT-security-related matters. Particularly in cases in which staff members are not dealing with security-related matters on a continuous basis the role that IT-security plays is still too small. Measures such as training staff and providing corresponding information, do not yet have the desired effect.

To make matters worse, it is rather hard to recruit and keep sufficiently qualified expert personnel to take care of one's information technology. Among other things, authorities consider a lack of financial resources as one of the reasons for this situation.

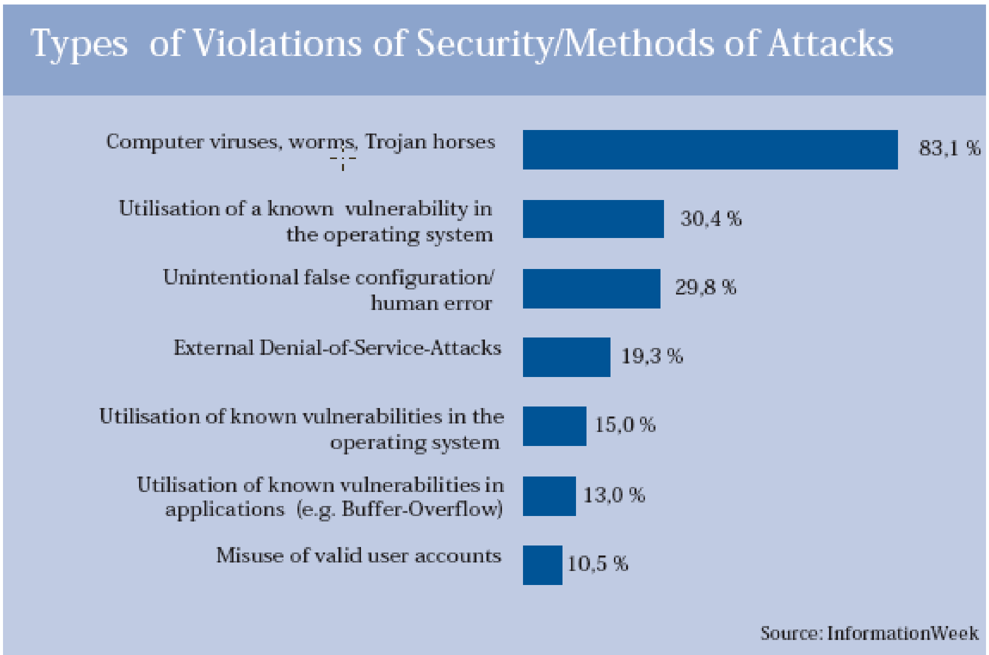


Vulnerabilities of and Threats to IT Systems

4 Vulnerabilities of and Threats to IT Systems

4.1 Security Gaps

It is impossible to completely avoid security gaps in complex software. The quality of any software can also be determined by how well and how rapidly its manufacturer comes up with respective updates in order to prevent security gaps from being exploited by malware. All too frequently, today's updates are erroneous themselves, they do not fix the vulnerabilities, and they are introduced too late. In addition, available updates are not used everywhere or immediately due to the fact that users are either ignorant or negligent or because they do not have the necessary time for updates at their disposal. Between July and December 2004, more than 1,400 new vulnerabilities were discovered [15] — which is a 13-percent-increase compared to the previous six months.



Source: InformationWeek

Figure 3: Pervasiveness of attack methods in German and Swiss companies [8]

The "exploits", with which attackers take control of any given system, are easily available through the Internet [15]. According to a study, about 30 percent of all attacks on IT systems in 2004 were carried out by exploiting a single known vulnerability in an operating system and 15 percent by exploiting a hitherto unknown one. Thus, exploits ranked second and fifth respectively in the league of attack methods (cf. Figure 3). Nevertheless, only every other IT-security officer wanted to place more emphasis on the security of their operating systems in the coming twelve months. [8].

The period of time between reporting a vulnerability and its exploitation is already very short today. On average, it takes attackers 6.4 days to develop methods to take over systems [15].

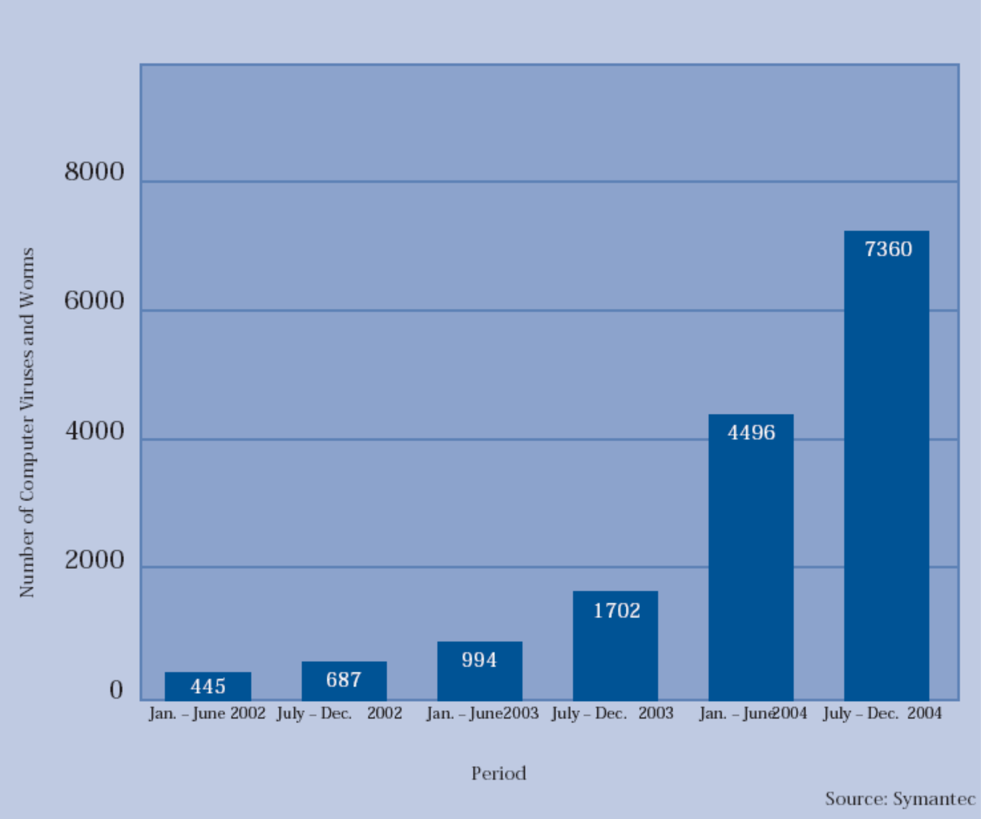
The necessary program updates are often not made available during this short period of time, nor are measures developed to protect the respective systems in other ways. The number of so-called zero-day exploits is increasing. These attacks are particularly threatening because corresponding exploits are made available just a few hours or even at the time that given vulnerabilities are publicised. In those short periods of time, the victims do not have updates or instructions for counteraction available to them.

4.2 Malware

4.2.1 Viruses, Worms, Spyware

The great prevalence of standard software and so-called "monocultures" in operating systems increasingly endanger the entire information technology realm. Since an individual product dominates the market, the vulnerabilities inherent in this product are particularly widespread and, if exploited, lead to substantial damage. For this reason, attackers prefer using malware, which constitute the most widespread attack method against IT systems, in order to target the security gaps of such products. The main source for distributing computer viruses are therefore innocent users of personal computers and company computers.

In the second half of the year 2004, more than 7,360 new variants of viruses and worms were registered. This constitutes a 64-percent-increase compared to the first six months [15].



Source: Symantec

Figure 4: Number of computer viruses and worms globally [15]

Eight out of the ten most frequent examples were different versions of mass mailer worms, among them Netsky, Sober, Beagle, and MyDoom. The multitude of different versions of malware indicates that malware are continuously being further developed: In total 4,300 independent versions of the Spybot computer worm alone have been registered. This represents a 180-percent-increase of the malware belonging to this family compared to the first six months of the year 2004.

At the network nodes of the communications network of the German Federal Administration, which is one of the largest information infrastructures of Germany, the BSI had never before recorded so many viruses that were so dangerous and so widely spread as in the year 2004. In a month, an average of about 6 percent of all E-mails, which were checked at the central E-mail gateways of the Information Network Berlin-Bonn (Informationsverbund

Berlin-Bonn or IVBB), were infected. More than 80 per cent of the identified malware were computer worms and Trojan horses. Malware coming through incoming E-mails are on the increase also. In the first quarter of 2005, the fraction of infected E-mails already lay at 8 percent.

The problem is intensifying because malware is becoming ever more effective both technically as well as in their psychological effect. For distribution purposes, programmers are increasingly using the effects of "Social Engineering". Through their targeted and, partly even, personalised way of addressing the recipient, they aim at luring them into opening contaminated attachments.

Another trend can also be observed: Computer worms are less and less programmed to directly cause irreparable damage. Rather, attackers try to bring infected computers under their control so that they can continue to misuse them. By using Trojans, hackers often misuse several thousands of computers and then rent out these so-called Bot Networks (cf. Bot Networks, page 21) for criminal use. They serve as platforms for spreading new epidemics of computer pests, for DDoS attacks (cf. DoS attack, p. 19), and for sending Spams (cf. Spam, p. 20).

The time intervals between new computer virus epidemics are continually decreasing since the authors of malware increasingly revert to already existing codes of computer viruses and worms. In the future, users have to reckon with malware that will allow for extremely short development cycles for "optimised" versions that spread even more rapidly.

Furthermore, espionage software, so-called Spyware or Adware, has become a security risk [15]. These programs gather the data of computer owners, unbeknown to them, and forward such data. Spyware, for example, can record all the data typed on the keyboard, can make screen shots and can read E-mails.

The threat potentials of Spyware and Adware differ. Dangerous Spyware versions search for personal data such as passwords, login data, or bank account numbers. Adware records user habits, which are thereafter analysed for marketing purposes. Although this type of software does not directly cause harm, it does give rise to concern with regard to data protection aspects.

The infection of IT systems with Spyware occurs through active contents on web pages and in E-mails. Since many users allow for the running of such contents in their Internet browsers or E-mail programs, the proportion of pure infections through multiple visits to the same web page is rather high. In addition, Adware is often part of software that can be downloaded from the Internet without charge.

4.2.2 Trojan Horses

In addition to having an official and useful function, Trojan horses are programs that contain and run damaging, undocumented functions independently and unbeknown to the user. In contrast to computer viruses, however, Trojan horses cannot spread themselves. By thoughtlessly running these "camouflaged" programs, IT systems can sustain serious damage, which results in corresponding financial damage on the user side.

Whereas in the past, Trojan Horses were mainly used to spy out confidential data on a given infected computer, today, the aim of the programmers is to gain control of third party computers. For this purpose, so-called "Backdoor" programs are installed so that the attacker may control such computers from the Internet by remote control. In the second half of 2004, Trojans made up a third of the 50 most frequently occurring Internet pests [15].

4.3 DoS Attacks

Attacks against Internet sites constitute a form of online sabotage. So-called DoS attacks (i.e. "Denial of Service”) aim at prohibiting legitimate users - for example the customers of an Internet-based shop - from accessing certain services. In order to achieve this goal, the attacker floods the server with useless data packages thus overloading the system. The larger the data quantities, the more effective the attack. That is why, more and more distributed Denial-of-Service-Attacks (DDoS) are being registered. In this attack method, hackers first of all gain the rights to run a given program on several unprotected third party computers. After a given DDoS software has been installed there, those computers can be used to launch co-ordinated attacks.

In Germany, 15 percent of all IT administrators in companies indicated that they had been confronted with DoS attacks between the end of 2002 and May 2004 [8].

DDoS attacks pose a serious threat for the day-to-day operation of web servers. With the methods that are currently available, DDoS attacks can be made more difficult, but it is not possible to completely eliminate such threats. Safe, state-of-the-art server systems can, at least, provide protection against those attacks that exploit erroneous program codes. However, Internet providers only make insufficient use of specific precautionary measures, for example to prevent IP spoofing (i.e. counterfeiting of IP addresses). This makes it more difficult to fight this attack method.

4.4 Spam

Besides to the World Wide Web, E-mails have developed into an important Internet application. Many users can only tolerate a breakdown of this service for a very short period of time. Spam mails can be the reason for such breakdowns. In the meantime, the fraction of Spam messages amounts to 60 to 90 percent of all E-mails [1]. In the IVBB administrative authority network, the figure lay at 65 percent in the year 2004. There was a significant rise compared to the previous year, when the fraction of Spams was still at 49 percent.

Increasingly, the senders adapt Spam mails thematically to current occasions and holidays, in order to persuade the recipients to open their messages. In Germany, chain mails (or hoaxes), false virus warnings, and, for the first time in 2004, also mails that have xenophobic contents are being sent in addition to commercial Spam advertisement. As a result of a large number of Spams, a loss of working hours, an overloading of technical components, and higher costs due to unsolicited data transfers are being incurred.

A direct correlation can be identified between Spam mails and malware: Special mass mail worms search infected computers for stored E-mail addresses in order to send Spam messages, computer viruses and worms there. The mass distribution of malware can lead to the breakout of real epidemics.

Despite the large number of Spams, anti-Spam measures are not yet being carried out by all companies and administrative bodies in Germany. At least nine percent of all organisations are unprotected from the flood of Spam messages [1]. In the league for the distribution of anti-Spam mechanisms, word and letterhead analyses ("header analyses") take the lead over so-called black and white lists where both known senders of Spams and of safe messages, are listed.

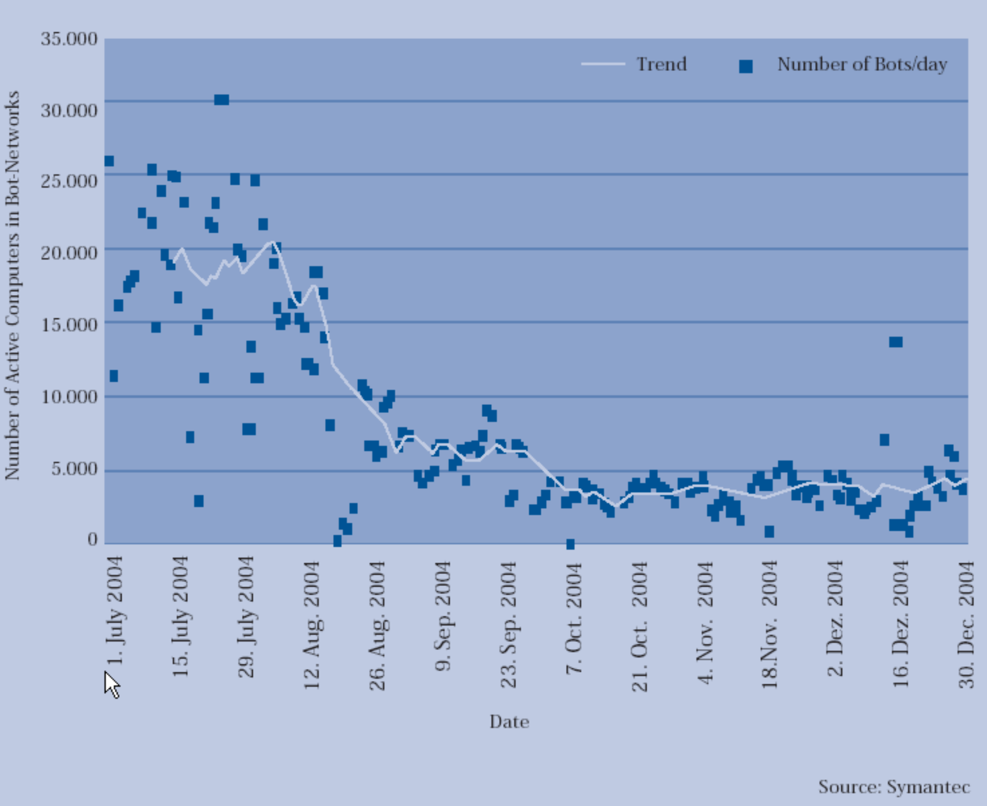
4.5 Bot-Networks

Many of the Trojan horses registered in the year 2004 contained functions for co-ordinated attacks against Internet sites (cf. DoS Attacks, p. 19). With this method, the number of computers that are controlled by a hacker, and, as a result the strike power of distributed DoS attacks are also increased. The thus-infected computers form so-called Bot-networks which can be used at any and all times against any Internet site and which can, therefore, also be used to blackmail companies. In this manner, the owners of infected computers are no longer simply victims, but, at the same time, though unknowingly also accomplices and perpetrators.

Bot-networks constitute a special danger because the attackers are able to establish contact with the infected computers at any time and to make further unnoticed software downloads. Later on, programs, for example, are installed that are then used to forward Spam mails via those infected PCs.

In then first six months of the year 2004, a steady increase of computers in Bot-networks was registered. On average, the networks that were monitored consisted of more than 30,000 computers. In the second half of the year, however, the size of those nets shrank rapidly. By the end of the year, an average of 5,000 infected and remote-controlled computers were counted per Bot-network. This cutback coincided with the introduction of the Windows XP service pack 2 [15].

The main reason for the rapid proliferation of Bot-networks lies in the large number of computers with rapid and permanently hooked-up Internet connection where users are hardly aware of any uncontrolled processes that are run secretly on their PCs. Although downloading security updates obviously does minimise the threat of Bot-networks, the fact that adequate protective measures are not used everywhere hinders a general prevention of their proliferation.

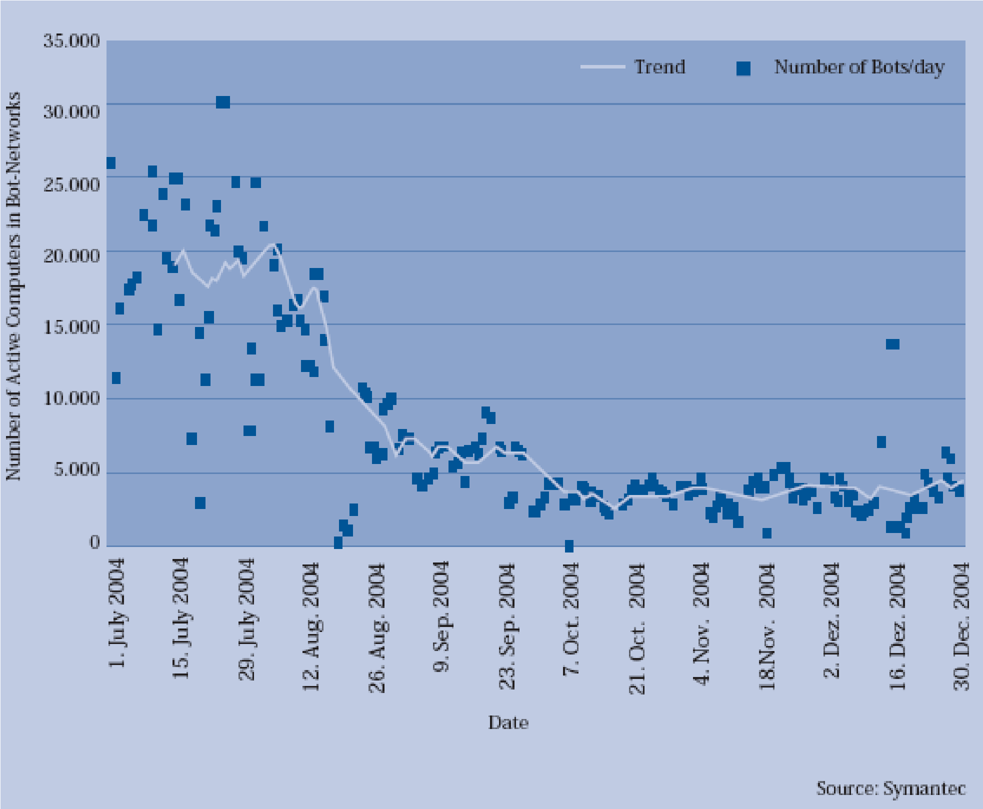


Source: Symantec

Figure 5: Number and size of Bot-networks globally [5]

4.6 Phishing

E-commerce infrastructures and online payment systems are increasingly threatened by attacks on confidential information. One widespread method of fraud attempts are falsified E-mails, so-called Phishing E-mails. These mails are sent in huge numbers and feature falsified sender addresses. The senders copy the layout of official E-mails of well-known companies, in order to obtain the customers' confidence by devious means. Via a link contained in such E-mail, customers are led to an Internet page, which is adapted from the real company's page. Here, fraudsters try to spy out user data and to obtain passwords, data for online banking, and credit card numbers of the customers. This data is then misused for financial transactions.



Source: Symantec

Figure 6: Number of Phishing-mails world-wide [15]

The number of Phishing-mails continuously increases. The method is so successful because it is easy to manipulate the display of URL addresses in Internet browsers and, currently, there are not enough users who pay close attention to "authenticity certificates" such as page certificates and the encryption of Internet pages. Simultaneously, fraud methods are becoming more and more perfidious. In some messages, the background of a real online bank opens up but the window that appears in the foreground, where the customer is to enter his data, originates from a Phishing server. Furthermore, Phishing E-mails in which bank customers were personally addressed with their names and current account numbers have already appeared in the US. This method can seem particularly trustworthy.

4.7 Diallers

Diallers are programs for calculating services rendered, which are then billed via telephone invoices (micro payment). On the Internet, it is used to bill payable information or downloads. For this purpose, the operator of the dialler must apply for a permit at the Regulatory Authority for Telecommunications and Post (Reg TP).

There are, however, illegal diallers that install themselves secretly on given computers and establish Internet dial-ups via expensive phone numbers without the user being aware of it. Often, these Internet connections are international connections or, else expensive satellite connections are established. In 2004, a significant increase in the numbers of these illegal diallers was registered.

4.8 New Technologies and IT-security

The significance of new transmission technologies such as Bluetooth, WLAN or UMTS is on the rise. The future of mobile applications that work with wireless communications systems decisively depends on whether security challenges can be overcome. Without security mechanisms, attackers can easily follow, tamper with, or otherwise manipulate data transfers. Below, you will find a presentation of the risk potential of the new main technologies and their applications.

4.8.1 Internet telephony – VoIP

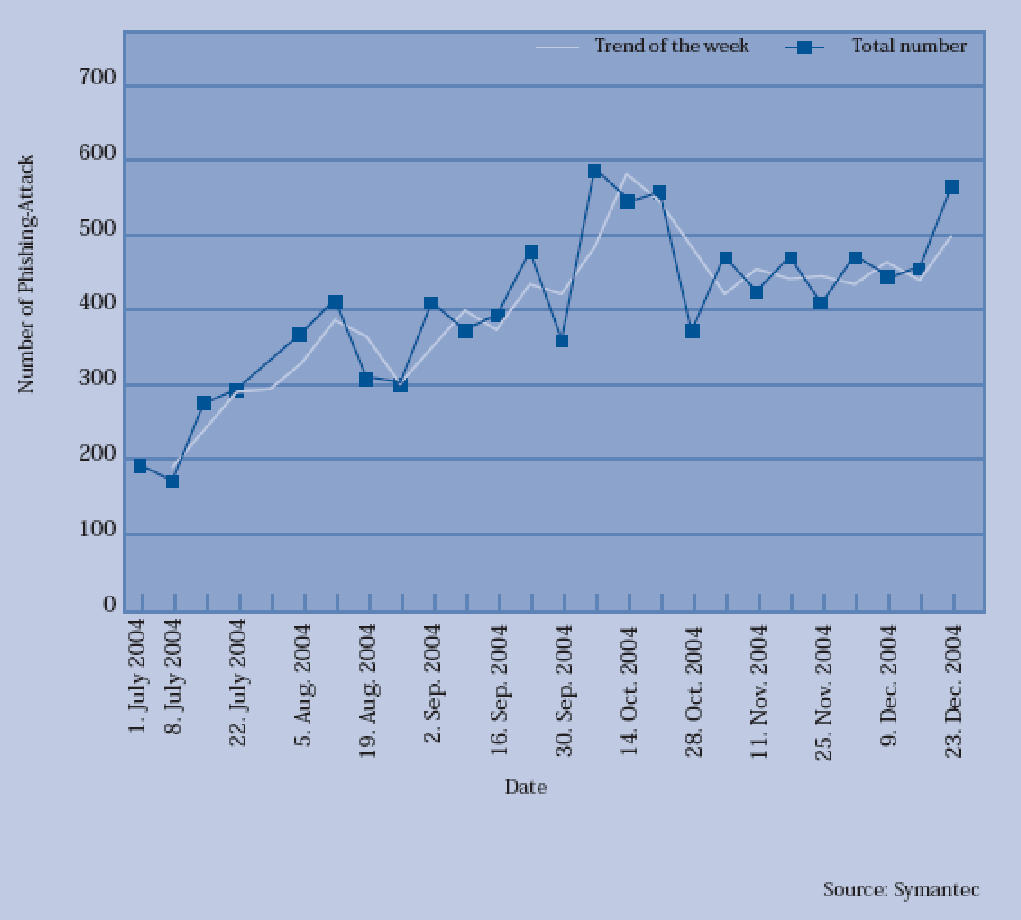
Thanks to Voice over IP (VoIP), voice communication is no longer limited to the telephone network but can also be transmitted via IP-based networks such as the Internet. In this case, a computer that is connected to the Internet takes on the function of the telephone. Experts believe that, over the next ten years, VoIP will completely replace conventional telephoning technologies.

However, the Internet does not offer any special security mechanisms for this situation; thus, there is a great threat potential for new types of VoIP applications. Unencrypted calls can be bugged more easily than telephone networks; in addition, attacks through large-scale Spam E-mails or the spreading of special malware has to be reckoned with as well.

4.8.2 Mobile Data Transfers – WLAN

Wireless Local Area Networks (WLAN) are being used more and more as an additional broadband access technology. Already, 11 percent of the interviewed companies in Germany were using wireless computer networks in the year 2004; the year before it was only 5 percent.

In the vicinity of a WLAN access point, which is also called a "hotspot", mobile computers such as notebooks or PDAs can establish a wireless Internet connection. Besides accessing the Internet via hotspots, the use of WLAN for expanding wired LANs constitutes an important field of application. However, an insufficiently secured WLAN involves large security risks. Through an open access, attackers can, for example, collect or secretly modify sensitive data. In addition, Spam senders can misuse unsecured WLANs to send out Spam e-mails. It is hard to proof such misuse because there are often no access protocols. In the future, malware could be spread directly through wireless networks. Furthermore, if, for example, criminal contents are downloaded, there is the possibility of image or financial damage.



Source: Symantec

Figure 7: Spreading of WLANs in German companies [13]

There are different reasons why WLANs are often only insufficiently secured. On the user side, the security measures that have been taken, e.g. access protection, user identification, restrictive data and resource access on the operating system level, local encryption as well as the use of non-trivial passwords, often do not suffice. On the manufacturer's side, the encryption system WEP (i.e. Wired Equivalent Privacy) that is part of many WLAN components is rather problematic. WEP has not met security requirements for a long time, because the protection it offers can be removed in a relatively short period of time by using currently available hacking tools. However, up until now, the WLAN adapters which are available on the market only rarely use the secure follow-up standards WPA and WPA2 (also known as IEEE 803.11i), in order to protect wireless connections.

4.8.3 Process Control Systems – SCADA

Companies, administrative bodies, and private households depend upon the continual availability of such infrastructures as for example electricity and water supplies. Many of these infrastructures make use of special process control systems, also called SCADA systems (Supervisory Control and Data Acquisition) to manage all of their different functions. Today, these systems use the same technology as computer networks to connect their various components. If attackers obtain access to the network's process control system, they can use attack methods that are known from "normal" computer systems to impair the system's operation.

The threat potential is high because standard security measures are not always used since many SCADA systems have special requirements. Precautionary measures such as network screens, intrusion-detection-systems, and the use of firewalls with very restrictive rules must not hamper the functionality of the process control systems.

IT-security-related aspects were not sufficiently taken into consideration in the development of many SCADA components. Furthermore, security mechanisms such as authentication and encrypting were not implemented. What makes matters worse is that the companies fail to carry out enough risk analyses for the process control systems that they do use.

4.8.4 Mobile Telephones and PDAs

In the year 2004, at least one person in 78 percent of all German households owned a mobile telephone. There was a significant increase in the number of Internet-compatible mobile telephones: In 2003, such a mobile phone was present in 17 percent of all households; in 2004, the fraction had already reached 22 percent. Fourteen percent of all households that have an Internet-compatible mobile telephone indicated that they actually use their mobile phone to access the Internet [13].

The development of modern cellular phones into small computers featuring their own operating systems as well as a large number of applications and external interfaces creates a whole range of risks. In June 2004, Cabir, the very first damaging program for mobile telephones appeared. This worm was only a "proof of concept", in other words a test worm, which does not feature damaging functions. By using Bluetooth contact, it endeavours to establish contact to other terminal units and to install itself in those.

Since the end of 2004, Dampig A, another damaging program, has been spreading itself also via Bluetooth and is trying to install Cabir variants on mobile phones. The new feature on this worm is that it destroys the de-installation data within the system and can therefore only be removed with an anti-virus kit. By the end of 2004, there were approximately 21 known malware for mobile applications, some of them already existed in several variants.

Currently, the risk of malware infecting mobile terminal units is still low. Up until now, only a few viruses are in circulation; in addition, the Bluetooth transmission path limits their range to only a few metres. However, it is in fact possible to use other wireless interfaces, such as e.g. GSM or UMTS, for the proliferation of malware. In this case, it would be possible to transmit them over greater distances.

Given the growing range of functions of mobile communication devices, there is a general increase in the number of possible attacks. In the future, data may be destroyed or misused or undesired high telephone connections might be established. In addition, professionally used mobile terminal units are often outside of the security boundaries of a given company's network. If they are equipped with net access, they could be misused to break into the IT systems of such a company. Although precautionary measures such as virus scans and firewalls are now being offered for a number of mobile terminal units, they are hardly ever used at this time.

4.9 Insiders, Errors, and Negligence

In many cases, IT damage within organisations is caused by insiders, i.e. by their own staff members [5]. Since this group of people is often authorised to access IT systems that cannot be accessed from the outside and because they have detailed in-house knowledge at the same time, the consequences of unintentional mistakes as well as of premeditated manipulations are grave indeed.

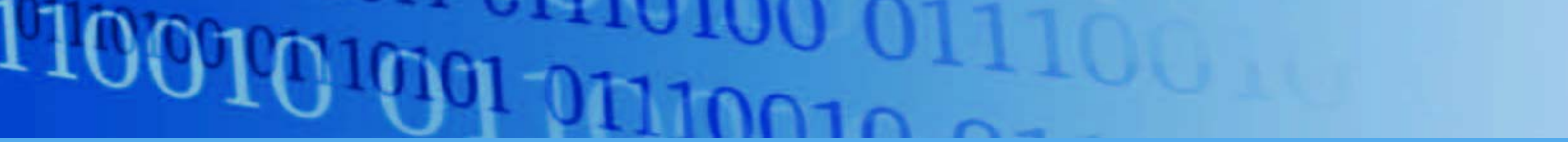
Premeditated action may not lead to damage as often as error and negligence but their consequences are more critical and, above all, harder to discover. Possible motives of such perpetrators are curiosity, revenge, envy, and unjustified personal enrichment. Insiders manipulate internal data to the disadvantage of the organisation or access confidential information about staff members, development projects or contractual negotiations.

Carelessly opening E-mail attachments containing malware as well as deleting important files by accident can also cause much damage.

4.10 Structural Vulnerabilities

Today, the reliability of IT structures often no longer complies with the latest security requirements. One of the reasons is an increasingly more complex set-up of individual IT systems, the correlation of which — within the entire system of a given company or administration — is becoming increasingly harder to understand. Furthermore, there are large investments to be made in information technologies as well as insufficient resources available to IT departments both in the economy and in administration.

The BSI’s observations have shown that, today, significant IT disruptions in critical infrastructures can often not be blamed on internal or external attacks. Instead, simple breakdowns of the systems themselves incur serious damage. Due to extensive networking with other systems, disruptions cause domino effects which, prior to this point, have not been taken into consideration adequately. Great problems result from lacking process analyses, few redundancies in IT systems and in wiring arrangements, inadequate crisis and emergency plans as well as from an insufficient sensitisation of management.



Trends and Developments in IT Threats

5 Trends and Developments in IT Threats

In addition to damage caused by computer viruses and worms, hackers also relaunch specific attacks against IT systems repeatedly. Some of their attack methods have been described in the previous sections. The following section describes trends in IT attacks as well as the changes in the motives of the attackers.

5.1 Industrial Espionage

The Internet opens up new dimensions for industrial and competitive espionage. In the process, the methods for spying out and manipulating data and services are becoming increasingly more professional. Classic targets are technology and know-how theft as well as getting the competitive advantage, e.g. through spying out tenders, contracts, or price lists. Within the next ten years, the significance of spying out company networks with the aim of gaining unauthorised access to company data will increase [4].

In this context, insiders, thus for example employees of a given company or external consultants, constitute a special security challenge. Whereas hackers, for instance, still have to overcome the IT-security systems of the company, insiders are already on the inside of these systems. Even the continuing trend of outsourcing services is problematic. In this case, external persons can be granted access to sensitive data or be given access to internal security structures.

The loss of data confidentiality can result in economic damage to the companies thus affected. Competitors could gain access to sensitive research and development documents for products or services. And, last but not least, if the general public learns about the misuse of data, a company's image also suffers.

Although almost all areas of a company are threatened by industrial and competitive espionage, research and development departments are affected most seriously. Companies with large valuable development departments, such as pharmaceutical enterprises, companies in the automotive industry as well as the software industry, are especially vulnerable to such threatening scenarios [6]. Protecting intellectual property is not given the proper attention in many areas, the reason being that on the management level, a consciousness for IT-based industrial espionage has not yet developed adequately.

5.2 Attacks Aimed at Infrastructures

In the future, it will not just be individual computers that are targeted by hackers. One has to reckon with a rapid increase, for example, in attacks on name servers (Domain Name System or DNS), which are responsible for allocating host names to IP addresses. Through such manipulated servers, scores of Internet users can be led onto false Phishing web pages.

Attackers are increasingly focusing on routers, firewalls and other security tools, which are intended to protect the systems of companies and administrative bodies. Such attacks have a new quality since entire computer networks are affected by them. Connected nets can be cut off from the Internet if routers are attacked.

Last but not least, as a result of the increasing IT penetration of all areas of life, the protection of the process control systems as described in Section 4.8.3 poses an important challenge. To date, IT-security has only played a minor role in the product development in this area.

5.3 Targeted Attacks against Companies

Even in 2004, attacks on IT systems were primarily characterised by an economic background. Sixteen percent of hacking activities were aimed at E-commerce companies. This represents a 400-percent-increase compared to the previous year [14]. Above all, the objective was to spy out credit card information and other sensitive financial data. It is feared that this trend will continue in the future.

Targeted DDoS attacks against companies also pose a major security problem. Such attacks, which may be launched by competitors, dissatisfied personnel, or otherwise motivated groups of people, obstruct the smooth operation of web sites massively. This can result in considerable economic consequences, especially for E-commerce companies.

5.4 Criminalisation and Focus on Financial Gain

While, up until now, attacks on IT systems were presumedly fuelled by "sportly ambitions", this aspect is becoming increasingly less significant [6]. We observe a new trend whereby Internet criminality is conducted in a professional and commercial fashion. Instead of isolated computer hackers, targeted attacks are increasingly carried out by organised criminals. Hackers and virus authors work together with criminals and write malware for Phishing, credit card fraud, and blackmailing tricks.

Financial interests are the decisive driving power. It is possible to make money by misusing IT systems through the distribution of Spam as well as by misusing sensitive data such as credit card numbers or online banking data.

To date, it is hard to evaluate how much the threat situation has changed as a result of an increasing criminalisation of the attacks. Since it is financially lucrative, the BSI also expects that the degree of the criminalisation will be a serious problem as early as next year.

5.5 Regionalisation of Malware

Although programmers of malware have used E-mails written in the English language, in order to spread computer worms so far, now more and more German texts are being registered. This regionalisation leads to a far-reaching distribution of such malware in Germany.

In May 2005, for example, a version of the Sober computer worm was spread in E-mails in connection with the ongoing distribution of tickets for the 2006 Football World Cup in Germany. The senders sent out phoney notifications about the ticket sale.

Activities

6 Activities

This situation report provides an overview of the status quo but also of the looming development of IT threats in Germany. The analysis of the current situation calls for action to be taken. In the following sections, necessary measures as well as activities for an improved IT-security situation will be introduced.

6.1 The General Public

In the IT-security realm, each individual computer user also has a responsibility in the fight against hacking attacks and the dissemination of malware and Spam. In light of the threats described above, it is not just the industry or the authorities but also the citizens who have to ensure the IT systems which they are using are secure. Each IT user can get access to up-to-date information about all security-related issues on its homepage www.bsi-fuer-buerger.de (i.e. the BSI for citizens in Germany).

The BSI addresses private Internet users, in particular, with its www.bsi-fuer-buerger.de Internet portal. Here, even people who have no previous knowledge of IT can find important information on all aspects of IT security, which is written in an easy to understand manner. In addition to advice and information, numerous programs can be downloaded free of charge. Internet users can also subscribe to the free "SECURE • INFORMED" Newsletter, which contains current IT security information, is published every two weeks, and sent by email.

6.2 The Economy

The deficits described in this report make it absolutely clear that the management of companies but also the members of staff have to be briefed about the issue to a greater degree. The confidentiality of company details must be secured, and there has to be better protection against targeted attacks. In order to reach this goal, companies should first of all carry out IT structure analyses. Protection requirements are to be defined on the basis of these analyses. The results thereof are then to be channelled into a security policy that is adapted to their individual needs. All necessary personnel and financial resources have to be made available for the implementation of such IT-security strategies. Having a security culture must be an integral part of a company's corporate culture.

In order to be able to respond quickly and efficiently to incidents within networks, crisis management skills including emergency plans are necessary. The efficiency of security measures taken must be guaranteed through frequent security revisions.

Mcert (www.mcert.de) is an initiative under the overall control of the Federal Association for Information Technology, Telecommunications and New Media (BITKOM) in the form of a public/private partnership with the Federal Interior Ministry, the Federal Ministry for Business and Labour and business partners. Mcert is a neutral competence centre for IT security. The services are specially harmonised with the needs of small and medium-sized companies. Mcert provides understandable and reliable security information and recommendations for action. This includes, for example, specially adapted and evaluated warning messages on malware or information on current security problems.

6.3 The Administration

From an IT-security point of view, functioning IT systems, data privacy protection, and confidentiality as well as staff members with adequate IT-security competence constitute the basic elements of a functioning administration. An important step toward safe IT systems in administrative bodies is the implementation of a sufficiently high security level in all agencies. In a manner analogous to that used in the economy, IT-security management systems should also be installed in administrative bodies. A first step towards that would be the naming of IT-security officers, who would co-ordinate the drafting and implementation of IT-security concepts on behalf of the management of a given agency.

As in industry, crisis management capabilities and emergency plans are necessary for official bodies. Similarly, examining security measures by means of appropriate revisions must play a central role.

The Federal Computer Emergency Response Team (CERT-Bund – www.bsi.bund.de/certbund) is the central contact point for preventative and reactive actions for security-related incidents in the federal administration's IT systems. The role of CERT-Bund includes notification of vulnerabilities in hardware and software products, provision of warnings and alarms about special IT threats and the recommendation of reactive actions to limit and eliminate damage. The services of CERT-Bund are primarily made available to Federal authorities. In addition to being on-call 24 hours a day, these services also include a warning and information service and alarms to the federal administration about acute IT threats. Enquiries from other public authorities, private persons or private institutions are handled if resources are available.

6.4 National IT-Security Competence Centre

The Federal Office for Information Security (BSI) has been assigned the task of improving the IT-security in Germany. For this purpose, the BSI examines security risks in the application of information technology and develops corresponding security measures in individual cases. It informs those affected about risks and dangers related to the use of information technology and provides assistance in finding solutions to concrete problems.

This includes the examination and evaluation of the security of IT systems, along with their development in co-operation with the industry. In order to minimise or even avoid the risks mentioned, the BSI addresses a large number of target groups, by providing advice for manufacturers, distributors, and users of information technology. Furthermore, the BSI analyses developments and trends in the field of information technology.

The BSI offers specific information and consulting services to various social target groups. While the Computer Emergency Response Team of the Federal Authority (CERT-Bund) provides comprehensive information about new vulnerabilities and threats through its warning and information service, private IT users are being informed by means of the following portal: www.bsi-fuer-buerger.de.

Increasing and changing IT threats force the BSI to come up with new ways of thinking and acting. In order to be able to fulfil the tasks described above, to develop effective protective measures against new threats, and to implement them promptly, the BSI works in close co-operation with experts from other authorities at home and abroad but also with the economy. Newly created positions also guarantee that the significance of new tasks is recognised and that expert knowledge can be accessed at any and all times. With its competencies, among other things, in the area of certification, basic IT protection, and decryption technologies, the BSI creates the foundation necessary to effectively meet future IT-security challenges in Germany head-on.

In the future, the BSI will become more active in an operative sense. Besides the tasks mentioned above, taking care of the IT-security of the federal authority continues to be the central component of its work.

The BSI homepage www.bsi.bund.de provides current warnings, online offers and other information on all aspects of IT security. The key issues handled by the BSI include IT baseline protection, certification/accreditation, Internet security and the protection of critical infrastructure; there is a wide range of online offers available on these subjects. In addition, numerous BSI studies on various specialist subjects are also available.

6.5 Joint Action

IT-security is also indispensable for the inner security as well as for securing Germany as an economic site. The State is not only required to make offers to sensitise and educate people with regard to the risks that exist when dealing with IT available. It should also ensure that IT-security is comprehensively incorporated into all processes both on a federal level as well as in companies.

Corresponding measures target various levels: On the one hand, IT systems must be secured against existing and future IT threats to the greatest possible degree. Since it is impossible to exclude disruptions in complex IT systems completely, it is, furthermore, necessary to provide for a rapid reaction capability by means of national IT crisis management. Finally, in order to guarantee a sustainable protection of IT systems, the IT-security competence in research and industry has to be promoted.

Summary

7 Summary

To the same extent to which information technology touches all areas of life, targeted attacks and malware are increasingly threatening private users as well as the economy and administration. This report shows already existing and arising threats to information technology, which all groups of society have to deal with.

Currently, the situation is still under control. However, for our information technology to continue to function properly and reliably in the future, the degree of awareness as far as the importance of IT-security is concerned has to be further heightened. At the level of companies and authorities, measures such as risk analyses, drawing up IT-security concepts, designating IT-security officers as well as IT-security revisions ought to be the norm. However, the general public must also be further sensitised and informed so that they can also increase their security competence.

The framework conditions for secure and reliable information technology can only be significantly improved with a new security culture that is backed up by all social groups in Germany.

8 Sources

[1] BSI: Antispam-Strategien. Unerwünschte E-Mails erkennen und abwehren. Cologne 2005.

[2] BSI: Bevölkerungsrepräsentative Umfrage des BSI zur IT-Sicherheit in Deutschland. October 2004.

[3] BSI: BSI-Monitoring. Repräsentative Umfrage unter IT-Beauftragten, Datenschutzbeauftragten und Journalisten. February 2004.

[4] BSI-Erhebungen.

[5] BSI: IT-Grundschutzhandbuch 2005. Bonn 2005.

[6] BSI: Kommunikations- und Informationstechnik 2010+3: Neue Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit. Bonn 2003.

[7] Capgemini-Studie: IT-Trends 2005. Paradigmenwechsel in Sicht. http://www.de.capgemini.com/servlet/PB/show/1556864/Capgemini_IT_ Trends_2005.pdf.

[8] InformationWeek: IT-Security 2004.

[9] kes/Microsoft-Sicherheitsstudie: Lagebericht zur Informations-Sicherheit. http://www.kes.info/archiv/material/studie2004/04-4-006.htm.

[10] McAfee-Studie: Virtual Criminology Report. http://www.mcafeesecurity.com/de/local_content/brochures/studie_virtuelle_kriminalitaet.pdf.

[11] Metagroup: IT-Security im Jahr 2003 (Deutschland). http://www.metagroup.de.

[12] Silicon.de: IT-Security 2004. Im Wettlauf mit der Lernfähigkeit der Hacker. Auszüge aus einer Studie von silicon.de zum Thema IT-Sicherheit. http://www.silicon.de/cpo/downloads/siliconDEStudie_IT-Sicherheit2004.pdf.

[13] Federal Statistical Office: Informationstechnologie in Unternehmen und Haushalten 2004. http://www.destatis.de/download/d/veroe/pb_ikt_04.pdf.

[14] Symantec Internet Security Threat Report, Volume VI (September 2004). http://enterprisesecurity.symantec.com/content.cfm?articleid=1539.

[15] Symantec Internet Security Threat Report, Volume VII (March 2005). http://enterprisesecurity.symantec.de/content.cfm?articleid=1591.

9 Glossary

Backdoor

A part of a program which makes it possible to access IT systems past all security mechanisms. These backdoors can only be identified if the source code of the program has been revealed.

Bot-Nets

In specialist terms, Bot describes a program which works by remote control. Bots can be used as a distribution path for computer viruses. Worms and attackers can remote-control them centrally. Bot nets are a virtual network of infected IT systems, i.e. a network of several Bots or infected computers.

Computer virus

A computer virus is a program routine which is not self-sufficient; it reproduces itself and carries out manipulations in sections of the system, in other programs, and in their surroundings, none of which can be controlled by the user.

Computer worm

A computer worm is an independent, self-reproducing program which spreads itself in a system (particularly in computer networks).

DoS-, DDoS-attacks

An English abbreviation which stands for "Denial of Service". They are attacks on the availability of resources and services of an IT system aiming at blocking them off and thus at denying regular users their access. DDoS: Attacks which lead to blockages are not just being carried out by one single computer, but by several computers at the same time. Thus, such attacks are more intense and it is harder to take counteractions since they would have to be applied to more than one source.

Targeted attacks

Targeted attacks are malicious attempts to impair the protective aims and the corresponding security guidelines of a given system by exploiting weak spots in operating systems or programs. Please also confer DoS and DDoS attacks.

IVBB

The "Informationsverbund Berlin-Bonn (IVBB)" - Information Network Berlin-Bonn constitutes the infrastructure of the internal communication within the Federal Agencies. The IVBB is used to implement electronic information, communications, and transaction services.

Patch

A small program for fixing software errors, such as e.g. security gaps in application programs or operating systems.

Phishing

Made-up word, composed of "password" and "fishing" used to describe a method aiming at obtaining confidential data by means of false e-mails.

Spam

Undesired electronic messages and "circulars" (E-mail). Often, they are commercial in character and are sent to multiple recipients who are not interested therein.

Trojan Horse

Trojan Horses (also Trojans) are programs which, in addition to having seemingly useful functions, also have undocumented damaging functions which they carry out independently, while the computer user is not aware of it. In contrast to computer viruses, Trojan horses cannot disseminate themselves.

VoIP

VoIP (Voice over Internet Protocol) describes telephoning via the Internet. Spoken data is transformed into digital data, sent through the Internet in small data packages, and put back together again on the recipient's side.

Publisher

Federal Office for Information Security - BSI
53175 Bonn

Subscription agent

Federal Office for
Information Security - BSI
Department III 2.1 (Public Relations)
Godesberger Allee 185-189, 53175 Bonn
Tel: +49-228-95 82-0, E-Mail: bsi@bsi.bund.de
Internet: www.bsi.bund.de

Texts and editorial department

BSI - Department III 2.1 (Public Relations)
Zucker.Kommunikation, Berlin