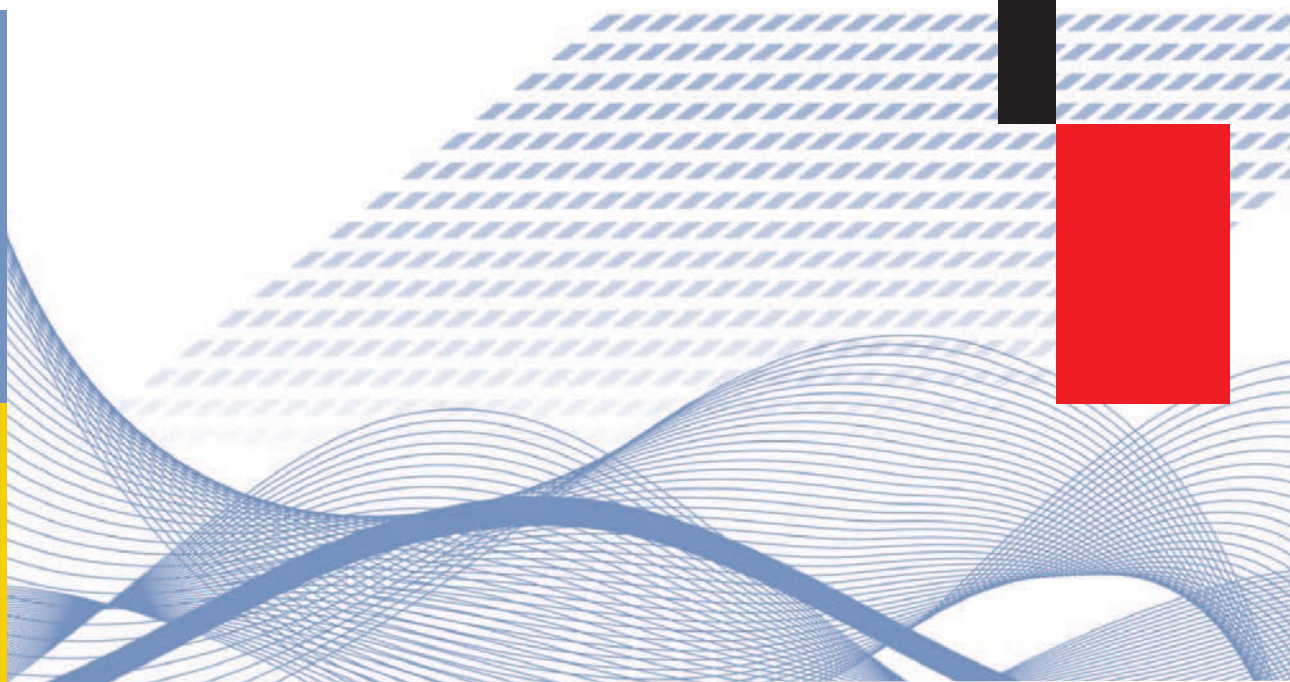




Federal Office
for Information Security

The IT Security Situation in Germany in 2009



Contents

1	Preface	4
2	Introduction	5
3	IT Security Awareness and IT Security Expertise in Society	7
3.1	Citizens	7
3.2	Industry	9
3.3	Administration	11
4	Vulnerabilities of and Threats to IT Systems	12
4.1	Security Gaps	12
4.2	Malware	13
4.2.1	Trojan Horses	15
4.2.2	Spyware	15
4.3	DoS Attacks	16
4.4	Unsolicited E-Mails (Spam)	17
4.5	Bot Networks	18
4.6	Identity Theft	20
4.7	Fraudulent Web Offers	21
4.8	Compromising Emissions	22
4.9	Material Security, Inside Perpetrators, Errors and Negligence	22
5	Activities	24
5.1	Citizens	24
5.2	Industry	25
5.3	Public Administration	27
5.4	Fund for the Future (Zukunftsfonds)	28
6	Summary	29
7	Sources	33



Table of figures

Figure 1:	Top Internet use activities in Germany	7
Figure 2:	Reasons for investments in security in German companies	9
Figure 3:	Security risk rating in German companies	10
Figure 4:	Increase of spam volume in Federal administration in percent	17
Figure 5:	2007 and 2008 numbers of C&C servers specializing in information theft	19
Figure 6:	IT threat trend according to the BSI	29
Figure 7:	Risk potential for attacks in selected applications and technologies according to the BSI	30
Figure 8:	Risk profiles of innovative applications and technologies according to the BSI	30

1 Preface

This is the third year the Federal Office for Information Security (BSI) is presenting this status report on IT security in Germany, and the situation remains as critical as ever.

IT systems are attacked for a number of reasons; a major one being financial gain. Due to the increasing shift of everyday activities – such as banking or shopping – to the World Wide Web, IT crime has become a lucrative business with comparatively low risk. Hence, the continued professionalization of internet crime is no surprise.

Psychologists tell us that in order for people to be sensitized to a topic, the activities in question have to be ongoing. During hazardous situations, the intensity of the response tends to increase, and then decrease again. Due to the rise in actual losses, the issue of IT security has assumed a higher degree of urgency on the agendas of government, business and also, private users. Fortunately, there is currently also a push among product developers and providers for improving product security features.

And yet, lasting success cannot be achieved overnight. The continuous advancement of IT systems, and ever more sophisticated methods of attack are making fighting and preventing Internet crime increasingly difficult.

With its over 500 employees and partnerships on the national and international levels, the BSI is working continuously on improving the level of IT security in the Federal Republic of Germany. While the development of a security culture that is firmly established and supported by all facets of society is still in its proverbial infancy, the country is already on the right track.

January 2009

A handwritten signature in black ink, appearing to read 'U. Helmbrecht'.

Dr. Udo Helmbrecht

President of the BSI

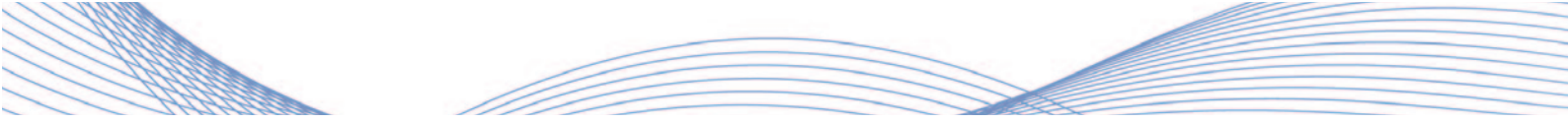
2 Introduction

The IT domain is as dynamic as ever. Users in companies, government entities, but also in the private sphere, are constantly confronted with new applications and hence, also with new threats.

The increasing ubiquitousness of information technology as well as its miniaturization only serve to reinforce this trend. Communication with business partners or one's own company from "on-the-road" via a variety of devices is now commonplace. The information and services the digital world provides have become mobile and are accessible from anywhere. The permanent use, creation, processing, transmission and storing of information have long ceased to be mere trends; they have become indispensable in many areas. Intelligent systems and objects rule our daily lives.

An increasing number of criminal attacks on the data of companies, government entities, and private users is reported in the media. Recently, cases in which the privacy of data was violated have attracted much attention. How data is handled within companies is often problematic. Frequently, there is a lack of personnel and financial resources, as well as technical expertise. But having technological solutions for protecting data privacy is particularly critical since these attacks are becoming increasingly difficult to fight due to the new and complex technologies they employ. However, even the most innovative technological security measures can only provide limited protection if employees or external suppliers can access data and misuse them. In addition, security experts also have to worry about the careless handling of data in the interactive Web 2.0 applications, particularly, on the increasingly popular social network sites. Without hesitation, users provide detailed personal information in their profiles; often forgetting that information on the Internet is, and will remain, accessible to practically anyone.

This has added an additional facet to the manipulation of systems and to securing them by technological means. The current report shows clearly that attackers increasingly demonstrate psychological finesse. They fake mails that are intended to induce the user to click on included links, thus unknowingly installing applications or providing confidential information. Here again, Web 2.0 with its dynamic and user-generated content is of great help to criminals. So much is clear: the risk from online crime is increasing. The protective measures must be taken by each individual, defining the degree of security they require. Consequently, there is a critical need to raise the awareness of Internet users in a comprehensive and ongoing manner.



The third report on the IT security situation in Germany presents an overview of current risks and dangers, forecasting the development trends of potential threats that benefit from the use of innovative technologies and their applications. In addition to BSI surveys, analyses from public and private sector partners, as well as IT provider studies have been used as sources for this report.

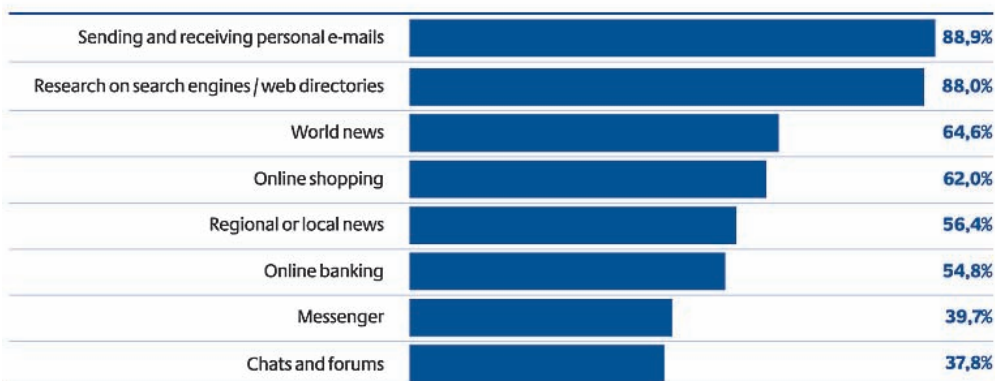
3 IT Security Awareness and IT Security Expertise in Society

There is hardly a citizen, a government entity, or a company nowadays that is a so-called “of fliner” – i.e., someone who does not use the Internet. That is why the issue of IT security has never been more urgent. And yet, there is great diversity with regard to the degree of dependency on the integrity, authenticity, and confidentiality of the technologies used. Different users are impacted differently by the consequences of lacking or insufficient IT security measures. In addition, the degree of awareness and expertise of different societal groups is influenced by factors such as their technology affinity and acceptance, as well as their very own security needs and expertise.

3.1 Citizens

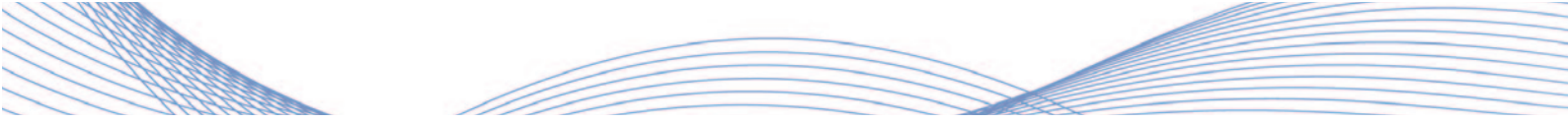
The number of private Internet users continues to increase, while the number of “of finers” sank below 30 percent for the first time in 2008.[1] Broadband connections are meanwhile standard. In sync with these trends, use of the Internet for everyday transactions and activities is increasing. While communication by e-mail is still the most frequently used Internet service, more than half of all users use it now also for shopping or banking.[2]

Online use



Source: AGOF e.V.

Fig. 1: Top Internet use activities in Germany [2]



And the need for good security measures is especially high for handling sensitive data, such as in online banking and E-commerce, so that confidential data is protected. After all, almost four million Germans have already fallen victim to computer crimes, suffering financial losses, such as due to viruses, during Internet auctions, or online banking transactions.[3] And even if, according to their estimates, the majority of users have not suffered noticeable damage, the risk emanating from computer bugs should not be underestimated. Often, users are unaware of the fact that their computer has been tampered with.

Studies show that the positive trend from the 2007 Report has continued: Security is an issue that is meanwhile considered important by most users. German users, as an international comparison shows, have a high need for security.[4] Consequently, security measures are also implemented more consistently than just a year or two ago. That is why almost all security technologies show an increase in use. Firewalls and anti-virus software are largely used almost ubiquitously. And the update frequency for operating systems has also risen considerably. The number of users who perform an update immediately upon its release has increased by 17.6 percentage points and stands at 74.1 percent now.[1]

The rapid increase in time-sensitive security gaps is reflected in a change of behavior regarding information among Internet users. Newsletters – instead of computer magazines or friends – are now the leading sources of information regarding current security issues.[1] This shows that users have recognized the need for prompt and specific information.

However, in the long run, implementing technological security measures alone will not be sufficient. User behavior is also a big factor with regard to data privacy. For it has been clearly shown that even individuals who check and update their computer's security features regularly, handle confidential data in an inattentive way. Web 2.0 has meanwhile become a fixture in the everyday lives of primarily younger Internet users. Social networks are booming, boasting millions of members. Even users who otherwise emphasize data security freely share personal information such as their mailing and e-mail addresses, date of birth and hobbies. The thought that a contact from a social network could also turn out to be a hacker or spammer seems to escape most users. Consequently, it is easy for cyber criminals to spy out potential victims and target them for attacks. Hence, the Web 2.0 issue will play a significant role in raising citizens' levels of awareness and information.

3.2 Industry

Companies in Germany are faced with the challenge of implementing new information technology in order to be competitive and able to work efficiently today. Due to a succession of new threat scenarios to the systems used, the 2007 Report already pointed out the need for a security process initiated at the highest level of management.

In summary, it can be said that IT security is now indeed handled in a more systematic manner: the percentage of companies planning to set up security management projects in 2008 has increased by 20 percent.[5]

73 percent of IT security coordinators in companies and organizations now emphasize the importance of secure IT operations for ensuring that work processes run smoothly in their workplaces. In 2005, only 66 percent did so.[6] A potential loss, based on a risk assessment, is listed as the main reason for investments into security. But the increase in legal requirements regarding regulations on liability law and lending predicted in 2007 are also listed as reasons for investments in the area of security.[7]

Investments in security



Source: InformationWeek

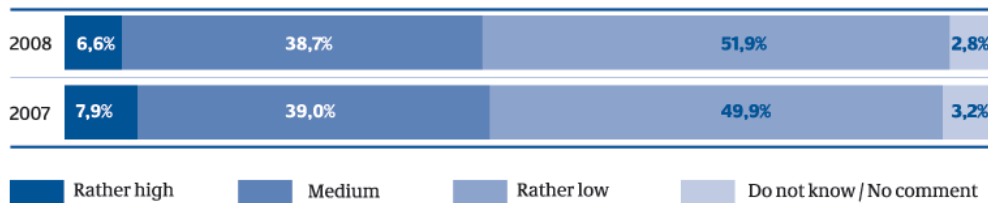
Fig. 2: Reasons for investments in security in German companies [7]

Based on this, it is not surprising that the market for security solutions and services showed an average annual growth of 12.7 percent between 2006 and 2009. The 2008 market volume of 4.4 billion euro in Germany comprises 2.34 billion euro for security hardware and software, and 2.1 billion euro for security services.[8]

More than half of the companies want to maintain the prior year's spending for improving their security architecture, while 42 percent want to invest more in this area. When compared to the total expenses for IT, the budgets for IT security do, however, show different weighting. 54 percent of the companies surveyed wanted to invest less than five percent of their total IT budget into IT security. Only just under two percent of companies are investing more than ten percent of their total IT budgets. In 2006, the number of companies was five times as high. Other investment areas – particularly those improving customer relations – are currently taking precedence. [5]

Overall, however, security awareness on the part of the companies seems to have increased. According to a survey, the security risk of one's company is assessed as lower in 2008 than in the year before.[7]

Security risk rating



Source: InformationWeek

Fig. 3: Security risk rating in German companies [7]

In past years, companies saw their data at risk primarily due to mistakes or a lack of awareness on the part of employees. Malware and external attacks only came in second. The expectation that this order of things would change came true in 2008. Hacking and intentional tampering with IT systems have increased strongly in importance.[9]

Critical infrastructures (KRITIS)

Among operators of so-called critical infrastructures, IT security awareness and expertise can be rated highly at the management level as well as in their implementation. This is also reflected in the KRITIS implementation plan (UP KRITIS) that has been developed by experts from about 30 critical infrastructure companies together with Federal government entities, and that was published by the German Ministry of the Interior (BMI) in 2007. The companies and organizations involved in creating UP KRITIS set out to implement the recommendations made there regarding security measures in critical infrastructures, and to develop further measures. Special emphasis has been placed on measures that go beyond individual companies, requiring intensive and bona fide cooperation across company and industry boundaries. (Cf. Chapter 5.2).

3.3 Administration

A modern State needs an innovative and capable administration that utilizes up-to-date technology securely. Public administration entities that provide a host of electronic services will face new responsibilities and challenges. This includes, among others, all processes placing advanced requirements on a secure and modern identity management, such as the new Health ID card, or the consolidation of public registers. Citizens' expectations of administrative services are diverse. They must be accessible, have a maximum degree of reliability, and treat all information as confidential without exceptions. In addition, the data must be protected from unauthorized access while they are transmitted between government entities. At the same time, these services have to be adapted again and again to modern technologies or new standards in order to maintain good customer service and user-friendliness.

The fundamental awareness that IT security must not be neglected has indeed taken hold over the past years. This can be traced back to cases of misuse that have become public, such as in data privacy violations in particular, and it is also the reason for the public's heightened expectations for the security of administrative services. This was one of the main reasons why in late 2007, a basis for IT security implementation was created for the Federal government's administration in the shape of the Federal Implementation Plan (UP Bund), which has been coordinated among all branches of government. As a consequence, the implementation of IT security in public administration has morphed from a multitude of one-off activities into a continuous process that is to be maintained by qualified and authorized personnel. But even though the situation has objectively improved, difficulties continue to exist. The fact is that the awareness among decision makers in public administration with regard to IT security must be increased further. Often, the financial means provided are still insufficient. In addition, staffing measures must be taken to ensure the organizational maintenance of the IT security process. There is often still a lack of qualified personnel in this area.

4 Vulnerabilities of and Threats to IT Systems

4.1 Security Gaps

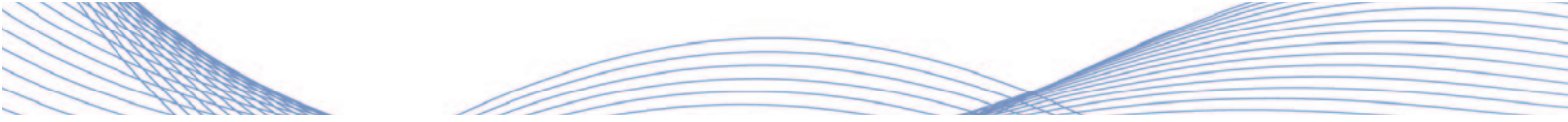
By their very nature, complex products such as software include errors. The resulting security gaps can be exploited by attackers.

In 2007, the number of newly discovered security gaps decreased somewhat over previous years' volumes. From an October vantage point, an increase to 2006 levels seems likely for 2008. As in previous years, approximately half of the new vulnerabilities analyzed in 2007 and 2008 allowed obtaining user and even administrator privileges.[10]

The trend that has been observed over the past years for constantly increasing numbers of security gaps that could be exploited by attackers remotely has been confirmed further: More than three quarters of the new vulnerabilities discovered in 2008 can be exploited by a remote attacker. For approximately half of the newly reported vulnerabilities, the product manufacturers did not provide updates to fix the security issues.[10]

Often, the period between the public identification of a new security gap and the publication of its exploitation is too short to provide the necessary software updates or to develop other protective measures. As the BSI predicted in its 2007 Report, there has since been a clear rise in so-called zero-day attacks. In this type of attack, a security gap is exploited before or on the day it is made public.

Over the past years, users increasingly seem to have realized how important it is to install operating system upgrades on a regular basis. Attackers respond to this fact by increasingly exploiting vulnerabilities in popular user applications. This approach provides them with considerable advantages because many developers do not provide updates for user applications very often. In addition, this type of software frequently does not have automated update mechanisms, and users often do not know how to install updates manually. Besides, many users are not aware of the fact that software applications they use must also be updated.



So-called drive-by downloads have become more of a risk. For this purpose, attackers increasingly manipulate even legitimate websites, enabling them to infect user computers with malware without them noticing. This is done by exploiting security gaps in web browsers or installed plug-ins. The BSI's findings show that the majority of vulnerabilities of web browsers lie in their ActiveX controls used to show active content.


4.2 Malware

Dividing malware into the different categories such as viruses, worms, Trojan horses, or bots is becoming increasingly difficult. Most malware has a modular design and several damaging functions. A Trojan horse, for example, can have backdoor and spyware functions, use a key logger, and additionally, connect the infected computer to a bot network. Besides, most malware has update functions, so that new programs or camouflage mechanisms can be added at any time. That is why bot computers that are updated several times a day are standard.

Creating malware or customizing existing copies to one's criminal needs has become very easy. That is why statements regarding the exact number of malware applications have become useless. Depending on classification and method of counting, the numbers given by IT security companies differ widely. However, there is one thing on which they can all agree: There are millions of malware applications, and their number is growing rapidly. Tens of thousands are added every month.

Creating and using malware result in profits worth billions for organized crime figures, and they are a fixture in their "value-added chain".

Despite the fact that more and more malware is in circulation, individual malware applications are now used in a more targeted manner than in the past, and they are no longer distributed randomly to as many victims as possible. The less widely distributed a certain malware program is, the lower the probability of it becoming quickly known to anti-virus software manufacturers, and consequently, also being recognized by anti-virus software via an ID signature update. This allows using a malware application longer.



While two years ago, most malware was still sent by e-mail, it is now spread in large numbers via prepared websites (drive-by downloads.) According to studies, an average of 15,000 infected websites were discovered per day during the first quarter of 2008. 79 percent of these were basically harmless Internet offers. [11] Most attacks were executed by inserting so-called inline frames, which can easily be automated (e.g., via SQL injection) if the website is vulnerable. Using this method, a single attacker can infect several thousand websites within a few hours. In most cases, active content (such as JavaScript) must be activated on the website visitor's computer for the malware to be introduced and executed.

The authors of Trojan horses and bots, in particular, who invest a high level of criminal energy to try and gain a financial advantage, are constantly improving their protective mechanisms to make detection and analysis of the malware more difficult. Most malware is meanwhile using cryptographic methods for protection, and adjusts its behavior depending on whether it is being executed in a typical analysis environment or on an actual victim's computer.

So far, anti-virus software has mainly been signature-based, i.e., an anti-virus application will only recognize malware that is already known. This technology has reached its limits. Work is under way on technologies that can also recognize new malware by its characteristics or its behavior. This results in the following problem: Behavior-based detection methods always result in a higher number of unjustified alarms (so-called false positives.) This creates a problem for the anti-virus software user; in particular, if it causes critical operating system software to be deactivated or even deleted erroneously. Attackers are constantly working on improving their camouflage mechanisms. So for example, we should expect malware that moves the operating system to a virtual environment; i.e., it will insert itself in between the hardware and the operating system so that it can no longer be detected by traditional anti-virus software.

4.2.1 Trojan Horses

Trojan horses install themselves secretly and allow attackers to control individual computers. They are the most important tool for stealing passwords or spying on a victim in detail. The statements from the 2007 Report regarding the growing number of targeted attacks using multi-function Trojan horses for spying purposes apply unchanged. The annual reports from the Federal and State Offices for the Protection of the Constitution include information on the types and originators of electronic attacks from foreign secret services visited upon companies and government entities. While in the past, attacks targeted primarily the centralized servers of a government entity or company in order to spy on the network behind them, the targeted attacks have shifted to individual workstations. Via clever social engineering, IT users are enticed to open a doctored e-mail or website, or to insert a data carrier (e.g., a USB stick) that has been tampered with. In attacks using manipulated e-mail attachments, mostly Microsoft Office files (such as Word or PowerPoint) or PDF files are misused, due to their widespread use. Generally, the victims cannot recognize that the files have been tampered with.

Traditional protective measures such as anti-virus software and firewalls are no longer sufficient for effective protection from the aggressive methods used in industrial espionage. More advanced IT security measures are indispensable.

4.2.2 Spyware

Spyware programs are used to spy on a person's Internet surfing behavior in order to create user profiles. These are then either utilized by the spyware manufacturer himself or sold to companies, allowing them to place targeted advertising pop-ups.

Spyware is particularly dangerous if it also secretly logs and transmits user names or passwords. This data can allow identity theft. For removing spyware, special anti-spyware software must be used since only very few anti-virus programs offer this function. From a legal point of view, spyware is not considered malware, but instead "potentially unsolicited software". The threat from spyware has increased in recent years, resulting primarily from the fact that the boundaries between spyware and Trojan horses have meanwhile become blurred. Both types of malware are distributed primarily via manipulated websites, or bot networks.

4.3 DoS Attacks

The DoS issue suddenly became the center of public attention through the Estonia Affair in the second quarter of 2007, followed by other DoS attacks culminating, for now, during the conflict in the former Soviet Republic of Georgia in the fall of 2008.

A denial-of-service attack (DoS attack) is an intentional effort to interrupt the availability of an IT system. In extreme cases, any and all use of the system is prevented over a prolonged period of time. The resulting damage depends on the use of the interrupted IT application and can range from loss of production, revenues or reputation to supply bottlenecks for individuals or companies. Consequently, a DoS attack can threaten the existence of those affected. The increase in distributed denial-of-service attacks (DDoS attacks) was pointed out as early as in the 2007 Report. This trend has continued to this day. A high traffic load situation is created using many distributed client systems to effectively block the data connections or the IT systems involved.

But an availability interruption affecting an organization is not always caused directly by a targeted DoS attack. IT applications from different organizations are often centrally maintained by service providers, or IT infrastructure components are shared. Massive attacks on one target will then automatically affect adjacent areas.

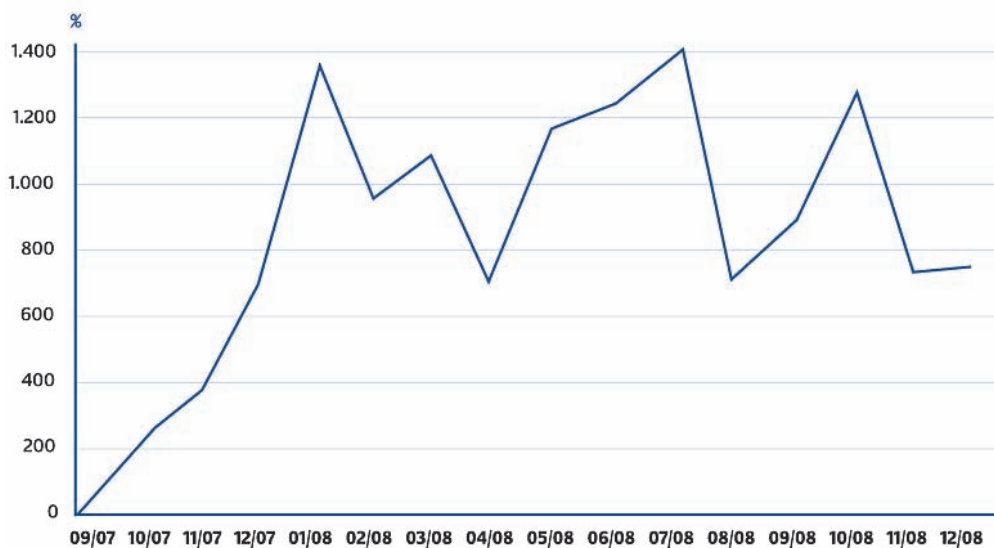
DoS attacks have been a well-known phenomenon for quite some time, and the threat level has not abated. In addition to the classic motivations such as doing damage to a competitor, extorting protection money, or demonstrating one's superiority, the number of ideologically or politically motivated actions continues to rise. The Estonia affair as well as the Georgia conflict illustrate this drastically.

Generally, DoS attacks present a threat for any IT system. Depending on the protection needs of particularly sensitive systems, comprehensive precautionary measures and emergency plans should be prepared in order to mitigate the consequences in case of an attack, and to be able to resume regular operations as fast as possible.

4.4 Unsolicited E-Mails (Spam)

As expected, the volume of spam has continued to increase considerably in the past two years. The mailboxes of internet users are deluged by this unwanted flood of information every day. At the gateway for the Federal government entities it was determined that out of 100 e-mails received, a whopping 1.5 were wanted.[6] If filtering methods are insufficient, the receipt of mass spam mailings can suddenly turn into a DoS attack.

Trend in unsolicited e-mail



Source: BSI

Fig. 4: Increase of spam volume in Federal administration in percent [6]

The flood of spam mail is more or less kept in check by increasingly more capable anti-spam methods. But whether spam is detected based on sender address, content, or meta data, the fact remains that spam senders' methods are also becoming more professional.

The contents of mails are diverse and are becoming more and more individualized. Recipients are increasingly addressed by their name. Frequently, mail contents cannot be recognized as spam immediately since their linguistic quality has improved a lot. The contents range from offers regarding online games and games of chance to medications to financial bargain offers, as well as job offers. In addition, there is mail with dangerous content.

In order to circumvent the content spam filters in particular more effectively, so-called container or attachment spam is used. It comes with an image, MP3, Excel or Zip file attached. The trend for this method is sending files in PDF format, which can be looked at using Adobe Reader.

Advertising mail can be a nuisance. Spam mails that are sent in order to defraud the recipient are additionally dangerous. This includes e-mails that refer to phishing sites, financial bargain offers, as well as mails intended to entice recipients to donate money, or which come with destructive attachments or links. Sending spam is lucrative for criminals since it is practically free. The financial burden is borne by users; primarily in the shape of loss of work time, unnecessary data transfer, the consequences of DoS attacks, or as a victim of fraud.

4.5 Bot Networks

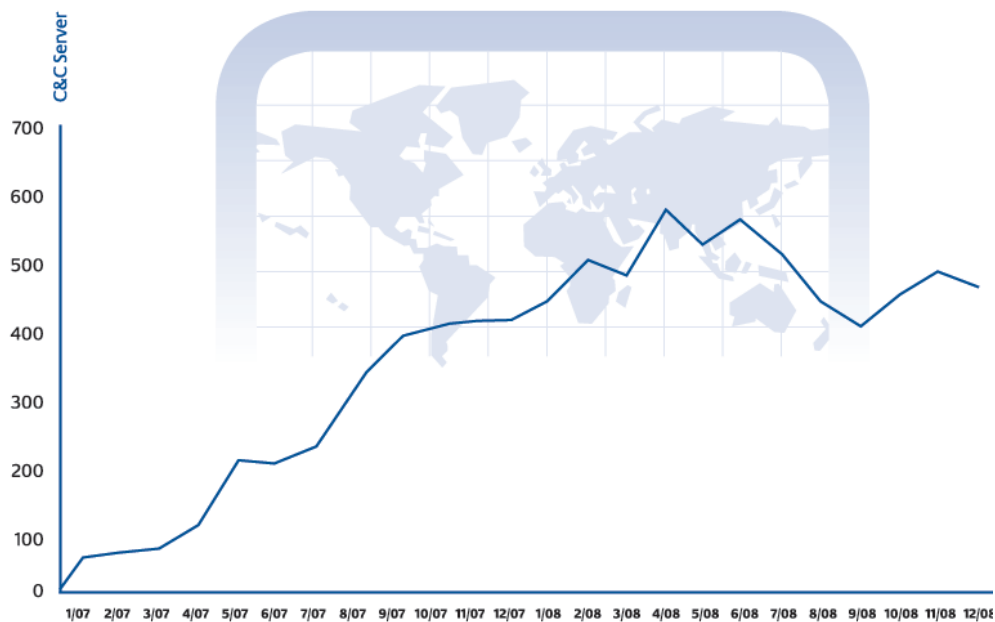
A PC can be infected with bots by, e.g., exploiting known security vulnerabilities in system services and applications. Another effective infection method is the use of social engineering in order to entice the user to act impulsively, such as clicking on malicious e-mail links or instant messages, or executing e-mail attachments. Most recently it has also been found that legitimate, well-known and highly frequented websites are tampered with in order to misuse them for distributing malware.

Bot networks are used for many illegal activities. Among them are mass mailings of unsolicited e-mails with malicious attachments and links, but also key logging in order to obtain personal information. In addition, bot-infected computers are used to deposit illegal software, or to execute targeted DDoS attacks.

An important aspect of bot networks is their command-and-control infrastructure. In most cases, they are controlled via one or several command-and-control servers (C&C servers). Among the advantages of a centralized control model using a single C&C server is its simple development and administration. One of the essential disadvantages for the attackers is, however, the fact that turning off this server will result in this bot network being unusable. Consequently, since the last report was published, criminals are increasingly using sophisticated communication structures with back-up mechanisms on several C&C servers, and P2P protocols, due to their already decentralized architecture. In individual cases, cover-up techniques such as compression and encryption are used. The BSI confirms a trend from IRC-based to HTTP-based bot networks. In 2007, an average of 267 HTTP-based C&C servers specializing in information theft were identified. In 2008, the annual average was 503 C&C servers. This is an 88.35 percent increase over the previous year.[6]


The type of criminal activity outlined here is part of a professionally and internationally organized shadow economy. Organized crime is increasingly using the Internet and IT for its purposes. On the Internet, bot networks can be leased, and people can join others for the purpose of sending spam.

Controlling bot networks



Source: BSI

Fig. 5: 2007 and 2008 numbers of C&C servers specializing in information theft [6]



Related offers can be found on websites and in e-mails. The increasing professionalization of malware authors and the increasing commercialization in the bot network environment point to the unchanged high risk potential represented by bot networks. Additional factors are the many utilization scenarios and the enormous capability of bot networks: A bot network consisting of 1,000 bot-infected computers is, e.g., capable of paralyzing the infrastructure of many small company networks.

The risk of infection for private users can be lowered by consistently applying traditional security concepts such as anti-virus software, desktop firewalls, regular updates of the operating system and its applications, accounts with restricted privileges for Internet applications, and above all, responsible behavior on the Internet. And companies and government entities can also reduce their infection risk and monitor and defend their networks by implementing organizational and technical measures.

4.6 Identity Theft

Identity theft is committed by criminals in order to try and use personal data for gaining an advantage, mostly of a financial nature.

The typical phishing mails that are supposed to entice customers to visit forged credit institution websites where their online banking data can then be harvested are rare nowadays. The increased use of Trojan horses for the purpose of spying was described as early as in the 2007 Report. Meanwhile, data thieves use almost exclusively Trojan horses.

The losses in this area decreased considerably in 2008 thanks to the introduction of improved security measures for online banking such as iTAN or mTAN processes. However, this reduction in losses wiped out by the addition of new areas of fraudulent criminal activity.

While in recent years, it was primarily the user data for online banking and credit cards that was used for fraudulent financial transactions, now it is not just short-term/instant access and transaction data that is collected. Information regarding a person's identity, such as date of birth, address and drivers license number are now also being targeted by criminals. This new data is now used to perform criminal activities in the E-commerce area. So far, this has resulted in billions of losses worldwide, and the trend is up.

Federal government measures for ensuring a secure electronic identity and protection from identity theft are projects that will allow definitive authentication of citizens as well as service providers in the electronic realm.

But identity theft is facilitated not only by the criminal energy of fraudsters, but also increasingly, through active help from users. The popularity of social networks, where members voluntarily release a host of personal data, make phishing and misuse of data much easier.

The fact that the 2008 cases of skimming have almost doubled in number compared to the previous year should also be cause for concern.[11] The information contained in magnetic strips of debit or credit cards is read by devices added to automated teller machines, while the PIN is captured by hidden cameras. According to information from the Federal Criminal Police Office (BKA), more than 90 percent of the perpetrators are from Romania, and the fake cards are primarily used in Romania, Spain, Italy, and France. Losses from skimming are currently in the mid tens of millions.

4.7 Fraudulent Web Offers

In order to do financial damage to third parties, fraudsters used to employ illegal dialers. These dialers installed themselves secretly on computers and created Internet connections via expensive phone numbers. As early as 2007, it was pointed out that, thanks to new processes on the part of telecommunications providers, as well as stricter legal regulations, this fraudulent scam has disappeared almost completely.

Consequently, practically the same circle of people is meanwhile using a new type of crime to defraud users financially. Expensive subscriptions are being planted via supposedly free offers of information on the Internet. The user is provided with a free offer of information through a supposedly free test on legitimate-looking websites. Frequently, the fact that the user is entering a long-term subscription or has to pay a user fee if s/he accepts the offer, is often mentioned only in the fine print. The fraudsters are intentionally working with small font sizes and hard-to-distinguish colors in order to hide the fact that there is a cost. All Internet offers should be carefully reviewed, and in particular, the Terms & Conditions should be read thoroughly to protect from such fraud.


4.8 Compromising Emissions

One illicit way of gathering information is the capturing of the electromagnetic radiation from IT devices. All electronic devices create a certain amount of electromagnetic emissions during operation. In IT devices, these emissions can also transport the information that has just been processed. By capturing and analyzing these emissions, the data processed can be read from a certain distance. This will result in the confidentiality of the data being compromised. So, for example, the screen content that has been displayed can be reconstructed from computer screens. Such electromagnetic emissions containing information are called compromising emissions. In recent years, analog monitors have almost completely been replaced by digital flat screens. Accordingly, the analog VGA interface of PC's has been replaced by a digital DVI interface. Due to the high speed and the special encoding of the data transmission between computer and monitor, digital interfaces were long considered relatively safe from compromising emissions. Current studies have shown, however, that the signals of a digital DVI interface can also be captured over a distance of several tens of meters, and can be made visible after appropriate processing.[6] Consequently, the risk potential due to compromising emissions will probably remain a topic in coming years.

4.9 Material Security, Inside Perpetrators, Errors and Negligence

Even if companies have secured their IT infrastructure sufficiently against external attacks from computer criminals, so-called inside perpetrators are representing a risk potential for companies that should not be underestimated.

As the competitive climate becomes fiercer, the issue of industrial espionage will increase in significance. Modern means of communication allow sensitive data to be secretly spirited out of companies. In such cases, firewalls and anti-virus software do not provide effective protection. The theft of information by a company's own employees represents a high risk. At 24 percent, they are the largest group among perpetrators.[12] The causes that turn employees into perps can be financial incentives or revenge.



A great risk for data confidentiality and integrity is, however, also simply the negligent or improperly trained handling of the provided IT systems and applications by employees. Often, IT security measures are not observed, due to a lack of security awareness, sabotaging comprehensive and expensive security solutions. Consequently, the technical precautions taken to protect from hackers, which are usually the focus, must be complemented not only by raising employees' awareness, but also by setting strict rules for the sensitive handling of data.

Companies are predicting unchanged, and in a third of cases, even rising budgets for expenditures on outsourced services for the years ahead.[5] This area also requires a high level of security. For one, data from outsourced areas can become accessible to other clients of a service provider, either intentionally or due to human error. And secondly, external consultants with access to the Intranet can also access confidential data.

To sum it up, there is a need for organizational and technical security measures to protect information. From technical monitoring by means of access control systems for the premises or "sensitive" rooms, to the storage of data in steel cabinets, to the access rules for computers (e.g. by PIN's or tokens), to access protection by express release of authorizations. In addition, proper handling of information and data carriers that are no longer needed is required. For this purpose, the appropriate deletion and disposal devices must be used.

5 Activities

While the awareness that IT security is necessary has increased across all groups of society, the situation remains as challenging as ever. Increasingly insidious tricks on the part of Internet criminals on the one hand, and the increase in online activities on the other will continue to require grappling with this issue. IT security must be assured a continuing presence in the public dialog in order to help solve the problem.

5.1 Citizens

While for many citizens, the IT security issue has increased in significance, the measures that must be taken are still often regarded as too time consuming and expensive. The BSI is trying to help citizens deal with this problem. It provides tools that are customized specifically for the heterogeneous group of private users and their needs.

In 2008, the BSI was able to celebrate the fifth anniversary of its online information offerings at www.bsi-fuer-buerger.de. Just in time for the occasion, the related websites were revised. In addition to the extensive information around the topic of IT security, there are now also more checklists and illustrative short videos available. Through the bi-weekly newsletter “Sicher ◦ Informiert” as well as its special issues during time-sensitive security incidents, the BSI fulfills the public’s requests for competent, targeted, and especially, timely information on existing security risks. Both services may be subscribed to via the platform www.buerger-cert.de. In addition, the BSI offers a wide range of informational materials such as brochures and flyers for private users. They are used in schools as well as in adult continuing education, and increasingly for raising employee awareness in business environments. The public also has an opportunity to obtain information on all aspects of the IT security topic directly from BSI employees at trade fairs and events.

Concerted Action

Establishing an IT security culture is a goal that cannot be achieved by a government entity acting in isolation. For addressing the public, the BSI increasingly relies on sharing and collaboration with its cooperating and disseminating partners who are also hard at work on the topic of IT security. This will allow addressing the technical, educational and psychological aspects of IT security in a

competent and comprehensive manner. In addition, the BSI is an advisory board member of the association Deutschland sicher im Netz e.V. (DsiN), which was founded as a public-private partnership in 2006. With its practical campaigns and services, DsiN provides assistance and practical solutions around IT security for children and youths, consumers, as well as small and medium enterprises. The BSI actively supports the work of this association. The BSI is also active at the international level in the areas of awareness raising and information regarding IT security topics. So, for example, the BSI participates in the Awareness Raising Community of ENISA (European Network and Information Security Agency), and is represented with activities at the “Safer Internet Day”, which is annually initiated by the European Union.

From a technical point of view, the introduction of the electronic ID card has an additional security bonus. The eID function for proving the digital identity of the card holder allows using data that is stored on the electronic ID card to be used for online authentication. It will result in a reliable digital proof of identity. This allows the public to protect itself better from identity theft or involuntary data capture. In business correspondence with the government and industry, such as for online banking or E-commerce, the electronic ID card will allow its holder to be identified in a simple and secure manner. The Portals for the Public project (Projekt Bürgerportale), a concept for secure and confidential communication over the Internet, will also use the eID function to make sure that e-mails can be sent in a reliable and secure manner.

5.2 Industry

The value of IT security measures is hard to quantify. Data loss or the failure of a data processing center due to an attack on a company results in high costs. With regard to the security of expertise and data, companies often do not realize that they need to be protected, until there has been an attack. The BSI provides informational materials for industry in order to promote and advance the level of security in companies. Among these are brochures and guidelines on various aspects of IT security that can be downloaded from the website at www.bsi.bund.de. In the shape of standards based on IT-Grundschutz, the BSI also offers information on topics that are of general importance for information security in companies or government entities. They can use the BSI recommendations and adapt them to their own requirements.



The BSI is represented at numerous domestic and international events and trade fairs, presenting its broad range of offerings to industry and governments. In addition, there is a series of talks in Berlin that is held at regular intervals, addressing decision makers in industry, administration and academe. The goal is to initiate a dialog with influential high-level representatives from these organizations regarding likely future topics.

Another focus of the BSI's work is the certification of IT products and systems. Last year, the demand increased considerably. Certifications according to the internationally recognized Common Criteria create transparency and comparability for manufacturers as well as customers, and they can be advantageous for positioning a product in the market. Besides, the use of certified information technology increases the level of IT security and can contribute to protecting from attacks on a company's infrastructure. The BSI also certifies according to ISO 27001 on the basis of IT-Grundschutz. This allows a company, e.g., to prove to its customers that the handling of IT risks complies with certain requirements. Through its certification activities, the BSI contributes to the improvement of the IT security level in Germany.

Critical Infrastructures (KRITIS)

The KRITIS implementation plan (UP KRITIS), which was passed in September of 2007, defines in its roadmap essential steps for further improving IT security in Germany's critical infrastructures: The representatives from the critical infrastructures operated by private industry, and appropriate government entities such as the BSI, are preparing in working groups for how to handle IT-related incidents and IT crises.

The working groups are designing IT crisis scenarios across industry sectors and appropriate drills. Initial plan reviews and communication drills have already been organized. In addition, approaches for how to respond to IT crises across industry sectors have been developed. For this purpose, e.g., a network of single points of contact (SPOCs) for incident-related communication as well as for alerting and crisis handling is being built. Initial SPOCs are in the process of forming in the insurance, credit and petroleum industries. The cornerstones of continued cooperation were defined in a master concept on crisis response and drills, which was completed in 2008.

Starting in 2009, the activities for "maintaining critical infrastructure services" will be stepped up. Critical processes and components within critical infrastructures will be determined in order to allow further improvements in the stability of services by means of protective measures and adapted/customized crisis response mechanisms.

At the international level, the main emphasis is on information exchange on the 'European Programme for Critical Infrastructure Protection', as well as on studies to define appropriate criteria for identifying European critical infrastructures in the ICT sector.


5.3 Public Administration

The Federal implementation plan (UP Bund), which was passed in late 2007, represents the first uniform IT security guideline for all branches of government. The UP Bund defines technical, organizational, and process-related standards for the Federal administration, which are being realized in all its government entities by means of appropriate IT security measures.

In this context, the BSI supports the creation and maintenance of the underlying security processes by providing numerous tools for the strategic and conceptual areas. Here, the revised BSI standards, as well as the frequently updated IT basic protection catalogs are central to this task. In order to maintain the security processes on an ongoing basis, tools for security reviews are also provided.

The BSI provides practical assistance by conceptualizing and implementing a training series for IT coordinators in Federal government entities at the Federal Academy of Public Administration (BAkÖV). The definition of the job profile for an "IT security coordinator" and the related training plus certificate are creating a structure with regard to responsibilities and expertise. In late 2008, 70 participants had been certified. The 3-week training program takes place several times a year. It is to be expected that an average of 50 certified coordinators will be added annually. In addition, the BSI offers an advising concept that will support particularly the IT security coordinators at government entities in their daily work.

In the technical operation area, the protective measures already established will be expanded further. Early warning systems and crisis response processes are being optimized on an ongoing basis in order to be able to effectively address IT crises. CERT-Bund (Computer Emergency Response Team for Federal government entities) at the BSI represents a centralized point of contact for preventive and response measures regarding security- and availability-related incidents in computer systems serving primarily Federal government entities.



Given the heightened threat situation of the past years, the critical network infrastructures of the Federal administration, the Information Network Berlin-Bonn (IVBB), and the Information Network of the Federal administration (IVBV) will be developed further.

5.4 Fund for the Future (Zukunftsfonds)

Intensive research is indispensable in order to address the changing threat situation in a proactive manner. In its own IT security research program (Zukunftsfonds), which is financed from the six billion program of the Federal government, the BSI addresses priority issues in the IT security area. The program's goal is to develop application-related innovations – particularly, in the technology areas of early warning systems, trusted computing, as well as biometrics and ID card systems – and to implement them practically. Close cooperation and communication are required between the government entities as the client on the one hand, and the contractors from academe and industry on the other in order to achieve a sustainable effect from the results.

6 Summary

This report on the IT security situation in Germany illustrates the seriousness of the threats. Some attack methods are gaining in popularity among Internet criminals, while others are becoming less important. The fact is that thousands of new malware programs are flooding the Internet every day. Additionally, there are new technologies whose risk potential may be hard to assess today but is likely to increase as they spread and find acceptance. The following Tables show timelines for different threat trends. Future developments are predicted based on careful research and surveys.

Risk trends

Threats	2007	2009	Forecast
Zero-day exploits	↑	↑	→
Drive-by downloads	—	↑	↑
Trojan horses	↑	↑	↑
Viruses	↓	↓	→
Worms	↓	↓	→
Spyware	↑	↑	→
DDoS attacks	→	↑	↑
Unsolicited e-mail	↑	↑	↑
Bot networks	→	↑	↑
Identity theft	↑	↑	↑
Fraudulent Web offers	—	↑	→
Emissions	—	→	→
Material security, errors, negligence	→	↑	→




 Risk increasing
  Risk remaining the same
  Risk decreasing

Source: BSI

Fig. 6: IT threat trend according to the BSI [6]

Risk potential for attacks in selected applications and technologies

Technology / Application	2007	2009	Forecast
Voice over IP	↑	→	→
Mobile data transmission	—	↑	↑
Web 2.0	—	↑	↑
SCADA	→	↑	↑
DNS	—	↑	↑
Multi-function devices	—	↑	→
Interfaces and storage media	—	↑	→
Network coupling elements	—	↑	↑
SOA	—	↑	↑




 Risk increasing
  Risk remaining the same
  Risk decreasing

Quelle: BSI

Fig. 7: Risk potential for attacks in selected applications and technologies according to the BSI [6]


Risk profiles of innovative applications and technologies

Technology / Application	2007	2009	Forecast
RFID	→	→	↑
Biometrics and personal ID's	—	↑	↑
IPv6	—	↑	→
Automotive	—	↑	↑
Health ID card	—	↑	→

 Risk increasing
  Risk remaining the same
  Risk decreasing

Source: BSI

Fig. 8: Risk profiles of innovative applications and technologies according to the BSI [6]



So much is certain: Internet crime is profitable business. And where profit is to be expected, there will be copycats. In addition, the rising number of transactions conducted via the Internet will cause the risk potential to increase.

But there are also positive trends. The increase in security awareness in public administration, industry and society is very welcome. Many users and institutions are motivated to take precautionary measures for their systems by the fact that IT security is also protection for company or private assets. It is obvious that users are more familiar with technical security measures than they were only months ago. But in order to counteract the increasingly insidious criminal attacks, the level of IT security expertise will also need to increase considerably. The effective protection of users and their systems in society, industry and government will only be possible if this expertise is maintained and expanded continuously.

However, technical knowledge and security measures alone will not be sufficient. The examples for an increase in psychological manipulation demonstrate how important it is that Internet users think about their behavior and the extent of personal data that they provide, e.g., on social networks. However, users are often negligent when it comes to protecting their own data.

For the same reason, the same applies to companies and government entities: Protecting company information no longer ends at the gate. Company gates have become virtual. In addition to using technical protection measures, it is essential that employees be thoroughly sensitized for using IT devices and handling company information appropriately. An additional problem in a business context is the issue of espionage for realizing a competitive advantage over the competition. Integrated security concepts that take into account the required personnel and financial resources are indispensable for protecting institutions lastingly from losses.

Given the attack options described in this report, comprehensive IT security research is also necessary. At this point in time, the IT security industry is primarily in a reactive mode: A patch or update will not be developed and delivered until there are new security vulnerabilities, viruses, or Trojan horses. In future, sustainable, application-oriented security research shall be improved through preventive measures. The reasons for this problem do not only lie in the entrepreneurial or industry-associated environment. Purely academic research, on the other hand, does not seem sufficiently able to make IT more secure in actual practice, due to its mostly theoretical focus. Nevertheless, the situation is quite promising. There is large number of approaches in which industry, universities and public administration entities are cooperating in the field of IT security research in Germany.



And finally, users are also challenged to contribute. The responsible and thoughtful handling of IT and data represents an essential factor for achieving a lasting increase in the level of security. Responsible citizens cannot delegate this task to the State and the provider alone. Common goals require common action. Only then can we create the foundation for a lasting secure use of IT and effectively counter Internet crime.

7 Sources

- [1] (N)ONLINER Atlas 2008, TNS Infratest GmbH und Initiative D21 (Hrsg.).
- [2] internet facts 2008-I, Arbeitsgemeinschaft Online-Forschung e.V.
- [3] BITKOM press release, July 6th, 2008.
- [4] 4. ePerformance Report 2008 – Sonderbericht zum Dritten Nationalen IT-Gipfel, Bundesministerium für Wirtschaft und Technologie (Hrsg.).
- [5] IT-Trends 2008, Capgemini.
- [6] BSI surveys.
- [7] IT-Security 2008, InformationWeek.
- [8] IT-Security-Agenda 2007+ - Schlüsselthemen und Trends in Deutschland, Experton Group AG.
- [9] kes/Microsoft-Sicherheitsstudie 2008.
- [11] Sophos Security Threat Report, Q1 2008.
- [10] Secunia Monthly Report, Q1 2008.
- [11] Federal Criminal Police Office.
- [12] Studie: Industriespionage, Corporate Trust GmbH, 2007.

Published by

Federal Office for Information Security – BSI
53175 Bonn, Germany

Text and editorial staff

Federal Office for Information Security – BSI
pressto GmbH – Agentur für Medienkommunikation, Cologne

Layout and design

artwork factory kommunikation und design, Cologne

Date

January 2009

Reference office

Federal Office for Information Security – BSI
Section 321 – Information, Communication, Public Relations
Godesberger Allee 185-189
D-53175 Bonn
Phone: +49 228 99 9582-0
E-Mail: publikationen@bsi.bund.de
Internet: www.bsi.bund.de