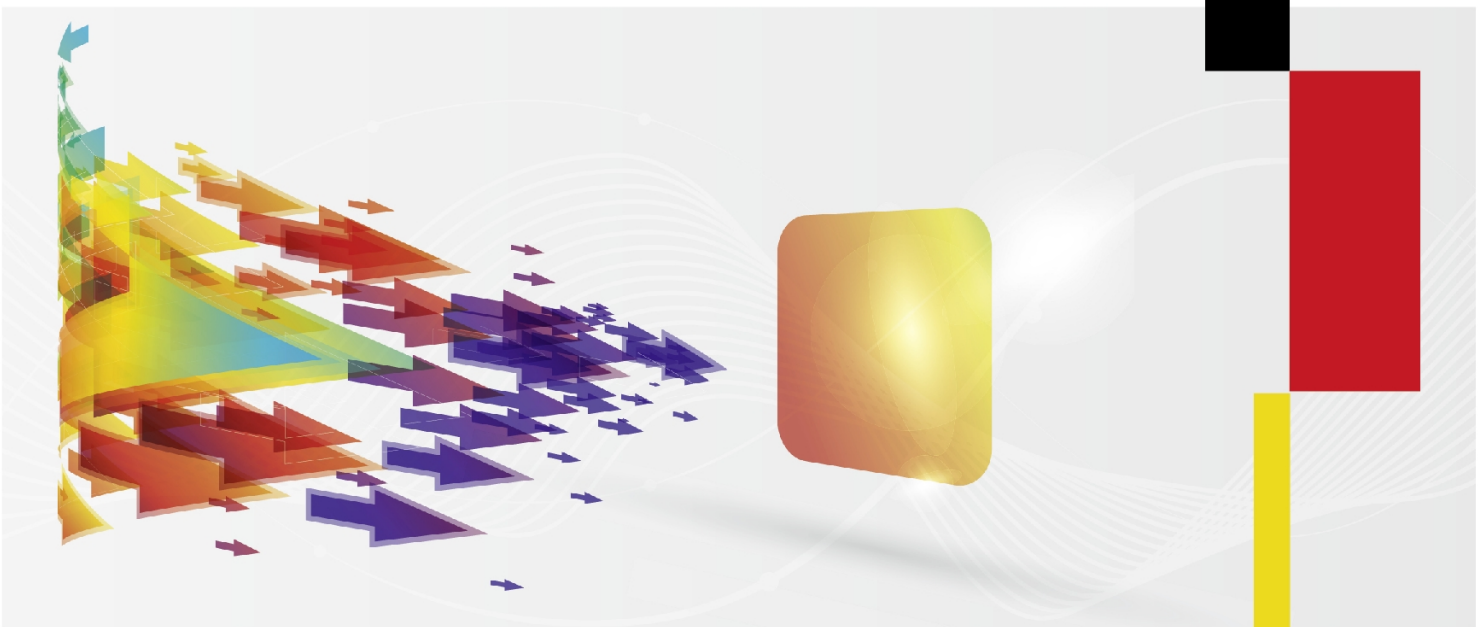
Federal Office
for Information Security

The IT Security Situation in Germany in 2011



Federal Office for Information Security
www.bsi.bund.de

Contents

Preface

The opportunities offered by present-day IT in both our private and professional lives are many and varied. Just as many and varied, however, are the risks we face as we increasingly shift our business transactions and social interaction into the virtual world.

For attackers also keep tabs on developments and are constantly working out sophisticated ways of staying one step ahead of their potential victims. Authors of malware are using ever more diverse technical measures to make their programs harder to detect or analyze. For example, there is malware out there that can scan its target system to pick up on features of an analysis environment. If it detects any, it will stop trying to infect the system. This makes it harder for specialists to analyze the program. It also increases the demands on users; it is becoming more crucial for them to play an active role than ever before. There is need to be every bit as alert and curious in the online lives as there is in the offline world.

Internet criminals have long since created a market for their services which helps to increase their "earning potential". A botnet consisting of 10,000 bot PCs, for example, can be rented for around US$ 200 a day. And as botnets can consist of several millions of PCs, the financial potential of such attacks is something we can only guess at.

But we will not allow this to discourage us: on the upside there have been plenty of successes. Like the dismantling of large-scale botnets, for example. Often this is achieved through the joint efforts of many companies, IT security organizations and investigators all over the world. This worldwide network is constantly expanding. April 1 saw the opening of the National Cyber Defense Center, a joint venture of German federal security departments operating under the auspices of the BSI, tasked with defending critical federal government and industrial IT infrastructures against electronic attacks.

My employees and I are doing our bit to make the online world safer for all of us. And this is something we are fully committed to.

Bonn, May 2011

Michael Hange

President of the Federal Office for Information Security

Overview

Countless processes and tasks in the public and private sectors are supported by IT nowadays. Even in our private lives, it is hard for most Germans to imagine doing without their PC and cell phone. Business and industry, the public sector and private individuals are therefore all highly dependent on properly functioning information technology and secure information infrastructures.

Organized criminals, but also intelligence services, are carrying out highly professional IT attacks on companies, authorities and even private individuals. The methods the attackers are using are becoming ever more sophisticated, making them increasingly expensive and complicated to defend against. A recent example was the Stuxnet Trojan horse which targeted industrial process control systems. Its programming was highly complex and was done by people who were experts in their field. There have always been attacks on IT systems, but their intensity and nature have changed. Alongside mass attacks, we are also beginning to see a new quality of specifically targeted attack. Mass attacks mainly exploit standard vulnerabilities like banner ads, whereas targeted cyber attacks use secret or as yet undiscovered weak points. The attackers do not "waste" their knowledge; their methods have become ever more devious since we published our last report in 2009. Besides vulnerabilities in operating systems, attackers exploit weak spots in third-party applications and software components. Targeted attacks geared towards specific individuals that use highly sophisticated social engineering to disguise themselves are also on the increase.

The number of new malicious programs is also continuing to rise dramatically. But malware is no longer being spread randomly across the internet in massive waves. A malware program will often only infect a small number of computers worldwide, making it extremely difficult to detect.

"Conventional" phishing is much less common these days. But that does not mean that identity theft no longer poses a threat: in fact, quite the opposite. A criminal field of activity has developed in this area which has all the hallmarks of highly professionalized structures.

As far as spam is concerned, attackers are seemingly opting for a much less random approach nowadays. The volume of spam e-mail may have reduced, but it is becoming increasingly targeted, so the risk potential remains just as high.

Security experts involved in malicious code analysis are finding their work turning increasingly into a race against the attackers. One positive outcome of this is that cooperation between manufacturers, providers and security experts is constantly improving. For example, some dangerous botnets have been disabled as a result of joint initiatives. An international network has also been set up for CERTs: the Forum of Incident Response and Security Teams (FIRST). There is now a general realization that working together can benefit everyone concerned – but we will all need to continue to up our game in order to keep the overall situation under control.

The rapid expansion of smartphones, netbooks and tablet PCs also presents a growing challenge, as it significantly increases the number of potential vulnerabilities open to cyber criminals. Assuming that internet attacks can potentially be financially rewarding and that the risk of being caught is relatively low, it is likely that they will continue to increase.

The much-talked-about topic of Cloud Computing is set to become ever more widespread in view of its potential for cost-cutting and increasing availability. Ensuring information security will therefore take on a new international dimension as data leave the jurisdiction of the Federal Republic of Germany. Stronger international cooperation is becoming increasingly necessary. Just as with the omnipresence of IT systems in our everyday lives – and with the imminent introduction of the Smart Grid/Smart Meter – IT managers are facing growing organizational challenges in areas such as risk management.

Risk trends

Threat	2009	2011	Forecast
DDoS attacks	↑	→	→
Unsolicited e-mails (spam)	↑	→	→
Botnets	↑	↑	↑
Identity theft	↑	↑	↑
Security vulnerabilities	–	↑	↑
Drive-By Exploits	–	↑	→
Malware	–	↑	↑

Source: BSI

Fig. 1: Development of IT threats as assessed by BSI [7]

Risk potential of attack opportunities in selected applications and technologies

Technology/Applications	2009	2011	Forecast
Mobile communication	↑	↑	↑
SCADA	↑	↑	↑
DNS and BGP	↑	↑	→
Interfaces and storage media	→	↑	↑

Source: BSI

Fig. 2: Risk potential of attack opportunities in selected applications and technologies as assessed by BSI [7]

Risk profile of innovative applications and technologies

Technology/Applications	2009	2011	Forecast
Cloud Computing	–	↑	↑
Smart Grid/Smart Meter	–	↑	↑

Source: BSI

Fig. 3: Risk profile of innovative applications and technologies as assessed by BSI [7]

1 Security Vulnerabilities

The number of published security vulnerabilities was once again at a high level in 2010. It remains to be seen whether this trend will continue through 2011. It is difficult to establish exact numbers, as we do not know how many cases of vulnerabilities go unreported. What is more, some manufacturers fix vulnerabilities on the quiet with so-called Silent Fixes which are not counted in the statistics.

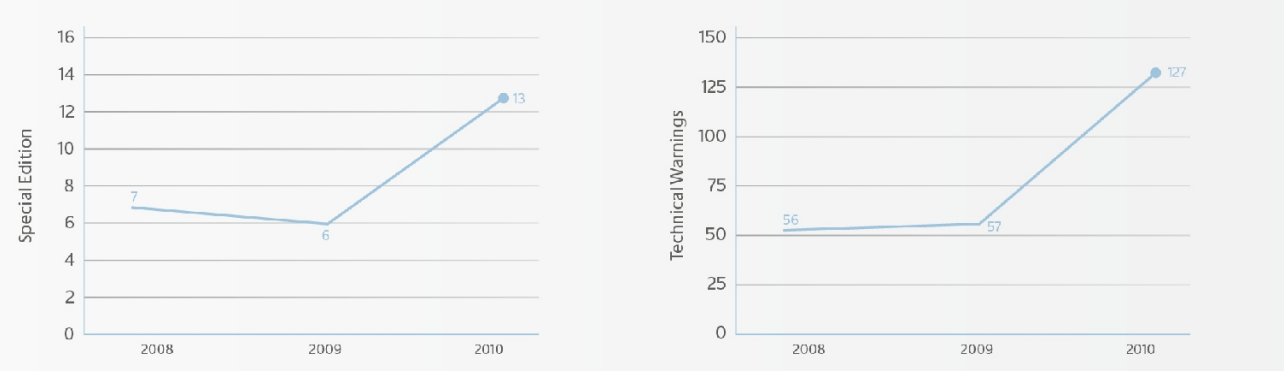
Software vulnerabilities on the rise

As far as the typical end-user PC is concerned, the ratio between the number of vulnerabilities in the operating system and in third-party software is changing. While vulnerabilities in operating systems such as Microsoft Windows are becoming less and less attractive to attackers, the number of security weaknesses in third-party software rose significantly in 2010.[1] This is particularly critical given the high prevalence of many applications. For example, Adobe Flash Player is found on more than 99% of all PCs in Europe, according to the manufacturers, and CVE[1] reports that it was affected by 60 vulnerabilities in 2010, 53 of which were able to be exploited for running malcode. Mozilla Firefox now has the biggest web browser market share in Europe.[2] According to CVE it had 107 vulnerabilities in 2010, 60 of which enabled malcode to be executed. The potential scope for attacks therefore increases with every application that is used.

The BSI's alert and information service, Bürger-CERT, is issuing increasing numbers of alerts about time-critical vulnerabilities. In the 2010 special edition of its newsletter, for example, it published 13 alerts – more than in previous years. Since 2008 there has also been a constant rise in the number of technical alerts issued by Bürger-CERT.

Software manufacturers have acknowledged the fact that they share responsibility for IT security and are working actively on improving their products. So it is no longer only third parties who are discovering vulnerabilities: the manufacturers themselves are also reporting them. But time is and remains a critical factor. Zero-day attacks, in which vulnerabilities are exploited on the day they are discovered, are now the rule. At the same time, so many vulnerabilities are being discovered all the time that manufacturers risk not being able to keep pace with this development, potentially resulting in vulnerabilities remaining in place over long periods of time. According to CVE, for example, on February 15 this year more than 20 vulnerabilities in various Microsoft products (Windows, Office, Internet Explorer) were known about, 16 of which enabled malcode to be run. Many of these had been described several weeks earlier.

Security vulnerabilities reported



Source: BSI

Fig. 4: Number of time-critical security vulnerabilities reported by Bürger-CERT and Technical Warnings issued by CERT-Bund [7]

[1] "Common Vulnerabilities and Exposures" (CVE) is an industry standard for cataloguing information security vulnerabilities in a uniform way.

Central patches help

Against this backdrop, users must call for effective update mechanisms to eliminate security vulnerabilities effectively and fast. Automatic update functions have proved very helpful in this regard. They enable a user to keep their software up to date without any involvement on their part; security-relevant updates are simply downloaded and installed as soon as they become available. Most common applications have these functions nowadays. But this system is also not without its problems. Because there are no central update functionalities, applications typically have their own specific update mechanisms and cycles. And there can even be big differences between an individual manufacturer's products. In addition, some manufacturers do not provide their updates as they develop them but have set patch days on which they publish their patches. In the worst case scenario, vulnerabilities can then exist for anything between one month (Microsoft's current patch cycle) and three months (Adobe's current cycle). So manufacturers are increasingly being forced to respond to critical vulnerabilities with workarounds – temporary measures which involve additional effort on the part of the user and the administrator. However, patch releases are sometimes brought forward when a particularly critical vulnerability is discovered.

The BSI is therefore in constant contact with the major software manufacturers with a view to driving forward the development of central update mechanisms and ensuring that updates are made available promptly. The aim going forward is to have updates downloaded fully automatically as soon as they are available so as to keep pace with the security threat caused by the discovery of new vulnerabilities. In administered environments, these mechanisms need to be put in place by the administrators.

Summary:
The security threat caused by vulnerabilities in software products is at an extremely high level and is continuing to rise. This situation is made worse by long periods during which no patches are released for known and critical vulnerabilities. Prompt updates that can be installed centrally and automatically are therefore absolutely vital.

2 Drive-By-Exploits

Drive-by exploits automatically exploit vulnerabilities in software on a PC without user interaction. When a user visits a website containing a drive-by, it can exploit vulnerabilities in the browser, in browser plug-ins or in the operating system to install malware such as trojan horses on the PC without the user's knowledge.

How vital it is to fix vulnerabilities in software straight away is illustrated by the fact that you can infect your own computer simply by "surfing" to a website containing one of these drive-bys. In the past, similar malware was predominantly spread through shady websites. In another variant, attackers would set up specially crafted websites and lure users to visit them by sending out spam e-mail containing links to these websites. Today, malware distribution via drive-by exploits almost exclusively happens using compromised legitimate websites.

Every day, attackers manipulate several thousand websites across the world and inject malicious code which leads to drive-by exploits. These websites are usually compromised using stolen FTP login credentials for the web servers that have been previously harvested by malware on the website operators' computers. Analysts investigating attackers' servers regularly come across lists with 30,000 or more stolen login credentials for FTP servers. Additionally, security vulnerabilities in content management systems and other server software are often used by attackers for manipulating websites.

Infected without clicking

CERT-Bund, the German Governmental Computer Emergency Response Team, currently receives reports from various sources on more than 20 German websites per week that have been manipulated by attackers and lead to drive-by exploits. But this is just the tip of the iceberg, as the BSI is not actively looking out for compromised websites. CERT-Bund asks the operators of the websites concerned to remove the injected malicious code and fix the vulnerabilities being exploited by the attackers. A user’s PC can also be infected through specially manipulated banner ads on reputable websites. Attackers regularly compromise marketing service providers' server applications to get them to deliver a malicious payload that leads to drive-by exploits. And the user does not even have to click on the banner ad to activate the payload. Simply having a manipulated banner displayed on a website is enough to trigger automatic exploitation of vulnerabilities on the user's PC. In 2010, CERT-Bund notified more than 100 operators of banner ad servers in Germany of these kinds of manipulations. Some of the infected banners were displayed on the websites of well-known companies, popular online magazines and TV/ radio stations.

Exploit kits: malicious software packages

Malicious code injected by attackers into compromised websites usually does not target only one single vulnerability. Instead, it leads to a so-called exploit kit. An exploit kit (or exploit pack) is a software package that automates the exploitation of vulnerabilities on users’ PCs using drive-by exploits subsequently infecting them with malware. Besides a collection of exploits for various vulnerabilities (typically more than 10), an exploit kit usually also contains a web-based management interface that allows for easy configuration and generation of statistics. Exploit kits are traded by cyber criminals for between US$ 400 and US$ 2,000, depending on the number and up-to-dateness of the exploits they contain. In-depth technical expertise is not usually needed to install and operate an exploit kit.

Over the past few months, attackers have focused their attention primarily on weaknesses in older versions of the widely used software products Adobe Reader and Flash and in the Java Runtime Environment. However, exploit kits are also still successful at exploiting vulnerabilities in Internet Explorer and the Windows Operating System, many of which have been around for years, since many users have not yet installed the security updates that fix these vulnerabilities.

It gets particularly critical when the attackers use zeroday exploits that target vulnerable software for which the vendor has not yet issued a security update.

Summary:
It is not usually possible for a visitor to a website to tell whether it has been manipulated and leads to drive-by exploits. The exploitation of vulnerabilities and installation of malware on the PC goes undetected and without any additional user interaction. To protect against infection, it is therefore vital to install all available security updates for operating systems and applications as soon as they become available. Because of the large number of malware variants being distributed every day, an antivirus software alone will not offer sufficient protection.

3 Botnets

A botnet is a network of infected PCs that are controlled remotely by an attacker. Botnets are used for the distribution of spam, spying on keyboard inputs, or attacking other systems like web servers or entire networks unnoticed by the PC owner. Once a PC has been infected – by whatever means – and is part of a botnet, an attacker can abuse it for many different purposes.

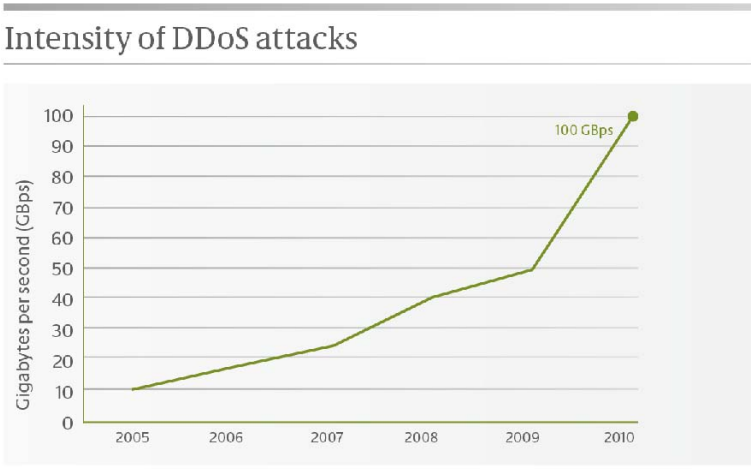
The threat presented by botnets has continued to rise dramatically over the past two years, partly as a result of the risk of infection by drive-by exploits. Botnets are now also being rented out professionally, and their "customers" use them to take revenge, gain competitive advantages and for criminal purposes like extortion. Attacks may also be politically or religiously motivated. Another trend began to emerge in 2010: "hacktivism". This is a mixture of hacking and activism, in which internet users voluntarily make their PCs available for attacks like DDoS on companies. A botnet can also be formed in this way.

Botnet operators can potentially infect an increasing number of PCs, because more and more users have broadband internet access and leave their computers connected to the internet 24/7. As a result, the intensity of cyber-attacks is also on the rise: according to BSI estimates, it already exceeds individual providers' service bandwidths, which can lead to network outages.

Users do not usually notice that their PC is part of a botnet, as the malcode runs in the background. This is confirmed by a security firm who analyzed 100 million compromised IP addresses worldwide. They discovered that 80 per cent of IP addresses of infected PCs appeared in the statistics for more than a month, and 50 per cent for at least 300 days.[3] One of the reasons for this is that some bot software deactivates antivirus software to prevent itself from being discovered. Computers without antivirus software or running outdated versions simply exacerbate the problem. Often the infection is only discovered when the user is informed about it by their provider. The number of multiple bot software infections has also risen. This is confirmed by an analysis in which multiple infection was observed in 35 per cent of cases.[4]

Summary:

Botnets have proved their worth as a business model for criminals and are therefore likely to continue to grow over the next few years. The emergence of "hacktivism" shows that people are increasingly carrying out attacks to express political views and make their voices heard.



Source: Arbor Networks

Fig. 5: Bandwidth increase in DDoS attacks [9]

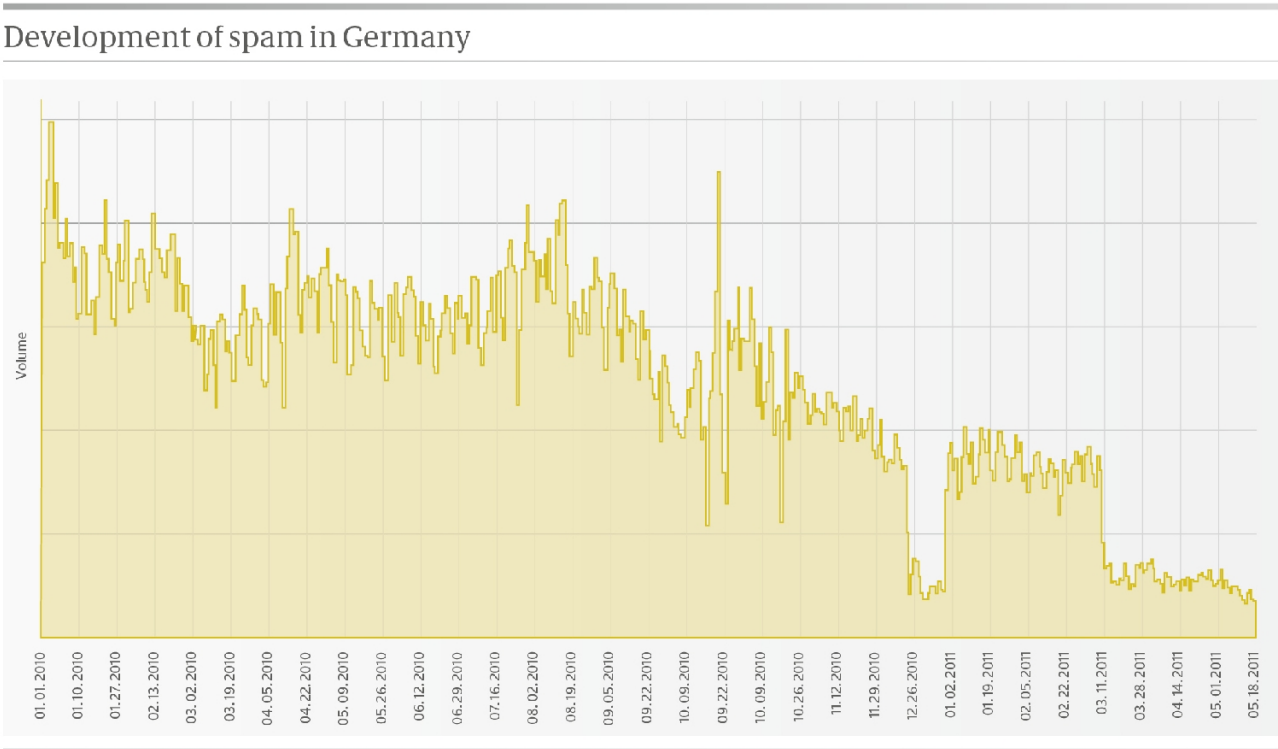
Anti-botnet initiative permanently knocks the bottom out of infections

According to BSI analyses, in 2010 Germany was among the top 5 source countries for botnets that send out spam e-mail. The BSI is therefore supporting the Anti-Botnet Advisory Center set up by eco-Association of the German Internet Industry. This initiative is being financed with start-up funding from the Federal Ministry of the Interior's IT Investment Program and aims to help rid computers of bot infections. This initiative, which was officially unveiled on September 15, 2010, is intended to make life more secure for the end user and knock the bottom out of botnets operating in or out of Germany for good wherever possible. The first step in the initiative is to identify infected computers. This is done by the Internet Service Provider (ISP) using honeypots and spam traps. Honeypot systems reside in the provider's network area and are attacked by the infected computers. The spam traps receive the spam e-mail sent from there. Then the ISPs inform the identified users that their PCs are infected. To eliminate the infection, they can obtain help in the form of information and tools from the central website, www.botfrei.de. Users who need additional help are pointed by their ISP towards the Anti-Botnet Advisory Service telephone advice hotline. Between September 15, 2010, when the project was launched, and April 30 this year, more than 994,000 visitors used the website. During this time, the DE Cleaners – special tools designed to remove bot software from computers – were used more than 522,000 times. The ISPs involved alerted more than 200,000 customers about infections on their computers.

4 Spam

The number of unsolicited e-mails (spam) has fallen compared with the record year 2008. However, spam still accounts for an extremely high proportion of all e-mail: 96.1% in 2010. Spam also seems to be being targeted more precisely of late. For example, the proportion of German language spam e-mails sent specifically to German e-mail recipients by international botnets is growing.

The vast majority of spam e-mails are sent by botnets. In a single hour, the BSI observed individual spam waves with over 100,000 different sources (sender systems with unique IP addresses). The Rustock botnet has been found to be the most prolific sender of this spam. As can be seen in the graphic below, the volume of spam in Germany dropped dramatically by nearly 75 per cent in Rustock's two-week silent period at the end of 2010 and when its command and control server in the USA were taken down in mid-march.



Source: BSI

Fig. 6: Development of spam volume in Germany since January 2010 [7]

Sending spam via private PCs

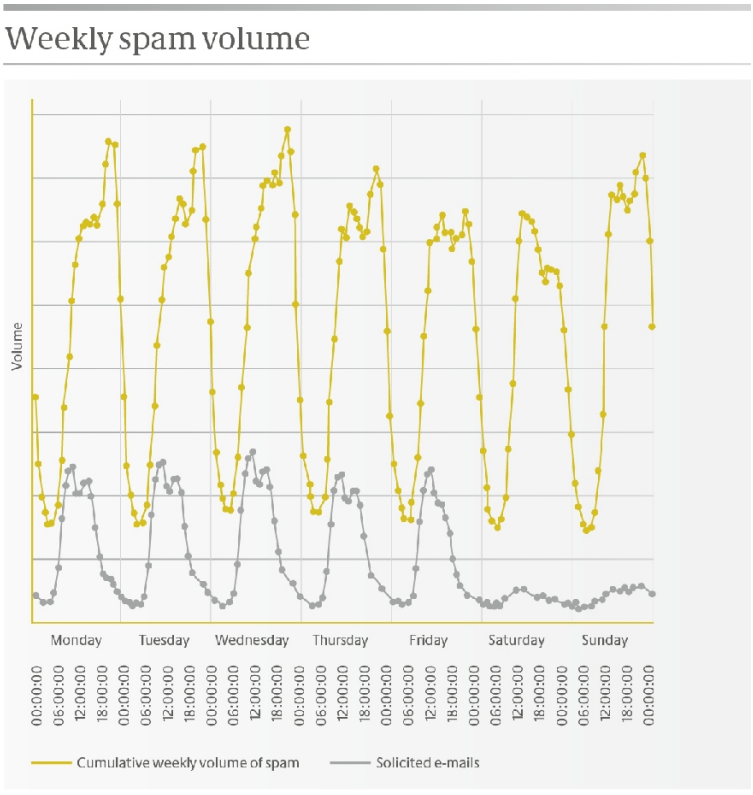
Spamming shows regularities both on a day-to-day and a week-to-week basis. It is also particularly interesting to look at the sources by country.

The following diagram shows a weekly pattern, accumulated over several months, of spam and solicited e-mail sent from Germany at different times of the day, measured against the BSI's e-mail early warning system.

According to BSI findings, most of the Spam sent in Germany originates from compromised private PCs. These are probably being used by schoolchildren in the afternoon, but mostly by adults in the evening after work. Fewer of the infected PCs are being used on Friday and Saturday evenings as people are more likely to have other plans at these times. In an international comparison, it is striking that there are countries in which the daily maximum falls within the working hours for that time zone and with a much lower volume at evenings and weekends. In these countries, spam is obviously being sent predominantly from workplace PCs.

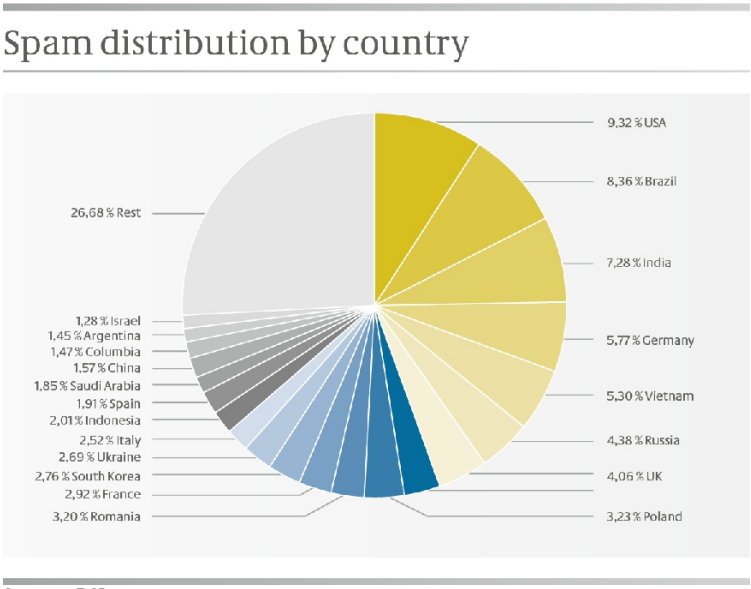
In the league table of spam-sending countries, Germany was in fourth place in 2010 with 5.77%, behind the USA (9.32%), Brazil (8.36%) and India (7.28%). The German share drops during the course of the year. The data refer to the distribution of spam in the Federal Republic of Germany.

The BSI expects Germany to be overtaken by some countries as a source of spam in 2011.



Source: BSI

Fig. 7: Cumulative weekly volume of spam and solicited e-mails sent from Germany [7]



Source: BSI

Fig. 8: Spam distribution in Germany in 2010 by country of origin [7]

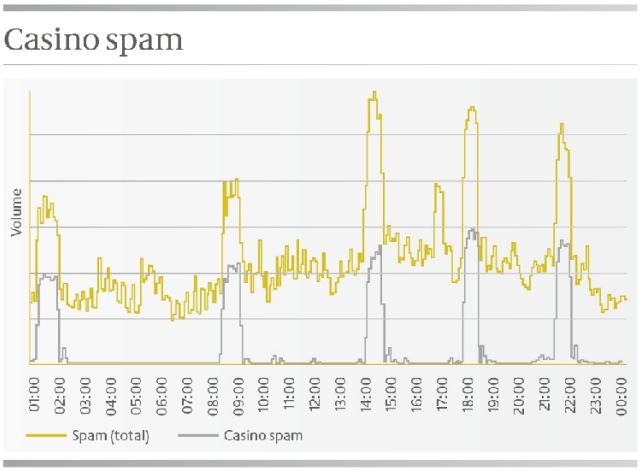
German-language casino spam waves from thousands of sources

One of the most distinctive and longlasting Spam campaigns is German-language casino advertising. The BSI monitors it since May 2009. It occurs roughly in hourly waves and increases the volume of spam by more than 100 per cent. Several thousand sources per hour from almost all countries in the world have been identified as the senders – mainly in Brazil, followed by Vietnam, India, Indonesia, China and Germany. They are most likely part of the Maazben botnet. From the variations in time, it can be concluded that large parts of this botnet concentrate simultaneously on one country domain and its language.

Internet users being recruited for criminal purposes

Since March 2010, a spam wave has been observed which recruits “manpower”. These “money mules” or “agents” are then used to forward illegally acquired goods or money. To increase the credibility of this offering, the spam often lists the German Federal Employment Agency (Bundesagentur für Arbeit, BA) as the supplier of the addresses. Several thousand sources per hour from almost all countries in the world have been detected as the senders of this spam – mainly in Brazil, followed by India, South Korea, Germany and Poland.

For this spam variant, the attackers started by performing a small-scale and obviously highly successful test in mid-March 2010. From the end of April to the end of August 2010 this form of e-mail was a firm fixture in the German spam landscape. Thereafter, the messages stopped mentioning the Federal Employment Agency. Another wave appeared at the end of the year. In the opening sentence it made it perfectly clear that people were being recruited for criminal purposes: “A job for someone who is quite clear that if anything goes wrong they can at best expect a suspended sentence, and at worst…” This example shows that the attackers are not afraid to involve large swathes of the population in criminal acts. Immediately after being alerted by the BSI, the Federal Employment Agency issued a series of press releases on this subject.



Source: BSI

Fig. 9: Casino waves and total spam volume over a typical day [7]

Summary:
The risk is diminishing as recipient e-mail infrastructures become overloaded. But the content of criminal spam is becoming ever more convincing. This increases the risks to the recipient, which include fake medication, compulsive gambling, (unintentional) participation in criminal activities, disclosing sensitive data, or malware. This trend is set to continue going forward.

5 Identity Theft and Identity Fraud

In IT, the identity of a person is generally defined as a dataset which differentiates this person from others in certain circumstances. The most straightforward example is the username/password combination. Gaining unauthorized access to these data constitutes identity theft, which often goes hand in hand with identity fraud. The perpetrators' primary aim is to gain financial benefit; more rarely, they may be trying to discredit someone.

Identity theft and identity fraud are not new crimes: they were happening long before we started using electronic media. In the past, the perpetrator and the victim would nearly always be in close geographical proximity to one another, and there would usually only be a few people involved. But as internet usage has increased, the situation has changed radically: nowadays there is usually no geographical link between perpetrator and victim whatsoever. What is more, a perpetrator can obtain data from hundreds or thousands of victims with very little effort using malware, as analyses of datasets captured from perpetrators have shown.

Malware steals personal data

Identity theft takes place using malware which transfers the stolen data to "drop zones", servers controlled by the perpetrators. Once there they can be deployed for identity fraud purposes. Occasionally data being transferred by malware to drop zones can be intercepted. When this happens, the owners of the stolen identities are usually protected by the operators of the internet services concerned, such as by preventatively changing their password or temporarily deactivating access.

In 2010 data from approximately 200 drop zones were analyzed. Of particular interest to the BSI are datasets that relate directly to Germany, such as with a domain name ending in ".de", for example.

Particularly common on webmail and online marketplaces

Analyses of examples of drop zone datasets from 2010 show that the perpetrators were particularly successful in gaining login credentials for German webmail service providers and widely used online marketplaces. When subsequently deployed for identity fraud, they may not be able to be turned directly into money but they nonetheless harbor considerable potential for damage. For many users, the e-mail account represents the central trust anchor for a range of other online activities, making it easy for the perpetrators to get hold of other login credentials. Stolen identities for online marketplaces provide the perfect basis for fraudulent buying and selling transactions.

Online banking data, on the other hand, can be exploited directly. In 2010 around 86,000 identities were found in the drop zones investigated. These login credentials do not lead directly to a transaction on their own. But as the malware on the target systems is usually still active, the attackers can often overcome the banks' other protective mechanisms such as transaction codes.

Trojan horses scour private PCs

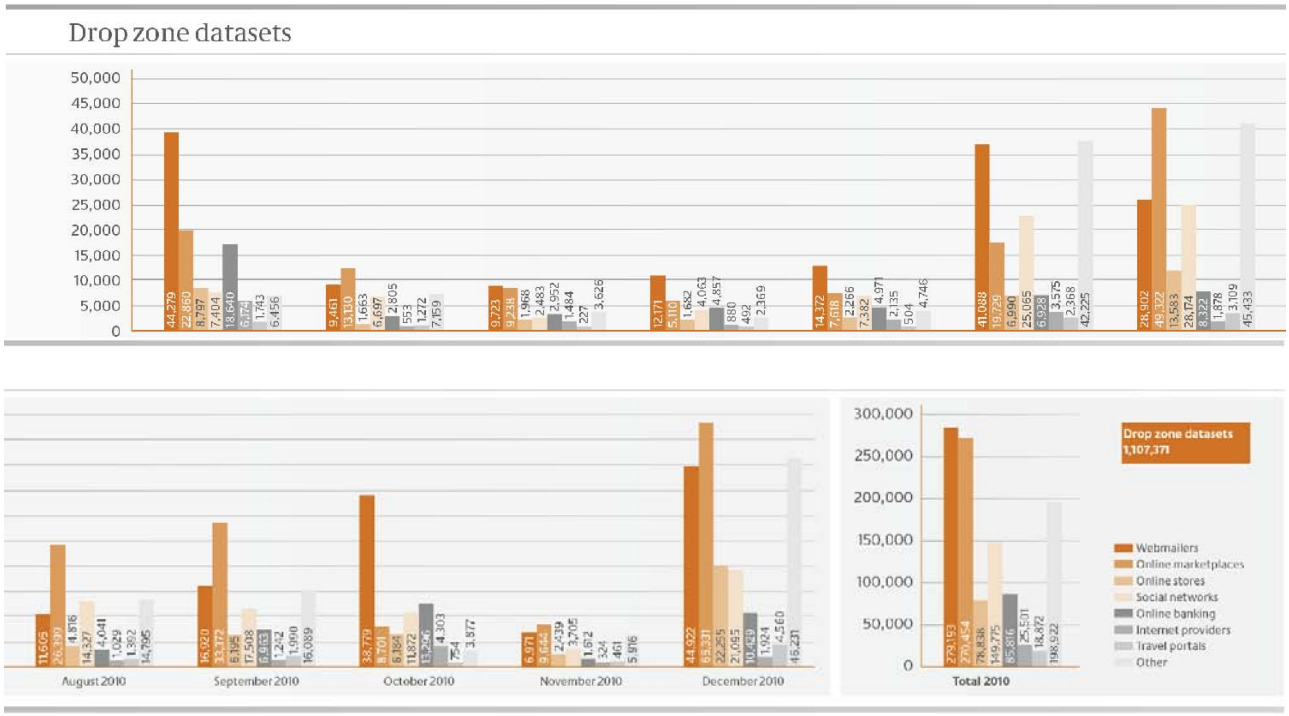
These days, perpetrators almost always use Trojan horses that cover their tracks on their victims' computers very effectively. They use them to track the owners' login or transaction keystroke combinations or to search their files for particular keywords. The data are then transferred to the drop zones.

Conventional phishing, on the other hand – luring unsuspecting users to fraudulent bank websites and asking them to enter their credentials, for example – is now relatively rare. But the increasing use of powerful Trojan horses has meant that the number of cases – and therefore the levels of losses – are once again on the rise compared with previous years.

Today's perpetrators divide up their tasks in a highly orchestrated way. First one group will produce the malware – a Trojan horse, for example. The next group will distribute it across the internet and use it, and a third group will collect the mined data from the drop zones and prepare it for the next stage, identity fraud. The next set of perpetrators will then use the data for criminal purposes.

As banks and service providers have tightened up security on money transfers abroad, financial agents with accounts in the home country are used. Recruitment and maintenance of these agents is also organized in a sophisticated way, including by sending out spam (see Chapter 4).

Summary:
Identity theft and identity fraud have become established as a criminal field operated with highly professional structures. Conventional phishing has declined over the past few years and is now relatively rare. Instead, attackers are almost exclusively using Trojan horses.



Source: BSI

Fig. 10: Drop zone datasets in 2010 from approx. 200 drop zones with direct relationship to .de domains [7]

6 Malware

In our 2009 status report we observed that the number of malicious programs was rising constantly, they were becoming easier to produce and the attacks were increasingly being targeted at specific victims. These trends have intensified since then.

Malware much harder to detect

The number of new malicious programs is continuing to rise dramatically. A new one is launched every one or two seconds. However, they are no longer being spread randomly in large waves across the internet. Whereas in the past one single malicious program could have several thousands or even hundreds of thousands of victims, today as few as 20 computers worldwide will be affected. Sometimes people visiting a manipulated website infected with a drive-by download may even pick up an individual malicious code. Particularly problematic are malware programs that can only run on the computer they first infected, as these are completely undetectable in an analysis.

Previously, a malicious program would be used actively over several months. These days they will be used for just a few days before being replaced by a new variant that cannot be traced by antivirus software.

A direct consequence of these trends is that it is becoming increasingly difficult to detect malware in the usual way based on signatures and checksums. Manufacturers of antivirus programs have severe problems localizing the large numbers of different malware and producing detection signatures.

There are two main causes for the spate of new malware. Firstly, exploit kits and virus construction kits are widely available. They can be expanded to accommodate newly published vulnerabilities and attack methods in just a few days, and they are easy for semi-professional attackers to use. Secondly, highly efficient techniques exist for automatically producing a thousand new variants of an individual malware with only very minor differences and different checksums.

Malware spread mainly by drive-by downloads

Distribution of malware via e-mail is dwindling. The BSI assumes that most malware is now distributed via drive-by downloads. More and more malicious programs that have infected a computer via the internet are being spread on USB sticks or internal networks. Manipulated Microsoft Office or Adobe PDF documents are increasingly being used. In addition, malware for mobile devices is on the advance: it is no longer a technical problem for malware to move between PCs and mobile devices during data transmission, although such cases are rarely observed at present.

One reason for the decline in e-mail-based attacks is the constant improvement in spam filters which stop infected e-mails being delivered.

Infected e-mails on government network

The total number of infected e-mails on the government network is falling. But at the same time the BSI is discovering increasing numbers of harmful e-mails that are not being picked up by virus scanners. The BSI currently detects about four or five targeted attacks per day.[2]

In 2004 more than 100,000 infected e-mails per month – many containing the same malware – were blocked by a standard virus scanner. On average there were 1.6 million harmful e-mails per month in 2004. Over the past five years there have only been six months in which more than 100,000 infected e-mails were detected. In relative terms, the number of harmful e-mails detected by the virus scanner has fallen even further, as around four times as many e-mails were received in 2010 as in 2004. The all-clear? Sadly not. Whereas infected e-mails were relatively easy to detect with antivirus software in 2004, the BSI is discovering more and more harmful e-mails with its own detection systems which were not picked up by the virus scanner. These numbers illustrate the benefits of central protective measures in the government network. The entire federal administration is therefore profiting from the high levels of technological expertise and manpower used by the BSI to protect the government network.

[2] The BSI refers to a "targeted" attack when the attacker tailors it individually to a particular person and uses a high degree of social engineering to disguise themselves. The malicious programs they use are changed repeatedly until current antivirus programs no longer recognize them.

Room for improvement

The race between the authors of malware and the manufacturers of protection programs is hotting up, and this is not without consequences. An internal BSI analysis has shown that the rate at which virus scanners detect documents with embedded malicious functions needs to be improved dramatically. On average, less than 50 per cent of malicious documents were identified in on-demand mode (i.e. without executing the file). Only a combination of at least three different virus scanners was able to identify more than 90 per cent of the infected documents. On-access virus scanners, which use additional detection processes when a file is opened, deliver better results. Antivirus programs on desktop PCs are therefore far superior to those on gateways which only work in on-demand mode – provided all behavior-based and heuristic detection processes are active.

Besides the use of antivirus programs, which offer inadequate security in many scenarios, what measures help? Virtualization techniques can protect against drive-by downloads collected during surfing. These encapsulate the browser in a virtual environment so that it is effectively separated off from the rest of the computer and the intranet, at least providing effective protection against data loss or sabotage actions by malware. Protection against the spread of malware via USB sticks is increasingly taking the form of programs that control computer interfaces, although their use can go hand in hand with considerable loss of convenience and function. To protect against malware in e-mails, there are virtually no measures one can take other than using several different antivirus programs. E-mails are such an integral part of typical work processes that it is not possible to virtualize e-mail clients. The IT security industry has responded to this situation and offers managed security services such as a central e-mail scan or spam defense. For many companies, but also for private individuals, security services provided by specialist firms or providers will in future be an attractive alternative to doing it yourself with protection software. The ever expanding use of mobile devices for processing and storing confidential information continues to present problems. Mobile devices are often poorly protected. Closer cooperation between manufacturers of mobile devices, operating systems and protection software is therefore urgently needed.

Summary:
Large waves of malware like Sasser or Loveletter are no longer being observed. A typical malicious program only lasts for a few days and is only targeted at a small group of victims. As attacks become increasingly individualized, the number of malicious programs with different checksums is continuing to rise unchecked. Signature-based antivirus programs therefore no longer offer reliable protection and must be supplemented with a combination of other processes. Targeted attacks for sabotage and espionage purposes increased significantly in the period under review and were carried out with a hitherto unknown professionalism. The BSI is concerned about the ever more widespread use of mobile devices for writing and reading e-mails, as these are often poorly protected due to a lack of suitable protection programs.

7 Stuxnet

Over the past few months, public attention has focused on the malware Stuxnet, which was discovered in 2010. This example very clearly illustrates the professional modus operandi of the attackers and the risks that targeted attacks pose to industrial systems. Stuxnet is malware with highly complex programming designed to circumvent special protection mechanisms. This enables them to attack industrial process control systems. Attacks that have taken place exclusively targeted process control computers running Siemens' WinCC SCADA software. This malware was used to sabotage a very specific system configuration in a highly sophisticated way. Worldwide, manufacturers of antivirus software observed several hundreds of thousands of infections of all kinds of PCs, all harmless – presumably as a collateral infection. The 22 infections confirmed by Siemens industrial customers had no impact on their industrial systems. The vulnerabilities exploited by Stuxnet in the Windows operating system have since been closed.

IT attacks on process control systems have long been the subject of discussion in specialist circles. But now Stuxnet has impressively demonstrated the real threat. This malware features some outstanding infection mechanisms and, unlike most Trojan horses, does not target "normal" PCs but industrial process control systems. These are the brains and nerve centers of many processes: they monitor, control, and regulate complex systems as diverse as refineries, pipelines, electricity grids, industrial bakeries, and assembly lines. With the speculation surrounding potential attack targets in the nuclear industry, the subject of Stuxnet has been raised and discussed in many media.

Under the surface, Stuxnet is in fact less alarming as a piece of actual malware; rather, its relevance lies in the fact that it clearly demonstrates the potential of attacks of this quality. It proves that there are people out there who will spare neither expense nor effort to attack what they perceive to be key targets and sabotage them unnoticed. Whereas attacks on critical infrastructure and their process control systems have often been accepted as a residual risk in the past because of their presumed unlikelihood, this risk now has to be reevaluated.

Separating process control systems from other networks

Stuxnet was programmed for a particular purpose and geared specifically towards it. A similarly high-quality attack on another target would require the same level of programming expense and effort. And yet there is a

significant risk that Stuxnet is just the tip of the iceberg and that similar attacks could follow. It cannot be ruled out that comparable malware may already be being programmed and used both for the process control systems of other operators and manufacturers and for other critical information infrastructures with as yet unknown infection channels and highly complex malicious functions. Besides such highly specialized and targeted attacks, there is also the risk of free-riders who could attempt to damage process control systems with a lot less expense and effort. It is therefore important to isolate these systems from other networks as strictly as possible and protect and monitor any key interfaces as effectively as possible. In some cases the BSI has proved that process control systems are directly visible and accessible via the internet. And if something can be seen, it can be attacked.

Summary:
Stuxnet has made it clear that the entire concept of security in process control systems urgently needs to be reviewed and adapted to the current threat situation wherever necessary.

8 Domain Name System and Routing

Users access the internet using services like e-mail or the World Wide Web (WWW). The basis for the operation of many internet services is the Domain Name System (DNS) service, which is responsible for name resolution. The DNS translates host names like www.bsi.bund.de into IP addresses (here, 77.87.228.49). So the user does not have to to deal directly with hard-to-remember numerical IP addresses. Host name or DNS integration into virtually all common internet services makes the Domain Name System one of the most important services on the internet.

Top Level Domains

Top level domain	Number of second level domains	DNSSEC support
.com	95,006,677	yes
.de	14,369,495	yes
.net	14,003,416	yes
.org	9,639,660	yes
.uk	9,373,754	yes
.info	8,200,168	yes
.nl	4,442,413	yes
.cn	3,379,441 (on 28/02/2011)	no
.eu	3,341,775	yes
.biz	2,254,683	yes

Source: BSI

Fig. 11: The ten biggest top level domains [7]

Domain Name System

The protocol used for communication between DNS servers for exchanging data has design flaws. Attacks on the protocol can result in DNS information on the internet being manipulated by third parties. In 2010 this problem continued unabated, and there were several incidents of data being corrupted. For example, some traffic to popular websites like YouTube, Twitter and Facebook was diverted to servers in China. To improve the underlying protocol, the Internet Engineering Task Force (IETF) specified the DNSSEC (Domain Name System Security Extension) protocol extension to enable both digital signing and validation of domain data.

Operators responding

To implement the improvements introduced with DNSSEC, however, it is necessary to roll out this extension actively throughout the whole DNS infrastructure. While both the domain registrars and the ISPs are still hesitant when it comes to implementing DNSSEC, last year some fundamental changes were made to the underlying basic infrastructures. For example, since July 15, 2010 DNSSEC has been supported by the Domain Name System root zone. Acceptance by top level domains has also risen strongly over the past two years. Between early 2009 and May 2011, the number of top level domains accepting the DNSSEC extensions rose from five to 72 out of 310. Fortunately, apart from China (.cn), the ten largest top level domains have already implemented DNSSEC. These include the German top level domain, .de, whose operators DENIC eG introduced DNSSEC on May 31, 2011.

Summary:
Implementing DNSSEC permanently increases internet security and protects against numerous risks. Domain registrars and ISPs therefore need to make the necessary conversions for DNSSEC in order to close the current vulnerability in the Domain Name System. The BSI believes that there are no technical reasons not to implement DNSSEC. The .bund.de domain has been operating successfully with DNSSEC since April 2010.

Attack on internet infrastructure availability

Another opportunity to use internet structures for attacks is in routing between connected systems. The structure of the internet is based on different providers' networks interconnecting with one another. Information on how the connected systems can be reached using networks and lines (routing) is exchanged via the Border Gateway Protocol (BGP). Some of, there are very few control mechanisms in existence that enable reliable verification of the information being exchanged. So anyone with access to the BGP infrastructure can manipulate the routing information being transmitted. A potential consequence of a manipulation of this kind could be that a network is no longer accessible.

There have often been disruptions in internet routing in the past. The last major incident, which affected as many as 37,000 networks, happened on April 8, 2010. Some of the data packages addressed to these networks were diverted to China.

Summary:
At the present time, routing manipulations are a threat that needs to be taken seriously. The experts are currently developing a process which will make it easier for network operators to identify unauthorized changes to the BGP infrastructure. However, this process is not yet available. Network operators should therefore monitor the accessibility of their networks and use appropriate encryption processes when transmitting sensitive information over the internet.

9 Mobile Communication

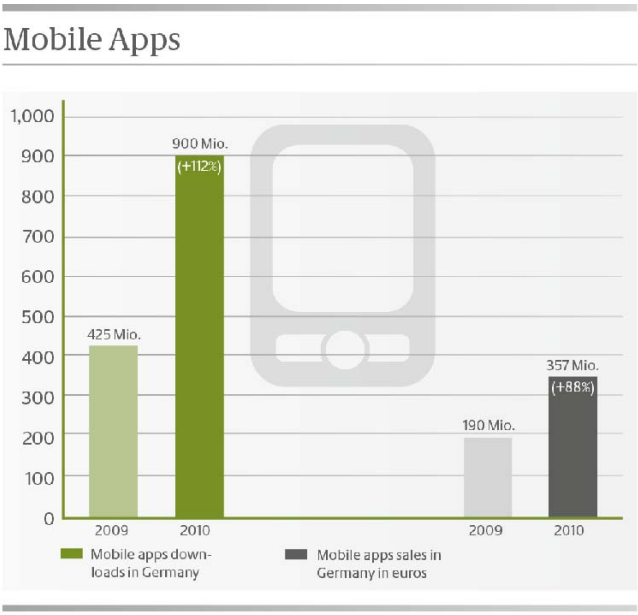
As the use of mobile devices for reading, using and transmitting important business data on the move increases, the BSI anticipates a rise in the number of attacks on these devices in the future. Around 10 million people in Germany regularly use their cell phone to go online.[5] The number of apps downloaded onto cell phones had reached the 900 million mark by the end of 2010.[6]

Not all smartphone users are aware of the risks of using mobile operating systems. According to a survey of smartphone users by the BSI, around 60 per cent know that their mobile devices have the same security requirements in terms of security updates and protection software as a PC. But 47 per cent of users have never downloaded security updates onto their cell phones, only 20 per cent do so at least once a week, and 11 per cent at least once a month.[7]

Risks at the mobile interface

GSM-Standard

Originally named after the Groupe Spéciale Mobile, today GSM stands for Global System for Mobile Communications and is the world's most widespread digital mobile network standard. A GSM network consists of four subsystems: the Mobile Station (MS), the Base Station Subsystem (BSS), the Operations and Support System (OSS) and the Network Switching Subsystem (NSS). The Mobile Station integrates into the GSM network by setting up a communication connection with a BSS via the air interface, i.e. via the wireless interface between the Mobile Equipment (ME) and a Base Transceiver Station (BTS) on the GSM mobile network (Um interface).



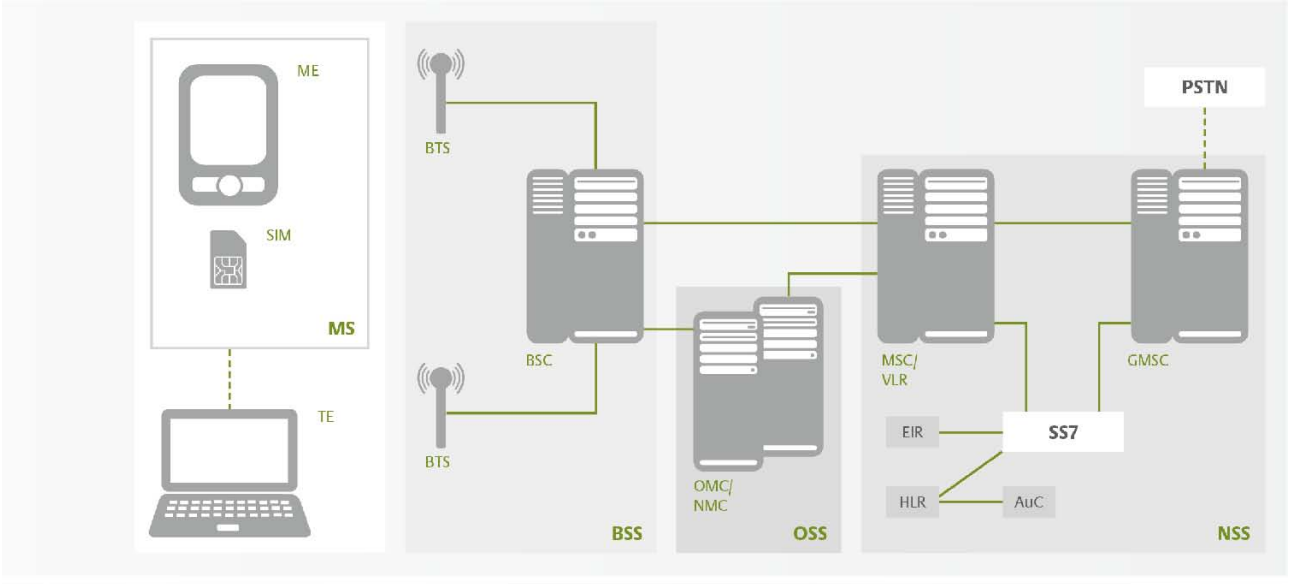
Source: Bitkom

Fig. 12: Development of downloads and sales of mobile apps for smartphones in Germany [6]

The insecurity of the GSM interface is a particularly significant threat to the use of smartphones. Users who are inadequately protected need to be aware that their connection data (telephone numbers and call times) and usage data (e.g. call data, e-mails and text messages) can be intercepted or that an attacker can find out their whereabouts and their movement profile.

All usage data crossing the GSM air interface are encoded according to the GSM standard. But this code is no longer up to date, and tools for intercepting GSM communication have been available for some time.

Thus a data thief can work out the GSM code if they manage to intercept data communication on the GSM air interface. Once they have this code, they can then decode GSM call data and sometimes even text messages. Data connections via UMTS (Universal Mobile Telecommunications System), GPRS (General Packet Radio Service) and EDGE (Enhanced Data Rates for GSM Evolution) and calls via UMTS are unaffected.



Source: BSI

Fig. 13: Simplified diagram of a GSM mobile network [7]

Other security risks in the use of mobile devices are:

- Back-end eavesdropping: the attacker captures the call data on a cable that transmits the calls unencrypted.
- Loading and installation of malware from the internet and manipulability of mobile devices by Trojan software. Malware can render a smartphone unusable and use it to infect IT systems that are networked with the phone. Mobile phones infected with a Trojan horse can even be used as a phone tap that is operated remotely via the mobile interface. Finally, user data can be mined and sent to the data thief.
- If a cell phone user's itemized bill shows evidence of additional or even missing calls, this may also be an indication of an attack, e.g. by a Trojan horse.
- Man-in-the-Middle attack: in this case, the attacker mimics a GSM base station. This is relatively easy to do, as no authentication to the mobile device is required. The attacker assumes a position between the mobile device and the mobile network and deactivates the GSM encryption.

Summary:
As GSM telephone calls are essentially insecure, sensitive information should not be exchanged willy-nilly via these mobile devices. There are alternatives which at least offer secure encryption via the air interface: GPRS, UMTS and the future LTE (Long Term Evolution). To provide better protection when using mobile devices, the BSI recommends not installing software from unknown sources and only installing and activating applications you actually need. IT security on cell phones can also be improved by configuring them sensibly. For example, local interfaces like WLAN (Wireless Local Area Network) or Bluetooth should only be activated when needed, and operated with the best possible security settings and the functions actually needed. When exchanging information that needs to be protected, you should always use cryptographic solutions that use a hardware security anchor (crypto smartcard or crypto module).

10 Cloud Computing

Cloud computing is a model that enables IT services (Software as a Service, Platform as a Service, Infrastructure as a Service) to be purchased and paid for fast, on demand on an online network at any time. The services can either be purchased from a Public Cloud, a Private Cloud or a Hybrid Cloud. In a Public Cloud, IT services are provided by a cloud provider and can be used by anyone with internet access. Alternatively, users can set up their own infrastructure and obtain the IT services from their own computer centers (Private Cloud). In a Private Cloud, all services and the infrastructure are controlled by the institution using the services offered. A Private Cloud can also be operated by third parties. These services can be accessed via the intranet or a VPN (Virtual Private Network). A Hybrid Cloud is a mixed form consisting of a Public Cloud and a Private Cloud.

The subject of Cloud Computing is very topical in the world of IT at the moment and has been gaining in significance worldwide in recent years. In Germany too, market researchers expect expenditure on cloud services to grow rapidly over the next few years. It is estimated that sales of cloud services in Germany will rise from €1.14 billion in 2010 to as much as €8.2 billion by 2015. This corresponds to an average annual growth in sales of 48 per cent.[8]

There are many reasons why interest in Cloud Computing and the use of Cloud Services are on the rise. Cloud Computing offers enormous flexibility in terms of booking, using and shutting down computer center capacity in line with actual demand. There is also massive potential for savings on IT systems that would otherwise have to be operated and maintained locally and replaced regularly. Another advantage is the ubiquitous availability of business applications regardless of the user's geographical location.

Opportunities versus risks

These potential benefits are offset by a series of risks associated with storing data and applications in a Public Cloud, including the following:

- Data and applications are kept off site and are therefore no longer accessible directly to in-house IT.
- Applicable guidelines and regulations such as data protection requirements could potentially be infringed if sensitive data is stored in a Public Cloud.
- Large numbers of unknown users share a joint infrastructure. This increases the risk of infringing the fundamental values of information security.
- Data and applications are accessed via the internet, so they cannot be accessed if the internet connection fails.
- If the interfaces provided by a cloud provider are insecure, vulnerabilities can be exploited to gain unauthorized access to data.

- Because of the extremely high complexity of Cloud Computing platforms, numerous security problems can arise such as data loss, unauthorized access to information, impairment of availability or even loss of services.

The BSI believes that the concept of Cloud Computing will gain a foothold in the market because of its technical and economic potential, provided the issue of reasonable information security is resolved. For as it becomes more widespread, the concept will become more attractive to attackers as resources are concentrated in central locations. Cloud Computing platforms are already being used to set up botnets, deposit malware, send spam or carry out brute force attacks on passwords. In addition, some cases have emerged of Cloud Computing platforms being targeted by DDoS attacks.

Summary:
The risk potential is expected to increase. For this reason, there is an urgent need to draw up and establish internationally recognized standards on the basis of which Cloud Computing platforms can be used and operated more securely and can be monitored and certified.

11 Smart Grid / Smart Meter

Since January 1, 2010, German law has required smart electricity meters to be installed in all new builds or major renovations that, unlike conventional meters, show the user the actual energy consumption and usage time. These new electricity meters should also be able to be read and controlled remotely. To encourage consumers to adopt more climate-friendly behavior, since the end of 2010 energy companies have also been obliged to offer more flexible energy tariffs based on grid load or time of day. "Smart Grid" is the term given to the move towards integrated, intelligent supply systems. This mainly applies to electricity grids, but it can also be applied to energy and water supplies in general. This development is well overdue in terms of electricity supply as there is an urgent need to manage the growing proportion of locally produced electricity being fed into the grid. In addition, it will also be important in the medium term to optimize electricity consumption patterns over time. This cannot be done with the existing hierarchical, electrophysical interconnected networks. Instead, new networked control technologies are called for.

The worldwide market volume for Smart Grid technologies could potentially be 100 times bigger than the internet, according to estimates by the US company Cisco Systems. The increasing complexity of electricity networks furthermore calls for new forms of whole-system protection against outages. These mechanisms are supposed to use networked IT systems, which in parts still need additional development and implementation work.

As energy and water supply systems are indispensable, the current very high level of security of supply will need to be maintained during this work. Supplies must not be put at risk by outages, faults or attacks on the IT infrastructures being implemented – and must be sufficiently robust even in crisis situations. Specific risks may also arise in future due to the fact that certain parts of the infrastructures will be networked in a complex way between different operators. This applies in particular if this networking takes place via information infrastructures that are used for very different applications with a large number of communication participants, or if the information is exchanged via the public internet.

Smart meters

Given the above, designing and setting up networks that can be controlled flexibly is the order of the day. We still have a long way to go before we see the introduction of integrated, intelligent supply systems: there is still a lot of fundamental development work to do in the sectors concerned. But the first steps are already being taken in the supply infrastructures, where various technologies are already being designed, built and even implemented. The BSI provides support for the development of the fundamental principles of intelligent electricity supply systems, thus ensuring that the most important aspects of IT security are taken into account. The introduction of smart meters will be a key element of supply infrastructure improvement . Because the smart meter processes and forwards personal consumption data and due to potential negative repercussions for the energy supply, there are high requirements for data protection and data security.

Summary:
Recent known hacking attacks on smart meters in the USA and hazards like Stuxnet have shown that urgent action needs to be taken in Germany to ensure that smart metering solutions are secure. The BSI will therefore be working with industry associations and relevant authorities such as the German Federal Network Agency (BNetzA) and the Physikalisch Technische Bundesanstalt (the National Metrology Institute Providing Scientific and Technical Services – PTB) to bring together the security requirements for smart meters in a special protection profile with a view to ensuring that all market participants meet compulsory data protection and security requirements. The intention is to publish a BSI-certified version of the protection profile by September 2011. The BSI will also be publishing a Technical Guideline which will set out the requirements for smart meter interoperability.

Conclusion

As IT penetrates into all areas of our lives and networks become ever more interconnected, we depend on it operating flawlessly. The BSI and other security agencies believe that the new hazards arising in parallel to this development, such as cyber attacks, attacks on mobile devices and attacks extending beyond conventional IT, represent a new, joint challenge to politics, industry and society in general.

Offers that provide reactive help to the federal administration, industry and private individuals are necessary and fulfill an important role. In order to effectively combat the threat potential, we will need to focus even more strongly on prevention going forward. In order to ensure a basic level of IT security and anticipate risks in advance as far as possible, it is becoming increasingly important to formulate security requirements for products and services and make these transparent to the general public. The BSI pursues this approach by formulating minimum standards, such as for Cloud Computing. This will create the technical basis for trusting secure IT and benefiting from its potential. Furthermore, manufacturer and service provider responsibility is increasingly in the spotlight.

Improving IT security is a goal that can only be achieved by working together effectively. Success in this area depends on cooperation between manufacturers, providers, security experts, security officers and, not least, users, whose awareness plays an important role in implementing widespread security measures.

BSI – Focusing on IT Security

With the coalition agreement and the BSI Act of August 2009, the German federal government has responded to the demands of IT security and has assigned the BSI a stronger role as a designer and provider of IT security services. The coalition agreement also emphasizes the BSI's duty to promote self protection and encourage the use of secure IT products.

Education and Awareness Raising

The BSI has been active in Education and Awareness Raising for many years. For example, it operates the BSI Information Portal for the general public: the website www.bsi-fuer-buerger.de is still the BSI's most important source of information for private users. Since February 2011, the public has had access to a revised and improved offering which provides detailed and easy to understand information on IT security and makes it easier for people to protect their computers.

Working Together

Education and awareness raising on the subject of IT security has many different faces. Exchanging information and ideas and cooperating with partners and disseminators are therefore particularly significant. For this reason, the BSI is represented on the advisory board of Deutschland sicher im Netz e.V. and supports the Anti-Botnet Advisory Center run by the eco-Association of the German Internet Industry, which opened in the fall of 2010. At the international level, the BSI is a member of the Awareness Raising Community of ENISA (European Network and Information Security Agency), and takes part in the European Union's annual Safer Internet Day with awareness-raising campaigns.

IT Security Provider to the German Federal Government

As the central IT Security service provider to the German federal government, the BSI is improving the level of IT security within the federal administration. In particular in the event of IT crises of national significance, it is vital to ensure that the federal government can continue to operate and take decisions by providing prepared information and competent analyses. With this in mind, several steps have been taken: an IT Crisis Response Center for the federal government has been set up at the BSI, the amendment to the BSI Act has established the BSI as a central reporting point for IT security incidents, and an IT crisis management department has been set up for the federal administration. So the administration now has an early warning system in place which enables assessments to be made and crisis response processes to be defined and practiced in accordance with crisis management principles.

Working Together in IT Crises

A targeted and complex attack like Stuxnet has long since been the subject of theoretical discussion. But now, for the first time, there is actual proof of the fact that with the right financial input and technical preparation, protective mechanisms can be evaded and circumvented. We need to be able to respond to this new quality of attack, since attack mechanisms as used by Stuxnet are not oriented towards the conventional task-sharing of German authorities. Stuxnet proves that even closer coordination between authorities and more intensive collaboration with business and industry is needed. For this reason, in 2011 the federal government adopted the

Cyber Security Strategy, which provides for the establishment of a Cyber Defense Center headed by the BSI and with the direct participation of the Federal Office for the Protection of the Constitution and the Federal Office of Civil Protection and Disaster Assistance, along with other authorities. There are also plans to expand cooperation with business and industry.

Trusting the Security of Technology

People will only use the possibilities and potential offered by IT and the internet if they trust the security of the technology concerned. Quality marks from authoritative sources and established IT security standards form the basis for this trust. With IT security standards in mind, the BSI is taking part in forward-looking projects like smart meters (intelligent energy supply meters) and Cloud Computing. For smart meters, the BSI is working with industry and data and consumer protection organizations to develop a joint protection profile. The aim of this profile is to achieve a reasonable level of security which adequately takes account of functionality as well as data protection and IT security. It is also working with manufacturers to produce minimum security standards for Cloud Computing. In addition to this, BSI certification ensures that compulsory safety standards for products are guaranteed and implemented.

Two important projects in which the BSI played a key role on the technical implementation side and which represent a step forward in terms of secure online communication and interaction are the new German ID card and De-Mail. De-Mail enables legally binding documents and messages to be sent confidentially via the internet. It increases the security of electronic communication compared with conventional methods. The main security goals of confidentiality, integrity and authenticity in De-Mail communication are guaranteed with defined security measures. De-Mail enables the identity of the communication partners and the delivery of the De-Mail to be proved. The content of a De-Mail cannot be intercepted or changed on its journey through the ether.

In the new ID card introduced in November 2010, German citizens have more than just a new credit-card format identity document. This card also has various electronic functions which greatly improve security on the internet. These include the eID, electronic ID which people can use to prove their identity beyond doubt. A radio frequency chip (RF chip) integrated into the card contains all the information that is also displayed visually on the document. In addition, the QES (Qualified Electronic Signature) function enables the user to sign documents and declarations of intent online in a legally binding way.

Critical Infrastructures (KRITIS)

A particular focus of our collaboration with industry concerns the protection of critical infrastructures – a responsibility shared by the operators and the state. The BSI and operators of critical infrastructures in Germany have been working closely together since 2007 within the framework of the KRITIS Implementation Plan to discuss new threats and strategies and implement new measures. Exercises are held regularly to prepare for incidents. One of the most important exercise formats is the LÜKEX (National Crisis Management Exercise). The KRITIS companies will be working intensively on this in 2011, as an exercise on the loss of major IT systems and crisis management in this emergency situation is due to take place this year.

Bibliography

[1] Secunia Yearly Report 2010

[2] http://gs.statcounter.com/press/firefox-overtakes-internet-explorer-in-europe-in-browser-wars

[3] Trend Micro September 16, 2009 http://blog.trendmicro.com/the-internet-infestation-how-bad-is-it-really/

[4] Damballa 14 February 2011 http://www.damballa.com/knowledge/Feb2011report.php

[5] BITKOM press release, August 15, 2010

[6] BITKOM press release, February 14, 2011

[7] BSI surveys

[8] BITKOM press release, October 6, 2010

[9] Arbor Worldwide Infrastructure Security Report 2010

List of illustrations

Imprint

Published by

Federal Office for Information Security – BSI
53175 Bonn, Germany

Text and Editorial Staff

Federal Office for Information Security
DauthKaun Public Relations

Layout and Design

DauthKaun Werbeagentur

Printed by

Durckpartner Moser, Rheinbach

Date

Mai 2011

Article Number

BSI-LB11502

Distribution Office

Federal Office for Information Security – BSI
Godesberger Allee 185 – 189, 53175 Bonn, Germany

Section 321, Information and Communication, Public Relations
Tel.: +49 228 99 9582-0, E-mail: publikationen@bsi.bund.de
internet: www.bsi.bund.de