Federal Office
for Information Security

The State of IT Security in Germany 2014

Table of contents

Foreword

The 2014 report on the state of IT security discusses the quality and quantity of the threats and risks facing information technology (IT) in Germany. The report draws on the comprehensive information about IT threats, attack vectors and vulnerabilities, as well as specific IT attacks, which is collected and evaluated every day by the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI).

The threat situation to which IT is currently exposed remains critical given the attack potential reported below. The most widely used IT systems contain large numbers of vulnerabilities, and the existing tools for exploiting these vulnerabilities are available to ever more attackers, who are only too willing to use them for their own purposes under the cloak of anonymity provided by global cyberspace. These attacks have many different motives. Their targets include ordinary citizens, government bodies, research institutes, business enterprises and also the operators of critical infrastructure in Germany.

Unquestionably globalisation, driven forward at an ever increasing rate by information technology, has exacerbated competition for resources, markets and political influence. It would be naïve to assume that newly created digitally interconnected technologies will not also be exploited in the furtherance of disputes in economic, social and political arenas. Indeed, it can be seen that businesses and administrative bodies are increasingly falling victim to highly skilled IT attacks which are executed with great professionalism and can draw on ample resources. Such attacks are usually hard to detect and defend against. Frequently a worrying time window opens up between attack and detection thereof, during which the successful attacker enjoys unhindered, unobserved access to the IT systems concerned.

Information technology innovation proceeds at a breakneck pace. Due to the enormous economic potential involved, this innovation drives correspondingly rapid changes in the IT landscape in every industrial sector and social sphere. Cloud computing, mobile systems and the opportunity to evaluate information using Big Data fuel economic growth, while on the other hand opening up new vulnerabilities to IT attacks which cannot be adequately addressed using conventional IT security tools. Accordingly, IT innovation must go hand in hand with the evolution of security mechanisms designed to ensure that defenders succeed in keeping pace with the technology employed by their attackers.

Successful IT security demands independent initiative and skill. The activities of foreign intelligence agencies uncovered in 2013, as well as millions or even billions of cases of identity theft, have led to a crisis of confidence in the Internet. Although awareness of this issue has increased greatly, both private and professional users ever more frequently feel powerless against these seemingly overwhelming threats. This sometimes leads to a mood of resignation and failure to make full use of the effective security measures which are available and which do afford an impressive level of protection against up to 95 per cent of all attacks. As a result, potentials remain untapped, thus unnecessarily exacerbating the IT security situation.

This threatens to create a vicious circle of self-fulfilling negative prophesies which needs to be broken. The standardisation, certification and transparency of key functions are vital to restoring and building up users' confidence in IT security. Germany has a broad, highly skilled technological base in this respect, with an IT security industry dominated by SMEs. The challenge is to effectively exploit this favourable situation to the benefit of the German economy in the face of the impending digitalisation of every aspect of our everyday and business lives and to create a positive climate for IT security measures. IT security may come at a price but it is bound also to be rewarded in the marketplace.

What I would like to see is for business and government to redouble their efforts to promote wider-ranging security technologies and encourage their use. To this end the federal government is fostering the dissemination of basic security infrastructure through such measures as Internet identity verification based on the new identity card, De-Mail

and the smart meter profile. We are encouraged by the various forward-looking enterprises who have built on these measures to implement smart and creative solutions and augment applications with scalable IT security in order to vigorously combat the IT risks faced by a digitalised world.

Meanwhile, the envisaged IT security law will form a further tool in providing better protection for vital IT infrastructure. The BSI's character as a civil, technical-preventive agency has proven its worth over the past 20 years, and because of this its role in our cyber security architecture is to be further reinforced. As a trusted expert body the BSI will perform an advisory and accrediting IT security function in the field of critical infrastructure. To speed up response times, exchanges of information on threats and attacks on IT systems are also being intensified. It will only be possible to ensure that reliable and appropriate security measures for information technology in Germany are in place if a cooperative working relationship and partnership between business and the government can be guaranteed. The BSI faces corresponding challenges both for its professional expertise and its role as a coordinating body working with the various other federal and state security agencies.

I am convinced that the BSI's robust organisational structure will enable us to create an improved security situation despite the ever-growing threats emanating from cyberspace.

Dr. Thomas de Maizière
Federal Minister of the Interior

1 Information technology: interconnected, complex, pervasive

1 Information technology: interconnected, complex, pervasive

Digitalisation features three central characteristics from which the challenges facing information and cyber security derive:

1. Technological permeation and interconnection: all physical systems are embraced by IT and connected step by step with the Internet.
2. Complexity: the complexity of IT increases significantly as a result of vertical and horizontal integration into the wealth creation processes.
3. Pervasiveness: every system is available practically all the time and in any place via the Internet.

Technological permeation and interconnection

The information technology of today is characterised by its powerful, value-adding capacity for integration into virtually any technological system, thereby driving the continuing digitalisation of the world we live in. Attractive features and prices help develop a market for private users, while mobile solutions and applications on intuitive end devices also open up promising development opportunities in the professional sphere. The rapid adaptation of such solutions in business and industry means that the boundaries between the private and professional use of IT disappear. This also leads indirectly to the traditionally strictly segregated IT networks operated by companies becoming ever more open to the Internet. This applies not only to office communication but also to manufacture and production.

How far this wide-ranging interconnection of different systems extends may be illustrated by taking a look at the factory of the future, which goes by the name of 'Industry 4.0'. With the objective of making as much information as possible digitally useable, the entire company's digitally enabled systems are networked with each other both internally and externally: the machines, sensors and field devices in the production facilities, enterprise resource planning (ERP) systems, marketing, sales and purchasing. Along the value chain too the ongoing interconnection of IT systems with supplies, customers and service partners will be fostered. This trend will continue to shape technological development within companies, with some 11 billion euros of Industry 4.0-related investment expected in Germany between now and 2020[1]. No business will be able to opt out of this trend, because the efficiency and productivity gains achievable through Industry 4.0 will have to be harvested if the business wishes to remain competitive.

A consequence of this rapidly progressing digitalisation and interconnection is that the protection of IT networks and IT systems at a company's perimeter is becoming ever more eroded and new attack interfaces are opening up. In addition, IT systems hitherto unreachable from the Internet are becoming potential targets. For IT security this entails a far more complex risk situation, as well as holding out the prospect of an increasing risk of existence-threatening situations due to the breakdown or malfunctioning of production or business processes.

IT complexity

The interconnection of all systems and things, creating an Internet of things, coupled with the digitalisation of physical systems (cyber-physical systems) greatly increases the complexity of the digital infrastructure. Today many household appliances, building control systems, threat and fire alarm systems, traffic systems and automobiles are interconnected and linked with the Internet. A trend now foreseeable for the near future is the emergence of the digitally enhanced smart city.

As the complexity of systems increases, familiar conventional IT security mechanisms rapidly reach their limits and become incapable of guaranteeing the accustomed degree of reliability and manageability. The need for innovative approaches designed to ensure an adequate level of IT security for the entire system is already apparent, and it will only increase over the coming years.

Pervasiveness through smartphones

Innovation and change are inextricably linked with modern information technology. However, even in the IT industry the extent of the smartphone boom is unrivalled, having been sustained over a period of many years. Smartphone and tablet users now number in the billions, as the devices exert a huge influence over the daily lives of their owners. The smartphone is not just a wireless extension of established PC technology, rather it involves the bundling of a whole array of technological and conceptual considerations which, taken together, delineate a new, self-contained sphere of information technology. Our existing IT security knowledge and techniques are not directly transferable to this sphere and will have to be rethought and adapted.

A standout feature of smartphones is that they are always on, with a continuous broadband Internet connection and incessant device activity even without any intervention by the user. Furthermore, most smartphones are taken by their users wherever they go and provide a detailed record of their whereabouts and the communications they engage in. In future the smartphone will evolve into an electronic wallet with which people will be able to make payments both over the Internet and directly at the checkout via a radio link, and then, if not before, we shall have to address the question of the actual effectiveness of the security systems with which this mobile platform is equipped. As a rule smartphone users are reliant upon the operating system's security mechanisms cutting in. There is little scope left for users to take individual action to strengthen security, such action being largely confined to the secure configuration of the devices.

Not only the device itself but also the 'economic system' to which a smartphone is assigned play a central role in its IT security. This overall economic system comprises not only its operating system but also an array of background systems such as the app store, content download platforms and cloud-based backup systems offered by that provider. The self-contained nature and central management of this 'ecosystem' do offer a degree of basic security that cannot be achieved in the traditionally open world of the PC without additional protective mechanisms, but it is not transparent for users, and there is no provision for scalability where security needs may be greater. As a key component in the system's overall economy, security thus forms the foundation for the bundled marketing of goods and services and is therefore a principal objective for providers.

Among the factors driving the success of smartphones as a product category, the app takes pride of place. It represents the true quantum leap, because it means that acquiring a smartphone opens up for users access to millions of application programs via online marketplaces such as the Apple App Store, Google Play or the Microsoft Windows Phone Store.

Furthermore, smartphones not only facilitate the acquisition of software but also lower the bar for those wishing to take the plunge and become software producers to such an extent that over one hundred thousand providers are now represented on the various online marketplaces. To add to data privacy law considerations, apps pose the greatest potential for attack from an IT security viewpoint. The operating systems themselves are comparatively well protected, whereas what apps can do in the operating system is authorised by the users themselves. However, this kind of authorisation procedure is largely ineffective since in the great majority of cases requests are accepted by users without giving the matter any thought.

Pervasiveness via clouds

Cloud services provide processing and storage of information centrally via a network plus standardised interfaces. They outsource applications, computing power and storage from (mobile) devices to cloud data centres. The key benefits of cloud services are that often complex functions are offered in a recylable way by a central agency, managing the services is easier and can readily be scaled, while computing power is outsourced from the device to the data centre. Taken together these considerations can generate significant economic benefits.

Smartphones, tablets and apps now offer a variety of different interfaces with the cloud services offered by the various mobile systems and third-party providers. These services also allow such things as the synchronisation of contacts, appointments, e-mails, photos and documents on different devices. This means that some of the information stored and processed in the cloud is highly personal. However, there is no certainty that the data stored are both secure from unauthorised access and will be permanently accessible. As a rule cloud service providers' general terms and conditions largely disclaim liability for the data entrusted to them.

Accordingly, before a business chooses to use cloud services those in charge first need to address various questions. For instance, what information is suitable for cloud processing and storage, and whether this is permissible given compliance requirements, in particular concerning data privacy. More and more cloud service providers are setting up shop in this booming market and it is not easy to identify a trustworthy provider who complies with the company's own security requirements. The opportunity to benefit from economies of scale must than be set against a loss of control over the company's own information.

Outlook

For many private users the smartphone has become the linchpin of their access to worldwide information and services. The future integration of payment and health functions as well as home automation interfaces means that the boundary between the physical and virtual worlds will become increasingly blurred. As a result issues surrounding the security of mobile devices and their commercial ecosystem will become ever more relevant.

In a business context, from an IT security viewpoint issues other than mobility also have to be taken into account. The use of cloud-based information processing holds the promise of speed gains and cost savings, but is still often viewed with suspicion on organisational, technical and security-related grounds. Furthermore, companies using industrial control and automation technology are impacted by the convergence of this technology with classical information and communication technology, including mobile use, and this throws up a whole new raft of IT security challenges.

2 Security threats

2 Security threats

The increasing digitalisation and interconnection of many aspects of our private and working lives goes hand in hand with dynamic security threats. The causes of cyber attacks, attack methods and the use of attack tools evolve on a daily basis, all the while interacting and influencing each other in complex ways.

2.1 Causes

Cyber attacks targets companies, governments and private users are a daily occurrence. Many attacks are successful, both because the attackers are becoming increasingly professional and because they encounter circumstances which they know how to exploit to their advantage.

2.1.1 The Internet as a platform for attacks

The Internet is used as a platform of attack on account of its open structure, as well as the technical opportunities and anonymity it offers. This is reflected today in the huge number of cyber attacks. To launch a successful cyber attack all you generally need are a PC and an Internet connection. These modest investments can be set against a multitude of opportunities to make money through criminal activities, to acquire confidential information or to engage in acts of sabotage. The necessary attack tools and methods are cheap and easy to acquire. There is a thriving global market on which attack tools, vulnerabilities, malware or even website traffic can be purchased or ordered as a service (malware as a service). Illegally acquired data such as user account details and credit card information are also traded there, with both well-organised groups and individuals offering their skills and services on these criminal online marketplaces. The Internet's attractiveness as a platform of attack may be illustrated by the following factors which attackers exploit for their own ends:

- The increasing interconnection of information technology permits remote attacks from virtually anywhere in the world at any time and on ever more targets. As a result attackers do not have to take any direct risks at the scene of the crime.
- The increasing complexity of technology coupled with a frequent lack of security awareness leads to inadequately protected systems, increasing the prospect of a successful cyber attack.
- The careless exchanging of information over the Internet and the always-on status of mobile systems facilitates access to sensitive information.
- The decentralised, open structure of the Internet gives attackers a wide range of concealment opportunities which minimise the risk of discovery.
- Varying legal frameworks in different countries make criminal prosecution more difficult.

The professionalisation and separation of roles in the field of cybercriminality are steadily increasing. Thus the work involved in a cyber attack may be divided up among different people or groups who specialise in certain tasks which they perform independently of each other. These groups include:

- Hackers, who seek out new vulnerabilities in widely used software products and offer them for sale.
- Developers who design and adapt malware or tools for the generation of malware which can then exploit these vulnerabilities.
- Attackers who use this malware to steal information.
- Criminals who sell, exploit or make money from the use of the stolen information.

Thus even inexperienced attackers with no technical expertise can carry out or arrange the carrying out of professional attacks on a chosen target without having to concern themselves with the technical details or the execution of the attack.

2.1.2 'Digital carelessness'

In the wake of media reports about the Snowden revelations, cyber attacks on well-known companies and the associated loss of customer data, coupled with incidents involving large-scale identity theft, many users have lost confidence in information technology. Consumers appear to be increasingly aware of the issue of IT security. A study published by the German Institute for Trust and Security on the Internet (Deutsches Institut für Vertrauen und Sicherheit im Internet – DIVSI)[2] has confirmed that the German public's confidence in the Internet has significantly deteriorated. However, these concerns stand in contrast with the apparent carelessness which continues to be observed, both in business and private IT use. Despite increased awareness [of security issues] and loss of confidence [in the Internet], there has only been a very slight increase in numbers taking practical steps to improve their security. For instance, the uptake of e-mail encryption remains very low[3]. Solutions are available, but they frequently do not meet user requirements in terms of convenience, intuitiveness and ease of operation, and these factors are often decisive in determining whether or not such solutions catch on.

Where users have been duped through social engineering, it is once again convenience, or the prospect of an ostensible benefit, which induces them to disclose personal information or run malware. Every day we are inundated by waves of professionally produced spam and attempts to access personal data using fake websites, e-mails or texts. Often the spam fraudulently claims to be from well-known companies or institutions in order to induce recipients to click on a link or file attachment, thereby infecting their computers with malware. In the field of mobile communication, too, convenience is the main criterion when users install and run smartphone apps without considering the consequences. Furthermore, basic security measures such as effective patch management, whereby available security updates of programs are downloaded as soon as possible, are still often neglected.

Even if people are aware of the threats they face they do not always take appropriate security measures. This applies not only to private users but also to many small and medium-sized enterprises (SMEs). Thus we find that the systems used by SMEs[4], like those of private individuals[5], frequently have insufficient protection to fight off even the simplest attacks. However, the level of defensive and protective measures found in networks and associated infrastructure in Germany is very variable, with the networks of major enterprises generally having appropriate protective measures in place. Despite this, according to a survey conducted by the Alliance for Cyber Security (Allianz für Cyber-Sicherheit)[6] companies report growing threats from data theft attacks and targeted attacks by cybercriminals or government attackers. The main reason cited for attacks proving successful was software vulnerabilities. However, a patch management system was in place at only three quarters of the companies surveyed. Over half of the surveyed companies admitted that the measures currently in place to protect themselves from cyber attacks are not sufficient and that additional measures are planned in the medium term. It is disturbing that the majority of surveyed companies assign less than five per cent of their total IT budgets to IT security measures.

Alongside all these technical protective measures, user behaviour is another key factor for enhancing Internet security. The increasing complexity and mobility of information technology means it is ever more important for users, manufacturers and service providers alike to foreswear 'digital carelessness', address IT security issues promptly and conscientiously and convert their concerns into practical action.

2.1.3 Vulnerabilities

Vulnerabilities are the basis for the development of cyber attack tools and the reason why cyber attacks can succeed. As in earlier years, in 2013 and 2014 the number of critical vulnerabilities found in standard IT products remained high. In 13 widely used software products alone (see Table 1) 705 critical vulnerabilities were identified in 2013, and in 2014 the BSI is expecting over 700 more (Figure 1). Vulnerabilities are inevitable in modern software. Developing bug-free software is a practical impossibility outside of highly restricted specialist areas. For this group of widely used products alone the detection of an average of two critical vulnerabilities per day can be expected.

Given the sheer number of vulnerabilities manufacturers' software updating systems are of great importance. Manufacturers are increasingly forced to prioritise when eradicating vulnerabilities, concentrating on the critical ones.

Details of vulnerabilities generally do not emerge until after the software manufacturer releases the corresponding security update or patch. Accordingly it is vital to download these software updates as quickly as possible. If details of the vulnerability, or even exploits of a given vulnerability, enter the public domain before the soft-

ware manufacturer's patch comes out (zero-day exploits), great care should be taken if using the affected software. Up to the end of July there had been five known incidents of this nature in 2014.

Software products

- Adobe Flash Player
- Adobe Reader
- Apple OS X
- Apple Quicktime
- Apple Safari
- Google Chrome
- Linux Kernel
- Microsoft Internet Explorer
- Microsoft Office
- Microsoft Windows
- Mozilla Firefox
- Mozilla Thunderbird
- Oracle Java/JRE

Table 1: Selection of widely used software products

2.1.4 Using out-of-date software and unpatched systems

Downloading software updates is fundamental to maintaining a secure IT system. Despite this, operating systems and applications with out-of-date patches are the most common problem identified by BSI audits and penetration tests of government departments, and many private users' systems are not always fully up to date.

Despite the standard recommendation to use auto-update mechanisms, according to IT experts at least ten per cent of all Windows operating systems and other widely used software products in Germany have out-of-date patches[7], and this figure should be regarded as a minimum.

Unpatched systems are not only a problem for desktops, they also afflict servers and mobile devices in a similar fashion. For instance, in February 2014 six million websites[8] worldwide were using the outmoded, easy-to-attack Version 1.3 of the Apache server software. Meanwhile, in the mobile sphere Android devices in particular are frequently found to be running on outdated versions of operating system[9]. Many manufacturers of devices only provide their updates for brief periods. Support for older versions is discontinued at the latest when the annual successor model appears. Once that happens patches are no longer produced for newly discovered vulnerabilities, which thus pose a threat to all older devices.

As a general rule, software products for which product support has been discontinued should no longer be run because these products have stopped receiving security updates. A recent example is Microsoft Windows XP, for which extended product support ceased in April 2014, since which time neither functional nor security updates have been produced for Windows XP. Despite this, the market share of Windows XP in Germany by mid-2014 still stood at over eight per cent, while the worldwide figure is over 15 per cent[10].

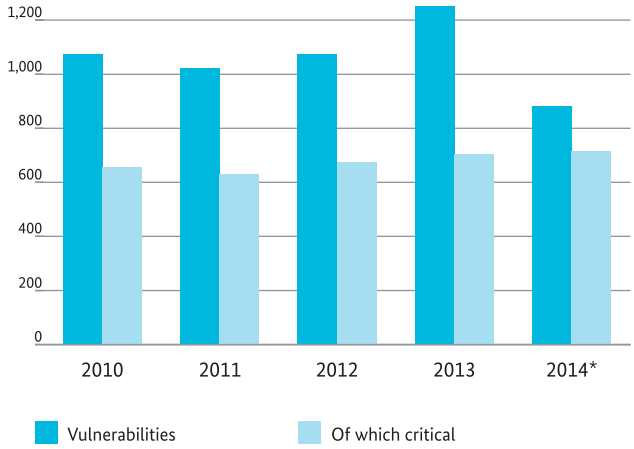

Figure 1: Total number of vulnerabilities in the listed software products
*The figures for 2014 are estimates based on the number of vulnerabilities detected up to September.

Typical security deficits

The BSI conducts regular security checks, penetration tests and information security audits of government departments. Among the security issues most frequently encountered are:

» Out-of-date operating systems and application patches and deactivation of available security mechanisms.
» Easy-to-guess passwords are used, even for critical applications. Not infrequently standard passwords, empty passwords or other weak passwords are used.
» Network management and monitoring measures are either non-existent or used as isolated solutions, log records are kept locally only and merely manually evaluated should the occasion arise.
» No use of network management controls (including for maintenance access and connections) designed to restrict access to the internal network to authorised official devices only.
» Interface controls are missing for mobile storage media, and unencrypted mobile devices.
» Changes are made to applications, operating systems and networks without any suitable change management or documentation.
» Training and awareness-raising activities, in particular for users, either do not take place or are insufficient.
» Responsibilities for information security among company directors, government department heads or senior management are often unclear.
» Security concepts are incomplete and inconsistent.

2.1.5 Mobile devices

Classical desktop and laptop computers are increasingly being complemented or even replaced by smartphones and tablets. Mobile devices represent an attractive target for attacks because they usually reflect the entire 'digital lives' of their owners, from e-mails to social media, flight tickets, banking or location information. Alongside the risks of loss or theft, they pose special IT security challenges in terms of operating system updates and apps. Due to rapid developments in the hardware sphere software updates are often available only for short periods, after which vulnerabilities are no longer be fixed. A further threat arises from the bewildering variety of available apps, which not infrequently contain malicious and espionage features. Due to its open approach Android is particularly susceptible to these.

Particularly when using mobile devices people want to be able to access their data whenever and wherever. As a result sometimes very personal information is stored in a cloud, and if access to the cloud is inadequately protected this information is at severe risk, as for instance demonstrated by a recent incident in which intimate photos of celebrities were stolen from the iCloud and published on the Internet.

Threats to mobile devices increasing steadily

Reports from all producers of antivirus software indicate that the amount of malware targeting mobile devices is steadily increasing. In addition to established attack methods of the kind directed at PCs, the 'always on' nature of mobile devices opens up further attack opportunities:

» **Infection with malware via apps**
Alongside their ostensibly useful features apps may also conceal malicious code. For instance Trojans which masquerade as apps while actually gathering information in the background, sending costly text messages at the user's expense or making undesired phone calls.
» **Use of public hotspots**
Most public hotspots do not offer encryption. The data are transmitted openly and can thus be read by unauthorised third parties. Particularly risky here are online banking or the transmission of confidential information.
» **Surveillance and data theft**
The location of mobile devices, and therefore their owners, can be traced at any time not only by the operators of wireless networks and app providers but also by cybercriminals who have access to the device. Smartphone surveillance coupled with the theft of information such as passwords, images, log files and GPS coordinates allows criminals to compile comprehensive profiles of their victims.
» **Tapping phone calls**
Calls made via the GSM standard for mobile voice and data transmissions are not safe from eavesdropping, meaning that sensitive or secret information may fall into third-party hands.

2.1.6 Inadequate security for Industrial Control Systems

Production and process automation systems, collectively known as Industrial Control Systems (ICS), are deployed in virtually all infrastructure in which physical processes take place. Implementing Industry 4.0, one trend is towards the extended interconnection of these Industrial Control Systems beyond a company's internal networks.

As a result IT components become ever more integrated into the actual production networks in order to render industrial processes more efficient and effective on a global scale. However, few of these systems were designed with potential attacks in mind.

Threats to Industrial Control Systems in industry and manufacturing

Production and process automation systems are increasingly susceptible to cyber attack. Operators have to bear in mind the risk and harmful potential not only of non-targeted malware but also of targeted, high-quality attacks on ICS infrastructure which are mounted at significant expense.

The central threats to which ICSs are currently exposed are[11]:

1. Infection of control components with malware via office networks
2. Infiltration of malware via removable storage media and external hardware
3. Social engineering
4. Human error and sabotage
5. Unauthorized use of Remote Service Access

Alongside attacks which succeed due to software implementation errors, social engineering plays an ever greater role. In this method largely non-technical contrivances are used to gain unauthorised access to information or IT systems, exploiting human proclivities such as helpfulness, curiosity, trust or fear. To combat this, measures such as raising awareness and training are further key components of any effective ICS security system.

Moreover, from this appraisal of the most significant threats facing Industrial Control Systems it is apparent that devising IT security systems, architectures and standards will be key factors determining the success of efforts to implement and secure acceptance for Industry 4.0.

2.2 Attack tools and methods

Tools and methods used in cyber attacks today are manifold. They are deployed and combined in myriad ways to launch both broad-based and highly targeted cyber attacks against individuals or institutions. This section discusses the attack methods in current use, outlines the current situation and offers brief assessments of each method.

2.2.1 Spam

Spam is defined as unwanted messages sent en masse and in an untargeted fashion via e-mail or other communication services. In harmless variants spam messages generally contain unsolicited advertising. However, spam often comes with attachments containing malware, links to websites with drive-by exploits, or it may be used for phishing attacks. To send out spam messages large-scale resources such as botnets or compromised servers are required.

Situation

- 2014 saw major growth of around 80 per cent as compared with 2013, bucking the trend of recent years in which spam volumes had stagnated (see Fig. 2).
- Germany is midway down the Top 10 in the global list of spam senders.
- 2014 saw a 36 per cent rise in e-mails with malware in the attachments.
- Since the beginning of 2014 a trend towards the generation and sending of pseudorandom malware variants has been observed.
- Criminals increasingly send Office documents as attachments, with malware being downloaded via macros in these documents.
- Due to identity theft spam is increasingly sent via compromised user accounts utilising established e-mail service providers.

Assessment

Spam is a long familiar phenomenon, and countermeasures such as spam filters or greylisting have generally reduced its volume. As a result, these days spam is largely unproblematic from an operational viewpoint. However, the quality and quantity of malware spam are continuing to increase. The one-time use of malware code variants increases the cost of analysis and slows down the provision of suitable defensive measures such as signatures for antivirus programs.

2.2.2 Malware

Malware programs are tools whereby attackers can exercise control over an infected system. Malware comes in a variety of forms, such as viruses, Trojan horses, bots and rootkits. However, modern malware is often difficult to unambiguously categorise as it is modular in structure and embodies or even downloads a variety of different malicious functions. Today malware affects not only classical PCs and notebooks but also increasingly mobile platforms such as smartphones and tablets.

Situation

- The total number of PC-based malware variants is now estimated at around the 250 million mark.
- In Germany there are at least one million malware infections a month.
- The number of malware variants increases at a rate of about 300,000 a day.
- The most common ways of spreading malware are drive-by exploits, spam attachments and botnets.
- The most frequently detected malware types are adware and Trojans.
- Microsoft Windows is by far the operating system most frequently affected by malware, accounting for around 95 per cent of all instances.
- Mobile platforms: at least three million malware programs exist for mobile devices such as smartphones or tablets. 98 per cent of these are designed for the Android operating system.
- Malware for mobile platforms usually masquerade as legitimate apps. They are predominantly distributed via alternative app stores or websites rather than official app stores like Google Play, or are installed unwittingly by the users themselves.
- Attackers' deployment of malware is increasingly professional, for instance involving improved methods of concealing the control servers, the use of Twitter channels or Google Docs as command-and-control (C&C) servers, as well as the use of cutting-edge encryption techniques such as elliptic curve cryptography to safeguard the communication.
- Alongside classical malware which steals data or manipulates online banking activities, ransomware, malware which blocks access to systems or encrypts user data in order to then extort 'ransom money', has become a further everyday tool in the cybercriminal's arsenal.

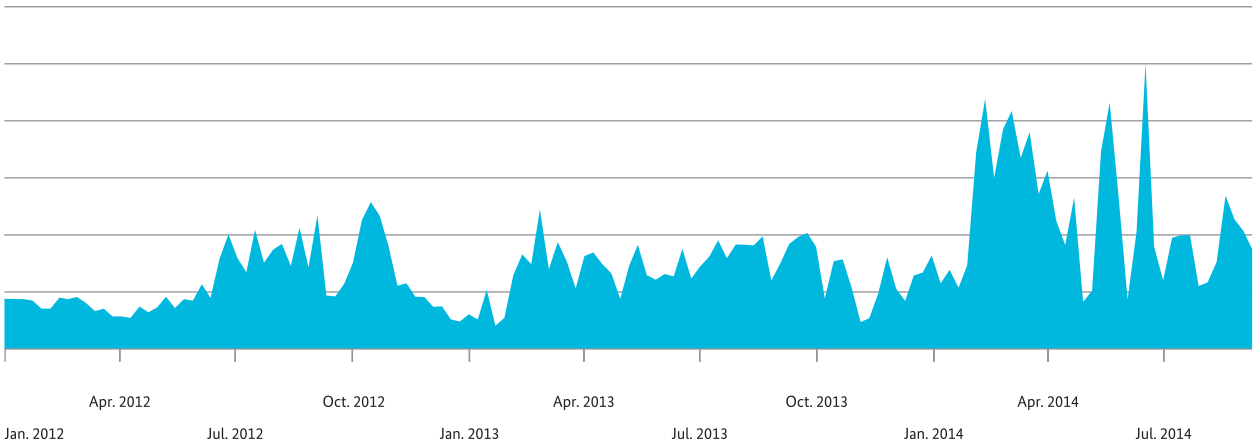

Figure 2: Qualitative weekly spam figures in Germany since January 2012

Assessment

Due to the sheer volume and complexity of new malware programs the time which elapses before new malware is detected by antivirus programs ranges from a few hours to several days. During this window a system may be unprotected. As a result the classical signature-based components of antivirus programs are increasingly reaching the limits of their effectiveness, meaning that the ongoing evolution of novel protective measures will be needed. Furthermore, malware developers put a great deal of ingenuity into coming up with a steady stream of new methods designed to hamper the manual analysis of malware and incidents by analysts and forensic scientists.

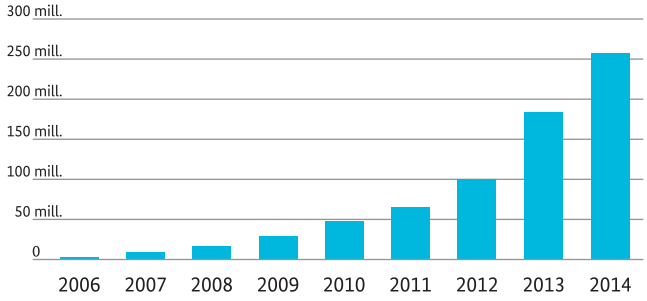

Figure 3: Number of Windows malware variants

2.2.3 Drive-by exploits and exploit kits

The term drive-by exploit refers to the automated exploitation of vulnerabilities when a prepared website is visited. It involves the exploitation, without any user interaction, of vulnerabilities in the browser, in plug-ins or in the operating system to enable the undetected installation of malware on the website visitor's system. Drive-by exploits are particularly effective when utilised in the form of exploit kits involving the use of not one but several exploits which automatically seek out multiple vulnerabilities in the browser or its plugins and use them for the installation of malware. In watering hole attacks drive-by exploits are used to execute targeted attacks.

Situation

- Drive-by exploits are placed either on large numbers of compromised websites or individually targeted ones.
- An evaluation of Google Safe Browsing data[12] indicates that the proportion of websites in Germany in the past 12 months infected with drive-by exploits or other means of distributing malware stood at four per cent.
- In recent months exploit kit attacks have most frequently been directed at vulnerabilities in Internet Explorer, while Oracle Java has also been a popular attack target, albeit not to the same extent as in 2013.

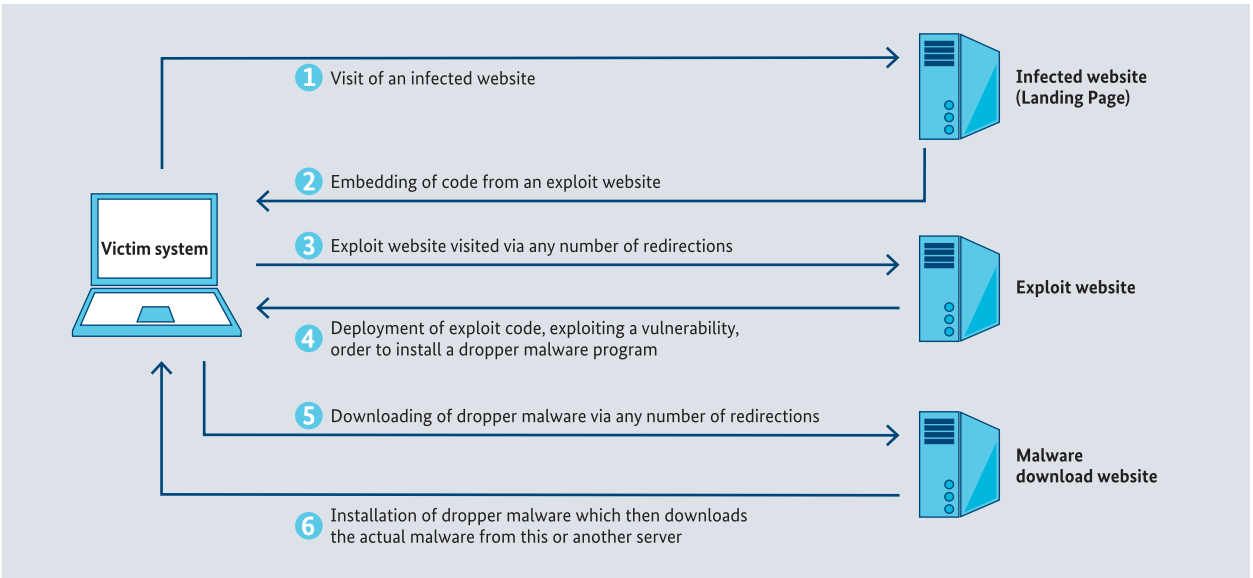

Figure 4: Example of a malware infection via drive-by exploit

Assessment

Exploit kits play a central role in cyber attacks of a criminal nature. An exploit kit integrated into a popular website will swiftly infect a large number of vulnerable systems without the knowledge of or any action by the user. In this kind of broad-based or untargeted attack method the victims are infected with a variety of malware, for instance ransomware designed to extort money, Trojan horses for identity theft purposes as well as bots to develop the infrastructure for sending spam or launching DDos attacks. Currently the various manufacturers have produced security updates for all the vulnerabilities used by exploit kits, in view of which efficient patch management should permit the thwarting of any exploit kit attacks. Utilisation of zero-day exploits in exploit kits are a rarity.

Malicious advertising banners

In 2013 the BSI identified over 350 compromised OpenX servers hosted in Germany from which malicious advertising banners were being superimposed over website images. The malicious code which came with the advertising banners was indicative of drive-by exploits. At potential risk were any visitors who had not installed the latest security updates for the Windows operating system or such software as Oracle Java, Adobe Reader or Flash Player. When users visit the website the infection occurs unnoticed and without any user action: they do not even have to click on the malicious banner.

Some of the OpenX servers were operated by media agencies, as a result of which some of the websites on which malicious banners appeared were popular ones with several thousand visitors a day. The BSI notified the website operators, OpenX servers and responsible providers about the compromises[13]. In some cases BSI had to do so several times, either because the operators did not respond or due to servers being compromised again after cleaning.

Apart from the need to promptly install security updates, this once again highlights the fact that the risk of malware infection via advertising banners is not confined to the dark areas of the Internet but also appear on popular, reputable websites.

2.2.4 Botnets

A botnet is a collection of systems which have been attacked by a remotely controllable malware variant known as a bot. The affected systems are controlled by the botnet operator via a command-and-control server (C&C server). Botnets are used by criminals to commit information theft and online banking fraud on a grand scale, to launch distributed denial of service (DDos) attacks or to send high volumes of spam, phishing mails or e-mails with malware as attachment.

Situation

- It is estimated that in Germany alone more than a million computers are part of a botnet.
- Due to the professionalisation and commercialisation of cybercrime activities, establishing and operating a botnet is comparatively cheap and easy even for people without significant technical expertise.
- Information theft is one of the greatest problems in relation to botnets. Alongside classical end user systems, attacks are being launched with ever growing frequency on Internet-enabled devices which process information such as payment details.
- Increasingly even web servers are being compromised and incorporated into botnets. Due to their broadband network connections and high availability these systems are particularly suitable for such activities as DDos attacks.

Assessment

As recent reports of information theft and online banking fraud by botnets clearly show, the situation may be viewed as critical. Botnet infrastructures provide Internet criminals with immense resources of computer capacity and bandwidth which they can use for their nefarious activities. Today botnets are predominantly composed of Windows systems, but cybercriminals are increasingly turning their attention to Mac OS X and Android devices as target platforms for botnets. Other Internet-enabled devices such as DSL routers or smart TVs have also fallen victim to attacks and infection. One reason for this is the weaker protective mechanisms with which these devices are equipped. In light of the trend towards an Internet of things this issue can only grow in importance.

2.2.5 Social engineering

In attacks using social engineering, criminals attempt to induce their victims to disclose data of their own free will, circumvent protective measures and willingly install malicious code on their systems. Just like in the field of espionage, cybercriminals skilfully exploit human weaknesses such as curiosity to gain access to sensitive data and information.

Situation

- The growing trend towards making personal data and information available to the general public via social networks or private websites makes it easier for criminals to use this information to prepare targeted attacks involving social engineering.
- Criminals frequently exploit human curiosity for interesting information, the desire for a bargain, prudence or bad conscious in the face of official threats or threats of criminal action, as well as the increased public attention stirred up by major events such as the football world cup, public holidays or current economic or social affairs such as the introduction of the Single Euro Payments Area (SEPA).
- Phishing attacks, in which e-mails with falsified senders are sent in an attempt to induce users to disclose personal details, continue to proliferate. The ostensible senders are well-known companies and organisations, financial service providers and familiar online shops, e-mail or communications providers. Fictional orders, invoices, warnings or security notices direct users to fraudulent websites where they are asked to update or confirm access data, account information or other customer details.
- In one particularly exhaustive attack on German companies employees received e-mails which allegedly came from their personnel departments. The e-mails, which came complete with long falsified threads and spurious Executive Board decisions, asked the recipients to disclose details such as their personnel and account data. The criminals then used the data to make withdrawals from accounts and order new electronic cash cards.
- In online banking users are induced via manipulated test credit transfers or user verifications involving TAN or mTAN to enter data in fraudulent web forms or install ostensible security apps which contain malware. Often the spurious bank websites can barely be distinguished from the genuine articles.
- Social engineering is a fundamental component of targeted attacks.

Assessment

Technical measures increase your level of IT security but they cannot guarantee complete protection on their own. This is particularly apparent from cases of attacks involving social engineering. While users continue to unnecessarily disclose private details or click on an e-mail offering a spurious commercial inducement, criminals will continue to use social engineering to gain financial advantage from the data they thereby obtain. Because social engineering also often constitutes the gateway for targeted attacks on companies and government departments, employee training and awareness raising are vital. The example of phishing clearly shows how important prudent behaviour by users is for data security.

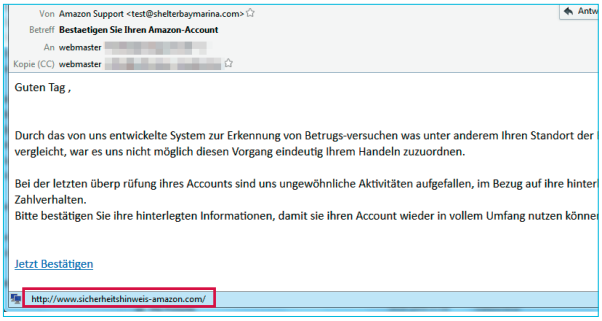

Figure 5: Example of a phishing e-mail – recognisable by the falsified sender address

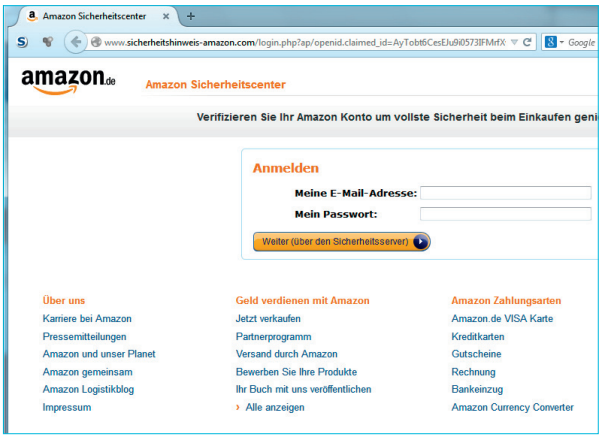

Figure 6: Example of a phishing website – recognisable by the falsified URL

2.2.6 Identity theft

Identity theft or misuse involves the acquisition and unauthorised use by third parties of personal data such as postal and e-mail addresses, dates of birth, bank account and credit card numbers. The attackers' aim is generally to gain financial advantage using the confidential information, or more rarely to discredit the person whose details have been stolen. Identity theft is chiefly done via social engineering, malware on infected systems or data theft after hacking of online services.

Situation

- Identity theft is an everyday occurrence. Every month large numbers of digital identities are stolen from infected computers of private users alone.
- The amount of identity theft malware is steadily increasing. The BSI alone analyses approximately 11,000 malware programs a month which are implicated in identity theft in Germany.
- These days criminals use malware which specialises in certain data such as digital identities which are then highly likely to be misused, for instance in the fields of online banking or shopping.
- In spring 2014 the BSI published details of two major identity theft incidents in which a total of 34 million e-mail addresses and passwords were stolen.
- Attacks on service providers are also attractive, indeed today the number of identities stolen through attacks on the servers of online sellers and service providers is significantly greater than the number of identities stolen from infected user machines. For instance, one attack on eBay in May 2014 affected 145 million customers worldwide, around 15 million of them in Germany.

Assessment

The cyber threat posed by identity theft will continue to rise as long as professionally organised attackers have a large number of inadequately protected systems, run both by private users and service providers, at their disposal. Password management and the regular downloading of all relevant system updates make an important contribution to the protection of personal data for minimal effort or outlay. Online service providers should also be more diligent in providing better protective measures for their systems and their customers' data. For instance, customer data and the corresponding databases should be operated in encrypted form as a matter of course, while users should be offered secure authentication procedures such as those involving two-factor authentication. This can for instance be done using the new identity cards, which millions of German citizens now possess.

2.2.7 Denial of service

Denial of service (DoS) attacks are directed at the availability of services, websites, individual systems or entire networks. If such an attack is launched in parallel by several systems this is known as a distributed denial of service (DDoS) attack. DDoS attacks frequently involve very large numbers of computers. The computers in question may have been brought together unwittingly to form a botnet or may be compromised systems, but could also be computers which have been linked up by willing participants, as for instance in politically motivated attacks. DDoS attacks on large companies or governments often involve political or ideological motives, whereas attacks on e-commerce providers increasingly stem from competitors or extortionists. There are also increasing numbers of DDoS attacks on critical infrastructure operators such as banks, transport companies and media organisations. Here too criminals are chiefly motivated by financial gain, for instance through extortion.

Situation

- So far in 2014 there have been over 32,000 DDoS attacks in Germany alone.
- Virtually every sector is afflicted by DDoS attacks.
- The Alliance for Cyber Security[14] survey found that over a third of the companies questioned reported being the target of a DDoS attack on their websites during the past three years.
- A quarter of the companies surveyed had suffered DDoS attacks on their network infrastructure.

- Since 2013 there has been increased use of reflection attacks, whereby the target system is not attacked directly but rather through the misuse of publicly available Internet services (e.g. DNS[15] or NTP[16]). These involve attackers sending small queries to a public service in the name of their victim. The services then send their replies to the victim's system. Because the replies are usually a lot larger than the queries, even a small number of attacking systems can do great damage and cripple the victim's system. In reflection attacks unwitting parties such as the service providers become unwilling accomplices.

- To date the largest DDos attack took place in February 2014, involving a bandwidth up to 400 gigabits per second. This attack was based on NTP reflection.

- The number of NTP servers in Germany which could be exploited for this kind of attack fell between June 2014 and August 2014 from over 4,000 systems to around 2,500. This was due to information given to the operators by the BSI.

Assessment

Global comparison shows that Germany is less badly affected by this issue than other countries. All in all, Germany is neither a major source of such attacks nor a particularly frequent victim. Nevertheless, DDos attacks can threaten the survival of companies affected by them.

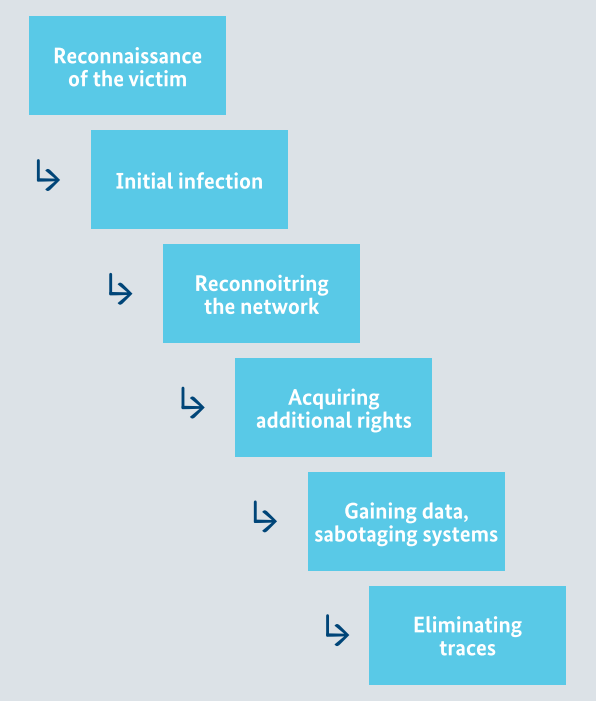

Figure 7: Procedures of an APT attack

2.2.8 Advanced Persistent Threats (APT)

Advanced persistent threats are targeted cyber attacks on specific institutions in which the attackers gain persistent access to the victim network and then widen the attack to additional systems. The attacks involve the deployment of major resources and considerable technical skill on the attackers' part and are generally difficult to detect.

Situation

- APT attacks focus chiefly on the defence industry, high-tech sectors such as the automobile industry, shipbuilding and aerospace, research institutes and public administration.

- In APT attacks the initial infection is frequently introduced using an e-mail with a prepared attachment plus targeted social engineering. Information from the recipient's professional milieu which is plausible or expected is used, along with the name of a trustworthy sender. With this kind of targeted social engineering it is often impossible to distinguish between authentic and fraudulent messages.

- Another trend in the launching of APTs is the use of watering hole attacks. In these a website which is frequently visited by a target individual is first compromised. When the target individual visits that website their computer is infected with malware via a drive-by exploit. Alternatively the victim may be sent an e-mail with a link to a prepared website. The e-mail content produced via social engineering induces the recipient to click on the link.

- Frequently attacks initially focus on less technologically aware target individuals within companies.

- Within larger organisations the central directory structures are generally the focus of the attack. The next phase of the attack involves exfiltrating data or sabotaging target systems. Attackers attempt to keep the victim's systems under control as long as possible without the victim becoming aware of the attack. Indeed, practical experience shows that APTs often remain undetected for months or even years. In the final phase of an APT attack any traces of it are eliminated as thoroughly as possible.

Assessment

APT attacks pose a serious threat to the German economy and public administration. Hacking into poorly protected company servers will continue to grow in significance. To permit companies potentially at risk to be warned at an early stage and produce a comprehensive picture of the situation it is vital to more precisely evaluate the mode of operation and attack tools used in APT attacks. The reporting of incidents to the BSI by affected companies makes an important contribution to this end.

2.2.9 Cyber attacks by intelligence agencies

Germany is subject to continuous cyber attacks with the objective of obtaining information and gaining financial advantages. During 2013 and 2014 both the technologically improved detection systems integrated by the BSI into the government's networks and the evaluation of the Edward Snowden revelations have increased our technical knowledge and understanding of cyber attacks launched by intelligence agencies and the methods they use.

The BSI's improved detection systems have uncovered strong and unambiguous evidence of cyber attacks by intelligence agencies against German infrastructure in the business, research and public administration spheres. These attacks have also been observed both by BSI partner agencies and BSI private sector partners. The Snowden revelations were also instrumental in increasing knowledge on intelligence activities. What was surprising about them was the degree of professionalism they revealed, along with the scale and extent of the surveillance measures and the copious resources assigned to the enterprise, both in personnel and financial terms.

A more precise analysis of the available technical findings allows to identify four principal attack vectors:

- **Strategic reconnaissance:**
  All the data accumulating at Internet and communication nodes are collected, stored and analysed. This involves gathering the (connection) data of large numbers of Internet users, from which attackers can determine who has communicated with whom, at what time and in what place. If the content is unencrypted it can be eavesdropped in its entirety, for instance in the case of VoIP phone calls.
  The same applies to data obtainable from Internet service providers such as social networks or search services.

- **Individual attacks in communications and cyberspace:**
  These attacks are targeted at the IT systems of prominent people and institutions. To this end intelligence agencies first systematically analyse, purchase and collect hitherto unpublished hardware and software vulnerabilities. This knowledge base is then used to devise specifically adapted cyber attacks to attack and control IT systems identified at the strategic reconnaissance stage. Radio and mobile communications can be individually tapped through corresponding attacks. In this way individual users' computers can be infected with malware, whereafter they can be monitored in real time from anywhere in the world. If target individuals use a smartphone they can be tracked, meaning that their location may be determined at all times, and in many cases strategic reconnaissance allows the identification of the person's interlocutor, who is also carrying a smartphone or laptop.

- **Influencing standards and implementations:**
  This involves manipulating IT standards and cryptographic standards in advance of the technical reconnaissance, thereby systemically undermining the implementation of inherently stronger security mechanisms designed to reinforce confidentiality. This means that strong, internationally standardised cryptoalgorithms used in hardware or software implementations are for instance combined with weak random number generators, as a result of which they no longer provide adequate protection of confidentiality.

- **Targeted manipulation of IT equipment:**
  This involves intervention in ordering processes, delivery or supply chains in order to manipulate IT equipment. The process includes inserting back doors or weakening technical security features. For instance, monitors, keyboards and video or audio cables are fitted with miniature transmitters which allow radio signals to be detected from a greater distance. Network components like routers can be manipulated by changing their software so that they can be remotely controlled or even switched off, thereby also facilitating cyber sabotage.

Exemplifying these attack vectors are attack scenarios directed at mobile communications shown in the following illustration.

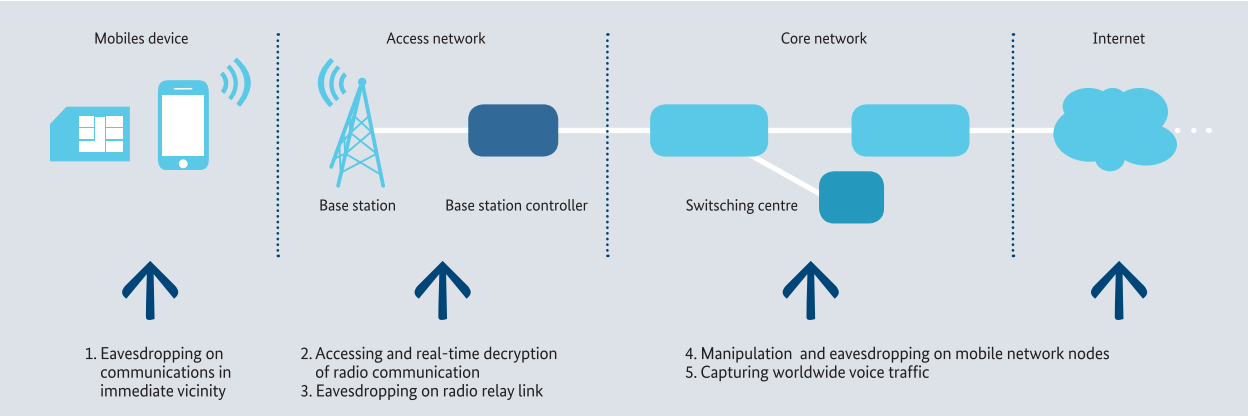

Figure 8: Mobile communication attack vectors

All the options discussed above for compromising ICT systems for technical or cyberespionage purposes can also be used in a similar fashion to carry out cyber sabotage. This is particularly true of the information and communication technology used in critical infrastructures.

2.3 Typology of attackers

Despite the great proliferation of different attack targets and possible attack methods, the motivation behind a cyber attack can frequently be put down to financial interests, information procurement, sabotage, gaining of influence or the pursuit of political interests. We may broadly distinguish between three different categories of attacker: criminals, intelligence agencies and hacktivists, while malicious insiders forming a special category.

2.3.1 Cybercriminals

Introduction
The motivation of cybercriminals is to make money by illegal means through the use of information technology. The activities of organised cybercrime include identity theft, product fraud, using stolen banking information to steal money and extortion. Organised cybercriminals are highly professional in the way they exploit the advantages gained via cyber attacks. In addition to organised crime we also find individual criminals or smaller groups, though they are generally characterised by a lower level of professionalism.

Capabilities
The methods and variants used by cybercriminals focus on technological progress as well as existing defensive systems. In the process attackers exploit the entire spectrum of technical options. For private users that involves the use of spam, phishing e-mails and malware, identity theft, manipulation of online banking, adware, scareware and ransomware. In addition, spurious job offers are used to turn private individuals into financial agents or goods agents who become unwitting accomplices in financial or product fraud.

The range of attack scenarios affecting companies include various forms of extortion and hacking into server services. Furthermore, malware is increasingly being infiltrated into point of sale systems in order to read off customer data directly from the checkout during the payment transaction.

In addition, in return for suitable payment criminals offer cyberespionage and competitor research services. Spying on competitors enables companies to obtain sensitive internal information on them and their products which can be converted into a material advantage in global competition.

Objectives
Today cybercrime is pervasive. All user groups, from private citizens to the worlds of business, science and public administration, are affected. As long as criminals see opportunities to make money this way they will exploit those opportunities and continuously refine their methods.

The Cybercrime 2013 Federal Situation Assessment (Bundeslagebild) published by the Federal Criminal Police Office (Bundeskriminalamt – BKA) cites over 64,000 cases for the year 2013, though the BKA assumes that the true figure is much higher[17]. According to a survey by the Alliance for Cyber Security, cybercriminals are the attacker group that will pose the greatest threat over the coming years.

Ransomware

Digital extortion using ransomware which blocks access to infected systems or encrypts user data is as widespread in Germany as elsewhere. The BSI Service Centre is regularly contacted by German citizens who have fallen victim to ransomware attacks and are seeking help. To date in 2014 there have been almost 1,200 such enquiries, while the total in 2013 came to over 8,500. Since the start of 2014 several new ransomware variants have been identified which are equipped with better methods and are able to infect and encrypt user systems or servers. The first variants designed to attack Android smartphones have also now been detected. If an extortion victim gives in to the criminal's demands a direct money transfer from the victim to the criminal takes place, which is what makes ransomware attractive to criminals. Anonymous payment systems such as prepaid cards or so-called cryptocurrencies are used for the purpose. Thus, unlike product fraud or where financial agents are used, there is no intermediary. The BSI advises victims not to pay the sum demanded under any circumstances, rather cleaning the affected computers and reporting the case to the police.

2.3.2 Intelligence agencies

Introduction
The primary purpose of cyber attacks by government intelligence agencies is military and economic espionage[18]. In the military sector cyberspace has today become a further key domain alongside the classical military domains land, sea, air and space.

Capabilities
The cyberspace capabilities of government intelligence agencies are limited only by the resources devoted to them, which in some cases are vast. As government organisations, intelligence agencies have a great many methods at their disposal, from access to central infrastructure components or their operators, interventions in IT products ex works or the insertion of back-doors into products via manufacturers in their own countries. Classical cyber attacks, for instance via Trojan horses, are used in targeted fashion and are of higher quality than the attacks launched by cybercriminals. Alongside standard tools and approaches we find the use of specialised malware designed independently by them or by service providers. Furthermore, intelligence agencies can invest a great deal of money in the search for vulnerabilities to exploit. Given that, depending on their size and quality, software packages will inevitably have a certain number of vulnerabilities, new gateways for cyber attacks are always open to them.

Objectives
The targets of attacks by intelligence agencies are companies in key industries, critical infrastructure and the government agencies, administrative bodies and research institutions of other countries. Depending on their background, espionage and sabotage attacks are executed either with the aim of furthering their own national interests or gaining advantages for national businesses on international markets. Due to their wide-ranging capabilities, business, public administration and private citizens may equally be the targeted or unintended objects of intelligence agency activities. Given their quality, defending against these attacks is only possible by putting a great deal of effort and money into countermeasures.

2.3.3 Hacktivism and cyber activists

Introduction
In the hacktivism sphere attackers ostensibly use computer systems and networks as a means of protest and in the furtherance of political or ideological objectives. Through their actions hacktivists aim to draw attention to what they see as political, social, economic or technological injustices. They often equate this form of protest with conventional forms of protest such as demonstrations, activism or civil disobedience. However, for the organisations under attack hacktivism can do serious damage.

Capabilities
The hacktivist scene is heterogeneous and includes many different groups within which individual grouping or even individual hacktivists may be pooled together, for example the Anonymous movement, the revelation websites or cyber occupiers. Hacktivists often act on the spur of the moment and organise themselves very rapidly. Hacktivists are capable of launching DDos attacks, manipulating websites and sowing targeted disinformation via social networks. They also engage in targeted information theft followed by publication of data in order to gain publicity for a specific demand. Not infrequently hacktivist activities proceed in parallel with conventional protest campaigns.

Objectives
Given their motivation the chief focuses of hacktivist activities are governments, government organisations and major companies. The current overall threat level in Germany is low. However, the international threat level may be rated as critical, with a large number of incidents affecting critical infrastructure such as information and communication technology (ICT), the food industry, media and culture.

2.3.4 Malicious insiders

Alongside the three types of attacker outlined above, malicious insiders constitute a further grouping who come into consideration as potential culprits for attacks on in-house or confidential information or acts of sabotage. Due to their less restricted access to in-house know-how and resources as compared with external attackers, their chances of success in accessing undetected into key corporate data and information is particularly high. Furthermore, malicious insiders are able to analyse the protective measures in place over long periods, thus making them easier to circumvent. On top of this, malicious insiders can exploit the trust placed in them by their own organisation. Apart from employees, external service providers may also become malicious insiders if their activities give them influence over or direct access to in-house information or processes.

2.4 Summary

The current IT landscape and the multifaceted nature of the security threats of today pose a permanent challenge for users of information technology. A wide variety of factors and circumstances are currently favourable for the execution of cyber attacks. Meanwhile, the continuous refinement and professionalisation of attackers and attack methods further increase the threats facing information security.

Table 2 summarises the existing security threats, attack methods. In view of the overall attack potential posed by these threats, the state of IT security in Germany may be viewed as critical.

Central causes and threats for private users
Private users' systems are currently subject to security threats deriving from the following causes:

1. Inadequate patch management and use of out-of-date software on all devices
2. Cyber attacks via spam e-mail containing malicious attachments and social engineering involving the use of spurious invoices, order confirmations or reminders to induce users to run malware
3. Cyber attacks via compromised websites or manipulated advertising banners which install malware when visiting a website
4. Cyber attacks on service providers with a view to stealing their customer data
5. 'Digital carelessness' in handling mobile devices and apps and disclosing personal information

Central causes and threats for business and government

Many of the most prevalent threats affect private citizens, business and the government in equal measure as users of information and communication technology. This applies in particular to untargeted attacks such as spam e-mail or drive-by attacks from compromised websites or advertising banners. However, given the greater complexity in business environments and the presumably higher levels of security in place as compared with private users, the central threats they face and their causes do differ:

1. Targeted espionage attacks on businesses, research bodies or the government executed using precisely tailored social engineering, unknown vulnerabilities and specially designed tools
2. Cyber attacks on company websites or service offers
3. Insufficient protection of networked Industrial Control Systems in manufacturing and production industries
4. Challenges posed by the integration of mobile devices ('bring your own device') and external service providers into existing ICT infrastructures
5. Inadequate patch management and use of out-of-date software on all devices

The threat assessment is underpinned by the analyses and publications of antivirus software vendors and IT security service providers. Experts are unanimous in that the most severe current threats include ransomware attacks, a sharp rise in the number of malware programs for mobile operating systems as well as increasing numbers of targeted attacks.

High number of undisclosed cases

On top of the known threat situation we also have to assume that there are a great many undisclosed cases. Here too the situation assessment is based on the observation and analysis of a cross section of the actual situation in Germany and worldwide. The frequency with which incidents go unreported makes it all the more difficult to accurately appraise the actual situation. A study on economic espionage[19] came to the conclusion that only around a quarter of all incidents come to the attention of external experts or government agencies, while only five per cent of cases ever get reported to the police or public prosecutors. Accordingly, rich sources of information on attack methods, tools used and targets, as well as on criminals and their motivations, are often beyond the reach of investigators.

The incidents reported in the following chapter illustrate the impact that vulnerabilities, malware or inadequate security have had in the past. The incidents serve as examples of how an apparently abstract threat to institutions or individuals can rapidly transform into concrete risks which cause real damage.

Threats	2013	2014	Forecast
Vulnerabilities	↑	→	→
Spam	↓	↑	→
Malware	↑	↑	↑
Drive-by exploits and exploit kits	↑	→	→
Botnets	→	→	→
Social engineering	→	↑	→
Identity theft	↑	↑	↑
Denial of Service (Dos; DDos)	→	→	→
Advanced Persistent Threats (APT)	↑	→	↑

↑ Increasing → Unchanged ↓ Decreasing

Table 2: Summary of threat situation for various security threats and attack methods

3 Incidents

3 Incidents

At the beginning of 2014 two incidents involving millions of cases of digital identity theft were uncovered, and this marked a turning point in public attitudes to cyber attacks. Since these incidents current IT threats and cyber attacks have become a focus of political and media attention. Apart from the above-mentioned cases of identity theft the incidents selected also highlighted how skilled, flexible and thorough the attackers' methods had now become. The attacks affected all information technology user groups, from companies, government departments, research institutes and private citizens to critical infrastructure operators. Incidents affecting critical infrastructure operators are particularly serious because any damage done by cyber attacks could rapidly have severe consequences for the general public and the economy as a whole.

3.1 Incidents affecting the federal government

The BSI Situation Centre is the central reporting office for IT security incidents affecting the federal government. Since 2010 government departments have been required to report serious security incidents to the Situation Centre immediately and less critical incidents monthly. This enables the BSI to not only monitor the immediate reaction to the actual attack but also to identify trends and developments in relation to the threats facing the federal government's IT and networks and take correspondingly early countermeasures.

The protection of federal government systems and communication is based on a multilevel security model. Alongside standard antivirus programs additional protective measures are used at different stages which can defend against malicious e-mails in real time. Since May 2014 the associated procedure has led to the interception of up to 60,000 additional infected e-mails a month in the federal government's networks. To successfully defend against high-grade attacks an additional system is designed to detect attacks which have already circumvented standard protective mechanisms. Thus far in 2014 some 15 to 20 attacks a day on the governmental network have been detected which would have eluded normal protective measures. An average of one attack per day is a targeted attack attributed to an intelligence agency. An additional protective stage involves the blocking of outgoing communication. Internet traffic is checked to determine whether it connects to known command and control servers for botnets or espionage programs. These connections from governmental networks can be directly blocked and reported to the responsible authorities so that infected computers can be cleaned. Thus, around 3,500 attempts to access malicious servers are blocked every day. Since the beginning of 2014 34 infected systems have been identified which, despite being protected by commercial IT security products, have been compromised by malware. Around 1,100 website operators have been informed by BSI that their websites are distributing malware.

The BSI records an average of one denial of service (Dos) attack a month against individual federal government websites. Many of the cases reported to the BSI from federal government organisations also related to the exploitation of vulnerabilities in web applications. For instance, in several cases attackers sent between 20,000 and 200,000 spam messages by using scripts which automatically fill in the 'Forward' or Recommendation function of websites to send the spam messages. In this case the government department website's 'Recommend page' feature was vulnerable, and in response it was permanently deactivated or furnished with additional protective measures.

In another attack over 900 employees were e-mailed a link to a phishing website designed for that government department. The e-mail claimed that the storage limit for the mailbox had been exceeded and that it was unable to receive any more e-mails. Because of this, in order to be able to receive any more e-mails it would be necessary to confirm the e-mail account. The phishing website asked for people's e-mail address, username and password. Once the attack was detected access to the linked phishing website was blocked.

Incidents which are not attributable to a cyber attack can also have a major impact on the availability of IT infrastructure and therefore on IT security. An evaluation of additional messages that the situation centre received from the federal government clearly showed that faults or breakdowns suffered by the data centre power and air conditioning systems were often not adequately compensated by the emergency power system and could thus lead to power cuts lasting for hours. Another cause of reports is the use of mobile devices such as laptops and smartphones with

access to government networks which are then lost or stolen. Despite this, attacks on government networks involving lost or stolen mobile devices have not been registered.

3.2 Incidents affecting private users

3.2.1 Millions of cases of identity theft in Germany

Incident
In spring 2014 two cases of identity theft became public in which attackers gained access to the usernames and passwords of 16 and 18 million Internet users respectively.

Method
The criminals gained access to the data via systems infected with malware and attacks on online services.

Impact
The criminals tried to use the e-mail addresses and associated passwords to log in to e-mail accounts and then use those accounts to send spam e-mails. It can be assumed that the addresses and passwords in question allow access not only to e-mail accounts but also to other online accounts, for instance to online shops, Internet forums or social networks.

Target groups
The attackers focused on Internet users in Germany and other European countries.

Technical capabilities
Attacks on Internet users via e-mails containing malware, social engineering or drive-by exploits have become an everyday matter. However, the sheer volume of user data accessed at the beginning of the year is indicative of the criminals' professionalism.

3.2.2 Vulnerabilities in home network routers

Incident
In early 2014 a vulnerability was identified in the FRITZ!-Box routers produced by AVM.

Method
Attackers exploited an unpatched vulnerability to gain access to the device and all configuration data stored.

Impact
By gaining access to the configuration data the attackers were able to manipulate the system. They were also able to read data giving access to e-mail accounts and other online services if that data had been stored on the router. In addition the attackers used the vulnerability to make expensive calls to premium-rate telephone numbers at the victim's or the telephone company's cost. The manufacturers have issued several warnings to users on the need to download the security updates.

Target groups
Several million private users' devices were affected in Germany alone. Many SMEs and other companies who use these devices in their business operations were also affected.

Technical capabilities
In both technical and organisational terms the criminals acted in a professional fashion, exploiting a previously unknown vulnerability in the router's operating system to obtain information and cause the victim financial damage.

3.2.3 Online banking Trojans: from Feodo to Geodo

Incident
In May 2014 the online banking malware Geodo superseded the Trojan Feodo, which had been known since 2013.

Method
The attackers e-mailed deceptively authentic-looking invoices and reservation confirmations in the name of telecommunications service providers and banks to distribute malware which was either contained in a file attachment or provided as a link in the message. The links led to compromised websites on which the attackers had placed malware for downloading.

Impact
The attack wave persisted for several weeks and, as had been the case with Feodo, was highly successful, leading to large numbers of infections. In addition to manipulating online banking transactions Geodo obtained credentials from the infected PCs and transmitted them to the attackers' command and control servers. This account data was subsequently used to further distribute the malware.

Target groups
The attackers focused on Internet users and bank clients in Germany.

Technical capabilities
The federal government's BSI-based Computer Emergency Response Team CERT-Bund assumed the role of a bot and for three weeks received packages of stolen access data from the control and command servers. This enabled BSI to identify over 200,000 compromised e-mail accounts. CERT-Bund has informed the various network operators about the compromised e-mail accounts. The malware's capabilities, coupled with the immediate exploitation of the stolen access data to send spam indicate a technically and organisationally sophisticated attack on German users.

3.2.4 iBanking: malware for smartphones

Incident
Since mid-2013 underground forums have been offering malware for monitoring and manipulating Android smartphones. The malware was used for such purposes as attacks on online banking transactions using mTANs.

Method
First the victim's PC gets infected with malware. The next time the victim logs on for online banking the malware manipulates the banks website and requests information on the victim's mobile telephone. The victim then receives a text message containing a link to an app infected with iBanking malware and is induced via social engineering to install this app on his or her smartphone. The attack on the online banking service involves interaction between the malware on the PC and the smartphone. The malware on the PC initiates its own money transfer. The mTAN sent by the bank to the client's mobile phone is intercepted there by iBanking malware and transmitted to the infected PC. The malware then uses the intercepted mTAN to complete the credit transfer on the PC.

Impact
The attackers were able to compromise the online banking services of various international banks. The malware can relatively easily be adapted for attacks on other Internet services. For example, variants of iBanking have already been discovered which facilitate attacks on two-factor authentication (username or password + SMS code) for Facebook and Gmail.

Target groups
The malware is used to attack bank clients who use mTANs to do online banking.

Technical capabilities
The malware offers the attackers wide-ranging opportunities to control smartphones: monitoring text messages, recording phone calls, acoustic room surveillance, access to various data on the smartphone, etc. All the information collected can be transmitted to servers controlled by the attackers. In the iBanking package developers also offer server software with which the infected devices can be controlled. The malware's functionality reveals a high level of technical expertise on the part of the developer, who has sold the software under various different license models.

3.3 Incidents affecting business

Unlike the federal government, companies are not currently required to report serious IT security incidents to the BSI. The UP KRITIS initiative has for many years given participating operators of critical infrastructure the opportunity to share information on incidents. In addition, together with the Alliance for Cyber Security BSI offers a reporting centre via which incidents can be reported, anonymously if desired, which could be relevant for other bodies or in connection with which the reporter would like evaluation or assistance. The objective of the reporting centre is to gain information on new attack techniques and critical incidents with wider-ranging implications. The BSI analyses the reports and makes its anonymised conclusions available to participants. The aim of this procedure is to give companies early notice of new attacks and possible preventive measures. To date the reporting centre has been used predominantly by SMEs who have fallen victim to DDos attacks or malware infections.

3.3.1 APT attack on industrial installations in Germany

Incident
Targeted attack on a steel mill in Germany

Method
The attackers used spear phishing e-mails in tandem with sophisticated social engineering to gain initial access to the steel mill's office network. From there they worked their way progressively into the production networks.

Impact
Breakdowns of individual control components or entire installations proliferated. The breakdowns led to the uncontrolled shutdown of a blast furnace, leaving it in an undefined state and resulting in massive damage.

Target groups
Operators of industrial installations

Technical capabilities
The attackers' technical skills can be rated as very advanced. A variety of different internal systems and industrial components were compromised. The attackers' expertise extended not just to classical IT security but also to detailed technical knowledge of the Industrial Control Systems and production processes being used.

3.3.2 Heartbleed: critical vulnerability in widely used software library

Incident
The vulnerability known as Heartbleed, discovered in April 2014 in the OpenSSL software library, permits the unauthorised access to the program memory.

Method
All that is needed to exploit the vulnerability is to send specially crafted queries to systems which use the function affected by the OpenSSL vulnerability.

Impact
Virtually everyone on the Internet uses the Secure Sockets Layer Protocol (SSL) or Transport Layer Security (TLS), normally without even knowing it. This very widely used technology is of great importance for encrypted communication on the Internet and is for example used on almost all websites to check their authenticity and encrypt communications between users and websites. The OpenSSL free software library is often used for the purpose. The Heartbleed vulnerability in OpenSSL permits unauthorised access to program memory. This could include the usernames and passwords entered by website visitors, and in rare cases it may also be possible to read secret cryptographic keys. This would mean that attackers could masquerade as the service provider and read users' supposedly encrypted data transmissions.

Target groups
All products and services using the vulnerable OpenSSL software library function were affected. Major online services, social networks, bank websites and federal government servers were all affected by the vulnerability. Given the extent of the vulnerability it must be assumed that, despite the availability of patches, there continue to be systems in Germany which are still vulnerable to Heartbleed.

3.3.3 Dragonfly: targeted attacks on production networks

Incident
The Dragonfly group (also known as 'Energetic Bear') used the malware Havex, which was detected in 2014, to attack several dozen German companies.

Method
The attack campaign made use of a new attack method: in the first stage the criminals attacked the manufacturers of industrial control system software. The malware Havex was attached to the relevant installation files on the vendors' download servers, meaning that customers who installed the legitimate software simultaneously downloaded the malware onto their systems. In some cases a module was downloaded which collected information on devices and systems used in the production network and passed it on to the attackers.

Impact
Havex facilitated the targeted use of malware in Industrial Control Systems in order to collect information. It must be assumed that the criminals then used this information to launch further attacks. In collaboration with the Federal Criminal Police Office the BSI informed several dozen companies in Germany which had fallen victim to the Dragonfly campaign.

Target groups
Production facilities and production networks

Technical capabilities
The skills which became apparent during the Dragonfly attack campaign, for example the targeted compromising of download servers, highlighted the attackers' technical sophistication and demonstrated that attacks on Industrial Control Systems in Germany are a reality.

3.3.4 Operation Windigo: Linux malware Ebury collects SSH access data

Incident
Ebury is malware with back-door functionality. It is a rootkit for Linux and Unix-like operating systems which intercepts Secure Shell (SSH) credentials.

Method
The malware is installed by attackers on compromised servers either by exchanging SSH program files or a library used commonly by these programs. Ebury steals access data from infected systems (usernames and passwords) to incoming and outgoing SSH connections and transmits the data to the attackers. In addition the private SSH keys used for outgoing SSH connections were stolen from the compromised systems.

Impact
The back-door gives the criminals full control over the infected system at all times. Servers infected with Ebury were used by the criminals for various criminal activities making up 'Operation Windigo'. For instance, web servers were manipulated so that visitors were redirected from the websites hosted there to other servers. These involved either dating portals, websites with pornographic content or servers hosting drive-by exploits which infected the website visitors' computers with malware. Our analysis revealed that several hundred thousand such redirections were taking place every day. On other systems the criminals used the access data stolen using Ebury to install malware for sending spam. During the monitoring period an average of 35 millions spam e-mails were sent every day.

Target groups
Server operators (primarily) and Internet users (secondarily)

Technical capabilities
Ebury is of high technical quality and the infrastructure created on the compromised servers is professionally organised. The criminals made huge profits from distributing the malware via drive-by exploits, redirection from websites and sending spam. CERT-Bund joined the 'Ebury Working Group', an international association of security analysts which has detected some 30,000 servers infected worldwide with Ebury since February 2013. About ten per cent of these servers are located in Germany. CERT-Bund regularly notifies German hosting providers and national CERTs in over 60 countries of known Ebury infections.

3.3.5 Great Britain: bankruptcy due to cyber extortion and sabotage

Incident
In June 2014 the collaboration and development platform for software developers operated by the company Code Spaces became the target for extortion accompanied by a DDos attack lasting over 48 hours.

Method
The criminals gained illegal access to an administrator account for cloud storage rented by the company from Amazon Web Services and placed several messages there demanding money. The criminals were clearly prepared for Code Spaces' fruitless attempt to change the access data.

Impact
After the company refused to pay the money demanded, the criminals began indiscriminately deleting data. As a result the company lost virtually all its data, backups and machine settings, and in the end the company, which had been trading successfully for seven years, was forced to discontinue operations. There are no plans to reactivate the business because the financial cost of restoration measures and paying compensation to clients is too great.

Target groups
The attack illustrates the fundamental risk of a company collapsing due to cyberspace extortion and sabotage as well as from the outsourcing of business-critical services.

3.3.6 ShellShock: vulnerability in the Bash command line interpreter

Incident
In September 2014 a vulnerability dubbed Shell Shock was published in the Bash command line interpreter. Bash allowed the propagation to a shell not only of environmental variables but also functions. The function name is transmitted to the shell as an environmental variable, followed by the function definition. The vulnerability allowed an attached program code to be executed in the function definition.

Method
Bash is a standard component which is correspondingly widely distributed. It is used for such things as system services and remote access to both web and mail servers and also some smartphones. There is a correspondingly wide range of scenarios whereby the vulnerability can be exploited to executed unauthorised program code on affected IT systems. If services linked over the Internet are affected by ShellShock the vulnerability can be exploited remotely.

Impact
The unauthorised execution of program code, in some cases with administrator rights, allowed attackers to access confidential information and manipulate or crash IT systems. Malware has been detected which uses the vulnerability to put IT systems out of action. CVSS, the recognised industry standard for evaluating the severity of vulnerabilities, has given ShellShock its top score of 10.

Target groups
Bash is the standard shell for most Linux distributions and is also installed on many other systems. Also affected are the Apple operating system OS X and various Industrial Control Systems. It must be assumed that at the time it became known there were vulnerable systems in virtually every institution.

3.4 Incidents affecting critical infrastructure

3.4.1 Social engineering at large companies

Incident
In May 2014 high-ranking employees of several internationally operating large companies were targeted by particularly sophisticated phishing e-mails.

Method
Bogus e-mails informed the employees that, due to an update of the personnel department's IT systems it was suspected that there could be inconsistencies in some data sets. On this pretext the recipients were asked to send a copy of their official photo ID and the details of the bank account into which their salaries were paid. The e-mails were in virtually perfect German or English and came complete with a full mail history plus e-mail headers featuring authentic company e-mail addresses designed to lend apparent legitimacy to the process. A noteworthy point was that the employees mentioned in the fake history were actually employed in the various personnel departments.

Impact
Some of the recipients took the e-mail to be authentic and transmitted the requested document copies and account details to the sender, whereupon the attackers closed the victim's bank accounts by post, using counterfeit signatures or ordered new electronic cash cards and PINs to be sent to a new address in China.

Target groups
Senior employees of major German companies.

Technical capabilities
The expense and effort involved in planning and researching an attack of this kind is estimated to be very high, so it must be assumed that the attackers are extremely experienced. The near perfect German used is noteworthy, being a feature which distinguishes this attack from many others of this type.

3.4.2 Austria: malfunction in the controlling of energy grids

Incident
In 2013 anomalies were detected in the data streams in several Austrian control networks for the management of energy grids. These caused malfunctions for grid and power station operators as well as a number of data transmission disruptions.

Method
It is suspected that the malfunction was triggered by a command during commissioning a gas grid operator in southern Germany which also extended to the Austrian energy grid. This was then passed on to various different operators. Due to the unspecified processing of this message in individual network components the command was sent as an infinite loop, thereby triggering serious disruption of the grid management control.

Impact
During the incident the grid's stability could only be maintained at great expense. During the disruption considerable volumes of data were created, leading to log data overflows. Accordingly it has not yet been possible to finally determine the cause of the incident.

Target group
Energy grid operators

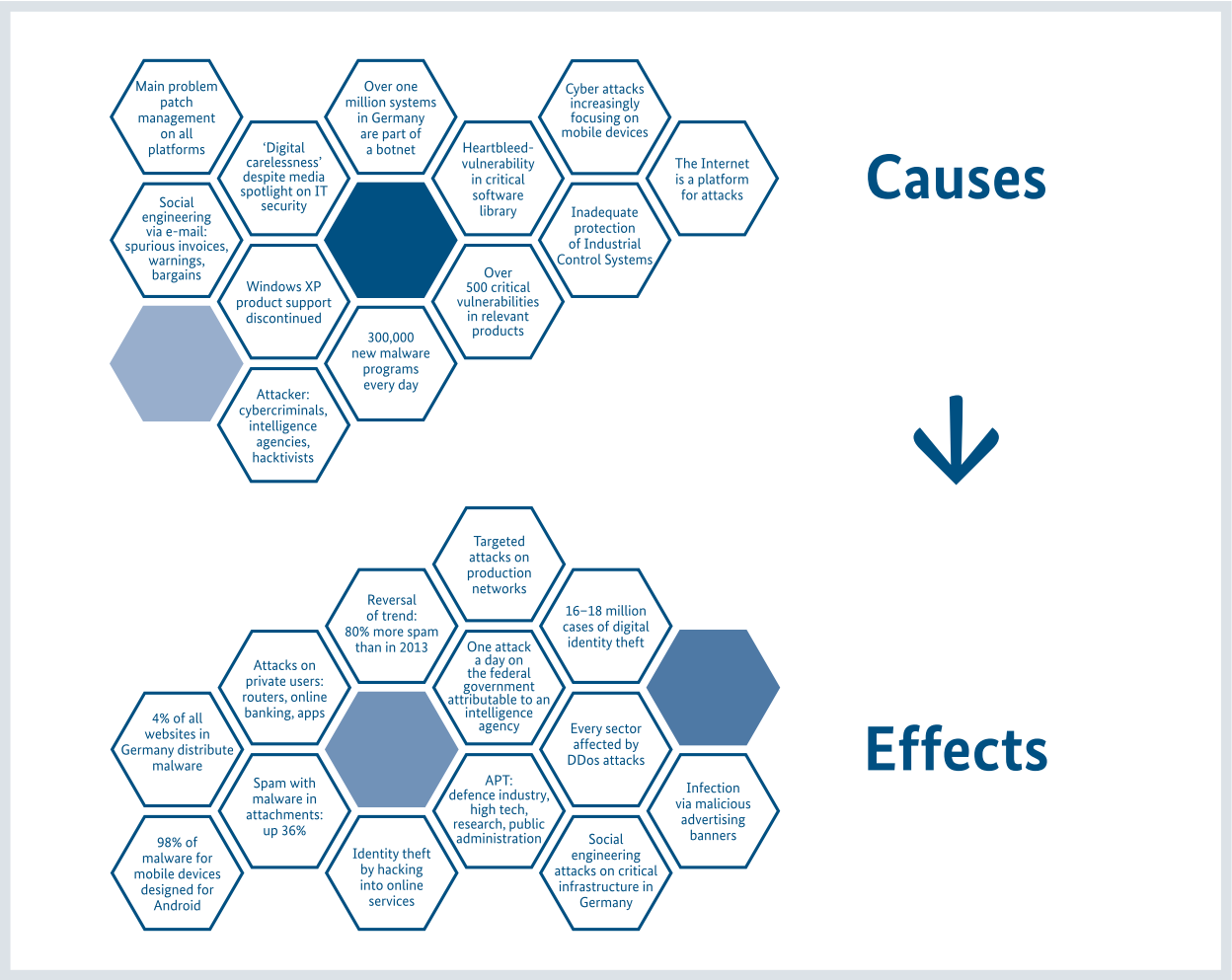

Figure 9: Overview: causes and effects of security threats and incidents

4 Solutions

4 Solutions

Solutions for improving the risk situation in cyberspace must focus on the development of measures designed for specific target groups, as well as supporting both businesses and private individuals in protecting themselves. A key feature of these measures must be scalability in order to be able to select appropriate measures to protect everyone from individuals to large organisations. From the aforementioned security threats and challenges posed by the current IT landscape the following spheres of action may be derived:

4.1 Promoting expertise and trustworthiness in the field of IT security

A key requirement for guaranteeing information security is the deployment of effective and reliable security mechanisms on a technical level, because despite thorough reviews and examinations, manipulation of IT components cannot be entirely ruled out. Accordingly, promoting the provision of thrustworthy information technology is a central pillar in ensuring a high level of IT security in Germany. This is also significant in light of the recent debate on the cyber activities of foreign intelligence agencies.

Essentially, cooperative efforts of the government, business and research communities should focus on the following strategic objectives:

- Protecting fundamental values in the digital world by safeguarding our technological capacity to act and promoting trustworthy information technology.
- Creating market conditions and incentives conducive to persuading foreign market leaders to adapt their products at technical level via trust anchors (such as national cryptocomponents) to German trustworthiness expectations, in particular where security requirements are high.
- Empowering the German economy to combine its core industrial skills with the existing expertise in Germany in the field of information security in order to ensure the implementation of the necessary IT security standards in central economic sectors.

Among the key success factors are the development of sustainable business models designed to ensure the long-term market success of these products. IT security can be an important factor in carving out a strong competitive position in the major markets of the future. One example of a technology of this sort, designed and promoted by the BSI, is the SINA product family. SINA provides IT-supported 'secure stations' which permit the risk-free use of market leaders' applications despite a deficit of trust.

German e-mail providers have joined forces for a campaign promoting a trustworthy e-mail service – 'E-mail Made in Germany'. Initiatives like this can be supported by standardising suitable security and trustworthiness requirements and awarding a corresponding certificate.

In the fast-moving IT world even the most up-to-date activities must always keep one eye on the future. For instance, there is a need for stronger security mechanisms to be integrated into smartphones given the prospect of them being more intensively used for payment and money transfer purposes in the future. A key requirement for guaranteeing information security is the deployment of effective and reliable security mechanisms at technical level. Fields not yet embraced by this report, such as e-health, smart cities and automotive with partial reference to safety (safety of life and limb) may in future be subject to higher security requirements. Further challenges in prospect are crypto- and cyber technologies, cloud solutions, security technologies to protect Industrial Control Systems and the development of intelligent networks (SDN).

4.2 Commitment to standardisation and certification

Standardisation and certification are effective tools for increasing transparency in the field of information security, raising the trustworthiness of products and services and forcing up information security levels throughout the economy. In the field of IT security Germany already possesses an effective certification scheme and internationally renowned auditing bodies.

Despite this, redoubled efforts will be called for in order to successfully safeguard Germany's leading position and confront new technological challenges. Currently there are shortcomings in Germany's representation on international standardisation bodies. Leading information and

communication technology companies frequently attempt to impose their own proprietary standards on international standardisation committees in order to gain a competitive advantage. This results in security standards which often fall far short of what is advisable from an information technology viewpoint.

Accordingly there needs to be stronger coordination of industry and government commitment to IT standardisation, with special reference to IT security and particular focus on technological transparency and the application of open standards.

The federal government is already actively working on the specification of IT security standards, for instance in the form of technical guidelines and BSI standards, in fields where security is critical, with a view to promoting the development of national best-practice solutions. For instance, the BSI is assisting in the implementation of the German Energy Act (Energiewirtschaftsgesetz) by cooperating with measurement system manufactures in the energy industry on the development of protection profiles and technical guidelines for intelligent measurement systems on the smart grid of the future. These technical standards are being developed in collaboration with the entire industry and are embodied in the VDE/FNN requirements for the Measurement System 2020.

Current market analyses forecast that demand for services to defend against cyber attacks is set to grow further. In view of the likely establishment of national cyber security service providers it makes sense to put in place a system for the certification of the companies in question as proof of their expertise and trustworthiness. In certain fields such as information security auditing, advice and penetration testing the BSI is already certifying service providers.

In the manufacturing sector there is a need for an increased involvement in the important OPC UA industry standard (a central protocol in connection with Industry 4.0), one of the key future fields in enabling German industry to position itself both as user and provider. The BSI is working together with a leading sectoral association on standards for secure data transmission.

4.3 Promoting IT security in society and the widespread use of secure technologies

A vital requirement for the effective use of security technology is raising users' awareness of IT threats. All users are responsible for their own IT and must therefore also take responsibility for security measures. Only by acting on their own initiative users can protect themselves from some of the threats discussed in chapter 2. In its capacity as the national IT security agency the BSI provides a range of support for the various target groups.[20]

Another key requirement for increasing IT security in Germany is the use of more secure and more reliable technologies. From an information technology viewpoint the development, provision and universal application of trustworthy crypto and cyber technologies for all target groups is of decisive importance in order to minimise the risks posed by critical security threats.

To this end it will be essential to provide scalable cyber security options which facilitate the provision of levels of protection adjusted to the specific needs of the target group in question. Given that over 80 per cent of all cyber threats can be warded off simply by taking basic security measures, it is necessary to make basic technologies available to private individuals and SMEs, thereby allowing them to contribute to enhancing cyber security. In this connection it will also be necessary to provide overall solutions which, in conjunction with crypto- and cyber security mechanisms, provide protection against threats at different levels.

Through the structural options it has implemented, for instance in the shape of De-Mail, the federal government has for the first time created a universal public key infrastructure in Germany. The solution will in future support both transport encryption and end-to-end encryption. Currently over 90 per cent of all e-mails are transmitted in unencrypted form. Furthermore, the two-factor-authentication process means that De-Mail offers security mechanisms against identity theft, which is often successful due to the fact that many providers use the standard software-supported password procedure.

Another indirect promotion of IT security in society is the continuous security analysis of universally used open-source IT security and crypto-libraries as well as the ongoing development and maintenance of their security. This allows vulnerabilities such as Heartbleed, with its widespread impact, to be virtually eradicated and brings about a sustained improvement in the security characteristics of these software libraries.

In this context the business world has a responsibility to come up with IT security solutions. Providers could make easy-to-operate IT security solutions available to their customers across the board. A key success factor here would be the virtually complete automation of the process of setting up security functionality. Online providers too could provide individuals with greater protection, for instance by introducing multi-factor authentication systems to protect them from identity theft.

However, the business world too can fall victim to cyber attacks, particularly in the form of cyber-espionage. Accordingly, mechanisms need to be developed and universally applied which will provide adequate protection against high-grade forms of attack such as Advanced Persistent Threats (APTs). To this end, close collaboration between government, business and science are called for in order to allow the earliest possible detection of attacks and attack forms and compile a joint situation assessment and share this knowledge, including defence mechanisms, as it already happens in the CERT association. Another central cooperation platform for government and industry is the Alliance for Cyber Security, which around 1,000 companies and institutions have now joined and which has come up with 180 concrete recommendations. The development of such voluntary models is vital to ensuring the rapid sharing of information faced with a world of dynamically changing technology and circumstances in order to quickly come up with pragmatic security solutions and defensive measures.

Our current knowledge of ICS attacks, with Stuxnet being the starting point, have put the spotlight on the security of Industrial Control Systems and indicates that greater attention will have to be devoted to this issue in future. In order to tackle this threat the following measures in particular must be addressed:

- Increased attention to Industrial Control Systems security by Computer Emergency Response Teams (CERTs).
- The development of security profiles specially tailored to Industrial Control Systems at both system and product levels as well as the devising of technology-specific minimum standards.
- More intense analysis of attacks on clouds and development of security standards and measures.

4.4 Guaranteeing critical infrastructure protection

Operators of critical infrastructure have a duty to maintain minimum IT security standards due to the potentially far-reaching societal consequences of a breakdown or failure of infrastructure provision and their consequent responsibility for the common good.

The federal government maintains especially close relationships with these operators. In 2007 the UP KRITIS association was formed as a cooperation between the government and the critical infrastructure industry.

In light of the developing security threats since 2011 there is a need to further strengthen the working relationship between the government and critical infrastructure operators. UP KRITIS has been upgraded in terms of content and structure, allowing it to become significantly more deeply involved in the critical infrastructure sector. The IT security bill drawn up by the Federal Ministry of the Interior provides among other things for minimum standards and reporting duties to which operators of critical infrastructure should be subject. These reports will be used to compile a situation assessment which will be made available to the companies concerned. Simultaneously the reported incidents can be used as the basis for reinforcing and optimising the support and advice provided for companies by the BSI. That way the BSI will be in a position to provide critical infrastructure operators with more effective support in the event of an IT security incident.

5 Glossary and list of abbreviations

Advanced Persistent Threats
Advanced persistent threats (APT) are targeted cyber attacks on selected institutions in which the attackers gain persistent long-term access to the victim network and then widen the attack to additional systems. The attacks involve the deployment of major resources and considerable technical skill on the attackers' part and are generally difficult to detect.

Adware
Adware are programs which finance themselves via advertising. Malware programs which serve advertising purposes are also described as adware. When adware is downloaded programs are generally installed which perform espionage functions. In most cases you are notified of this in the license and conditions of use.

Application/app
An application, or app for short, is a piece of user software. The term is frequently used in connection with applications for smartphones or tablets.

Attack vector
Attack vector denotes the combination of attack routes and techniques whereby the attacker gains access to IT systems.

Bot & botnet
A botnet is a collection of computer systems which have been attacked by a remotely controllable malware program known as a bot. The affected systems are controlled by the botnet operator via a command-and-control server (C&C server).

Bring Your Own Device
Bring Your Own Device (BYOD) denotes the use of private devices for professional purposes and their integration into company networks.

CERT/Computer Emergency Response Team
Computer emergency team made up of IT specialists. Many companies and institutions have now established CERTs to take care of defending against cyber attacks and preventing IT security incidents and responding to them should they happen.

CERT-Bund
CERT-Bund (Computer Emergency Response Team of the Federal Government) is a unit of BSI which functions as the central coordinating body for the government department for both preventive and reactive measures in relation to security-related incidents affecting computer systems.

CERT Association (CERT-Verbund)
The German CERT Association is an alliance of several German CERTs at companies and in government departments.

Bürger-CERT
The Bürger-CERT (see CERT/Computer Emergency Response Team) of the BSI (www.buerger-cert.de) warns citizens and SMEs rapidly and expertly about malware and vulnerabilities in computer applications and provides information on security updates.

Cloud/cloud computing
Cloud computing refers to offering, using and charging for IT services over the Internet. The services provided can be rapidly adapted to changing needs. These services are offered and used exclusively via defined interfaces and protocols. The range of services offered under cloud computing embraces the entire spectrum of information technology, including infrastructure (e.g. computing power, memory), platforms and software.

Command-and-control server
See 'Bot & botnet'.

Critical infrastructure/KRITIS
Critical infrastructure means institutions and enterprises of particular importance for the common good of a country whose breakdown or impairment would lead to long-term supply bottlenecks, significant disruption of public security or other dramatic consequences.

Critical infrastructure sectors
Currently, nine sectors in Germany have been defined as critical infrastructure: Transport and traffic, Energy, Information technology and telecommunication, Finance and insurance industries, Government and public administration, Nutrition, Water, Health, Media and culture.

DNS
The Domain Name System (DNS) assigns the names used on the Internet, such as www.bsi.bund.de, and the associated IP addresses.

Dos & DDos attacks
Denial of service (Dos) attacks are directed at the availability of services, websites, individual systems or entire networks. If such an attack is launched in parallel by several systems this is known as a distributed denial of service (DDos) attack. DDos attacks frequently involve very large numbers of computers or servers.

Drive-by download/drive-by exploits
Drive-by exploits involve the automated exploitation of vulnerabilities. When a PC user visits a website infected with drive-by exploit vulnerabilities in the Web browser, in browser plug-ins or in the operating system are exploited in order to install malware undetected on the PC without any interaction on the users' part.

End-to-end encryption
To send particularly sensitive information securely by e-mail both the transport channel and the e-mail content can be encrypted. To use end-to-end encryption both the sender and the recipient require encryption software suitable for the message which must be installed on both computers.

Exploit kit
Exploit kits (aka exploit packs) are tools for cyber attacks which are placed on legitimate websites. A variety of different exploits are used in an automated attempt to detect and exploit a vulnerability in a Web browser or plug-in in order to to install malware.

ICT
Short for 'Information and communication technology'. This refers to the entirety of information technology, communication technology and their interactions, for instance in the form of communication networks.

Identity theft
Identity theft or misuse involves the acquisition and unauthorised use by third parties of personal data such as postal and e-mail addresses, dates of birth, bank account or credit card numbers. The attackers' aim is generally to gain a financial advantage using the confidential information, or more rarely to discredit the person whose details have been stolen. Identity theft is chiefly done via social engineering, malware on infected systems or data theft after hacking of online services.

Industrial Control System (ICS)
Systems for automating production process are known as Industrial Control Systems (ICS).

Industry 4.0
Industry 4.0 is an umbrella term for the merging of the real and virtual worlds into an Internet of things, with the focus on the future shape of industrial production and logistics. It will involve the interconnection of systems right across a business, both internally and externally: machines, sensors, production facilities, marketing, sales, procurement and logistics.

Internet of things
By Internet of things we mean the linking up of clearly identifiable physical objects with their virtual representations in an Internet-like structure via an embedded electronic chip.

IS audit
Information security audits are a key component of any successful information security management system. Only regular checks on established security systems and information security processes can ensure their effective implementation, up-to-dateness, completeness and appropriateness, and therefore the current state of your information security. The IS audit is thus a tool for determining, achieving and maintaining an acceptable level of security in an institution.

Log data & log file
A log file contains the record of actions and processes on a computer.

NTP
The Network Time Protocol (NTP) performs the time synchronisation of IT systems in networks.

NTP reflection
This is a specific kind of DDos attack. In a reflection attack the victim's system is not directly attacked. Instead the attacker operates via reflection, sending a simple query carrying the falsified sender address of the victim's system to the target system. Due to the falsified address the answer to the attacker's query is then sent not to the attacker's system but to the victim's. The answer to the query will be significantly larger than the query itself, and as a result the attacker is able to generate a lot of attack bandwidth without expending much of their own bandwidth. We refer to this as the amplification of the bandwidth used.

OpenSSL
OpenSSL is a free software library which implements encryption protocols such as Transport Layer Security (TLS).

Patch/patch management
A patch is a software package which software manufacturers create in order to eradicate vulnerabilities in their programs, or make other improvements. Many programs offer an automated update function to facilitate the downloading of these updates. Patch management refers to processes and procedures to ensure that an IT system receives available patches as quickly as possible.

Penetration test
A penetration test is a controlled attempt to infiltrate a given computer system or network in order to try and identify vulnerabilities. For the purpose the same or similar techniques are deployed as would be used in a real attack. Their aim is to assess the prospect of a real attack succeeding, thereby assessing the efficacy of the existing security measures and determining whether there is a need for additional security measures.

Phishing
The term 'phishing' is a blend of the words 'password' and 'fishing', i.e. going fishing for passwords. The attacker attempts via bogus websites, e-mails or text messages to extract personal data from an Internet user and thus commit identity theft.

Plug-in
A plug-in is an extra piece of software or a software module which can be integrated into a computer program in order to extend its functionality.

Ransomware
Ransomware is malware, with the help of which an attacker prevents access to or the use of data or entire computer systems. The usual purpose of this is to extort money (the 'ransom').

Shell
A shell is software which functions as the interface between people and a machine. In normal usage the word shell has come to mean both the command line interpreter and graphic user interfaces such as Windows Explorer or the Apple Finder.

Social Engineering
In cyber attacks using social engineering criminals attempt to induce their victims to disclose data of their own free will, circumvent protective measures and willingly install malicious code on their systems. Just like in the field of espionage, cybercriminals skilfully exploit human weaknesses such as curiosity to gain access to sensitive data and information.

Spam
Spam is defined as unwanted messages sent en masse and in an untargeted fashion via e-mail or other communication services. In harmless variants spam messages generally contain unsolicited advertising. However, spam often comes with attachments containing malware, links to infected websites or is used for phishing attacks.

SSH
SSH stands for Secure Shell, an application allowing the establishment of an encrypted network connection to a remote device.

SSL/TLS
TLS stands for Transport Layer Security, an encryption protocol for the secure transmission of data over the Internet. Its predecessor was SSL (Secure Sockets Layer).

Twitter
Twitter is a real-time digital application for sending short messages.

UP KRITIS
UP KRITIS (www.upkritis.de) is a public-private collaborative initiative between critical infrastructure operators, their professional associations and the relevant government agencies.

VDE
Stands for Verband der Elektrotechnik Elektronik Informationstechnik e.V. (Association for Electrical, Electronic & Information Technologies).

Watering hole attacks
The analogy is to a watering hole which attracts prey animals and is thus also frequented by their hunters. In this type of attack websites which are highly likely to be visited by a target individual are first hacked into and infected with malware. When people then visit this website it automatically installs malware on their computers, for instance via drive-by download.

Web browser
Web browsers are special computer programs for displaying websites on the World Wide Web or documents and data generally.

Zero-day exploits
Zero-day exploits make use of a vulnerability as soon as it has been discovered by criminals. This leaves users and developers very little time to take countermeasures.

6 List of figures, tables and footnotes

List of figures

List of tables

Footnotes

1 (page 7) BITKOM statistic: http://www.bitkom.org/de/markt_statistik/64086_79916.aspx
2 (page 12) DIVSI: PRISM and the impact: Confidence in the Internet deteriorates; https://www.divsi.de/prism-und-die-folgen-sicherheitsgefuehl-im-internet-verschlechtert/
3 (page 12) http://www.bitkom.org/de/presse/8477_79728.aspx
4 (page 12) IT Security Survey: SMEs are an at-risk group (Germany Secure on the Net); https://www.sicher-im-netz.de/press/releases/umfrage-it-sicherheit-kleine-unternehmen-sind-risikogruppe
5 (page 12) http://secunia.com/resources/countryreports/de/
6 (page 12) Allianz for Cyber Security: Cyber Security Survey 2014, in which 257 companies, government departments and other undertakings of all sizes and sectors took part. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/Umfrage/umfrage2014.html
7 (page 13) http://secunia.com/resources/countryreports/de/
8 (page 13) http://news.netcraft.com/archives/2014/02/07/are-there-really-lots-of-vulnerable-apache-web-servers.html
9 (page 13) http://developer.android.com/about/dashboards/index.html
10 (page 13) gs.statcounter.com/#desktop-os-ww-monthly-201302-201407
11 (page 15) Complete description of threats and best practice in the document 'Industrial Control System Security – Top 10 Threats and Countermeasures 2014'; https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/hardware/BSI-CS_005.html
12 (page 17) http://www.google.com/transparencyreport/safebrowsing/malware/?hl=de
13 (page 18) The BSI warns again about the widespread distribution of malware via advertising banners; https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2013/Verteilung_von_Schadprogrammen_ueber_Werbebanne_05042013.html
14 (page 20) Allianz for Cyber Security: Cyber Security Survey 2014, in which 257 companies, government departments and other undertakings of all sizes and sectors took part.
15 (page 21) The Domain Name System (DNS) assigns the names used on the Internet, such as www.bsi.bund.de, and the associated IP addresses.
16 (page 21) The Network Time Protocol (NTP) performs the time synchronisation of IT systems in networks.
17 (page 24) http://www.bka.de/DE/Presse/Pressemitteilungen/Presse2014/140827__BundeslagebildCybercrime.html
18 (page 24) Further information on the subjects of espionage and economic espionage in the Report on the Protection of the Constitution (Verfassungsschutzbericht) 2013 produced by the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz). http://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/verfassungsschutzberichte/vsbericht-2013
19 (page 26) Study: Industrial Espionage 2014; http://www.corporate-trust.de/pdf/CT-Studie-2014_DE.pdf
20 (page 38) https://www.bsi-fuer-buerger.de/BSIFB/DE/Wissenswertes_Hilfreiches/Service/Checklisten/Massnahmen_gegen_Internetangriffe.html; https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/kataloge.html

Legal notice

Publisher
Federal Office for Information Security
(Bundesamt für Sicherheit in der Informationstechnik – BSI)

Source
Federal Office for Information Security
(Bundesamt für Sicherheit in der Informationstechnik – BSI)
Godesberger Allee 185–189
53175 Bonn, Germany

Email
bsi@bsi.bund.de

Phone
+49 (0) 22899 9582-0

Fax
+49 (0) 22899 9582-5400

Version
November 2014

Design
Serviceplan Berlin

Printing
Druck- und Verlagshaus Zarbock, Frankfurt am Main

Texts and editing
Federal Office for Information Security
(Bundesamt für Sicherheit in der Informationstechnik – BSI)

Title page picture credit
Fotolia

Graphics
BSI

Item number
BSI-LB15503e

This brochure is part of BSI's public relations.
It is distributed free of charge and is not destined for sale.

www.bsi.bund.de