Federal Office
for Information Security

The State of IT Security in Germany 2016

Foreword

The 2016 BSI Status Report provides a reliable and in-depth description of current developments in IT security. It outlines the current exposure in Germany, assesses vulnerabilities in IT systems and illustrates both means and methods of attack. The Status Report finally provides information about the structures and framework conditions of IT security in Germany.

The reporting period was characterised by a continued increase in the professionalisation of attackers and their methods of attack. The number of known malicious program versions increased further in 2016 and, in August 2016, the recorded figure was over 560 million. At the same time, current conventional defence measures are continuing to lose their effectiveness. This affects all users – private, corporate, state and administrative.

The threat from ransomware in particular has increased in Germany significantly since the end of 2015. The crippling of information technology systems in hospitals, companies or in administrative bodies in order to extort ransom money is a development to be taken seriously and which demands decisive action.

This also applies to attacks on the IT systems of the German Bundestag and on parties represented in the Bundestag. The specific targeting of all organisations involved in the democratic decision-making process represents a new dimension to the threat from such cyber-attacks. If they are successful, I anticipate a long-term risk to liberal society and our democracy.

IT, of course, is always dynamic and requirements in terms of its security grow just as quickly. IT security, however, must always be kept in mind right from the start, regardless of how rapid technical developments might be.

The new cyber security strategy is the Federal Government's strategic framework relating to increased security in cyberspace. We want to enable secure and autonomous action in a digitalised world. Only in this way are we able to exploit the opportunities offered by digitalisation without restriction. Collaboration between state and business must therefore improve and Germany must also continue to take an active role in European and international cyber security policy.

The reporting year shows that vulnerabilities in software and hardware can be easily exploited by attackers, and this is indeed occurring. Increased prevention, detection and response is needed to prevent this. All stakeholders must give this the attention it requires and contribute to increased digital security. This BSI Status Report clearly underlines this necessity.

Dr Thomas de Maizière, Member of the Bundestag
Federal Minister of the Interior

Foreword

Digitalisation has become an important basis for technological progress as well as economic and social well-being in Germany. The Federal Office for Information Security is the national cyber security authority and organises information security in digitalisation by means of prevention, detection and response on behalf of the state, business and society.

In the 25 years since it was formed, the BSI has developed from the encryption of information, via protection of the government network, into the national cyber security authority with responsibility for the organisation of information security in the digitalisation process. The BSI offers solutions with which IT users are better able to confront the current critical IT exposure and minimise risks. The BSI also promotes opportunities for sharing information and experience. These include the Alliance for Cyber Security, the established cooperation platform which currently has approximately 2,000 participants, and UP KRITIS which has made an important contribution to the dependable provision of critical services for people in Germany since the official launch at the start of 2007.

The complexity of IT, and increasing digitalisation and networking provide cyber attackers with wide-ranging opportunities to spy on information, sabotage business and administrative processes and otherwise benefit by unlawful means at the expense of third parties. These attacks focus on companies and critical infrastructures as well as on administrative bodies, research institutions and citizens.

We are increasingly entrusting networked IT systems with sensitive processes – including autonomous vehicles and vital facilities involved in the provision of public services. Digitalisation without sufficient cyber security will not be successful.

The BSI is working together with a wide range of stakeholders from the state, business and society in order to counteract existing risks with effective and viable security measures. In addition to the significant risks, this report on the state of IT security in Germany therefore also covers approaches used by the BSI to contribute to promoting cyber security.

The BSI meets the expectations on us by performing our duties independently and in line with the latest technological developments. At the same time, support provided by the state cannot be solely responsible for security in the digitalisation process – all stakeholders in the state, business and society are required to take joint responsibility and implement the measures required. The BSI organises this cooperative process.

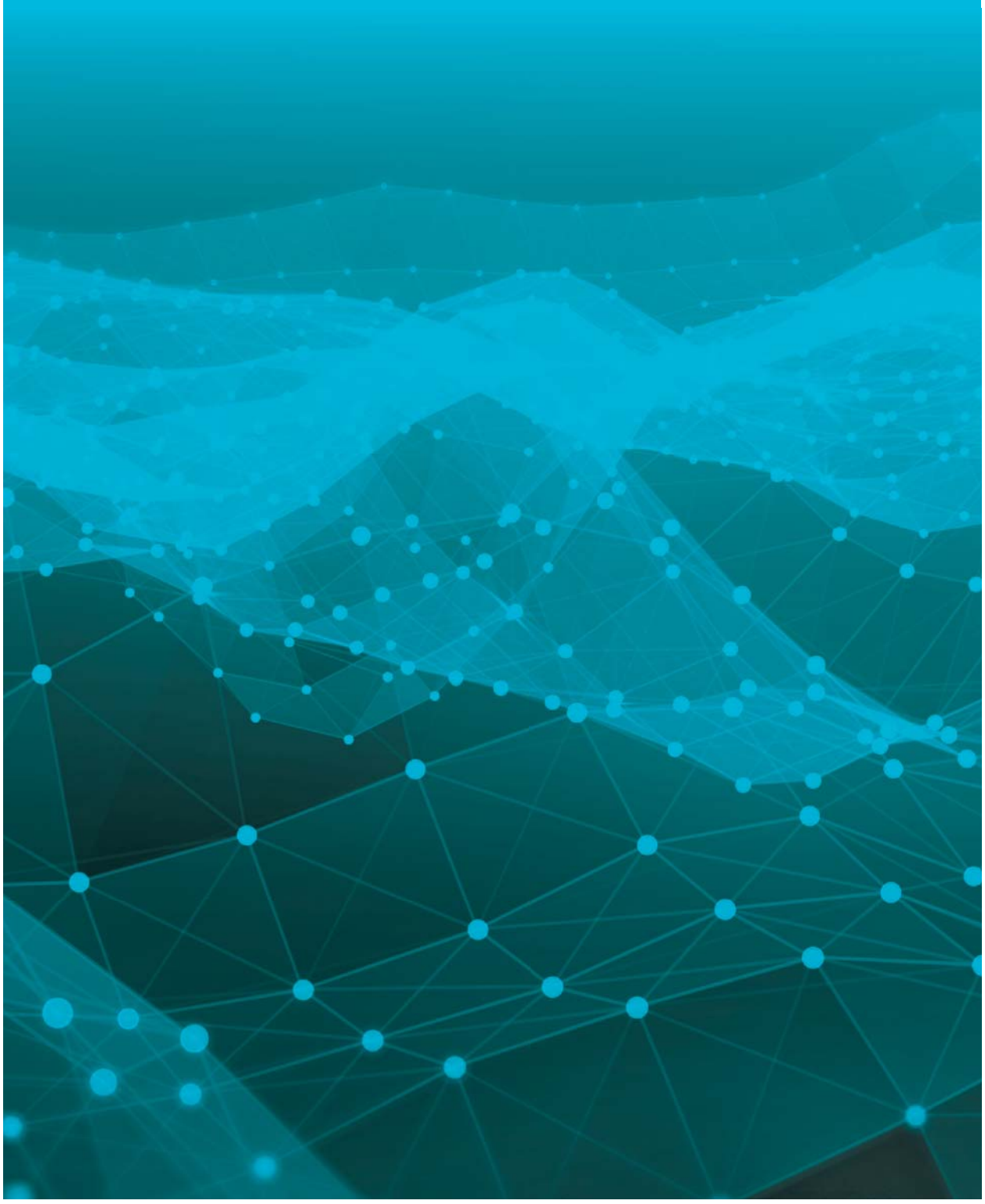
In this 2016 Status Report, the BSI provides information about current risks for IT security in Germany as well as countermeasures. The current exposure is described in detail in Chapter 1. Chapter 2 addresses the current exposure of the Federal Government and Chapter 3 focuses on the exposure of critical infrastructures. Chapter 4 uses selected core issues to highlight the approaches and services available from the BSI. Finally, following a summary of the main findings of the report, Chapter 5 looks ahead to future developments.

I hope you find this an interesting read. I am looking forward to your comments.

Arne Schönbohm
President of the Federal Office for Information Security (BSI)

Contents

1 Current exposure



1 Current exposure

The following chapter describes the current exposure in Germany which is characterised by the methods and opportunities exploited by attackers, but also by specific determining factors.

1.1 Causes and determining factors

1.1.1 Cloud Computing

Introduction

The BSI evaluated a range of public sources from September 2015 to February 2016 in order to assess the current IT security situation in cloud computing, for example relevant information portals or cloud providers' self-disclosures. The incidents recorded were classified in the IETF (Internet Engineering Task Force) cloud layer model according to risks such as manipulation, information outflow, loss of service, and privilege escalation and were broadly categorised in terms of severity.

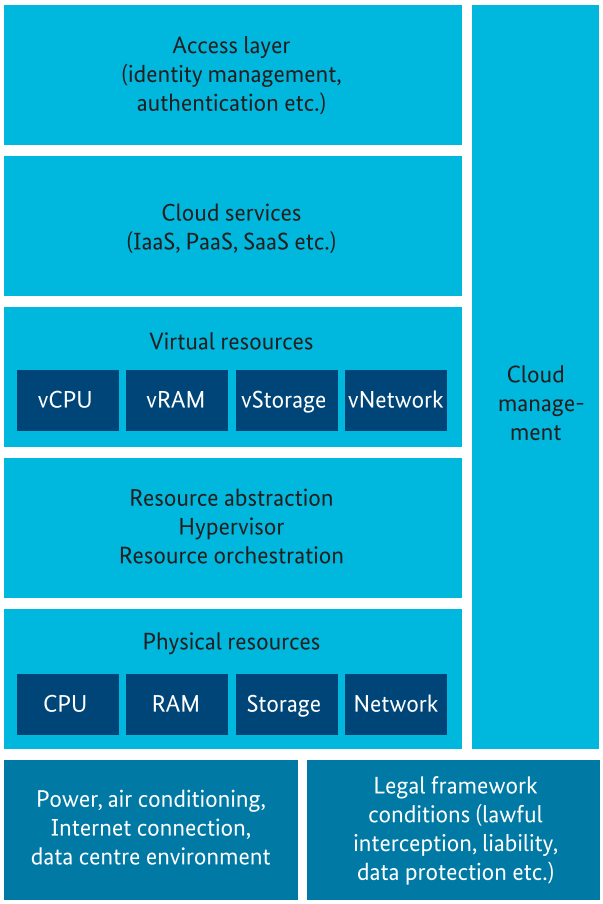


Figure 1: IETF cloud layer model

Current situation

During the investigation period, 404 incidents were recorded, 98 percent of which concerned the availability of cloud services. This high proportion can be explained by the fact that self-disclosures from cloud providers almost always relate to availability. It does not therefore follow that information outflow or manipulation only occurs on a very small scale. 78 percent of the service outages (317 incidents) occurred directly in the services layer of the cloud. Outages in this layer are in most cases due to software errors or problems with updates. Of the 317 outages in this layer, 92 were the result of technical failure, 13 were due to human error and two were due to intentional acts – no information was provided about the remainder. The virtual resources layer was the second most frequent source of outages with a figure of 12 percent (46 incidents). Outages in this layer mean that the service software does not have sufficient virtualised resources available (computing power, hard drive storage and network services). Technical failure and human error accounted for six incidents in both cases, and in 34 cases the cause is not known. The remaining 10 percent of cases regarding availability concerned cloud management and physical resources.

The majority of outages (377) were resolved within one hour and a further 12 outages were resolved within four hours. It is worth noting that 91 of the 92 outages due to technical failure in the cloud services layer were resolved within one hour.

Assessment

The figures show that the cloud providers examined here generally achieved availability of approximately 99.9 percent (up to nine hours of outages per year). Cloud providers appear only marginally restricted as a result of cyber-attacks in terms of the availability of their services since they have sufficiently effective countermeasures in place. Presumably, attacks on cloud service availability are also not as lucrative as the theft of customer data. The accumulation of customer data with cloud providers tends to be high, thus making such data an attractive target for data theft. This means complex attacks involving a high level of effort and cost for the attackers may be worthwhile. In order to counter this threat and to avert any damage, joint efforts are necessary in preventing and detecting cyber-attacks as well as in the response of cloud providers to this threat.

A welcome development is the provision of information platforms by cloud providers such as Amazon Web Services, Google, Microsoft and SAP on which detailed information is made available about the current security status of different parts of the cloud. This represents a step towards increased transparency for customers and serves as a source for assessing the current IT security situation.

1.1.2 Software vulnerabilities

Introduction

Software products are increasingly complex creations in which errors may occur during development. This results in software which contains vulnerabilities. Current software products used by millions of people worldwide are particularly relevant in terms of the current level of IT security. Due to their widespread adoption, the exploitation of vulnerabilities in these products may potentially result in serious IT security incidents across a wide area.

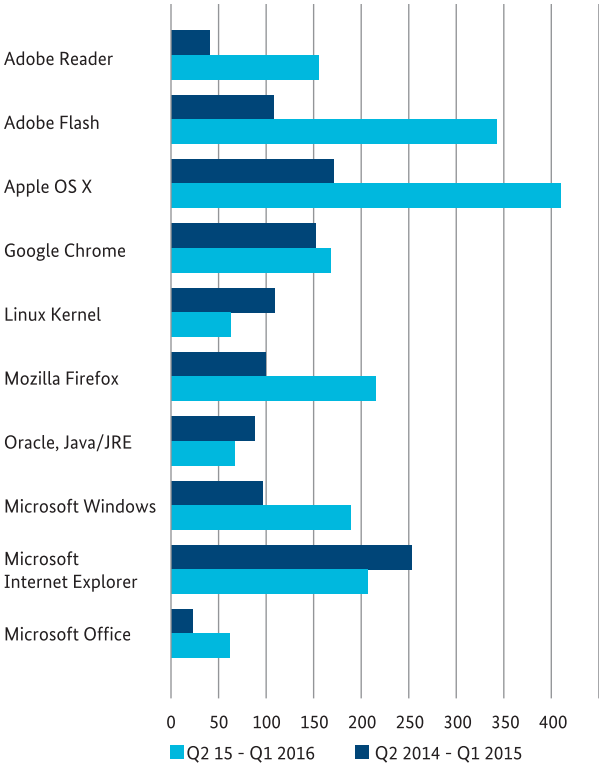


Figure 2: Incidence of vulnerabilities from Q2/2014-Q1/2015 to Q2/2015-Q1/2016

Current situation

- There was a relatively negligible level of variation in the number of vulnerabilities in half of the software products considered compared to the same period in the previous year (Figure 2). Of the remaining software products, Adobe Reader, Flash Player and Apple OS X were the focus of increased attention from security researchers who had reported a large number of detected vulnerabilities to manufacturers as a result of automated testing (fuzzing) in particular. Due to a strict disclosure directive from security researchers, manufacturers are under pressure to resolve vulnerabilities quickly and also document this publicly by means of a CVE entry.

- In 2016, 717 critical vulnerabilities were identified by the end of September for the ten software products (Fig. 3) which appear most frequently in the BSI traffic light system for vulnerabilities. The detection of a large number of vulnerabilities in itself is not necessarily a problem. It is however crucial to assess whether potential critical vulnerabilities have been detected by fuzzing with only minimal effort, as attackers also actively apply these techniques in their search for vulnerabilities. Due to vulnerabilities which were comparatively easy to exploit and due to their prevalence, attackers therefore shifted their focus in particular towards Adobe Flash. As a result, some vulnerabilities were initially or subsequently discovered and exploited by attackers. Microsoft Windows and Office have always been the focus of security researchers. Numerous vulnerabilities can repeatedly be found in Office by means of fuzzing, in particular using complex file formats.

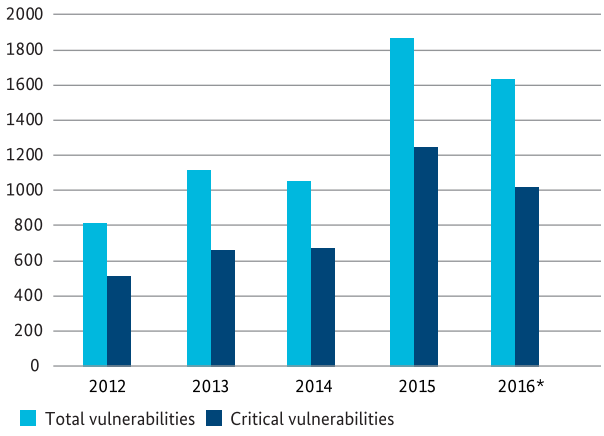


Figure 3: Number of all vulnerabilities in the ten most prevalent software products recorded in the BSI traffic light system for vulnerabilities* – figures for 2016 have been extrapolated from the vulnerabilities detected up to the end of September 2016.

The CVE list and its significance

The only globally recognised source for the publishing of new vulnerabilities is the MITRE Corporation's 'Common Vulnerabilities and Exposures' (CVE) database. The CVE list catalogues vulnerabilities according to a standardised procedure. The list currently contains over 76,000 entries. In the IT security sector, CVE numbers are often referenced in connection with vulnerabilities, often as the only source. Statements made regarding the security of a software product are justified in some cases with reference to the frequency of the entries in the list. Despite the list's general acceptance, frequent referencing and the information contained therein, the following questions need to be addressed:

» **What do the CVE entries indicate for a specific software product?**
Each manufacturer decides whether a vulnerability is entered in the list or not. It may also be the case that several independent vulnerabilities are combined in one entry in the CVE list.
The number of entries for one product is therefore of less significance, and it may also be the case that the CVE entry cannot be attributed to a specific vulnerability.

» **Is every vulnerability found also represented by a CVE entry?**
Some manufacturers receive a CVE number pool from which they can create their own entries. The remaining manufacturers and independent security researchers report vulnerabilities found to MITRE, who will then, if required, convert this into a list entry after verification. On the other hand, some manufacturers do not report any vulnerabilities whatsoever.

» **How high is the level of concern?**
The degree of severity and the potential for exploitation are listed in the NVD database (National Vulnerability Database), which contains further information about the CVE entries. No information is provided about the prevalence of the affected software. A vulnerability in a specific device driver, for example, has a different level of concern to a kernel vulnerability affecting all versions of an operating system.

The CVE database should therefore not be used on its own to assess the security of a software product. The significance is limited as a result of:

» variation in the reporting of vulnerabilities in software products
» the severity of the vulnerability not being assessed (only the link to the NVD entry provides further information in this regard)
» a lack of information about the prevalence of the software and therefore regarding the level of concern.

In addition to the CVE database, the BSI therefore also evaluates the related NVD entries so that vulnerabilities listed therein can be attributed to software products. The limitations described above regarding the significance related to the CVE database are therefore also reflected in the assessment of vulnerabilities in the software products: nothing can be said about the security of a software product based merely on the number of resolved vulnerabilities it contains. Even in the case of vulnerabilities that are publicly known, there is generally still exposure for the user – however, in this case the simple conclusion that the software is insecure likewise cannot automatically be made. Although, if the vulnerability is reported regularly, a conclusion of this nature would seem likely. The CVE and NVD databases cannot be used to analyse vulnerabilities in software products which have not been resolved because entries are almost never created until an update has been published. Since there is no generally accepted procedure for this, most analyses are restricted to drawing conclusions regarding software product security based on the resolved vulnerabilities.

Assessment

Vulnerabilities in software products continue to pose a relevant threat for the security of IT systems. In order to prevent malware intrusion into internal systems and avoid providing attackers with any opportunity to exploit these vulnerabilities, it is therefore always important to install the latest software or security updates.

Seasonal changes in the number of vulnerabilities detected reflect those software products which are currently the main focus of security researchers. This may be due to a high level of prevalence, poor software quality or a combination of the two. Conclusions may only be drawn in terms of improvements in software quality if there is a sustained reduction in the number and/or severity of vulnerabilities found in a software product over several years and where market relevance remains the same or increases.

For some manufacturers, it is only sustained public pressure which results in vulnerabilities in their products being resolved. The various quality improvement initiatives in the software industry are still in their infancy and, due to cost reasons, for example, they are not systematically implemented. Significant global changes in software quality are not currently identifiable, because selective improvements in one area generally compensate for deterioration in quality in another. A significant improvement would soon occur if all manufacturers directly implemented state-of-the-art technology from security research for all new products and gradually improved established products to this level. An enormous amount of catching up needs to be done at this point.

1.1.3 Hardware: Vulnerabilities in security elements

Introduction

The Kerckhoff's principle states that an encryption algorithm must not depend on the secrecy of the system itself but only on the secrecy of the key. Modern cryptographic procedures are a perfect example of adherence to this basic principle. It can be shown for these that the solution of what is taken to be a difficult mathematical problem is required to break the procedure. However, the secure storage and non-observable processing of the key itself is a problem. Hardware security elements are often used here which are forced to employ the principle of security through obscurity (which is actually disputed) in order to maintain the secrecy of the stored key – for example disguising operations executed via software by means of cryptographic blinding, by using physically implemented measures such as sophisticated sensor technology which constantly checks the operating conditions and detects attacks, or even by way of the minimal structure size prevalent in modern chips. All of these measures could be the target of an attack.

Current situation

In addition to faulty software, vulnerabilities in hardware may also constitute potential gateways for attacks. For example, hardware manipulation may take place as a result of modifications by additional modules, changes to existing circuitry, manipulation at the chip level or software modifications at the firmware level. In terms of the aforementioned opportunities for attack, the current level of risk compared to the previous year is unchanged.

Security elements are used in a wide range of forms and manifestations in order to protect digitalisation. These include smart cards in the form of a credit card or debit card, signature cards, identity cards or passports, FIDO token (token for two-factor authentication in accordance with the Fast Identity Online Alliance) or in the area of Pay-TV Trusted-Platform Modules on PCs, in connection with a Trusted Execution Environment on mobile phones, or in future in the area of Industry 4.0, the Internet of Things and in intelligent traffic infrastructures.

Attacks on security elements can be divided into two classes:

1. **Invasive** attacks which involve the physical manipulation of the chip, for example fault induction attacks by means of laser bombardments through to the modification of electronic circuitry.

2. **Non-invasive attacks** in which a side channel is exploited, for example the electromagnetic irradiation of the chip during key processing.

Vulnerabilities need to be identified in the first place and then exploited in the next stage for the practical implementation of attacks. The identification phase is often time-consuming, particularly in the case of hardware-based security elements. Up until a few years ago, both forms of attack were associated with very high financial outlay due to the structural size of semiconductors and the limited availability of the necessary laboratory equipment. However, the equipment prices for invasive and non-invasive attacks – such as a focused ion beam,

scanning electron or atomic force microscope and oscilloscope – have fallen to such an extent that new attack techniques must increasingly be anticipated.

Assessment

Even if the cost and effort required to successfully break a certified hardware security element is high, these types of attacks are often attractive for attackers. On the one hand, the high costs for specialised analytical tools are a one-off investment and, on the other, the target of the attack is often lucrative. For example, high profits can be made from the sale of copied Pay-TV cards or forged identity documents. Due to the increasing use of security elements as part of advancing digitalisation, new targets for attack are continually emerging which involve huge financial benefits for the attackers. Once a specific path of attack to a security element has been identified, it is often relatively easy to exploit the vulnerability detected, for example by means of template attacks. The exploitation of hardware vulnerabilities can be made much more difficult in practice, in part by the use of additional measures at the firmware level of the security element. However, software updates which are prevalent among traditional computer systems are not normally provided for security elements. Vulnerabilities in security elements therefore constitute a major threat. The replacement of parts is not intended for devices with embedded security elements which means that the entire device must be replaced. However, the ad-hoc replacement of a large number of chip cards already in use cannot be implemented practically for organisational reasons.

Server failure in the hospital computer centre

The facts: Three hospitals in Germany which receive IT services via a central computer centre were forced to work without electronic documentation as a result of a server failure.

The cause: A hard drive failure resulted in a complete server outage. The redundancy solution which was actually in place did not function correctly.

The effect of the damage: The disruption lasted for approximately 19 hours. Over this period, administrative computers could not be used. In the hospitals, the system for patient care documentation was also not available. This documentation therefore had to be completed manually and subsequently entered into the system once the disruption had been resolved. Since medical devices could be operated independently in 'stand alone' mode, patient care was not put at risk.

Target groups: Disruptions of this nature could in principle occur in any centralised IT network. It is therefore important that operators prepare themselves accordingly, and also set up and test redundancy mechanisms.

1.1.4 Hardware: Broadband router vulnerability

Introduction

In Germany there are currently around 30 million broadband connections. The network termination for these connections largely occurs by means of routers which are very often the only main security component used for protecting the user's internal network. It is therefore particularly important that the router is protected. If the router is manipulated or taken over by an attacker, the attacker is able to spy on or manipulate user communication data, for example, making the user's infrastructure become part of a botnet or conducting expensive conversations at the expense of the user.

Current situation

The number of known critical vulnerabilities in routers has risen over recent years. On the one hand, Figure 4 shows the trend in critical vulnerabilities since 2013. According to this, eight critical vulnerabilities were reported in routers overall in the years 2013 and 2014. This number almost doubled from 2015 to mid-2016. The chart also illustrates the period from when the vulnerability was reported to when the manufacturer provided the update. For example, it took 804 days for an update to be provided for four critical vulnerabilities. By contrast, other manufacturers publish the corresponding update when the vulnerability is reported, which means the period shown has a value of zero days. In this case, it is also likely that the vulnerability would have been open to attack for a while.

In light of this level of threat and the particular importance of a router, the BSI has published a test concept for broadband routers which is primarily targeted at Internet service providers and router manufacturers. The aim is to make the security of broadband routers measurable and to achieve a standardised level of security for devices. The test concept allows the relevant security properties of routers to be examined. This takes into account the basic security-relevant functions as well as support and also compliance with established safety standards. The test concept also covers examples of known security risks and attack scenarios. The test concept was developed in collaboration with Internet service providers, broadband router manufacturers and other interested parties.

Assessment

Following the removal of compulsory routers in August 2016, Internet users have more options when selecting their router. They should use this opportunity to make security the most important criteria when deciding on the purchase of a router. Manufacturers can implement safety functions with the help of the standards described in the test concept and explain this to users. Router owners should install security updates for their devices at regular intervals or make use of the automatic update function. Access to the web interface and to the router's WLAN should be protected in each case with an unique complex

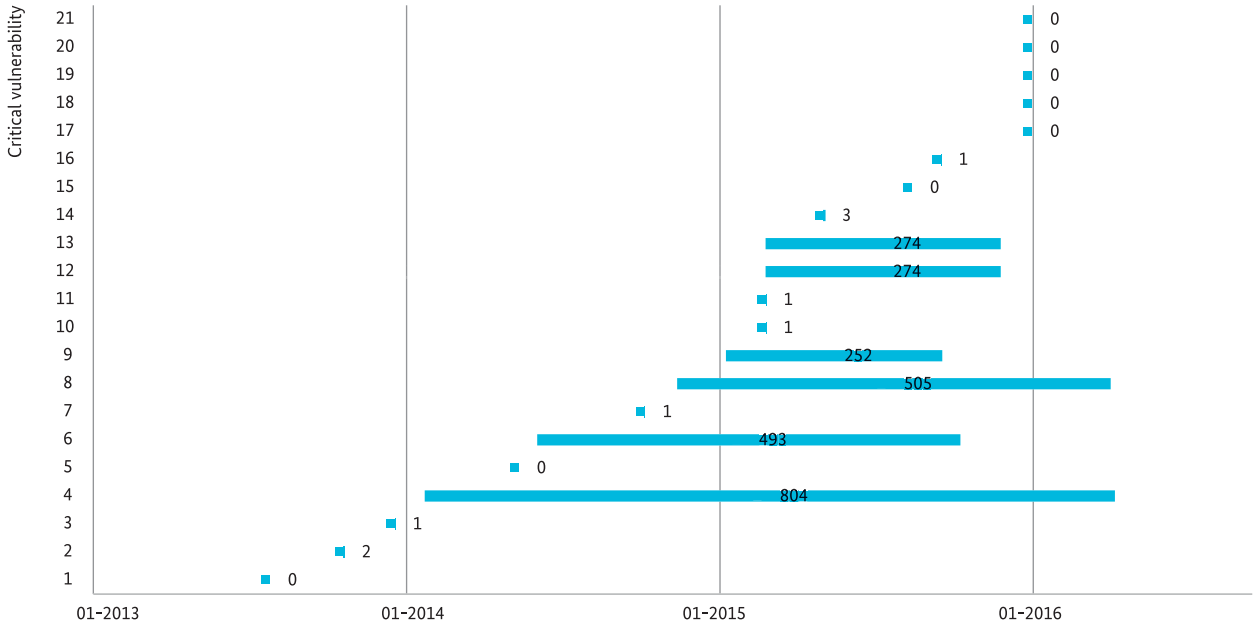


Figure 4: Critical router vulnerabilities, source: CVE details, last updated: June 2016

key in order to prevent attacks.

1.1.5 Cryptography

Introduction

The 'Digital Agenda' adopted by the Federal Government as well as the 'Charter for strengthening trustworthy communication' indicate that Germany's aim is to become the 'Number 1 encryption location' for the purpose of protecting its citizens, economy and administrative bodies from the spying or manipulation of communication. The work of the BSI is also focused on this goal. Cryptography remains a key component in the effectiveness of many IT security mechanisms.

Current situation

- Current cryptographic mechanisms in principle provide outstanding security guarantees.This means, for example, that two parties who may only reliably control their local computers and who do not share secrets with each other, are able to create a bug-proof connection to one another across a network – even if the entirety of the remaining network is controlled by an outsider. When strong mechanisms are used, the available computing power is, within practical boundaries, largely irrelevant for the outsider.
- This assessment is influenced by a variety of requirements which must be met in order that the intended security goals can actually be achieved:
  - the participating parties must control their own computer systems and the cryptographic endpoints must be protected against third-party control or from being compromised in other ways.
  - At least one instance of the secure distribution of individual public keys must be guaranteed by means of other mechanisms.
  - It must not be possible to monitor communication at the endpoints by direct means, for example by means of compromising irradiation or the use of monitoring equipment.
  - The implementation of cryptographic mechanisms must be mathematically correct and must also be tempered against attacks at the implementation level.
  - The cryptographic protocols used must not contain any vulnerabilities. This is clearly harder to ensure for complex protocols than for the security of basic cryptographic functionalities used such as block ciphers or public key encryptions.
  - The security guarantees for modern cryptographic mechanisms are generally very strong but technically are also very specific. If the intended security goals are not precisely aligned with the security guarantees of a cryptographic protocol, vulnerabilities may occur.
  - The outsider may well have any amount of computer power at their disposal in practical terms, but may not have the cryptographic analytical competencies which qualitatively extend far beyond the level of public research.
- In the area of public key cryptography, virtually all security guarantees are lost if the outsider has a scalable universal quantum computer.
- Besides the legitimate use of cryptographic mechanisms, use by criminals has recently again become the focus of public interest, for example in connection with ransomware.

Assessment

With few exceptions, cryptographic algorithms which reflect the current state of cryptographic knowledge can be regarded as secure. Many slightly older mechanisms still provide a high level of security when used correctly. Despite this, many cryptographic systems occasionally still fail to perform their security function even today.

Various problems may, in practice, result in the failure of a cryptographic system. These include insufficient endpoint security, errors in implementation, errors at the protocol level, security problems in the context of the backwards compatibility of protocols used, problems with the initial distribution of public keys or lack of alignment between security goals and the security provided by cryptographic mechanisms. In particular, errors in widespread implementation may also place the security of many systems at risk. The fact that many systems never, or only rarely, receive software updates or are not considered in security analyses means that vulnerabilities can be used productively even long after they have been detected. This last point concerns, in particular, embedded devices (Internet of things), hardware components of larger systems with their own firmware and mobile Internet devices. In addition to this, a series of attack paths exist which are mainly suited to targeted attacks on individual users, for example the extraction of key material by means of the side channel analysis of an implementation.

A traditional crypto-analysis is rarely successful

Current issues in cryptography

Examination of cryptographic implementation.
OpenSSL is a common cryptographic open source library. It implements a range of cryptographic functionalities. In practice, TLS implementation is the most significant. Due to the major importance of the library, the BSI has commissioned a study to examine the safety characteristics of OpenSSL. As part of this, the random number generator was examined, an investigation was conducted into implementation vulnerabilities and a systematic documentation of the library was undertaken. Information was also prepared which is intended to facilitate configuration in accordance with the requirements of Technical Guideline TR-02102 for components which use OpenSSL. The 'Source code based investigation of cryptographically relevant aspects of the OpenSSL library' study can be downloaded from the BSI website.

Analysis of Linux-RNG
Effective and trustworthy security mechanisms are a basic requirement for ensuring information security at a technical level. Many IT systems now rely on the Linux operating system. Besides PCs, these also include many embedded systems such as network routers or load balancers. Cryptography plays an important role in virtually all of these devices. Keys for the GnuPG encryption solution are generated on desktop PCs in order that emails can be encrypted; load balancers create TLS secure connections with web servers so that data can be transmitted in encrypted form. Secure keys are needed for these types of cryptographic operations. These are keys which an attacker cannot predict and therefore cannot use to break the encryption.
Good random numbers are the basis for strong encryption. In order for the cryptographic key generated to be secure, it must therefore be ensured that the Linux random number generator (RNG) really does supply random data and not predictable data. The BSI is currently having the RNG for each latest version of Linux tested for a specified period of time. This will allow the BSI to provide information about the security of this RNG, but in particular also about cryptographic systems which use this RNG for generating key material. One key aspect of this investigation is proof that the Linux RNG is compliant with one of the functionality classes specified by BSI. Once this compliance is assured, the Linux RNG will have proven that it meets certain characteristics with regard to the quality of the random numbers, the entropy content and security etc. This proof will enable, on the one hand, comparisons to be made with other RNGs and, on the other, this classification may make Common Criteria certification or even product approval easier if the products use the Linux RNG. The investigation report is available on the BSI website.

Technical Guidelines in the BSI-TR-02102 series
An important responsibility of the BSI is to provide recommendations to the Federal Government, businesses and private users regarding the secure use of IT systems, for example in the form of Technical Guidelines. The objective of the Technical Guidelines is to disseminate appropriate IT security standards. Technical Guidelines are therefore generally aimed at all parties involved in the installation or protection of IT systems. They complement the BSI's technical test specifications and provide criteria and methods for conformity evaluations and ensure the interoperability of IT security components as well as the implementation of defined IT security requirements. The recommendations support businesses, for example, in operating web servers securely. They also support Federal Government authorities in implementing data exchange procedures so that, when data is transmitted, it can be protected in accordance with state-of-the-art cryptographic techniques.
For this purpose, for example, the BSI has created and maintained the Technical Guidelines of the BSI-TR-02102 series over many years. The series consists of four documents which address general cryptographic recommendations such as key length or cryptographic methods (part 1), protocols such as TLS and SSH, and specific recommendations related to these for the use of these protocols (parts 2 and 4) and recommendations for IKEv2/IPsec (part 3). The Technical Guideline BSI-TR-02102-2 (TLS) forms the basis for the TLS minimum standard which makes this Technical Guideline binding for the Federal Government. The Technical Guidelines are updated at least once per year.

Sweet32
Sweet32 is a cryptographic attack which exploits the fact – which has been known for a long time – that each block cipher becomes insecure when very large quantities of partially known plain text are encrypted with a key. The point at which the insecurity occurs is related to the block size of the cipher and the selected operating mode. Sweet32 focuses on the use of relevant observations of (outdated) 64-bit block length ciphers (such as Triple-DES and Blowfish) in CBC mode and in particular on the exploitation of vulnerabilities occurring against TLS connections. In a similar way to other attacks against TLS (such as CRIME and BEAST) recently discussed, a 'man in the browser' scenario is also used here. Here, the victim is coaxed by the attackers into accessing one of the websites controlled by them and this makes the victim's computer transmit the same message continually via the TLS channel. Following the transmission of approximately 232 cipher text blocks, the attacker manages to decrypt a session cookie.
These attacks are not a problem if a block cipher with a block length of 128 bits is used or if a key change is enforced in good time when using a legacy cipher with 64-bit block length (see also BSI-TR-02102-1). It is possible to assess the point at which significant vulnerabilities are likely to become relevant for Sweet32. This therefore means that the countermeasure of a well-timed key change is reliable.

with modern encryption mechanisms. However, it is still important in practice because the identification of theoretical vulnerabilities in crypto-systems provides an early warning system against the likelihood of practical difficulties occurring. Crypto-analytical advances also have the potential of extensively weakening a procedure's security guarantees. However, it must generally be regarded as unlikely that cryptographic systems which are currently judged as being state-of-the-art by public research, can in practice, for example, be broken crypto-analytically by external intelligence services.

The development of universal quantum computers would render virtually all public key procedures unsafe, because the underlying mathematical problems (factorising and discrete logarithms) could be solved on a quantum computer in polynomial time using Shor's algorithm. A quantum computer suitable for executing Shor's algorithm for key lengths and public key algorithms in use today does not exist. However, in recent years there is evidence that clear progress has been made, at least in the area of pertinent basic research.

In order to avoid being outpaced by this development at some point, preparations for the post-quantum period must be initiated today. Confidentiality services with a long-term protection requirement and signature certificates with long periods of validity are particularly affected by this. In addition to potentially also protecting traditional public key cryptography by means of selected symmetrical cryptographic methods, the main focus here is on the development of public key procedures which are resistant to quantum computers. These are methods whose basic mathematical problems can also not be solved efficiently by a quantum computer.

A rise in research and standardisation activities in the area of quantum-computer-resistant cryptography is anticipated in the future, such as the 'Post-Quantum Cryptography Project' of the National Institute of Standards and Technology (NIST) which was initiated in 2016. An important area of work for the BSI will be to actively support these activities in the coming years. In addition to this, internal projects on the subject of quantum computers and post-quantum cryptography will be implemented in the BSI.

Besides quantum-computer-resistant cryptographic mechanisms, reference is also made to methods from the area of quantum cryptography as potential solutions for establishing secure data connections in a world with quantum computers. This concerns technical systems which use physical effects to solve a similar security problem to public key cryptographic mechanisms by mathematical means. Quantum cryptographic mechanisms require, in particular, specialist hardware for the data connection and a traditional cryptographically authenticated channel for key negotiation. The security guarantees of such mechanisms are also heavily dependent on implementation aspects. Both practically and in terms of security, quantum cryptography is therefore not currently regarded as a strong alternative to post-quantum methods.

The use of cryptographic mechanisms for criminal purposes, for example for arranging unlawful actions, is difficult to prevent from a technical perspective. The prevention of some criminal applications (particularly cryptic trojans) can be achieved to a certain extent if state, business and society are put in a position that enables them to configure their systems and communication with one another in a way which is overall as technically secure as possible.

1.1.6 Mobile communication

Introduction

Communication, navigation, fitness training, social networking and entertainment are just some of the ways in which modern smartphones and tablets can be used. The increasingly intensive use of apps means an increase in the sensitivity of data which is processed on the devices. Address books, location and access data, emails and other communication data as well as the use of smartphones for sensitive applications such as home banking mean that mobile devices continue to be a lucrative target for criminals.

Current situation

- Despite a number of industry initiatives intended to accelerate the provision of software updates for the removal of vulnerabilities, we still do not observe a quick and comprehensive provision of security patches in mobile communication. Due to the wide variety of types of device, comprehensive provision of security updates is no easy task. Its success is dependent not least upon whether the providers' use of security patches can become established as a quality feature in the minds of consumers.

- Individual improvements in the use of encryption technologies were seen in 2015/2016. For example, according to its own information, the popular WhatsApp Messenger introduced the end-to-end encryption of chat content. However, these selected improvements only have a minimal influence on the overall situation. Most of the personal and sensitive information which is held on mobile devices is either not encrypted at all or the encryption used is insufficient.

- The app stores of the large providers such as Google, Apple and Microsoft offer a range of different apps globally. However, security and data protection generally play a secondary role in user choices. The competition instead focuses on 'user experience', the combination of utility and convenience, as well as the cost of the app.

- Mobile devices can automatically connect to public hotspots. These are often open, meaning that the data may be transferred without encryption, and can also be read by unauthorised third parties.

- Mobile network operators and app providers – as well as cyber criminals – are able to locate mobile devices and therefore also determine the location of the owner. Vulnerabilities in the infrastructure of the mobile network operator may mean that in certain cases locating mobile devices is possible by third parties even without control over the end device. Attackers are therefore also able to create a comprehensive movement profile of the victim.

- Telephone calls that are made using second-generation mobile network technology (2G/GSM) can still be intercepted at the wireless interface. 3G and 4G telephone conversations can also be listened to in certain cases, for example if the attacker first arranges that these are switched to 2G standard.

Assessment

The current exposure in the area of mobile communication has changed little compared to 2015. Improvements in the area of encryption have been made in selected areas, however potential for risks in the area of mobile communication still remains high due to the factors described above as well as due to the high number of apps available, some of which are harmful. The example of mobile communication clearly shows that the care-free use of highly complex technologies comes at a price. The effects of different provider business models are also reflected in information security. App store operators and users must place greater focus on security. While operators must ensure that, as far as possible, no defective apps are offered in the app stores, users should carefully consider which apps they actually require and what rights they grant to the respective apps.

1.1.7 Standard setting

Introduction

Digitalisation can only fulfil its potential if all the necessary elements are compatible with one another and function reliably. Standards define all the relevant parameters for the interaction of different IT components, from the shape and size of connectors to the electrical field strength or programming interfaces. In doing so, standards not only fulfil their purpose in ensuring interoperability, but they also determine the quality requirements of IT products. In terms of its security characteristics, the way in which the mass use of information technology is organised is mainly determined by national and international standardisation. The BSI is able to establish standards in a direct and binding manner through Technical Guidelines or test requirements in accordance with the internationally recognised Common Criteria (CC) standards, provided this is stipulated by German or European law. Examples of this include intelligent measuring systems, the electronic health card and the identity card.

Current situation

- Whether or not a standard is successful internationally largely depends on whether the manufacturer produces and offers its products in accordance with this standard. The respective market leaders exert the greatest influence here. Due to their market position as IT sector leaders, they very often do not depend on the official standardisation bodies for setting standards but are able to set and change de-facto standards themselves. Very few leading technology and business IT companies are based in Germany or Europe; instead they are predominantly located in the USA or Asia. Germany generally therefore has only minimal influence on IT standards with the exception of individual areas such as smart card applications or as a result of its leading international position in high-quality test procedures.Due to a lack of business interests – in contrast to other sectors – participation by German industry in IT standardisation bodies is therefore relatively weak.

- IT manufacturers being based predominantly in the US and Asian regions, and the security policies of individual states which have been developed in different ways have resulted in conflicting interests in IT security standards. While the BSI pursues the goal of being able

to examine the IT security characteristics and potential vulnerabilities of critical components in as much detail as possible, this form of 'high-assurance testing standard' tends to be restricted in the international environment. For example, as early as 2014, the international recognition arrangement, CCRA, was reduced to virtually only low-level testing depths with the result that the ISO standards based on this and the European recognition arrangement SOGIS also came under pressure to restrict themselves to low-level depth testing or to use uniform, clearly defined test methodologies instead of open vulnerability analyses. The BSI is therefore demanding at international level that high testing standards can also be used in the future for sensitive infrastructure areas.

Assessment

In future, the BSI must also be able to issue IT security certificates with a high testing depth for the marketing of products or for meeting specific statutory regulations. In addition, the high recognition level in the SOGIS arrangement must be maintained within Europe. German industry's limited participation in IT security standardisation should be compensated for in the relevant areas by means of increased public involvement, for example through the participation of authorities, mandates to standardising bodies or commissioned experts. The BSI is increasingly providing recommendations regarding the selection and use of appropriate standards, for example by publishing BSI minimum standards or by means of collaboration in the sector standards for KRITIS companies in accordance with the IT Security Act.

1.1.8 Internet infrastructure

Internet infrastructure is a structure which has grown over the years. The structure is very robust in many areas but, in many instances, it is also very fragile.

Robust Internet

One robust service on the Internet is the domain name system (DNS). Names are translated into IP addresses via DNS – for example from '*www.bsi.bund.de*' into 77.87.229.76. The DNS has a hierarchical structure and is divided into zones. Name resolution generally occurs over several steps. Name resolution is a central service on the Internet for which there is no alternative. Many other Internet services depend on functioning name resolution and rely on the availability and integrity of the service. The operators of large zones – such as the root zone or the .de zone – are aware of this and, in general, ensure the reliability of their systems. A major DDoS attack on the name server of the root zone in November 2015 showed how well this functions. During the attack there was an unusually high level of demand – some instances received over 100 times the normal number of queries. Even though the attack resulted in delays and time-outs in individual cases, most regions and users were not affected by the incident. The DNS continued to function as an overall system.

The reason why even such a major attack could be cushioned was due to massive over-provisioning. There is indeed only one root zone, but this is served by 13 root name servers. Most of these servers in turn have several instances at different locations around the world which can be accessed at the same IP address. This process is called Anycast and ensures that the query is forwarded to the nearest server.

Fragile Internet

The precursor of today's Internet was comparatively straightforward. There were just a few players, all of whom had the same goal: to exchange data as reliably as possible. The confidentiality and integrity of the communication did not play a part at that time and were not taken into account when the protocols were developed. The Internet has now become a network spanning the globe with billions of users, however, the protocols from that time – with the exception of a few small changes – continue to be used. There is now a need for security and attempts are being made to upgrade or replace the old protocols. Some examples:

- It is possible to hijack entire blocks of IP addresses on the Internet. This means that communication content can fall into the hands of unauthorised recipients. A countermeasure is the use of Route Origin Authorisations (ROA) from the Resource Public Key Infrastructure (RPKI) framework. These enable a check regarding whether the individual professing to be reachable at an IP address also has the corresponding authorisation.

- DNS is certainly well protected against attacks on its availability, however data stored in DNS can be copied. Abuse is therefore possible, for example for phishing purposes. Use of what is known as Domain Name System Security Extensions (DNSSEC) can rectify this. The DNSSEC Security Extension allows DNS entries to be signed, or in other words, cryptographically secured. This means that the integrity of these entries can then be verified.

- If a domain such as 'bund.de' is signed using DNSSEC, then further entries for improving security can be stored in the DNS. These are frequently summarised under the tag DANE

(DNS-based Authentication of Named Entities). Examples of such entries include certificates (TLSA) for cryptographically protected websites and mail servers or PGP keys (OPENPGKEY)

Many German operators of Internet infrastructures are committed to implementing these measures and are actively contributing to security. For example, around one third of the address space is secured using RPKI. Germany is therefore in a good position in the higher-level region for which the European registration and issuing agency for IP addresses (RIPE NCC) is responsible. Across the entire RIPE region, approximately 12 percent of the address space is protected using RPKI. However, protection of the address space using RPKI is only the first step. Validation prior to forwarding is the second step. The De-CIX, one of the world's largest Internet exchange points, is planning to make the outcome of such a validation easily accessible to others.

With the help of the BSI, most German Internet providers inform their customers when they become aware that their IT systems have become infected with malware or that other security problems have occurred. This has made it possible, for example, to reduce the number of servers which can easily be misused for DDoS attacks.

The BSI is responsible for the protection of the government network and, in this capacity, has implemented all available security measures: RPKI has been set up for the Berlin-Bonn information network, the 'bund.de' domain has been DNSSEC-signed and a DANE record has been stored there. In addition to this, the BSI is pressing ahead with the distribution of this security mechanism. In order to facilitate the establishment of RPKI, the BSI has put together relevant instructions and has organised an RPKI workshop. DNSSEC and DANE have also been included in the Technical Guideline covering secure email transport.

1.2 Attack methods and means

1.2.1 Malware

Introduction

Computer programs that execute unsolicited or damaging functions on an infected computer are defined as malicious software, malicious programs or malware. Current malicious programs generally consist of several components which have different functions. These also include the option of downloading additional modules with different functions following the initial infection of a system.

Current situation

- Approximately 380,000 new malicious program variants are identified each day. By August 2016 alone, a total of more than 560 million different malicious program variants were known.
- Email attachments and infections unnoticed by the user when visiting websites – referred to as drive-by downloads – are two of the most frequent ways of infecting systems with malicious programs. Links to malicious programs also continue to play a major role. Sources of links to malicious programs are increasingly ad banners which are placed on the relevant platforms by attackers and which are displayed as legitimate online advertising, even on trustworthy websites ('malvertising').
- Ransomware has become even more prevalent in 2016 than in 2015. At the start of 2016, Germany, in particular, was affected by a massive wave of ransomware infections (see also Chapter 1.2.2).
- Conventional signature-based AV products continue to offer only basic protection because new variants of malicious programs are being generated more quickly than they can be analysed. Waves of malicious programs have often already come to an end before AV signatures can be created and installed.
- It is increasingly the case that the analysis of malicious programs is being hampered by the fact that malicious programs carry functions which they use to detect analysis tools and virtual machines. In order to make it more difficult to discover the communication of a malicious program, compromised websites are increasingly being misused as control servers and as a means of distribution. In this process, the established good reputation of a website is exploited in order to circumvent potential URL filters. Macro viruses are now also using a range of techniques in order to detect whether they are being executed in an analysis environment.

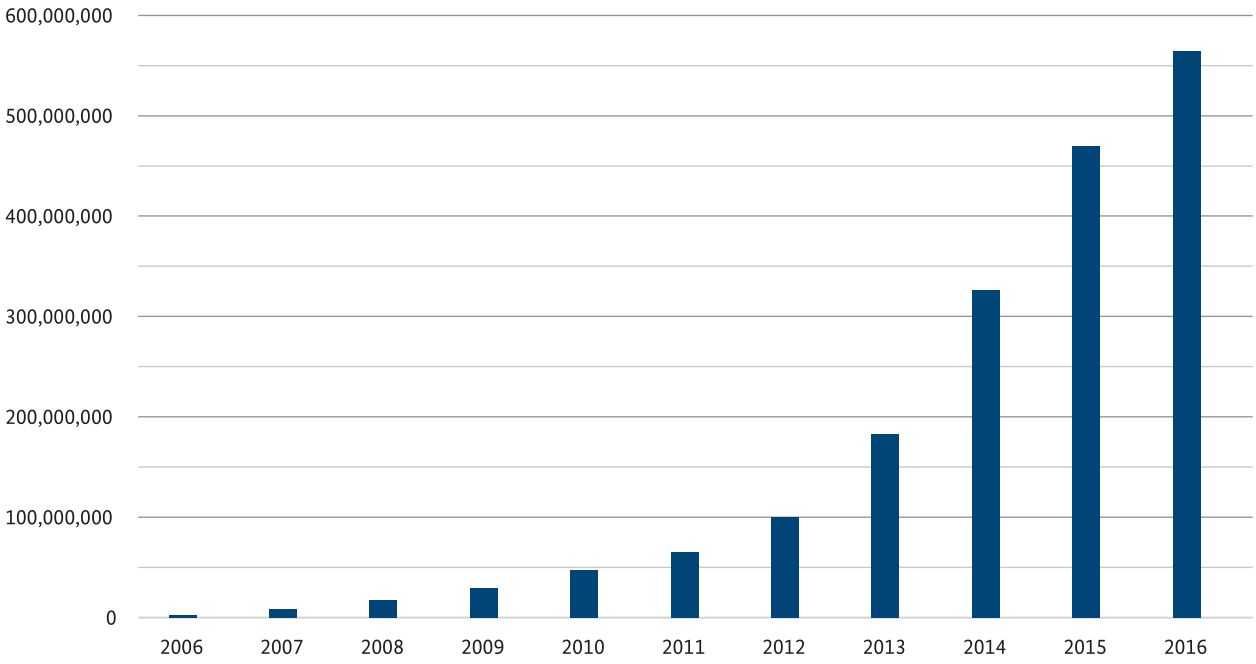


Figure 5: Known malicious programs (2016 up to August), Source: AV-TEST GmbH

- Aside from techniques for detecting analysis environments, malicious programs are increasingly using new techniques which, to date, have only been used by much more skilled attackers in targeted attacks. Technology is being transferred from the area of advanced persistent threats (APT) to general malicious programs.
- Malicious software infections following non-targeted attacks were named as the most frequent type of attack both in the Cyber Security Survey 2015 for the Alliance of Cyber Security and in the survey on the level of concern due to ransomware in spring 2016.

Assessment

As in 2015, malicious programs were also one of the most significant threats for both private users as well as for businesses and administrative bodies over the reporting period. Malicious programs have developed further once again, compared to 2015, and traditional defence measures are continuing to lose their effectiveness. Due to advancing digitalisation and mobility, attackers are also shifting their focus onto mobile platforms and alternative platforms. In the case of mobile platforms, it is still almost exclusively Android which is affected. Malicious programs are generally installed with the involvement of the user, meaning that technical protective measures are circumvented and attackers are able to penetrate protected networks. Users should therefore no longer rely on traditional AV solutions and firewalls alone. IT security must be considered and implemented as an overarching concept which also comprises user involvement.

Malicious software in a nuclear power plant

The facts: Over the course of preparations for inspection work, malicious programs were discovered on a computer used for presenting and highlighting operating steps on the fuel rod loading machine (visualisation computer) in a nuclear power plant in Germany.

The cause: The malicious programs that were detected are widely distributed and have been easily identified by virus scanners for a long time. The visualisation computer itself was no longer running with the current version of the operating system and did not have a virus scanner. This is not unusual in the SCADA system environment due to the authorisation procedures and compatibility requirements in this area. This combination enabled an attack by the Conficker worm which had been the cause of international concern in 2009. In addition to this, the malicious program Ramnit was found on the visualisation computer. The Ramnit control server had been shut down in the previous year by Europol.

Method: Besides computer networks, both Conficker and Ramnit use USB storage devices in order to infect other systems. The infection could therefore have been originally transferred onto one of these USB storage devices using a PC connected to the Internet which had been infected with the malicious software online. The USB storage device was then used at a later point in time on the visualisation computer and was thus able to infect the unprotected computer even though it was not connected to any network.

The effect of the damage: No damage occurred to the nuclear power plant itself, the associated infrastructure or the information technology. However, the operator incurred costs in terms of the working time involved in reconstructing the course of events, the ongoing analysis and the subsequent cleaning of the computers and data storage devices affected.

Target groups: This type of malicious program involves programs that are generally deployed in a non-targeted manner by criminals.

Technical capabilities: Both Conficker and Ramnit should be regarded as common and now even obsolete malicious programs which by today's standards do not use any special mechanisms. The distribution method via USB data storage is also not unusual.

1.2.2 Ransomware

Introduction

Ransomware is defined as malicious programs which restrict or prevent access to data and systems and only release these resources upon payment of ransom money. Ransom money must generally be paid in crypto-currencies such as Bitcoin. Cyber attacks using ransomware are a form of digital extortion. It is possible to distinguish two types:

- Ransomware which blocks or prevents access to a system. An image or a website is superimposed on the system and the user is prevented from using the system as a result. The user is informed that the system is blocked via a message, and payment is requested.
- Ransomware which encrypts data. This uses or combines symmetrical and/or asymmetrical mechanisms for the encryption of user data. When correctly implemented, the encrypted data can only be recovered using the correct key.

Current situation

- Current ransomware families almost exclusively target the Microsoft Windows operating system. In addition, ransomware exists which targets the Apple MacOS X desktop operating system, server systems under GNU/Linux and mobile operating systems such as Android.
- According to the evaluation of data available to the BSI, Germany was mainly affected by the ransomware families Locky, TeslaCrypt, Nemucod and Cerber in the first six months of 2016.
- The most frequent attack vectors via which systems are infected with ransomware are attachments to spam emails and drive-by attacks using exploit kits. Spam emails are often sent via botnets which appeared in the past as a result of the distribution of other malicious program types (Dridex/Necurs).
- The overwhelming majority of attacks are untargeted mass attacks. In addition, however, individual ransomware families also exist and there are also reports of incidents which suggest targeted or manual approaches to infection with ransomware.
- The attackers use cryptographically strong algorithms for encrypting the data. If these algorithms are used and implemented correctly, decryption of the data is impossible without the corresponding key. Backups performed before infection are often the only way to restore the data.

- Security researchers and IT security companies have published tools for some ransomware families which enable decryption of the data without payment of a ransom.

- An evaluation of detection data from virus protection programs for Germany shows a very sharp rise in the number of systems affected by attack attempts using the email attack vector. This number peaked at its highest level so far in May 2016. A significant reduction has been seen from June 2016 onwards which can be explained by the inactivity of the botnet responsible for Locky in the first three weeks in June. The number of systems in Germany actually infected by ransomware also increased over the first half of the year.

- Besides local drives, many ransomware families also encrypt connected external media such as USB sticks and network drives and utilise other methods to impede the recovery of data. Extensive access options in company networks in particular may mean that individual systems infected with ransomware may cause data loss across the company.

- According to a BSI survey, one third of companies questioned in the last six months had been affected by ransomware. Three quarters of the infections had been as a result of infected email attachments. While 70 percent of companies affected stated that only individual workplace computers were attacked, one in five of the companies affected (22 percent) experienced a significant outage of parts of the IT infrastructure and 11 percent of those affected suffered a loss of important data.

Assessment

Ransomware has been the focus of public attention since the start of 2016 even though this form of attack has been an established model for cyber criminals for some time. Data available to the BSI shows that the level of threat due to ransomware in Germany has increased significantly since the end of 2015. Incidents in hospitals, small and medium-sized enterprises or in public administration have been widely covered in specialist media. Unlike infections using other malicious program types, infections using ransomware result in direct and immediately identifiable loss and have specific consequences for the victims. Because systems and data are no longer available as a result of the infection, those affected experience a high level of psychological strain regardless of whether they are private individuals, companies or official bodies.

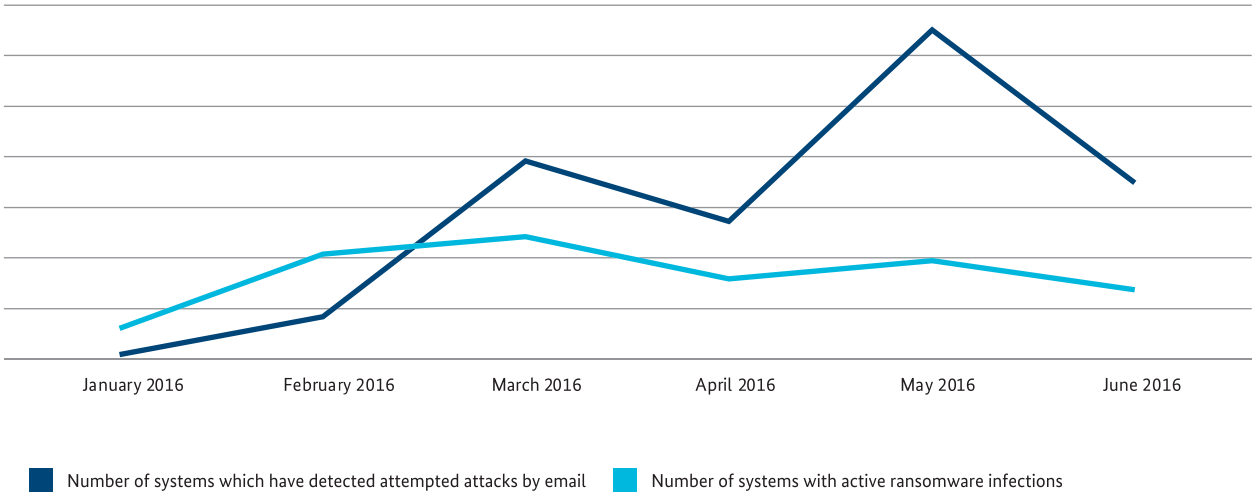


Figure 6: Trend in the number of systems with ransomware detections by virus protection programs in Germany in the first half of 2016

1.2.3 Social engineering

Introduction

Technical weaknesses and vulnerabilities are only a part of the risk in cyberspace. In situations where attackers are prevented due to up-to-date software and systems, firewalls and virus scanners, other means are used to attempt to induce users to install malicious software or to reveal sensitive data. In a similar way to confidence tricksters calling at your door, cyber attackers on the Internet also rely on feigning a personal relationship to the victim or making promises relating to personal gain. Many other variants of this approach, known as social engineering, are used.

Current situation

- Attackers use social networks in order to obtain personal information about potential victims which is disclosed on these platforms. Often the initial contact is also made via social networks and is subsequently intensified in order to induce the victim into acting rashly and without forethought, for example into opening an infected email attachment or accessing an infected website. As a result, the attackers are then able to infect the user's system with malicious software or gain access to a company network.

- When approaching the victim, the attackers often pretend to be prestigious, well-known companies or institutions. This reduces the recipient's reluctance to click on a link or file attachment because the sender appears to be known or trusted.

- Fictitious security problems, falsified invoices or simulated status reports regarding orders are used as part of these phishing attacks in order to mislead users into passing on sensitive company information or other sensitive information to unauthorised parties. Deadlines are set or minimal processing fees are charged for the purpose of side-tracking the victim from the actual issue at hand. Users are also lured onto fake company websites in order to enter or confirm login information, account information or customer data on the site.

- Popular methods of attack are still CEO fraud (see CEO fraud incident box) or contact via telephone. As part of this, attackers pose as support workers of well-known IT companies such as Microsoft or Dell who allegedly wish to resolve problems on the user's computer. To do this, the person concerned is expected to install remote maintenance software on the computer which will enable the individual purporting to be the technician to resolve the alleged problem. If the user follows this instruction, this software gives the attacker access and control over the computer.

- According to a BSI survey, more than two thirds of companies questioned actually implement awareness measures, however these are generally only implemented on a sporadic basis. There is frequently a lack of ongoing processes for building awareness among employees in a long-term and sustainable manner.

Assessment

Social engineering continues to be a widely used method for successfully conducting or supporting cyber attacks. For the attackers, it is often easier to overcome human vulnerability – often the weakest link in the IT security chain – instead of having to expend significant cost and effort dealing with complex technical security measures. Making the user aware and providing them with information is a key measure in counteracting successful social engineering. Relevant training measures should hence not be implemented as a one-off event, but regularly as part of an overall IT security concept.

1.2.4 Advanced persistent threats

Introduction

An advanced persistent threat (APT) attack is distinct from other cyber attacks in that the attackers carefully select their targets. The approach differs to some extent from criminally motivated attacks and, in most cases, the attacker is willing to deploy more resources. This means that, in general, individual computers are not infected by automated means. Instead, the perpetrators seek to spread across the internal network of the attacked organisation and secure long-term access for themselves. For this to occur, perpetrators usually have to connect manually to compromised computers and interact with the system over a long period.

Current situation

- In September and October 2015, China signed an agreement along with the USA and Great Britain which stated that governments should not implement or tolerate any cyber attacks on companies for the purpose of corporate espionage. Espionage attacks against governments and military-related organisations were excluded from this. The relevant negotiations were concluded with Germany on the occasion of the 4th German/Chinese government consultations on 13th June 2016 by means of a joint declaration under which both parties agreed neither to engage in or scientifically support the infringement of intellectual property or violation of business or trade secrets using cyberspace to gain a competitive advantage for their companies or commercial sectors.

- At the operational level, the situation in 2016 differs to that from previous years. At the end of 2015, the number of observed cases of APT attacks on key companies reduced and remained at this low level in 2016. Monitored activities of APT groups focused mainly on South East Asia, Russia, Ukraine, India/ Pakistan and generally in regions in which there were conflicts between nations. The targets were mostly government institutions, defence companies and individuals critical of the government such as journalists, opposition politicians or activists.

- The power failures in the Ukraine which were also covered in the media are one example of the use of cyber attacks in conflict regions. In this case, the perpetrators evidently used a malicious program called BlackEnergy in order to gain access to energy supplier networks (see incident box 'Power failure in the Ukraine', p. 40).

- Financially motivated perpetrators also occasionally adopt techniques which, up until now, have only been attributed to individuals engaged in APT attacks. For example the 'Samsam' ransomware was spread in a comparatively targeted manner. The perpetrators identified vulnerable servers, installed back doors on the servers and then spread across internal networks in the same way as APT perpetrators. Finally, they uploaded ransomware and encrypted data in order to extort ransom money.

Assessment

Germany is still a target for advanced persistent threats. While public reporting is limited to only a few prominent groups of attackers, companies are well advised to determine which states and which groups of attackers are interested in the technology and business interests of the company. Ideally, IT security prevention measures should be independent of potential perpetrators. However, it is advisable to also use perpetrator-specific indicators in order to be able to detect attacks which have circumvented the prevention measures.

CEO fraud

The facts: This variant of social engineering mainly involves finance employees being allegedly instructed, via email or telephone, by a manager of their own company who genuinely exists, to transfer a large sum from a business account to an external account.

Method: The contact information of the target person and the fake sender is often taken from public information on the company website, online career portals and in commercial register entries or by means of calling the company directly. The attackers use this information in order to credibly create the supposed sender, the content of the email and the style of communication in the company. The attacker masquerades as a managing director or member of corporate management, and arranges for an employee to transfer a large amount of money into a foreign account for an apparently urgent secret project. Instructions by telephone are reinforced by authentic-looking emails from the supposed manager. Alternatively, phone numbers are shared by initiated external parties, who confirm to the employee that the transaction is legitimate. The victim is put under time pressure and isolated by means of the obligation to secrecy regarding the transaction.

The effect of the damage: According to information from the Federal Criminal Police Office, there have been 250 cases of such fraud in Germany so far since 2013. Of these, 68 were successful, and 182 progressed no further than the attempt stage. According to information available, the overall loss amounted to 110 million euros. As in some cases it took several days before the fraud was detected, and because criminals transfer the payment abroad quickly, the money involved in the transfer is often irretrievably lost.

Target groups: The target groups include finance and accounting employees in particular who have access to company accounts. The focus is mainly on medium to large companies. The risk of CEO fraud exists in particular in the case of company investments and takeovers which are discussed publicly in the press.

Technical capabilities: The criminals are characterised by well developed competencies in research and social engineering. The emails with fake senders are generally written error-free and calls are made in the company language. When carrying out CEO fraud, technical ability tends to be less relevant than the persuasive ability of the criminals. A key countermeasure for the company is to make the employee aware of this attack method.

Cyber espionage in defence companies

The facts: Cyber espionage attacks against industrial companies are at a lower level in 2016 compared to attacks against government organisations. In the first six months of 2016, the general public became aware of a cyber attack on the RUAG defence company in Switzerland.

Method: Attackers managed to carry out an initial infection with the help of the Turla malicious program family by utilising watering-hole attacks via prepared websites. Attackers were able to exploit a vulnerability in an employee's browser using a drive-by exploit and install a malicious program. This then led to an extension of user privileges on the infected system and finally across multiple levels to complete control of the active directory in the company network. This allowed the attackers to obtain the highest possible user privileges. In total, attackers stole a data volume of 23 GB over several months.

The effect of the damage: The primary motivation of the attackers behind the cyber espionage was evidently not monetary. Instead, the attack was aimed at spying on information. States might then use this information to gain competitive advantages or to adapt their economic and armed forces policies.

Target groups: Groups targeted by cyber espionage include companies whose knowledge and information is of value for the attackers or their clients. Administrative bodies and non-profit organisations are affected whose exposed information enables a new strategic focus at a political or economic level.

Technical capabilities: The attackers behind cyber espionage generally have extensive personnel and capital resources. The potential technical capabilities are very highly developed when compared to cyber crime, and the attackers also operate efficiently. If the exploitation of known vulnerabilities combined with social information is sufficient for a successful attack, then no valuable zero-day exploits are used.

1.2.5 Spam

Introduction

Unsolicited emails are generally referred to as spam. This term can be subdivided into traditional spam, malicious program spam and phishing messages. Spam is generally sent either via compromised servers, infected client systems or with the aid of access data that has been spied via legitimate email accounts. Often, the systems sending the spam are connected to a botnet, making it easier for cyber criminals to market spam as a service. Traditional spam is often used for advertising products, securities or services, and also for attempts at deception, such as deception inducing an advance payment. Attackers seek to use malicious program spam to infect the recipients' systems with malicious programs. This can be effected directly, using malware in an email attachment, or indirectly, using a link in email text or an attachment, which redirects to the malware or a website with drive-by exploits.

Current situation

- The number of spam messages with malicious software in the attachment has figuratively exploded since December 2015 and, for the first time, has exceeded the distribution of other spam messages over the long term. December was dominated by the mailing of downloaders which uploaded the malicious programs Dridex (online banking trojan) or TeslaCrypt (ransomware). The distribution channel for Dridex (spam distribution using systems infected with Necurs) was also used in February 2016 to spread Locky ransomware and in some cases also by TeslaCrypt and Cerber.

- The volume of overall spam activity increased in the first six months of 2016 compared to the previous year by around 73 percent. A moderate increase of 16 percent was seen in traditional spam. The number of spam messages containing malicious software in the attachment increased by 1,270 percent (source: BSI).

- Malware spam is sent mainly from developing and emerging nations such as India, Vietnam or Mexico. It can be assumed that the pursued goal here is a globally optimised strategy to monetise compromised systems (developed countries: ransomware and banking trojans, other countries: spam and DDoS bots).

- There has been evidence of Microsoft Office documents with macros as download attachments and, since December, JavaScript – initially in the case of TeslaCrypt campaigns and later also Locky and other campaigns. Additional script and macro languages as well as file formats (JS, VBS, VBE, Powershell, VBA macros in Office documents, etc.) were also used. In some cases malicious software was also supplied in disguise as part of the attachment, extracted and launched via scripts (dropper vs. downloader).

- The following applies to all downloader and dropper variants: the techniques used here are continually being redeveloped and further developed in order to make analysis more difficult and prevent detection by means of virus protection programs.

- Dissemination via the Necurs botnet dominated spam distribution in numerical terms. There was also evidence of smaller ransomware campaigns with more targeted deployment in which, for example, supposed application documents were sent to companies.

- Today, conventional spam has hardly any impact on the availability of email systems.

Assessment

Numerous reports from those affected and the strong response in the press following the use of the Necurs botnet and also in relation to the spreading of the Locky ransomware illustrate the effectiveness of malicious program distribution via spam. This has remained largely hidden up to now because the malicious software distributed to date has behaved as inconspicuously as possible and infection has often gone unnoticed. The explosive growth in malware spam also shows that the distribution of malicious software and, in particular, of ransomware is evidently a lucrative business for criminals.

The spam emails prepared with increasing professionalism by attackers – using email templates used by well-known companies and with relevant subjects – are misleading more and more users into executing malware from spam messages. In some cases, multi-level deception techniques, the use of a wide variety of script languages and file formats for uploading and extracting the actual software, individual versions of the malware sent or provided for download every hour, and time-controlled sending mean that, when the spam message reaches the user, in most cases no signature-based virus protection program is able to detect the malware and prevent infection.

In terms of countermeasures, vigilant users therefore also need to treat emails with healthy distrust when these emails come from unknown senders, or if anything seems suspicious. However, this is also becoming increasingly difficult for professionals because, in some cases, the recipient's personal data such as name, address and telephone numbers – stolen previously from online service providers – are included in the spam emails.

One good, although time-consuming countermeasure is 'whitelisting' directories from which executable files can be started. The deactivation of the windows scripting host helps counter windows script variants. Above all, it is important for authorities and companies as well as private users to always have current backups of all important data available. The backup should not be permanently accessible from the system to be secured in order that this also avoids encryption in the case of a ransomware infection.

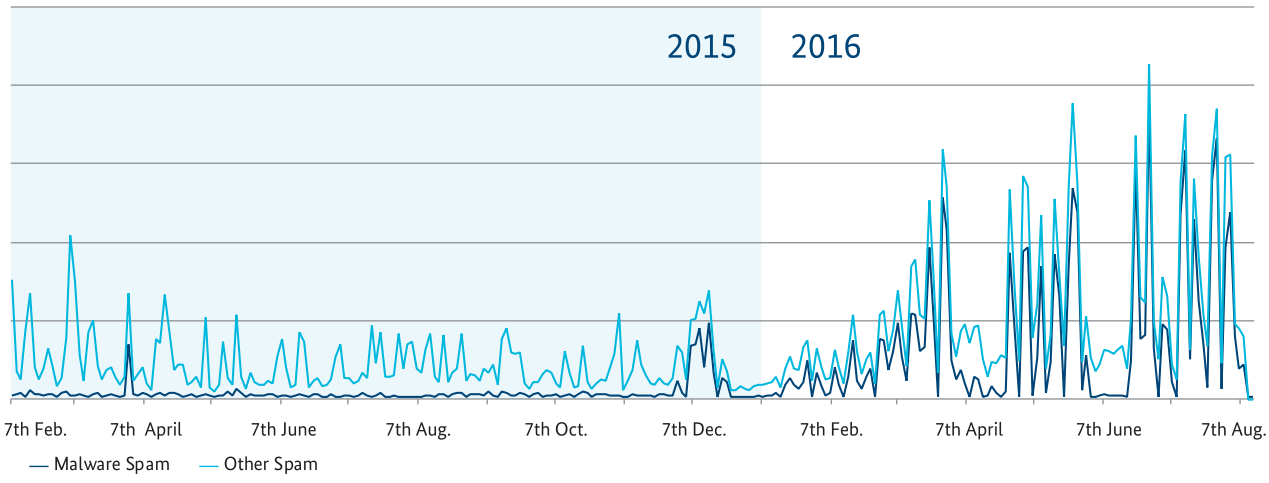


Figure 7: Spam overview per week in Germany since 1st January 2015

1.2.6 Botnets

Introduction

A botnet is a collection of systems that have been attacked by a remotely controllable malware program. This mainly concerns traditional PCs, but increasingly mobile devices such as smartphones or tablets are also being affected. Web servers are also an increasingly attractive target due to their high level of availability and broadband connection. Since, in principle, each web-enabled system can become part of a botnet, infected Internet routers or entertainment devices such as smart TVs are no longer excluded from this threat. Bots are accessed via central systems which are controlled by botnet operators and which enable the bots to send control commands. These systems are referred to as control and command servers (C&C servers).

Current situation

- Botnets are still used by criminals on a massive scale to steal information, attack the availability of IT systems and send spam.
- In the reporting period, up to 39,000 infections were registered daily by security researchers and reported to German Internet providers via the BSI. Over the period for the previous year, the number of infections was around 60,000 which means this figure has fallen considerably. Internet providers inform their customers about the infection and sometimes offer support in cleaning systems.
- In order to detect botnet infections, security researchers operate sinkhole systems which receive contact requests from bots instead of the C&C server. This is enabled by way of registering the domain names used or also the IP addresses. The level of visible infections is significantly influenced by the nature and number of the sinkhole addresses registered by security researchers and therefore fluctuates considerably. Since bots generally determine the addresses of the C&C server using specialist procedures, it may be the case that contact is not made with a sinkhole system if an active C&C server has been found previously.
- In June, the CERT-Bund (Computer Emergency Response Team of the Federal Government) observed an absence of relevant spam waves from the Necurs botnet for approximately three weeks. As the daily average number of Necurs bots logging onto the sinkhole systems used for the BSI warnings jumped from 500 to 5,000 almost simultaneously, this suggests that a key control system for the operation of Necurs disappeared and the bots therefore connected with the security researchers' sinkhole systems. By connecting to the sinkhole server, the bots no longer received any commands from the bot master and therefore no longer executed any damaging action. The botnet ceased its activities from 21st June onwards. So far, nothing is known about the precise background. At this point in time, Necurs was a large botnet with a size of approximately 1 million bots. This size, however, is not unusual; for example, it was exceeded by Citadel in 2014 and 2015. The largest known botnet to date was Bredolab in 2012 with 30 million bots.

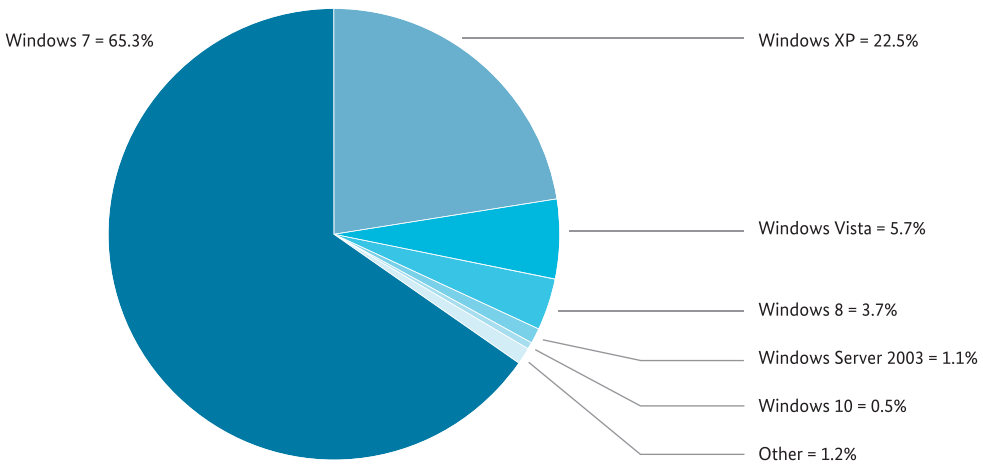


Figure 8: Operating system distribution of Nymaim infections

- Due to the high market share, it is predominantly Microsoft Windows systems that are affected by bot infections. Figure 8 shows a distribution based on a sample of Nymaim infections from mid-June 2016. Nymaim (main purpose: information theft) is one of the most active botnets in Germany. It transfers the operating system used by the victim system to a sinkhole server. Here, Windows 7 is most infected, accounting for approximately 65.3 percent of cases, ahead of Windows XP (22.5 percent) and Windows Vista (5.7 percent).The figures are lower for other versions of Windows.

- Cyber criminals are also increasingly focusing on Mac OS X and Android devices. Several botnets are currently known which focus exclusively on Android and are used to steal information. The trend of misusing compromised, legitimate web servers to operate C&C servers continues to persist.

- Even though, on average, only a few hundred infections of mobile devices were reported over the reporting period in Germany, the trend is rising and the number of botnets focused on mobile end devices is growing. Analogous to this, Apple iOS device botnets were also observed, but these are not relevant to Germany.

- Over the reporting period, the infections reported were distributed over almost 120 different botnet families. Closer examination of the twenty most frequent families at the start of June shows that the majority (approximately 55 percent) were mainly used for online banking fraud. Almost 25 percent of botnet families considered primarily act as droppers and are therefore used for uploading other malware programs. Approximately 15 percent are used for click fraud or Bitcoin mining, while only 5 percent are used for sending spam. Botnets whose principal purpose is DDoS did not occur in the sample.

- A daily average of 765 active C&C servers was observed which were attributed to more than 50 different botnet families. The number and localisation of systems varies continually because, due to countermeasures, many C&C servers only run for a short time with a specific web hoster, and often have already been moved to another provider after only a few hours.

Assessment

Since valid C&C addresses for sinkhole systems cannot be registered for all botnets that exist around the world, the 39,000 infections reported over the reporting period only represent a lower limit for Germany. As a result of experiences with successfully shutting down botnets, it has to be assumed that the number of known cases is significantly higher and is at least somewhere in the six-figure range.

As shown by the operating system distribution of the Nymain infection, most of the infected systems run on Windows 7. As it must be assumed that many malicious programs for Windows operating systems are able to run on all current versions, a clean reinstallation is recommended when switching to a newer operating system version. In the case of Nymaim, an existing infection on a Windows 7 system would remain after an upgrade to Windows 10 and the malicious program would continue to be active thereafter.

Botnet infrastructures offer criminals access to large-scale resources in terms of computer capacity and bandwidth, which they can use for their criminal activities. Due to the professionalisation and commercialisation of cyber crime, operating a botnet is also comparatively easy and cheap for technical amateurs. The current level of threat due to botnets in comparison with the previous year is consistently high. This is a result not only of the high number of vulnerable Internet systems that can be used as bots, but also as a consequence of the low barriers to entry for cyber criminals.

1.2.7 DDoS

Introduction

In the case of a distributed denial-of-service attack (DDoS attack), an attempt is made to impair the availability of a service by means of a high number of queries or data packages. The attacks are generally carried out either by botnets and/or by third parties as reflection attacks (DRDoS attacks) via the improper use of publicly accessible and incorrectly configured servers. As a result of attacks, the operators may in some cases incur significant losses if a service provided is no longer available, for example a website or an online shop. Imminent sales losses or reputational damage are exploited by attackers as leverage with which they attempt to blackmail their victims through the threat of DDoS attacks.

Current situation

- While the maximum bandwidth of individual attacks has again increased during the reporting period – individual attacks have reached bandwidths of more than 200 Gbps – evidence was found of only minimal increases in the average bandwidth of all DDoS attacks known to the BSI. The median attack bandwidth and attack packet rate actually fell in the reporting period.
- It was again found that attacks that lasted for long periods tended to be rare. Attackers frequently use more than one attack vector, for example HTTP flooding combined with DNS reflection.
- Over the reporting period there were numerous attempts at extortion by different attacker groups, although many of which were copycats. Some restrict themselves to sending extortion letters, while others substantiate the extortion letter with an initial DDoS attack.

Assessment

DDoS attacks are still a threat for Internet service providers. Even though the average number of attacks only indicates moderate increases and the median levels are in fact falling, attacks with very high bandwidths must also be taken into account for evaluating the degree to which an individual is affected. In the case of these attacks, one of the attack vectors is often a reflection attack. In collaboration with providers and other network operators in Germany, the BSI has been able to reduce the number of openly accessible server services which can be exploited for reflection attacks. The following diagram illustrates the trend in Germany and worldwide since June 2014. The number of open server services is indeed also falling worldwide, however this trend is stronger in Germany compared to the global average. (The number of systems in June 2014 is equivalent to 100 percent.)

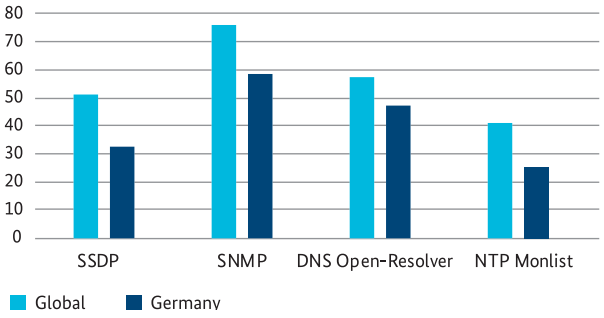


Figure 9: Percentage of open servers compared to June 2014, source: Shadowserver, last updated: June 2016

When looking at individual server types, the ongoing trend can be seen very clearly:

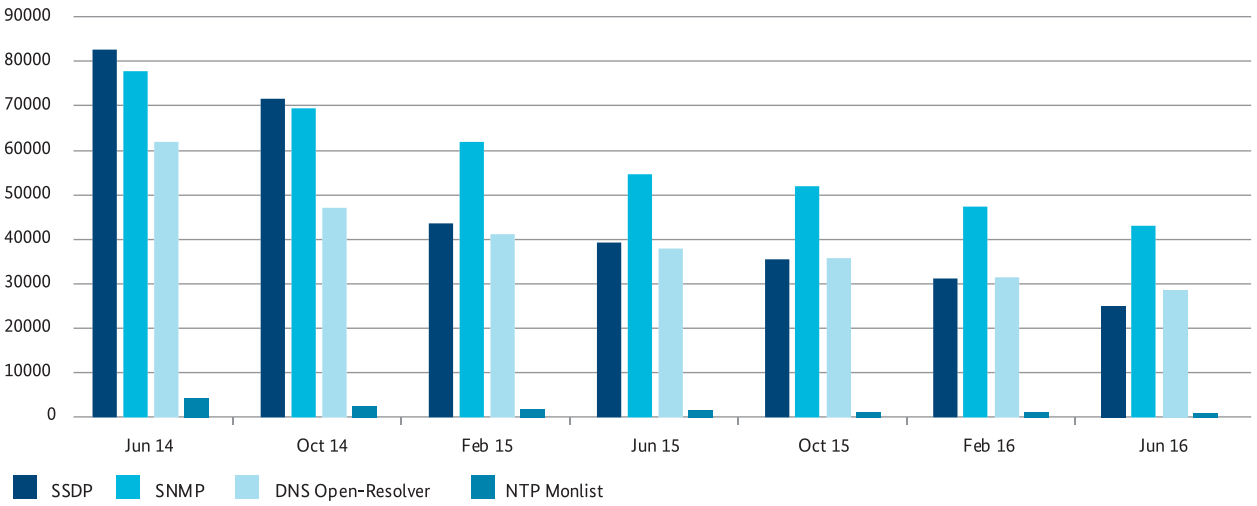


Figure 10: Trend in the number of open server services in Germany since June 2014, source: Shadowserver, last updated: June 2016

DDoS extortion

The facts: Numerous cases of DDoS extortion were reported to the BSI over the reporting period. In each of the incidents, Internet service providers and online shops received an extortion letter by email which warned of an attack if ransom money was not paid. In this case, the most prevalent groups of perpetrators were DD4BC, Armada Collective and Kadyrovtsy. Many of the companies affected filed criminal charges.

Method: In parallel to sending extortion letters, the perpetrators carried out short attacks in order to demonstrate their capacity to act and to underline the seriousness of the DDoS extortion threat. If those affected did not respond to the extortion, DDoS attacks were carried out by both the DD4BC and Armada Collective groups. In contrast, no such attacks were observed in the case of Kadyrovtsy. Due to public coverage in the media, several copycats became involved who were hoping for payment from the recipient without having actually carried out any such attacks. In many cases, ransom money in the form of the Bitcoin crypto currency was demanded.

The effect of the damage: Due to the DDoS attacks, Internet service providers and online shops suffered loss of sales, restricted service quality, costs as a result of implementing DDoS defence measures and damage to their reputations.

Target groups: It was predominantly online merchants and Internet service providers, whose business models were based on the availability of their offers and services, who were affected by DDoS extortion. In individual cases, banks also received the DDoS extortion letter.

Technical capabilities: Attackers do not need to have significant technical capabilities, as the attack methods required – such as botnets or relevant DDoS services – can be hired or commissioned on underground forums. In the case of copycats, the extortion letter was simply copied.

1.2.8 Drive-by exploits and exploit kits

Introduction

Drive-by exploits utilise vulnerabilities in web browsers, in browser plug-ins or in operating systems in order to install malicious programs onto vulnerable systems without the assistance or awareness of the user. This simply requires a visit to a website that has been prepared accordingly. Drive-by exploits are used individually or cumulatively in 'exploit kits'. They are distributed using manipulated advertising banners or directly compromised web servers. While exploit kits are primarily used in broad, non-targeted attacks; individual drive-by exploits are used both in targeted campaigns as well as in non-targeted attacks.

Current situation

- According to the evaluation of detection data available to the BSI for exploit kit attacks in Germany, attacks between March and June 2016 were most frequently a result of the Angler, Neutrino and Magnitude exploit kits. However, the exploit kit market currently appears to be very flexible. Established exploit kits such as the Angler or Nuclear exploit kit are evidently disappearing from the market, yet their activity is quickly being replaced by other exploit kits.

- Following a successful attack by an exploit kit, the malicious software installed varies and can be adapted at any time by the attackers. However – in addition to Spam emails – exploit kits are one of the most frequent infection vectors for ransomware. Angler, Neutrino and Magnitude – the most frequently detected exploit kits in Germany – are also used to install ransomware.

- Malicious advertising banners continue to be a main cause of drive-by attacks. The reason for this is that advertising banners are frequently provided by unknown third parties or marketed by agencies and are then linked into a website without any checks or quality control. This enables even popular and otherwise well-protected websites to become the starting point for attacks using drive-by exploits.

- In 2016, as in 2015, Adobe Flash Player remained the focus of drive-by attacks. Of the seven new vulnerabilities which were used for the first time in the first six months of 2016 in drive-by attacks and exploit kits, five affected Adobe Flash Player, one affected Microsoft Silverlight and one affected Microsoft Internet Explorer. The vulnerabilities CVE-2016-4171 (Adobe Flash Player), CVE-2016-4117 (Adobe Flash Player) and CVE-2016-0189 (Microsoft Internet Explorer) were exploited as zero-day exploits in targeted attacks before manufacturer security updates were available.

- Watering-hole attacks are targeted attacks in which drive-by exploits are placed specifically on websites that may be relevant for the organisation under attack. Espionage is generally the purpose

of such attacks. Targeted attacks using drive-by exploits also continue to occur via emails specifically tailored to the area of interest or activity of the recipient; these emails contain links to prepared websites (spear phishing). In June 2016, for example, a wave of these emails was detected which were tailored to the recipient using information the attackers had collected on the social network LinkedIn and which contained a malicious program in the form of a supposed invoice.

Assessment

In comparison to the previous year, the level of threat due to drive-by exploits and exploit kits is unchanged. As in 2015, new vulnerabilities – primarily in Adobe Flash Player – are still being regularly integrated in exploit kits over a short space of time or used for drive-by attacks. For successful infections, ransomware is then increasingly being installed on the victims' systems and, as a result, those affected sustain damage due to loss of data.

In view of this, the regular updating of applications is still particularly important as is, in the case of companies, the setting up of a patch management process by means of which software vulnerabilities are resolved. Security updates must be applied as soon as they have been provided by the respective manufacturer and installed in the corporate environment, ideally via central software distribution. If that is not possible, then at the very least a temporary deactivation of affected programs or plug-ins may be necessary in order to provide protection against attacks, such as from zero-day exploits.

1.2.9 Identity theft

Introduction

In the context of the Internet, the identity of an individual generally consists of identification and authentication data, such as the combination of user name and password, bank or credit card information and email addresses. 'Identity theft' is the term used to describe an unauthorised party gaining access to data of this type. The perpetrator is primarily interested in monetary gain. This can be achieved through the misuse or sale of stolen data.

Current situation

- From July 2015 to June 2016, the BSI analysed around 141,000 new malware programs which were connected with identity theft in Germany.
- The BSI is aware of approximately 62,000 infections in Germany from a single malicious program family, the function of which is identity theft ('peer-to-peer Zeus'). It must be assumed that the total number of infections is significantly higher.
- In 2015, the number of known infections was 100,000. The reduction is largely due to the perpetrators focusing on ransomware. For example, botnets, which have previously been used for distributing malicious banking programs, are now used for distributing ransomware. There are also correlations between the malicious banking program Dridex and the Locky ransomware. Here, it is evident that developer resources have been redeployed in favour of ransomware.
- There has been no change to the forms of attack compared to the previous year. Most identity data continues to be stolen either by means of malicious programs from client systems or by exploiting a vulnerability on company servers.
- Customer passwords are often only secured using inadequate hash procedures or by means of insufficient encryption. Successful server theft therefore often provides several million valuable data sets.
- Theft of databases containing customer information is now reported on a regular basis. Often, however, the quality of the data records put into circulation or offered for sale cannot be checked. In particular, if the service provider affected does not confirm the theft, it is questionable as to whether the data actually originated from a theft. In such cases, it cannot be ruled out that the data sets may have been generated by the fraudsters for sale to naive interested parties.
- There has been an increase in the trend of trading in data records originating from thefts which took place a long time ago. It is not uncommon for the number of identities stolen to be well above 50 million. In principle, the quality or validity of passwords traded is likely to be lower than usual because the passwords have either been reset in the intervening period by the provider or have been changed by the user affected.

Assessment

Attackers can often achieve a direct monetary gain from the sale or misuse of stolen identities. Nevertheless, there is a trend away from identity theft towards ransomware because, in the case of ransomware, payments can be made

anonymously and therefore the risk of detection for the perpetrator is significantly lower. Also, no work is required in the use of ransomware for the theft and misuse of stolen identities. This means that the costly use of intermediaries can be avoided.

1.2.10 Side-channel attacks

Introduction

In the case of side-channel attacks, conclusions are drawn from the observable effects in the processing of sensitive data – generally key material – about the data itself with the result that the entropy of the data is significantly reduced. Observable effects are, for example, runtime behaviour, energy consumption and electromagnetic radiation. Side-channel resistant implementations of cryptographic mechanisms utilise countermeasures for both software and hardware in order to reduce these undesirable side effects, i.e. the mechanism should be implemented in such a way that the processing of sensitive data is disguised and occurs in constant time. However, entirely side-channel-free processing is impossible. As a general rule: the fewer observable effects there are which can be exploited for side-channel analysis, the more the equipment needed to measure the effects costs and the more measurement data is required in order to separate a signal which can be evaluated from the background noise by means of statistical methods.

Current situation

As high-resolution oscilloscopes are now available relatively cheaply on the market as well as in research institutions, the measurement of local electromagnetic radiation, for example from a crypto coprocessor, no longer poses a major challenge. Significant advances have also been made in the academic field in the statistical evaluation of measurement data. While traditional side-channel attacks require a large volume of measurement data created with the same key in order to be able to extract this key using differential power analysis, more modern attack methods, such as template attacks, are distinguished in terms of the cost-intensive preparation of attacks and the simpler execution of attacks.

Assessment

As a result of the asymmetry in relation to the preparation and execution of side-channel attacks, attack scalability in the case of template attacks is significantly better which means that only a minimum number of measurements is required for the target object. Hence, in particular, the capturing of a sufficient amount of measurement data to extract the key cannot even be prevented by means of frequent key changes. Since research into this topic is ongoing and optimised attack vectors are continually being developed, side-channel attacks constitute a threat for many of the security elements currently in use, even if it has been possible in the past to successfully certify their security according to Common Criteria. For this reason, the validity of security certificates is limited, generally to five years in the case of chip cards and similar products.

New attack targets are continually emerging as a result of the increasing use of such chips in the course of advancing digitalisation. Hardware-based security elements are used, for example, in keyless entry and drive systems in the automotive sector, in entry systems in companies and administrative bodies, in electronic identity documents and for two-factor authentication for Internet services. If attackers manage to read material from a security chip, they gain the same access to data or services as the lawful owner. This means that the state, business and society are particularly affected by side-channel attacks wherever high profits can be earned from the sale of extracted keys.

2 Current exposure of the Federal Government

2 Current exposure of the Federal Government

2.1 Defending against attacks on government networks

Defence against attacks on Federal Government IT systems is a core task of the BSI. Since its formation, the BSI has been performing the task of protecting Federal Government networks. When the government network was created as part of the government move to Berlin (Berlin-Bonn Information Network (IVBB)), overall responsibility for the IT security concept was assigned to the BSI. The Key security measures for the central government network are consistently encrypted communication and a robust redundant architecture. In addition to this, regulated and trustworthy operation is ensured. Improvements to the security setup of the networks are implemented on an ongoing basis, and the networks of the federal states and municipalities are closely connected. The measures for protecting government networks are subject to continual review, further development and adjustment to the changing level of threat. Cyber attacks on government networks take place on a daily basis. Besides non-targeted mass attacks, government networks are also exposed to targeted attack campaigns. In order to protect IT systems and networks, the BSI has developed a multi-level security system in which individually adapted protection measures are applied in addition to commercially available virus protection programs.

In relation to defence against harmful emails, a monthly average of approximately 44,000 infected emails were intercepted before they reached the recipients' inboxes in government networks in real time in the first half of 2016. This is four times the amount compared to the previous year. Emails with attachments such as macro documents or JavaScript archives, typical for ransomware, account for the largest part of this increase. In order to block these emails, commercial virus protection programs are used in an initial step and internal signatures are added. By optimising detection mechanisms through experience and signatures, an average of over 400 attacks on government networks each day were also detected, which had not been recognised using the commercial protection products. These also included approximately 20 highly specialised attacks each day which could only be detected by means of manual analysis. On average, one of these attacks per week exhibited an intelligence service background.

2.1.1 Prevention, detection and response

Due to the dynamic level of threat and the increasing professionalisation of attackers, it has to be assumed today that IT system network boundaries can be overcome. Therefore, in addition to prevention, measures for detection and response must be set up which take effect in the event of a successful attack and minimise the negative effects of the attack. Another protective component in the government network therefore blocks outgoing network connections on infected websites that distribute malware and also blocks attempts by already activated malware to connect to control servers that are used for control and data flow. This measure not only has a preventive effect but also detects systems that have already been infected, in which applied IT security products have not taken effect. In the first half of 2016, around 3,600 attempts to connect to malicious code servers were blocked every day using this method.

Of particular note here are long-running watering-hole attacks in which perpetrators with a background in espionage place malicious code on websites relevant to government workers. The malicious code is replaced by new variants at intervals of several months.

Since the start of the year, active malicious programs have been detected on six occasions. These circumvented commercial protection systems and were clearly used for criminal purposes. This low number of infections is also due to the sensitive email filter which was set up in response to ransomware campaigns such as Locky. Other malicious software families were also filtered as a result of this because, in some cases, these use the same distribution mechanisms as ransomware.

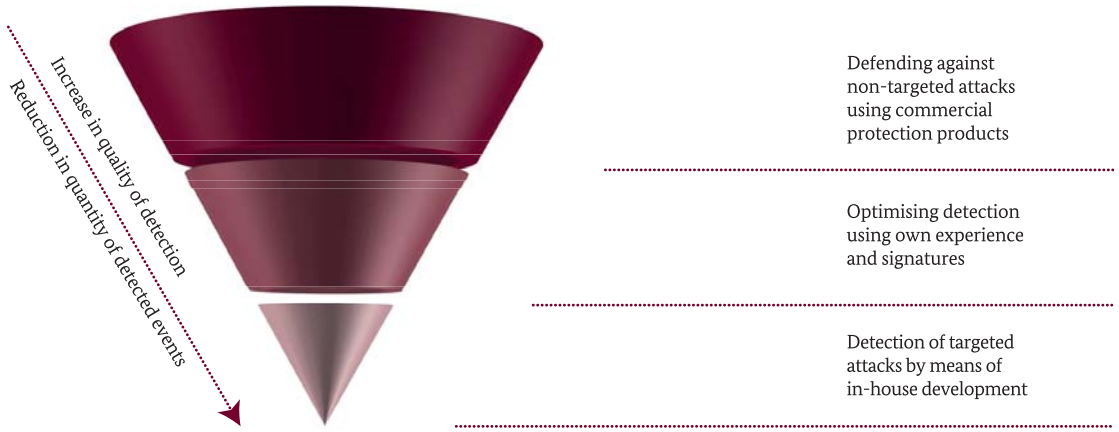


Figure 11: Tiered protective measures in government networks against email-based attacks

2.2 Findings based on notifications from the Federal Government

As stated by Section 4 of the BSI Act (Act on the Federal Office for Information Security), authorities within the Federal Government must report serious security incidents immediately, and less critical incidents on a monthly basis, to the BSI Situation Centre. Not all authorities in the Federal Government are connected to the government network with its central protective components.

Around 200 malicious software infections per month were recognised by commercial protection products in the Federal Government by the end of June 2016. The number of malicious programs on end systems which were successfully defended against was just under 95,000 per month.

Figure 12 illustrates the trend over recent years.

In government authorities, widespread malicious ransomware programs which lead to infections in many organisations, barely penetrated as far as the end systems. Government network mail servers filter out suspicious attachments. In addition to this, the BSI creates antivirus signatures itself from the malicious program campaigns observed. These are activated in the government network at short notice. Each month, 44,000 malicious programs on average are filtered out of email traffic.

In recent years the BSI has recorded continually rising figures for reported denial-of-service (DoS) attacks on individual websites of the federal authorities. Over the period from 2010 to mid-2016, the number of attacks for which the affected authority in question immediately requested support from the BSI quadrupled.

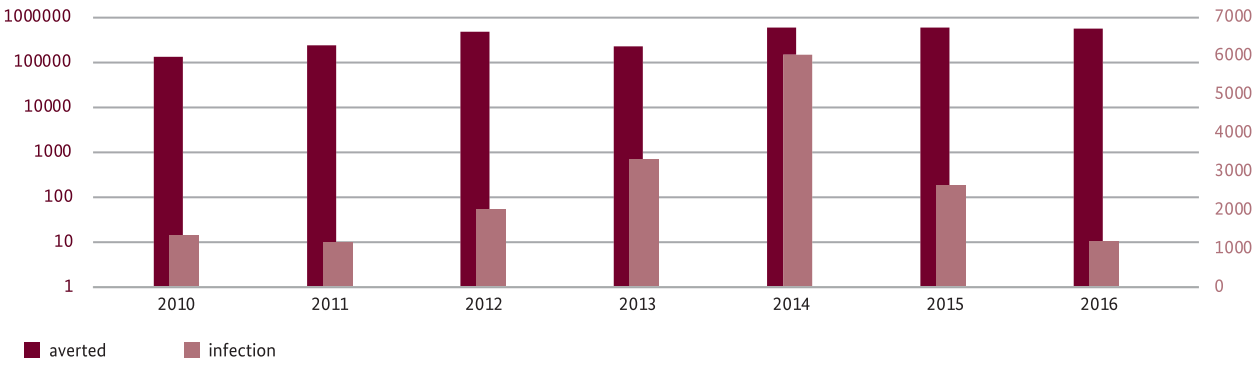


Figure 12: Malicious software infections and averted malicious programs

2.3 Findings from IT security consulting by the BSI

The BSI's security consulting is the contact point for authorities on all issues relating to IT security. Due to close contact with the authorities and collaboration in working bodies, the security consulting team is provided with an ongoing insight into the information security situation at a local level. The IT security officers (IT-SiBes) are the authorities' points of contact. The BSI has established efficient processes for consultation and support with authorities on issues of IT security.

IT security managers face particular problems if technology, functions and user behaviour from the consumer sector are transferred into the workplace without modification. Secure implementation is also made more difficult when personal, customised solutions are required – such as specialist products or 'bring your own device' – although there is comprehensive provision of alternative solutions for an organisation in the IT security strategy. Media reports about IT security incidents and successful attacks appear to contribute towards raising user awareness – consequently, awareness of the need for more security measures has risen. However, working towards the implementation of these security measures and also generating understanding and acceptance remains a fundamental challenge.

Changing technology

Opportunities for consolidation and virtualisation are being discussed and new concepts created for business and administrative reasons. Entire technology sectors are undergoing change. Vulnerabilities are being detected in audits and inspections, particularly in widespread monocultures of operating systems and carelessly configured application software. In many authorities, network structures have arisen which developed over time and which now need to be consolidated by way of network mergers or based on security analyses of network transitions. Now is a particularly good time for redesign efforts, if a large number of standard solutions such as operating systems, firewalls or virus protection products are being replaced due to obsolescence or because support has expired. The adaptation of security concepts is needed beyond the procurement of new hardware and software.

Information security management (ISMS)

Information security management is composed of a collection of individual measures for historical reasons. Many organisations still currently lack a structured ISMS with sufficient personnel and clearly regulated duties and areas of authority. Shadow IT continues to be a fundamental problem area because, in the case of security incidents, it is not those devices that have been internally checked and approved which are successfully used by attackers as gateways. Numerous authorities are not able to specifically state the criticality of IT-supported business processes, and established analysis and documentation procedures are rarely applied. In acute security situations, insufficiently documented processes can have fatal consequences for the entire organisation.

IT security officers

IT security teams need to be provided with sufficient personnel in order to handle their functional responsibility. Financial decisions regarding resources are still often made in favour of technology rather than personnel. Technological measures alone, however, are not sufficient as a defence against attacks. Technical advances by the attackers must be addressed by IT security experts who are equally well trained.

Summary

Information security in authorities can be further improved if IT risks and increasing complexity are addressed by personnel on an ongoing basis in IT security teams. This includes personnel, technical and organisational provision that is appropriate to the task. The BSI's 'Guide to determining expenditure and planning the deployment of personnel resources for IT security teams' (available for download from the BSI website) contains steps for achieving this.

IT security incidents impacting Federal Government

The BSI Situation Centre is the Federal Government's central reporting point for security in information technology within the framework of Section 4 of the BSI Act and, as such, has a broad overview of IT security incidents in the Federal Government. Besides the formal and statistical reporting of IT security incidents, the security officers in the respective authorities also have the opportunity to request additional support from the BSI in the reporting process. It is pleasing to observe that there has been a reduction in infrastructure outages, such as regarding power supply and air conditioning required for data processing centre operation, over the period observed. This is presumably a result of improvements in system reliability, for example by means of redundancy provision.

Website outages due to DDoS attacks: DDoS attacks on Federal Government websites were the most frequent IT security incidents that had a greater impact. DDoS attacks are common occurrences on the Internet. In contrast to attacks on Federal Government and German Bundestag websites in January 2015 which used highly varied attack traffic, the attacks in the current reporting period were relatively easy to avert using countermeasures, for example in the form of selective filtering and enforced standards-compliant protocol conduct. DDoS extortion letters, as reported by companies and municipal institutions, were not received by the Federal Government.

Misuse of telephone and video conferencing facilities: The rise in the incidence of misuse of telephone and video conferencing facilities was noticeable over the reporting period. In individual cases, financial losses amounting to five-figure sums incurred as a result of illegitimate international calls. In the cases observed, the cause of this was either security vulnerabilities in the software or insecurely configured telephone/video conferencing facilities with PINs which were easy to guess and possibly with call forwarding activated. In each case, these were not targeted attacks but automated dialling attempts which worked through blocks of numbers and searched for vulnerable video/telephone conferencing facilities. Voice-over-IP (VoIP) services that have been insecurely configured face the same problems. These services are frequently targeted by VoIP-specific session initiation protocol (SIP) scans. The testing of blocks of numbers and the execution of SIP scans now also form part of the background noise in IP/telephone networks such as SSH/RDP/SMB brute force scans.

Emails and calls in the name of authorities: Over the reporting period, mass emails were sent to citizens and companies by spammers in the name of authorities. In this case, the email content ranged from spam to prepared links to websites containing malicious code. As part of this, the spammers intentionally used a sender from within the namespace of the authorities in order to raise the interest of the recipient. Email administrators at the authorities noticed the use of their domains because they received non-delivery messages from victims on many occasions whose mailbox did not exist (or no longer existed). The BSI offers the following services to authorities connected with the Federal Government network in order to support email server validation and to improve the detection of fake emails.

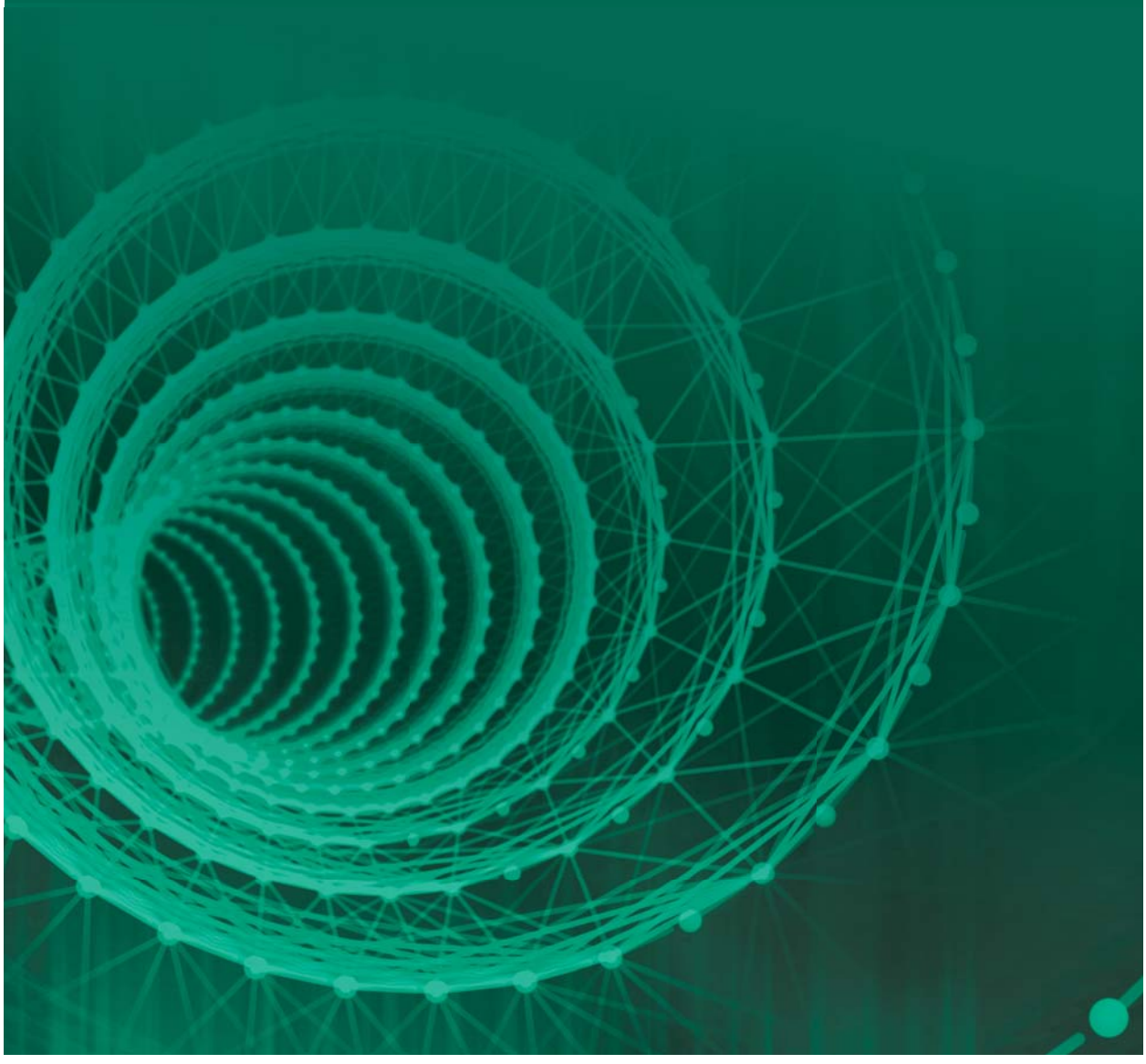
- 'DNS-based Authentication of Named Entities' (DANE) for email validation and web server SSL certificates (active as standard for the *.bund.de domain),
- 'Sender Policy Framework' (SPF) for avoiding address falsification in email traffic, and
- 'DomainKeys Identified Mail' (DKIM) also for the avoidance of address falsification.

Similar incidents also occurred in the past with telephone services. Third parties faked the number displayed to the call recipient by means of what is known as call ID spoofing, generated using prepared VoIP telephone facilities, and thereby created the impression that the call came from an authority. In these cases, the background was often advance payment deception.

Vulnerabilities in web applications: Due to the high rate of development and change in the area of web applications, vulnerabilities are detected in new and, in some cases, also existing Federal Government web applications which could potentially be exploited. These are detected both by means of internal penetration tests and as a result of third-party information. When a vulnerability is detected in a web application, the BSI contacts the contact partner in the authority affected and, where necessary, provides support in removing the vulnerability. Vulnerabilities detected in web applications and insecurely configured Internet services as well as botnet infections illustrate the importance of checking internal services in order to avoid security incidents.

Insecure configuration of server services and malicious program infections: The BSI's CERT-Bund (Computer Emergency Response Team of the Federal Government) regularly receives information from trustworthy sources about insecurely configured server services, for example relating to open DNS resolvers or NoSQL databases, and to malicious program infections on systems attributed to Germany based on the IP addresses. In the event that the Federal Government has been impacted, the CERT-Bund contacts, in each case, the relevant IT security officer in addition to the relevant network operators, as well as the KRITIS company and federal state governments registered for the notification, with the aim of securely configuring the server service and removing the malicious program infection.

3 Current KRITIS exposure



3 Current KRITIS exposure

3.1 Overview

Critical services such as the supply of drinking water or electricity, but also the smooth operation of logistics processes and food production, are increasingly dependent on functioning information and communications technology (ICT). KRITIS operators are essentially exposed to the same risks as other companies. However, in most cases, the risk for KRITIS operators is at a significantly higher level because ICT disruptions can easily result in the failure or restriction of supply services.

Over the reporting period, the BSI observed a series of threats to critical infrastructures which occurred with a particular frequency or noticeable impact:

- critical infrastructures are also affected by ransomware. Of these, in addition to a large number of smaller disruptions, the public has become aware in particular of cases in which hospitals and other health organisations have been impacted.

  Critical services impacted:
  Healthcare

- A power outage occurred in Ukraine in December 2015, which was evidently a consequence of a coordinated cyber attack on several energy network operators. Approximately 225,000 inhabitants were affected by this (see incident: 'Power failure in Ukraine' p. 40).

  Critical services impacted:
  Power supply

Cyber attacks on the SWIFT system

The facts: During the first half of 2016, several incidents came to light, in which unknown parties gained unauthorised access to 'Society for Worldwide Interbank Financial Telecommunication' (SWIFT) communication services. The Philippine news portal 'Inquirer.net' reported a cyber bank heist in March. According to this, attackers succeeded in removing 81 million US dollars from the Central Bank of Bangladesh without authorisation. The attempt at a further transaction for 830 million US dollars was detected and prevented in time. Additional reports followed about an attempted attack on a Vietnamese bank and regarding successful attacks against the Ecuadorian Banco del Austro (loss: 12 million US dollars) and a Ukrainian bank (loss: 10 million US dollars).

Method: The attackers' initial target is to penetrate the core banking systems of the banks affected. Conventional methods of attack are used for this purpose, as also seen in other contexts, for example spear phishing or watering-hole attacks. Attackers then attempt to retrieve valid authentication data for accessing the SWIFT communication infrastructure 'SWIFTNet'. Attackers thus acquire the same authorisations for use of the network which are also available to the bank under attack. Attackers then deploy measures in the compromised bank to disguise transactions. From this point onwards, messages can be sent to other banks via SWIFTNet. The aim of these is to induce the recipient to make a transfer. The money must be diverted out of the payment system and 'laundered' in order to prevent it being retrieved.

The effect of the damage: The three aforementioned successful attacks alone resulted in a total financial loss of 103 million US dollars.

Target groups: The attacks are targeted at financial institutions around the world.

Technical capabilities: Comprehensive knowledge of the financial sector and the target company is necessary for the success of such an attack, as well as knowledge regarding the extensive logistical processes involved in preparations and money laundering. This attack vector is not new from a technical perspective. No particular technical abilities are necessary. Attackers have managed to be successful using conventional attack methods as used in many other cases by criminals.

- Three major disruptions occurred in Germany among ICT providers which affected between 750,000 and 2.7 million people in each case and resulted in the loss of Internet access, telephone services and mobile communication.

  Critical services impacted:
  Voice and data transmission

Critical infrastructures are a target for politically motivated attackers such as hacktivists, intelligence agencies or terrorists due to the high level of potential damage. However, KRITIS is also being identified as a target by criminals. Extortion methods such as DDoS and crypto ransomware essentially affect all sectors and industries. In most cases, companies from the finance and insurance sector are targeted by extortion attempts threatening DDoS attacks because, here, customer portals are frequently used which also provide a direct vulnerability.

The barriers to protection against vulnerabilities which are already known are significantly higher in the case of industrial control systems used in critical infrastructures – as in other industrial sectors – than in the case of conventional office IT. Business- and supply-critical infrastructure systems or specialist systems frequently cannot be supplied with security updates and, in some cases, have life cycles far exceeding those of commercially available office IT. Operators of such systems are therefore often forced to find alternative methods of protecting vulnerable systems.

Ransomware in a hospital

The facts: In February 2016, unknown parties introduced a malicious program onto the internal network of Lucas Hospital in Neuss. This malicious program quickly led to disruptions in the IT system and also impeded patient treatment. The internal computer network was shut down to avoid further damage, and in particular to prevent compromising patient data and to analyse the disruptions. The analysis revealed the cause of the disruption to be a ransomware trojan. The malicious program left behind a number of clues as to how the hospital could receive the cryptographic key needed to restore the data. However, because the network had been shut down straight after the problem initially became apparent, only a very small percentage of the total data volume became encrypted. The hospital decided not to pay ransom money and restored the data from available backups, having checked all servers and computers using rewritten anti-malicious software. The BSI supported the hospital on-site with the analysis and in coping with the incident.

Method: Penetration of internal networks by malicious programs cannot be ruled out simply due to the fact that vulnerabilities that can be exploited by attackers are repeatedly found in common programs. These vulnerabilities can be exploited because the prevalence of IT in society has led to a large number of complex communication links in virtually all major organisations, and indeed through use of the Internet by means of computers controlled by malicious third parties. Computer network protection mechanisms must therefore be organised in such a way that a successful attack on an individual internal system does not immediately impact the entire network. In a specific case, the malicious program was able to damage other IT systems with very little effort because the internal protection mechanisms trusted the infected system.

The effect of the damage: Damage to life and limb was avoided in the hospital because operation was able to continue without comprehensive IT support. However, the Lucas Hospital management board stated that the cost incurred for analysing the attack and restoring the IT operation alone was approximately 1 million euros.

Technical capabilities: Attackers are able to purchase ransomware on the market and process ransom money anonymously via the Internet in such a way that no significant specialist knowledge is required for their attacks. The specialists behind these attacks are malicious software programmers who are constantly finding new methods to circumvent protection mechanisms.

Power failure in Ukraine

The facts: On 23rd December 2015, between 4 pm and 5 pm local time, at least three electricity distribution network operators in Ukraine fell victim to a targeted cyber attack.

The cause: The Sandworm group, who had already been associated with the BlackEnergy malicious software as a result of cyber attacks in the past, are presumed to have been behind the attacks. Attackers managed to install and run malicious software on systems with obsolete software versions. It is likely that spear phishing emails were used here which persuaded the operator employees to open the damaging attachments.

Method: The precise timing of the initial infection has not been determined, however there are reports of similar attacks using spear phishing on other operators in the energy sector in spring 2015. Following the initial infection, attackers gradually gained control of further computer systems in the operators' connected networks, up to and including systems used to run the actual control software for the substations and switchgear. Different versions of the BlackEnergy malicious software family were used for this. In each case the versions were used for specialised purposes. Within the different BlackEnergy versions, different modules were used for specific additional functions. This also included the relatively new 'KillDisk component' which significantly contributed to hampering the removal of the disruption later on in the attack.
During the actual attack on 23rd December 2015, attackers implemented a range of steps for creating, disguising and hampering the removal of the disruption in a highly coordinated manner. In the initial step, the high-voltage power switches for approximately 30 substations and switchgears were opened using infiltrated remote maintenance software which immediately resulted in power supply failure for those affected. Monitoring systems of the network control centres were simultaneously frozen or shut down in order that the disruption could not be identified there. The overloading of the telephone lines which occurred in the second step has been attributed to a TDoS attack (telephone denial-of-service) on at least one distribution network operator call centre, as a result of which telephone reports of disruption were prevented from being made by those affected. The KillDisk component was used in the third step. This module deletes data on Windows systems and thus renders the operating system unusable, significantly impeding the restoration of operational capability and analysis of the incident. Firmware on serial Ethernet converters – which form the interface between facility control and control software – was also overwritten. Consequently, they were effectively destroyed. The servers' uninterruptible power supply was also switched off by the attackers via the management interface, as a result of which the removal of the disruption was further hampered and delayed.

The effect of the damage: At least 225,000 people in Ukraine were affected by a power supply failure lasting several hours. Due to the sabotage of the control technology used in regular operation for the remote control of substations, the switching operations on-site in the substations had to be triggered manually. This significantly delayed recovery of the power supply.

Target groups: The BlackEnergy malicious software had previously been used against energy sector organisations as well as transport and traffic organisations, for example. With this type of targeted attack on critical infrastructures, however, the target group is not only the operator itself but also – at least indirectly – the general population.

Technical capabilities: The technical capabilities of the perpetrators must be regarded as highly developed. It is certainly the case that the malicious software used was not very sophisticated – for example, no zero-day vulnerabilities were exploited. However, the attackers were able to spread unnoticed in the victims' network over a long period and prepare their attack. The perpetrators were extremely coordinated in their approach and used several attack techniques in order to disguise the attack and impede removal of the disruption.

3.1.1 Findings from reports under the IT Security Act

A series of reporting obligations for KRITIS operators was introduced when the IT Security Act entered into force in July 2015. However, for most operators, these will only become relevant sometime after the BSI KRITIS regulation has entered into force. Once the act has entered into force, a reporting obligation only applies to that portion of KRITIS operators that is obligated to report under the Atomic Energy Act, the Energy Economy Act or the Telecommunications Act. A staggered introduction applies to the reporting obligation for other operators which means it is likely that all critical infrastructure operators will not be required to report until the end of 2017.

Three major disruptions affecting ICT providers were reported to the BSI during the current reporting period. As a result of these three disruptions alone, a total of approximately 36 million telephone service and Internet access user hours were lost. The largest disruption alone involved 27 million user hours and affected the mobile communications sector. All three disruptions were caused by a restriction to the availability of central authentication and routing components.

As part of a routine inspection, two malicious programs were found on USB data storage devices and on a computer used for control visualisation in a nuclear facility (see incident: 'Malicious software in a nuclear power plant', p. 20).

Two incidents were also reported in other KRITIS sectors, however these did not impair the delivery of critical supply services. Software and hardware problems were likewise the cause of these disruptions.

3.2 Findings from UP KRITIS

The BSI conducted a survey on concern about ransomware in the German health sector as part of UP KRITIS in spring 2016. The German Hospital Association provided a range of feedback relating to this on the basis of which the BSI was able to assess the situation.

As expected, the vast majority of operators have found evidence of attempted attacks using ransomware. However, these were only successful with some operators. In a level of concern survey conducted by the BSI, operators commented that, in the vast majority of attacks which had actually been successful, it had been possible to resolve the disruption within a few hours and the delivery of the critical supply service had not been endangered at any point. This illustrates, at least in this sample, that hospitals are aware of the danger and are using countermeasures effectively. Ransomware is nevertheless a problem which must be taken seriously because it ties up IT department resources which are already limited, and may result in significant disruption depending on the function of the system attacked.

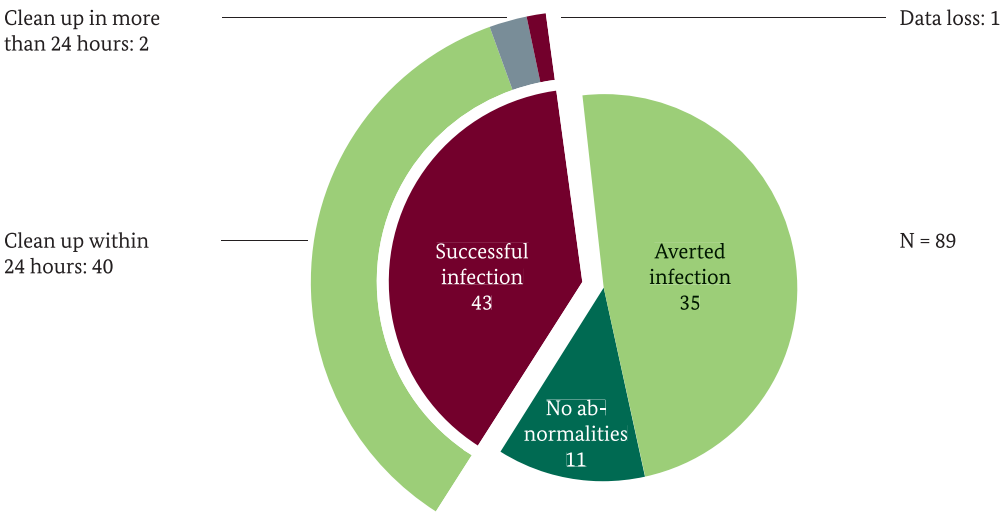
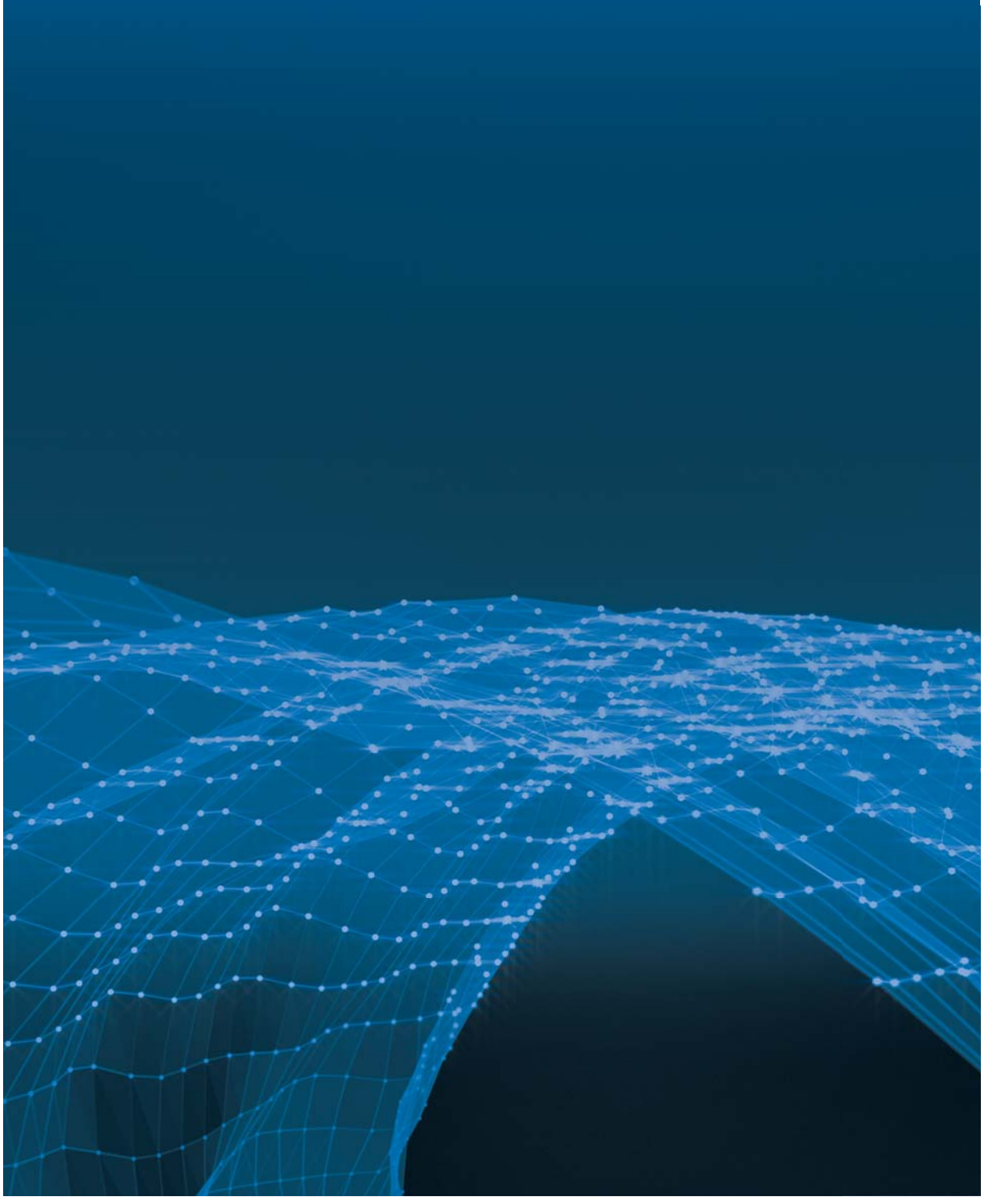


Figure 13: Results of the survey on concern due to ransomware in German healthcare

4 Shaping cyber security



4 Shaping cyber security

The Federal Office for Information Security is the national cyber security authority and thus contributes significantly to the successful organisation of IT security in Germany for the state, business and society. Core issues for the BSI's solutions are highlighted in the following chapter, accompanied by a number of selected topical areas.

4.1 IT security for state and administrative bodies

4.1.1 Federal Government IT consolidation

On the basis of decisions made by the budget committee of the German Bundestag and German cabinet, large parts of Federal Government information technology are consolidated in central data centres as part of the overarching 'Federal Government IT consolidation' project, led by the Federal Ministry of the Interior. Among other objectives, the goal of IT consolidation is to significantly increase the level of IT security in the Federal Government. This can be achieved particularly if security measures adequate for the level of risk involved are taken into account when planning infrastructure and services, and are put into operation (including the implementation of applicable and future security standards).

The BSI's remit in the 'Federal Government IT consolidation' project is to provide security-related support in the consolidation process using analysis, development of security measures and conceptual advice, and also to contribute on an ongoing basis to the security of consolidated IT. The BSI carries out the following tasks for this purpose:

- Analysis of the level of IT security of all Federal Government data centres
- Development of adequate security measures for the Federal Government's data centres
- Provision of information security advice to the Federal Government data centres, and in particular to the Federal Government Information Technology Centre (ITZBund)
- Provision of information security advice to authorities that are to be consolidated
- Support with the security design of the Federal Government cloud (Bundescloud)
- Development of an IT security guideline

Over the reporting period, the BSI investigated 15 data centres of the Federal Government's six central IT service centres in terms of their IT security level as part of pilot testing. The investigation was conducted using the 'HV benchmark' assessment scheme, the aid of which enables the analysis and evaluation of the reliability and IT security of IT service providers and data centres with comparatively little effort. The investigation results provide IT service centre operators, overall project management of the 'Federal Government IT consolidation' project and the BSI with important insights relating to IT security within the immediate Federal Government as well as indicators for the optimisation of IT security and the functional suitability of the data centres. Once the pilot testing in the six IT services centres has been successfully completed, the security analysis will be rolled out across all Federal Government data centres in two stages.

The BSI has developed security measures with the Government Information Technology Centre (ITZBund) which allow the benefits of centralised IT service delivery to be used, while at the same time ensuring the high level of IT security requirements for data processed by the Federal Government. The BSI also provides advice to overall project management and to sub-projects of the 'Federal Government IT consolidation' project on issues of IT security, for example on the secure transfer of IT operations into central data centres or on the security of centralised consolidation projects (for example, the development and introduction of the e-files basic service or the introduction of a federal client). The intention is also to assign a central role to the BSI in relation to information security management for Federal Government IT consolidation. Details are currently being defined in the IT security guideline and in the overarching management system regarding information security for Federal Government IT consolidation.

4.1.2 Protection of government networks/ protection of Federal Government

Defending against attacks on the Federal Government IT systems is a core task incumbent on the BSI under the BSI Act. Since its formation, the BSI has been performing the task of protecting Federal Government networks. The key security measures for the central government network are consistently encrypted communication and a robust redundant architecture. The measures for

the protection of government networks are subject to continual review, further development and adjustment to the changing level of threat.

Current attacks indicate that flat hierarchies in networks and insufficient segmentation measures between services and users constitute significant security risks. The BSI has therefore developed an overall strategy for segmentation to be implemented as part of the 'Federal Government network' project and taking into account the requirements of the 'Federal Government IT consolidation' project. In addition to segmentation between the internal and external area, this also involves segmentation by organisational structures and by functional areas of the same type. Effective separation using reliable mechanisms is the only way to limit the impacts of a successful attack and ensure operation is restored as quickly as possible. The protection of transitions between segments at a uniformly high level is a key task which must be considered at the planning stage of networks and data centres, such as in the transition from external to internal networks in the case of remote maintenance services by third parties.

Many IT service providers offer remote maintenance as a support service because, in most cases, these offer a cost saving and the ability to respond quickly. However, remote maintenance also involves many risks. The BSI has therefore developed requirements for a secure centralised remote maintenance service which take into account the operating requirements in particular, in addition to security characteristics. The service is intended to protect the confidentiality and integrity of sensitive data involved in remote maintenance work using sufficiently strong cryptographic algorithms. The central components of this will be operated by the Federal Government itself. The intention is also to ensure that authorities are able to determine and clearly differentiate systems to which remote maintenance service providers have access. The service is also intended to enable monitoring of actual access as well as live observation and recording of all activities. Although the remote maintenance of systems always presents an additional risk, the future application of this service will be able to provide a secure technical solution. In conjunction with the specialist monitoring of the work which is regulated by the organisation, there is an opportunity to reduce residual risks to a reasonable level.

IT security officers: Certified competence

The BSI offers 'Certified IT Security Officers' initial and advanced education and training courses in collaboration with the Federal Academy for Public Administration (BAköV). The advanced education and training programme covers specialist modules on IT security topics. The learning material delivered is tested by means of examination. The examination components also include project work and presentation thereof to an examination committee. The 'Guideline for IT Security Officers in Public Administration' contains information and samples to support the preparation and implementation of the advanced education and training as well as certification.

The BSI supports the BAköV in the conception and implementation of a training series for IT security officers in authorities. The 'IT Security Officer' job profile defines responsibilities and competencies. These are confirmed by a certificate for participants upon successful completion of training. The advanced education and training programme is targeted at groups of participants from Federal Government and federal state authorities.

The training content and course for IT security officers in authorities represent an excellent model for businesses and are also being adopted in this context. A number of universities have adopted the curriculum and handbook, and are delivering the learning content as part of a single-semester module. Certificates awarded by the universities are based on identical examination questions as those in BAköV courses. Completion of project work and presentation thereof are also required in order to obtain the certificate at the universities. Over the period in which the advanced education and training programme for certified IT security officers has existed (since 2007), 246 individuals have successfully obtained the certificate – and over the 2015/2016 reporting period, 27 individuals achieved the certificate.

During the course of the year, the BSI provides information events for IT security officers in public administration for sharing experiences as well as workshops on specific issues and also supports the BAköV with specialist contributions in the planning and implementation of the annual meeting for IT security officers in federal authorities.

As a result of close collaboration with the CERT-Bund and the National IT Situation Centre, IT security officers receive information, security advice and warnings via established email contacts. In the BSI's security advice internal area, there is an archive containing current information which, where required, also meets confidentiality requirements.

4.1.3 Cyber Response Centre

Nationales Cyber-Abwehrzentrum

On the basis of the cabinet resolution of 23rd February 2011, the National Cyber Response Centre (Cyber-AZ) was set up in 2011 under the leadership of the BSI and in collaboration with the Federal Office for the Protection of the Constitution (BfV), the Federal Office for Civil Protection and Emergency Aid (BBK), the Federal Criminal Police Office (BKA), the German Federal Police (BPol), the Central Customs Authority (ZKA), the German Intelligence Service (BND) and the German Armed Forces (Bundeswehr). Having been initially launched as an information hub, the Cyber-AZ then increasingly assumed the role of a cooperation platform via which the operational measures of individual authorities are coordinated in the event of cyber incidents.

In the case of cyber security incidents, a team is formed from the respective relevant authorities as part of 'coordinated case processing'. Such incidents demand an urgent need for action, for example in terms of incident response, technical emergency response or the identification of perpetrators. The team analyses the information available and also coordinates the subsequent course of action and, in particular, the operational measures of the individual authorities. Joint meetings are conducted on-site with those affected in special cases.

Basic issues are discussed and evaluated in working groups. The main focus of the issues in each case determines their composition, for example cyber crime, cyber espionage or threat to critical infrastructures. The BSI is the leading authority for the Cyber-AZ and is therefore represented in all teams and working groups.

A further development of the cooperation platform and the increased need of ministerial decision makers for information has been catered for by adapting internal processes and by means of increased Cyber-AZ reporting. The 'Cyber Situation' relating to current incidents and the more detailed 'National Cyber Response Centre Information' published approximately once a month, are used by the Cyber-AZ and provide up-to-date information to the relevant bodies which is appropriate for the target audience regarding important incidents and developments in the area of cyber security. This provides recipients with consolidated evaluations from the authorities involved, from a single source. Over the reporting period, 48 'Cyber Situations' were published on the issues of cyber espionage (12), cyber crime (10), vulnerabilities (9), KRITIS (10) and other issues (7), as well as five issues of 'National Cyber Response Centre Information'.

4.1.4 CERT-Bund and the IT Situation Centre

CERT Bund

CERT-Bund is the Federal Government's Computer Emergency Response Team and is the central point of contact for preventive and reactive measures relating to security-relevant incidents in computer systems. The emergency response teams have been in existence at the BSI since 1994 and as an independent section since 2001. In addition to its work which was originally focused on the Federal Government, CERT-Bund has increasingly been undertaking the work of a national CERT for business and citizens for many years and has excellent networks within the national, European and international CERT community.

CERT-Bund provides its target groups with a number of key services:

1. A warning and information service regarding technical vulnerabilities in IT systems:
   Each year CERT-Bund and the National IT Situation Centre jointly issue several thousand brief statements, which are available to the general public, and several hundred detailed warnings for the Federal Government. In addition to this, over 30 security events required a special target group briefing.

2. Provision of support for incident processing (incident response):
   The BSI supports the affected party in dealing with IT security incidents. IT support extends from specialist advice via telephone and passing on good practice documentation, through to the technical evaluation of samples or hard disks. In future, the intention is to further develop extensive on-site support, as was successfully provided, for example, in 2015 in the course of the IT security incident at the German Bundestag.

3. 'Abuse handling':
   CERT-Bund issues briefings every day – most of which are automated – to up to 100,000 affected parties and to Internet and hosting service providers, covering infections on their systems and regarding vulnerabilities or incorrect configurations which might enable abuse, such as for DDoS reflection attacks. Over the reporting period, the BSI dispatched approximately 5 million notifications relating to infected systems and more than 15 million notifications relating to vulnerable server services.

4. The 'Citizen CERT' is used by the BSI to provide a warning and information service at varying levels of technical detail for private users. The 'Citizen CERT' provides impartial information free of charge about current attacks by malicious software and regarding security vulnerabilities in applications.

5. Prevention and response in the government network:
   CERT-Bund operates key security components in the government network which are able to prevent infections by malicious programs and detect system compromises.

Since the end of 2015, CERT-Bund has been monitoring and analysing the unprecedented spread of ransomware which has had a significant impact on companies, authorities and private users. The results of the analyses have been incorporated in the 'Ransomware Briefing Paper' published by the BSI in March 2016. This outlines the increased level of threat as a result of ransomware and contains specific recommendations and assistance relating to prevention and response in the event of loss.

The National IT Situation Centre was founded in 2005. BSI employees monitor the current level of IT security on a daily basis at the Situation Centre in order to be able to quickly and competently assess the need for action and the options available in the event of IT security incidents, both at state level as well as in the economy. The Situation Centre has a large number of non-public sources as well as public sources available for this purpose. These include BSI experts with their specialist contacts, participation in a range of discussion groups such as the UP KRITIS, the German CERT association as well as various international groups such as Trusted Introducer and FIRST. Each month approximately 500 events are assessed as being relevant in the course of this work. Approximately half of these events trigger internal BSI measures.

One source in particular are the reports from the various reporting points which are bought together and arrive in the Situation Centre. In addition to established reporting under Section 4 of the BSI Act from the Federal Government and voluntary reporting from business via the Alliance for Cyber Security, in future the reporting point will also contribute important information about the current level of IT security in Germany. The reporting point, which was newly established under Section 8b of the BSI Act as part of the implementation of the IT Security Act, is responsible for receiving and evaluating disruption reports in the area of critical infrastructures. Information gained and evaluated as a result is incorporated into the various situation products which are then made available to the different BSI target groups so that they are able to adapt their security measures. The Situation Centre works closely with the Cyber Response Centre, which coordinates discussion with partner authorities when the situation requires it.

4.1.5 Secure mobile communication

The use of mobile solutions, smartphones and tablets is increasing within official communication. In addition to the mobile devices themselves, the connection to the relevant back-end infrastructure (mobile device management, mobile application management, VPN server, etc.) and its security have a key role to play in terms of security. The apps installed on mobile devices can also have a major impact on the security of the overall solution. The BSI takes all aspects into consideration before a mobile communication solution for processing classified data is authorised for official use by the BSI.

An area of conflict arises where users are continually wanting to use the latest hardware and software, but where time is needed in order to examine the product thoroughly. The BSI is therefore developing solutions with customers which both meet the needs of the user as well as fulfil the security requirements. Several security-related solutions are currently being reviewed by the BSI on an ongoing basis in the area of mobile communication:

- Smartphones
  - SecuSUITE by Secusmart/BlackBerry
  - SecurePIM by Virtual Solution/Apple
  - SiMKo 3 by T-Systems/Samsung
- Tablets
  - SINA Tablet by Secunet/Microsoft
  - SecuTABLET by Secusmart/IBM/Samsung
- Bluetooth auxiliary equipment
  - TopSec Mobile by Rohde & Schwarz.

To date, the BSI has provided the Federal Government with approximately 10,000 mobile devices for the purpose of secure communication. By the end of 2017, it is expected that a further 8,000 to 10,000 devices will be added.

Individual apps also need to be tested on an individual basis in terms of their security, in addition to evaluation of the basic system. The traditional PC virus scanner methods cannot be adopted due to the fact that apps are isolated from one another (sandboxing). Instead, the BSI has defined basic rules and criteria for assessing app security, according to which specialised companies subject apps to different test procedures. Since 2014, the BSI has had around 200 apps tested for the Android, iOS and Blackberry OS operating systems, using various criteria such as access to calendars and address books, location data and the use of tracking networks. While some apps infringe on only very few criteria, significant shortcomings are identified with other apps in the handling of user data. In order to enable differentiated risk management, further work is carried out using BSI test reports in which the different criteria are weighted against one another according to the application. In the tests to date, integration into tracking networks that cannot be switched off, the recording of geodata and the lack of data protection statements were apparent on many occasions. The test reports are made available to the Federal Government which is then able to make an informed decision about the use of the respective app on this basis.

4.1.6 Approval

It is the statutory duty of the BSI to test (evaluate) IT security products and provide an authoritative statement (approval) regarding the security value. This concerns IT security products which are used in the processing and transmission of officially classified information (classified documents, VS) in the area of the Federal Government and the federal states, or in the case of companies in the context of contracts with the Federal Government or the regional states. In the main, the process concerns IT security products that contain cryptographic elements, which are therefore defined as cryptosystems. The request for approval of an IT security product can in principle only be made by an official user (essential user).

According to Section 37 of the Classified Information Directive from the Federal Ministry of the Interior (VSA), approval must be provided by the BSI for products used to create encryption, for encryption itself, for securing transmission lines and for separating networks with differing maximum classification levels for the classified documents to be processed. Over the reporting period, from September 2015 to June 2016, the BSI has issued or extended 47 approvals for this purpose. 27 approvals were withdrawn or replaced by approvals of newer versions. BSI Document 7164, which is available on the BSI website, can be referred to for an updated list of approved IT security products.

In order to be able to continue to meet the (Federal) Government requirement for approved products, the BSI is currently dealing with more than 50 ongoing procedures seeking approval. In order to accommodate the rising demand for a quick response in the approval procedure, the BSI has developed and subsequently successfully validated a VSF procedure with the Federal Office for Equipment, Information Technology and Use of the German Armed Forces (BAAINBw). The goal of the 'Procedure for scenario-based release approval' (VSF) is to ensure rapid-response use in compliance with requirements in exceptional cases specific to the Armed Forces which deviate from normal circumstances – for example, in the case of urgent unforeseeable deployments. Examples of VSF procedures are approvals in the context of the EU operation NAVFOR MED for the emergency sea rescue of refugees in the Mediterranean Sea.

VS requirement profiles (VS-AP) and national protection profiles (nPP), which are necessary for the standardisation and clear definition of IT security requirements of different product classes and types, are used as an additional tool for approval. The BSI has developed – in part in cooperation with industry – a large number of VS-APs and nPPs for use in the VS area.

4.2 IT security for business

4.2.1 UP KRITIS and the IT Security Act

Critical infrastructures supply the population and the economy with essential services, without which modern life would be inconceivable. These range from the supply of water, food and health services, to electricity, telecommunication, finance and transport services, through to the availability of data networks and data processing on large data centres. These services are increasingly dependent on functioning IT systems including traditional office IT, specialist software for individual processes, embedded systems, process control hardware and software, and operational technology.

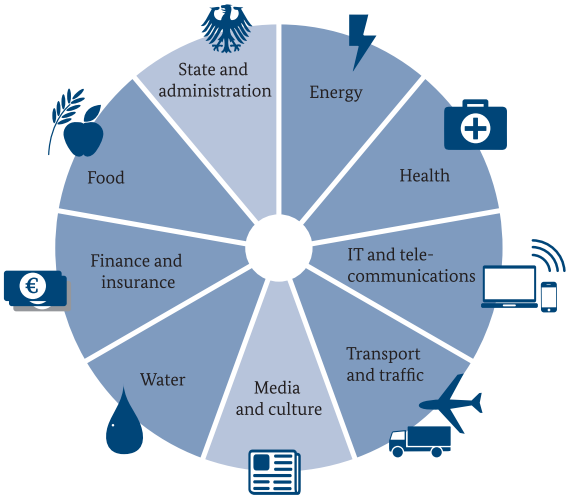


Figure 14: Seven of the nine KRITIS sectors come under the KRITIS revisions of the IT Security Act [1]

The IT Security Act entered into force on 25th July 2015. Amendments were made to the following acts when the amending legislation was passed: the BSI Act (BSIG), the Telecommunication Act (TKG), Energy Economy Act (EnWG) and the Atomic Energy Act (AtG). The focus here is on protecting IT in seven of the nine critical infrastructure sectors. Key elements of the revisions for operators of critical infrastructures concern the obligation

- to secure process-relevant IT appropriately and to consider current state-of-the-art technology when doing so,
- to subject their IT to an audit or other checks every two years and
- to report significant IT disruptions immediately to the BSI.

The BSI is, in turn, required to analyse all information available on the current level of IT security and to provide KRITIS operators and supervisory authorities with comprehensive information. The BSI also provides support and advises KRITIS operators on request.

UP KRITIS – a successful partnership

The BSI has been pursuing the goal of making critical infrastructures resilient for over 10 years. Following two years of preparation, the UP KRITIS public-private partnership was formed in 2007 in order to address the growing challenges in the context of increasing IT deployment in critical infrastructures. Initially around 30 of the largest critical infrastructure operators in Germany collaborated with the state without any regulatory basis. The partnership went well, however its scope was too limited and not all of the objectives could be achieved on this basis. The collaboration was reorganised in 2013/2014, which involved a distinct widening of the group of participants At present, 380 organisations cooperate in UP KRITIS. UP KRITIS is currently working on implementation of the IT Security Act. The collaboration has been built up over many years under BSI leadership and has proven to be an ideal complement to the new regulatory standards.

Critical infrastructures within the meaning of the BSI Act

The BSI KRITIS ordinance (BSI KritisV) uses specific criteria to govern which operators meet the standards of the IT Security Act. The ordinance was adopted by the Federal Ministry of the Interior. The preliminary work relating to content was based significantly on the collaboration in UP KRITIS. Core teams were formed for each sector in which, in addition to state representatives, speakers from the sector working groups in UP KRITIS and representatives of KRITIS operators or their associations were able to offer their expertise and present their positions. The sector working groups introduced in 2014 in UP KRITIS now exist in virtually all sectors. The sector studies *(www.kritis.bund.de/Sektorstudien)* prepared on behalf of the BSI were also discussed beforehand in these working groups.

[1] The Federal Government has no regulatory authority for the media and culture KRITIS sector. The same applies to regional and municipal authorities in the state and administration sector. For the federal authorities included in the state and administration sector, comparable obligations to the current new regulations have already existed since the 2009 BSIG amendment.

The first part of the ordinance entered into force on 3rd May 2016 and initially defines critical infrastructures in the sectors of energy, information technology and telecommunications as well as water and food. It is also intended that, by spring 2017, operators will be able to identify critical infrastructures in the sectors of transport and traffic, health, and finance and insurance.

Warnings and overview

Supplying critical infrastructure operators in all nine sectors and other companies with up-to-date warning information and information about the IT security situation has been an established BSI service for many years. The approaches and processes involved are further refined, for example, as part of the UP KRITIS issue working group. However, the information situation regarding IT disruptions and IT security incidents in the economy was a challenge right from the start and remains so. Often the operators' interest in maintaining secrecy outweighed the desire, which nevertheless existed, to share experiences regarding faults and breakdowns that occurred. Following an initial stage, the BSI anticipates that the IT Security Act and the obligation to report significant security incidents enshrined in the act will see a marked increase in the number of reports and therefore a significantly improved overview of the situation.

The strengthening of personnel as a result of the IT Security Act will enable the BSI to translate information gained more often, more quickly, and with improved results into products from which companies will be able to benefit. The processes prepared in the UP KRITIS issue working group addressing operating information exchange form the basis of this; the Single Points of Contact (SPOCs) in UP KRITIS form the blueprint for the relevant key players in accordance with the BSI Act.

Initial reports under the BSI Act have already reached the BSI and were processed in accordance with the new regulations. A large number of reports are anticipated once all KRITIS operators have registered their contact points. Operators who fall under the first part of BSI-KritisV have until the start of November 2016 to do so.

Robust, state-of-the-art IT

For KRITIS operators, the most important innovation enshrined in the IT Security Act is the obligation to implement appropriate measures to avoid disruptions to IT which is essential for the functional capability of their critical infrastructures. State-of-the-art technology must be taken into account in this regard. Implementation must also be demonstrated every two years as part of an inspection. The specific measures to be implemented are not stipulated by the BSI Act. In line with the collaborative approach of the act, sectors are given the opportunity to define the measures themselves as part of 'sector-specific security standards' (B3S). The BSI is able to determine the suitability of a B3S on request.

The BSI has published guidance for this purpose (*www.bsi.bund.de/Stand-der-Technik*) which compiles the requirements of a B3S and thus also the requirements for 'appropriate measures' in accordance with the BSI Act. The BSI will also publish a new guide on the topic of inspections and audits. This guide will be prepared in the new UP KRITIS issue working group 'Audits and standards' with inspectors and standard organisations. This sets out what the BSI expects in terms of testing under the BSI Act in order for these to be recognised as appropriate. This is because the tests, audits and certifications stipulated in the BSI Act are not performed by the BSI themselves. Operators can develop testing methods which are already in use.

Some UP KRITIS sector working groups are already working hard on their sector-specific security standards so that clarification of effective security measures prepared in the respective sectors will quickly be available to operators. Measures compiled in a security standard such as this also serve as a useful guide for companies which are not subject to the IT Security Act regulations.

Summary

UP KRITIS has laid the foundations for resilient IT in critical infrastructures. To date, however, the scope set out for asserting approaches developed against other interests has not been available. The IT Security Act builds on the collaborative approach and uses legal regulations to ensure that good ideas are more likely to be implemented. As a result of the consolidation in connection with the act, the BSI gains greater ability in the organisation of IT security in areas that are of great significance for the public interest.

4.2.2 Alliance for Cyber Security

Virtually all areas of the German economy face the challenge of exploiting the opportunities provided by digitalisation and, at the same time, effectively addressing the associated risks. This no longer simply concerns internal corporate use of IT in areas such as production, logistics and administration which has already been increasing for many years. New concepts from Industry 4.0, the presence of online marketplaces and the unavoidable exchange with customers and suppliers via the Internet provide a whole range of new opportunities for companies, but may also lead to new vulnerabilities. If a company becomes the target of a cyber attack as a result of this, damage may occur in the form of production and operational downtime or the theft of data. The strong and innovative small and medium-sized enterprises in Germany, in particular, which include numerous global market leaders and 'hidden champions', must expect to become the target of digital industrial espionage.

By forming the Alliance for Cyber Security in 2012, the BSI has set itself the goal of strengthening Germany's resistance against cyber attacks as a location for business. The initiative is open to all institutions from business, science and official bodies, and focuses on German small to medium-sized enterprises. The rapidly growing Alliance for Cyber Security is the largest national cooperation platform for the issue of cyber security and offers approximately 2,000 participants, almost 100 partners and 40 disseminators extensive information regarding prevention and response in the case of cyber attacks. Across all information provided, particular emphasis is placed on the ability of SMEs to use the measures proposed. Attempts are thus made to achieve the highest possible level of security with adequate, but limited resources. The information provided now consists of more than 100 documents sorted by issue, accompanied by monthly status reports and current warning notifications. These are also a good example of how participants can mutually benefit from one another. For example, voluntary reports on cyber security incidents which arrive at the BSI via anonymous Alliance reporting points, regularly contribute to the status reports when they are released.

In addition to information, participants benefit in particular from discussing practical experiences with one another. The Alliance for Cyber Security provides opportunities for this across the regions, including through the successful event format of the cyber security meeting. In the past year, approximately 600 individuals took part in one of four cyber security meetings. In addition to this, IT professionals and IT security experts regularly meet in different working groups to share experiences and to discuss current issues and events as panels of experts.

In the collaborative spirit of all the stakeholders involved in cyber security in Germany, all participants can actively contribute as partners to the work of the initiative by providing their own information. The fact that this year, more than 100 free places in training courses and seminars have been offered, as well as videos on employee awareness, free audits and security checks, demonstrates the huge commitment of the partners involved. The BSI also participated again last year in the free advanced training offered as part of the Alliance for Cyber Security in the form of two sessions at the 5-day network defence training centre. This alone meant it was possible to raise the awareness of 40 IT managers with regard to current threats.

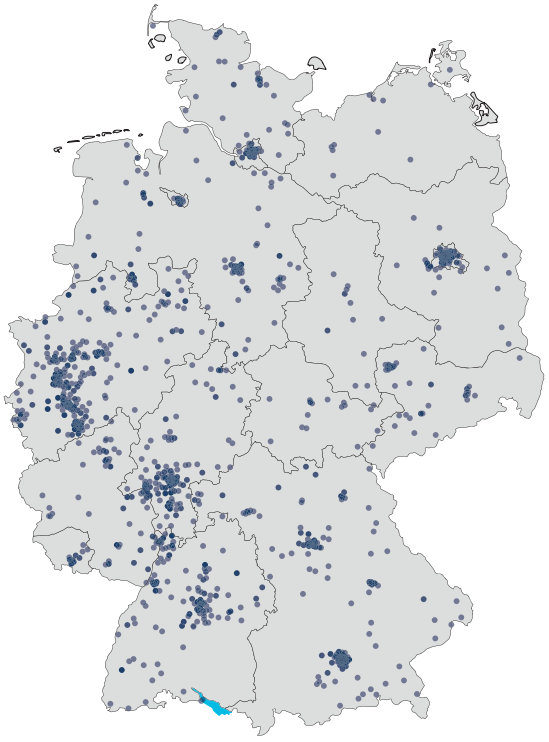


Figure 15:
The Alliance for Cyber Security: a nationwide cooperation platform

4.2.3 Increasing cyber security on the Internet

The BSI collaborates closely with Internet providers in order to increase cyber security on the Internet. As part of the Alliance for Cyber Security's 'Expert panel of Internet operators', the BSI is involved in ongoing exchange with leading Internet and hosting providers in Germany. The current exposure is compiled regularly in this collaboration. Nine cyber security recommendations from the BSI have already been published in response to this exposure, and these are being developed with members of the expert panel. Recommendations are regularly updated for the current situation and are also made available to small and medium-sized operators for the protection of their networks. In the event of acute incidents, the BSI supports operators as required. When more than just one single operator is affected, it is essential that the exchange of information regarding the incident and potential countermeasures is coordinated with all affected operators.

In cooperation with research institutions, the BSI has established the provider information system as a key measure for providing information to citizens with computers infected by botnets. If the BSI is provided with information about infected computers, the PI ensures that this information is forwarded quickly to the relevant Internet service provider. They, in turn, inform their customers who are affected. Since the launch of the system in August 2014, citizens with infected computers have been informed in this way of approximately 17 million different IP addresses in total (an average of around 15,000 IP addresses per day in 2016).

Important elements of the Internet include the many telemedia services on offer. Telemedia service providers are obligated under the IT Security Act to provide state-of-the-art security for their services. The BSI has published a discussion paper relating to this on protecting telemedia services, produced with the involvement of Bitkom and the Internet operator expert panel of the Alliance for Cyber Security. The paper proposes measures for how telemedia services can be protected against unauthorised access to technical equipment, breach of personal data protection and disruptions. State-of-the-art technology is considered in each of the measures proposed; the suitability of measures has thus been proven in practice. The discussion paper is targeted primarily at providers and managers of telemedia services offered on a business basis, online shop operators or providers of hosting and server services. Feedback received is taken into account in the subsequent development of the paper which is then subsequently published as a cyber security recommendation.

In addition to this, the BSI has reviewed the security of the most widely-used content management systems. Problems identified as part of the review were reported to manufacturers who resolved these wherever possible. Security recommendations with relevant checklists were developed for the different content management systems. These will soon be published by the BSI and can be used by all service providers to improve the security of their offering.

Broadband routers are generally used as telecommunication control centres for the use of modern broadband connections. These routers often also assume the task of protecting the proprietary internal network against attacks from the Internet. They therefore now constitute a key security component. In the past, however, security problems have occurred in these components which have been used by criminals, for example for conducting expensive telephone calls at the cost of those affected. In cooperation with manufacturers and providers, the BSI has therefore developed a test concept for broadband routers. The concept allows the relevant security properties of routers to be examined. In this case, the BSI takes into account the basic security-relevant functions as well as support and compliance with established safety standards. The aim is to make the security of broadband routers such as xDSL or cable routers measurable and to achieve a standardised level of security for devices. The BSI test concept is targeted primarily at Internet service providers and manufacturers of broadband routers. The intention is to test routers in accordance with the methodology described in the test concept in collaboration with Internet service providers and router manufacturers operating in Germany.

The BSI is also involved, in connection with international Internet bodies such as the Internet Engineering Task Force (IETF) or the Réseaux IP Européens Network Coordination Centre (RIPE NCC), in the continued development of secure Internet protocols such as DNSSEC, DANE or RPKI, and provides support for Internet service providers in Germany as well as for the Berlin-Bonn information network operators with the introduction of these protocols. The BSI also collaborates closely with the Federal Network Agency – the government authority responsible for the telecommunications sector – and with the Federal Commissioner for Data Protection in order to jointly increase cyber security on the Internet. The catalogue of security requirements in accordance with Section 109 of the Telecommunications Act was jointly developed in this manner. This catalogue is the basis of the security concepts for telecommunications providers.

4.2.4 Industry 4.0: BSI Study on the OPC UA communication standard

The networking of industrial control systems (ICS) is continually advancing, in particular as part of Industry 4.0. ICSs are complex systems developed over time in which components from many different manufacturers are used. These are typically not very dynamic, frequently have an operational life of decades and often use proprietary and insecure communication protocols. Ensuring security and at the same time meeting the requirements of a modern and flexible smart factory is a difficult challenge to meet.

The smart, but also importantly secure networking of production processes forms a fundamental component within the Federal Government's Industry 4.0 initiative. The platform-independent and globally recognised OPC UA communications protocol provides the necessary cryptographic mechanisms for a secure factory and is regarded as a key element on the road to Industry 4.0. It enables the integration of industrial components and processes across different layers of the automation pyramid. In order to ensure developments in the context of Industry 4.0 are made on solid foundations, the BSI conducted an independent investigation on the security-relevant elements of OPC UA in 2015.

The BSI study supplies an in-depth evaluation of OPC UA security functions that are specified and implemented in practice. The comprehensive analysis of the specification was able to show that the OPC UA was developed taking into account security aspects and contains no systematic vulnerabilities in terms of all relevant protection targets and threats. Only minor inconsistencies were identified, and these resulted in the revision of the specification by the OPC Foundation.

While reviewing a selected OPC UA communication stack reference implementation from the OPC Foundation, the implementation of the security functions described in the specification and also the protection against potential attacks in general – such as denial of service – were examined with the aid of statistical and dynamic analysis methods. In this case, just a few minor faults and inconsistencies were found compared to the specification as well as a vulnerability which could be exploited if security functions were to be deactivated. The OPC Foundation was informed in advance and quickly updated the reference implementation and, in response, set up its own information page on the topic of security. No systematic or critical errors were found in the analysis.

Even though it was only possible to examine subsections of the specification and the reference implementation of the communication stack as part of the 'OPC UA security analysis' study, the overall outcome is very positive. Apart from some minor issues, it can be said that the OPC UA has implemented the 'Security by Design' principle consistently and is facilitating the secure networking of industrial systems, when these are used correctly and with a comprehensively protected infrastructure. The study can be downloaded from the BSI website.

4.2.5 Revision of IT baseline protection Established information security today and in the future

Innovation cycles in information technology are becoming ever shorter. New products and services are being created and further developed at an increasing rate – and at the same time technical systems are becoming ever more complex. Due to its increasing penetration into many sectors of the economy and society, there is a growing dependence on functioning technology. As a result, the management boards of corporations and institutions are having to increasingly address the question of the impacts a cyber attack might involve. Besides their own organisation, the effects may impact customers, suppliers, business partners and other groups. The development and maintenance of an appropriate and sufficient level of security therefore necessitates a planned approach by all those involved. IT baseline protection (IT-Grundschutz) is the standard most frequently used for information security in Germany. The established management system for information security in Germany (ISMS) is currently undergoing substantial revision so that it can continue to accommodate the increased requirements for protecting the information in an organisation. Modernisation goals include the improved structuring and trimming down of the IT baseline protection catalogue, accelerating the implementation of security measures, a more flexible approach and taking greater account of user-specific requirements.

Flexible and more dynamic

The focus of IT baseline protection is increasingly shifting towards the issue of cyber security due to the rapidly changing level of threat for IT systems. All IT baseline protection publications in future should also reflect state-of-the-art technology. Individual formats such as the proven IT baseline protection modules can be prepared and published more flexibly and quickly within the overall IT

baseline protection methodology. Modernised modules will save users time and resources. And there are also greater demands for their expertise: in a new publication process, new modules will be published for comment on the BSI website in future as 'Community Drafts'. Input from practice allows even greater optimisation of content before the module is finalised. The first community drafts have already been published. The aim is that another 50 to 70 additional modules will be published by the end of 2016. In future, increased flexibility in implementation is also expected to be possible for the different IT baseline protection target groups. Small and medium-sized enterprises (SMEs) are also more clearly addressed in addition to larger business corporations. In future, the revised IT baseline protection methodology will provide these companies with provision relevant to their requirements.

New approaches, new issues

One fundamental innovation concerns the changed focus of the approaches embedded in the IT baseline protection. In future, institutions can choose between three approaches:

1. **Basic protection** This involves the basic protection of an institution's business processes and resources. It enables initial access to security management in order to reduce the major risks as quickly as possible. In the next step the actual security requirements can be analysed in detail. This approach is suitable for SMEs in particular.

2. **Core protection** Core protection is used as an additional access approach for protecting the most fundamental business processes and resources. It differs from traditional IT baseline protection in its focus on a small, but very important, part of an information network.

3. **Standard protection** Standard protection broadly reflects the approach under the current IT baseline protection in accordance with BSI Standard 100-2. The redesign of the IT baseline protection is also intended to cover an even broader range of issues. The aim is to incorporate new developments in information technology as quickly as possible in IT baseline protection publications such as, for example, the modules. Automation, process control and process management systems are new complex themes which are to be incorporated and supplemented with aspects relating to detection and response.

IT baseline protection profile: Sharing know-how and experience

The IT baseline protection profiles are an additional innovation. This is a flexible offering from the BSI which user groups can use to adapt IT baseline protection to their specific requirements and which can then be published for other interested users. In the step which follows, IT baseline protection profiles supply the basis for being able to develop and continually update sector-specific security standards. In addition to passing on know-how, companies can also network with others regarding the same security themes, and mutually benefit from the experiences of other institutions.

In future, the new IT baseline protection provision will be able to be used by institutions of any size in order to protect their information networks. The complex process of revising IT baseline protection methodology will be completed in 2017. The BSI shall inform the IT baseline protection community at an early stage about transition periods which will apply to certificates and will organise the switch from the old to new IT baseline protection approach so that this can be implemented effectively for all users. The fundamental modernisation of proven IT baseline protection methodology allows the identification and adoption of even more efficient standard safety measures relating to organisational, personnel and technical aspects. This holistic approach enables institutions of all sizes to develop a standard security level for the protection of commercially relevant information. The BSI's IT baseline protection therefore makes a significant contribution to raising the level of security in Germany.

4.2.6 Certification: Building confidence, organising IT security

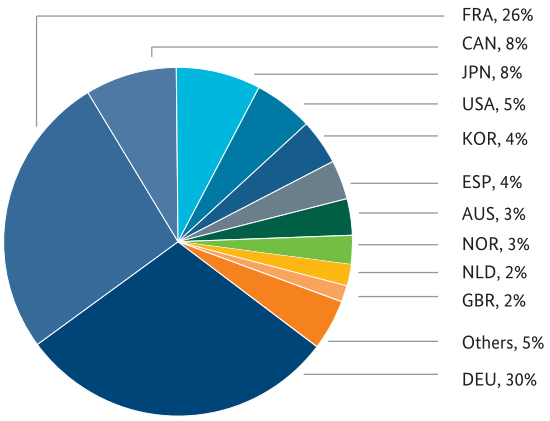


Figure 16: Common Criteria certificates 2007 to Q2 2016
(Source: certificates at http://www.commoncriteriaportal.org)

In global information and communications technology, Germany and Europe are only significant supplier markets of software and hardware products in sub-segments. In light of this, the IT security certification of these products is particularly important because a current security certificate may form the crucial element in purchasing decisions. From the user's perspective, the standardisation of security and IT security certification provides effective tools for increasing transparency in information security, for evaluating the trustworthiness of products and, in the interest of the user, for being able to establish a higher level of information security in the market. Due to the globality of the market, IT security standards and IT security certifications are only relevant for guaranteeing the trustworthiness of hardware and software products when based on international standards such as 'Common Criteria'. Large companies operating internationally in the ICT sector are only prepared to invest in testing with subsequent certification on the basis of international standards.

The BSI has been granted a key role based on the certificates awarded within the international recognition agreement, but also as a result of their major involvement in this sector. This is used to develop products of national and international manufacturers more securely and to conduct evaluations by means of vulnerability analyses through independent testing institutions. In Germany, nine test centres with the relevant authority are recognised by the BSI as part of the Common Criteria certification. IT security compliance can also be certified in accordance with Technical Guidelines.

IT products must satisfy demanding requirements in particular for applications with a high level of criticality, for example due to the need to protect infrastructure or personal data. These are standardised in protection profiles which are used to define safety standards for specific product groups or technical systems, compliance with which is ensured by means of certification. These protection profiles create comparability for the user in the various product classes. Whether and how the product has been analysed in the course of the evaluation is made particularly transparent through the different levels of testing. For acceptance by the user, it is essential that their need for security is objectively and transparently met, in particular if the direct or indirect use of IT is regulated. These are key technical pillars of major Federal Government projects within the framework of statutory initiatives which affect every citizen, whether in the form of the new identification card, the electronic passport, the electronic health card or in intelligent metering systems, such as electric meters.

In the certification process for which the BSI is responsible, the office works closely with the manufacturers as well as the test laboratories commissioned by the manufacturer and in doing so examines security issues and solutions which result from the product testing and analyses. This often concerns issues from areas such as

- the implementation of security-critical product changes
- actual integration of encryption methods into IT security products

- the integration of new manufacturers' production and development locations
- individual issues in the context of correctness testing for security functions
- the handling and consideration of information on product-related IT vulnerabilities provided by test laboratories and manufacturers, such as after simulating side-channel attacks, and
- the suitability of implementation of new security functionalities.

The BSI only issues the certificate if all issues have been clarified, and the security and function requirements specified in the protection profiles or Technical Guidelines have been verifiably implemented by the manufacturer. This certificate attests that the tested product actually includes the promised features.

In 2015, the BSI issued a total of 271 certificates including 61 Common Criteria certificates. The BSI currently (last updated July 2016) processes 149 Common Criteria certification procedures alone.

4.3 IT security for society

An increasing number of areas in everyday life and work are being affected by digitalisation. According Bitkom, more than 80 percent of Germans now use the Internet – more than half of the population in Germany do this using mobile devices, such as a smartphone or tablet. Increasing numbers of people are using smart household devices, controlling their blinds via apps, or conducting banking transactions and other business online. In addition to the immense advantages which these new technologies and opportunities offer, the scope for cyber attacks as well as other Internet risks is also growing. The more dependent society becomes on functioning information technology and secure information infrastructures, the more important IT security becomes for citizens.

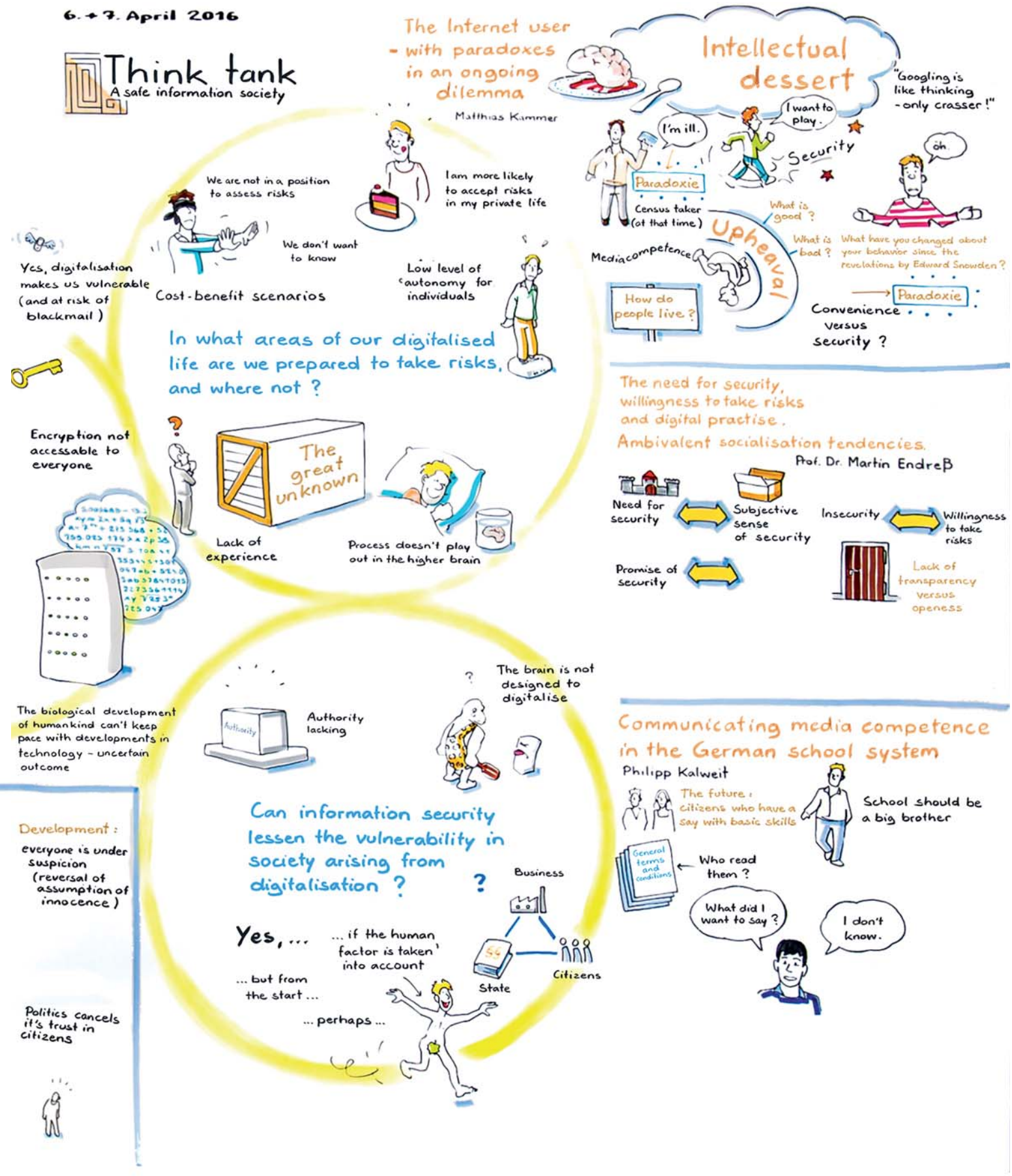
4.3.1 BSI provides a platform for social discourse

The BSI is therefore involved in generating and promoting social discourse on the issue of cyber security. To support this, the BSI offers a platform for open discussion on areas of concern between different sectors of society. For example, in April 2016 the BSI invited representatives from civil society, academia, business and administration to a 'secure information society ideas workshop'. During the two-day event, 51 participants discussed issues relating to the digital future.

Many constructive debates focused on the security-related impacts of digitalisation on society. The debates were conducted partly in plenary sessions but also in small groups, for example in the form of a 'world café'. The event format encouraged points of view to be questioned and developed further, and disputes to be addressed; it also encouraged recognition of the potential crossovers of interests of different stakeholders, which up to this point have not been made clear. In this way, it was possible to collect a broad range of positions in order to discuss the different ways of approaching issues, such as creating relevant incentive structures for increased information security, teaching media competency in the school system, data protection issues, security responsibility and many more issues. The outcome of the workshop was 'seven arguments for a secure information society'; an agreement was reached on their adoption, which can be accessed on the BSI website.

The ideas workshop forms the initial impetus for further projects and events. The BSI will continue the discussion – relating to society as a whole – on issues of IT security and thus pursue the organisation of cyber security with and on behalf of society.


Welcome !
Federal Office for Information Security
Goal for tomorrow
Experiment:
Concept paper
Keeping an open mind
Trust !
Tricky subject !
Why a think tank ?
IT
in focus
IT security
Digital transformation
We are right in the middle !
New horizons
Do we have a digital immune system ?
Do we have a digital social contract ?
Who is "we" ?
What is digitalisation ?
More opportunities – more risks
Trust
Transparency
How insecure is secure enough ?
We don't know it
Residual risk (bad word)
1 Technology developments
2 Usage patterns
3 Other approaches
Change of perspective
Friends don't do that to each other !
Computerized omnipresence
Shift of public and private spheres
Collapse of boundaries
Dependencies
Security culture
Does digitalization make us vulnerable, and if so, in what way ?
IT security is a question of trust
Interests in influencing society this way
This way
Secure communication
private commercial for political debates
No end !
leads to innovation
Cryptography
Ban cryptography ?
Code is free expression of opinion
runs into the sand
VISUAL FACILITATORS
Marcus Frey
Security as a democratic dilemma
Survival
Political strategy
SECURITY
is a kaleidoscopic concept
Bring together closed discussion groups
TRUST
the lubricant of society
Information security
can't be considered in isolation


6.+7. April 2016
Think tank
A safe information society
The Internet user - with paradoxes in an ongoing dilemma
Matthias Kümmer
Intellectual dessert
"Googling is like thinking - only crasser!"
I'm ill.
I want to play.
Security
Paradoxie
Census taker (at that time)
What is good?
What is bad?
Upheaval
Mediacompetence
How do people live?
öh.
What have you changed about your behavior since the revelations by Edward Snowden?
Paradoxie
Convenience versus security?
We are not in a position to assess risks
We don't want to know
I am more likely to accept risks in my private life
Yes, digitalisation makes us vulnerable (and at risk of blackmail)
Cost-benefit scenarios
Low level of autonomy for individuals
In what areas of our digitalised life are we prepared to take risks, and where not?
Encryption not accessable to everyone
The great unknown
Lack of experience
Process doesn't play out in the higher brain
The need for security, willingness to take risks and digital practise.
Ambivalent socialisation tendencies.
Prof. Dr. Martin Endreß
Need for security
Subjective sense of security
Insecurity
Willingness to take risks
Promise of security
Lack of transparency versus openess
The biological development of humankind can't keep pace with developments in technology - uncertain outcome
Authority
Authority lacking
The brain is not designed to digitalise
Communicating media competence in the German school system
Philipp Kalweit
The future: citizens who have a say with basic skills
School should be a big brother
General terms and conditions
Who read them?
What did I want to say?
I don't know.
Development:
everyone is under suspicion (reversal of assumption of innocence)
Politics cancels it's trust in citizens
Can information security lessen the vulnerability in society arising from digitalisation?
Yes, ...
... if the human factor is taken into account
... but from the start ...
... perhaps ...
Business
State
Citizens

4.3.2 BSI citizen services

In line with its statutory mandate, one of the BSI's tasks is to inform citizens and make them aware of the secure use of information technology, mobile communication methods and the Internet. Understanding the risks is the first step in achieving this. For this reason, the BSI provides a website at *www.bsi-fuer-buerger.de* which is specifically tailored to citizens. Wide-ranging issues, and information relating to the topic of IT and Internet security are addressed on this website in such a way that they are understandable for technical laypeople. Besides the information itself, the BSI also makes specific recommendations for action which can be implemented, for example, on issues such as email encryption, smartphone security, smart homes and social networks.

The BSI website was relaunched in November 2015. Up-to-date content, modern design and user-friendly structure are features of the citizen website *www.bsi-fuer-buerger.de* as well as the BSI websites *www.bsi.bund.de* and *www.allianz-fuer-cybersicherheit.de*. The previous separation between the stationary and mobile Internet has been removed and information recommendations are easier to find. The responsive design means all websites automatically adapt to the screen size of the respective device. The redesigned website has been very well received by Internet users. There has been a significant increase in site views for the citizen website since the relaunch from an average of 151,072 visitors per month over the period from July 2014 to June 2015, to an average of 172,592 visitors per month over the period from July 2015 to June 2016.

The BSI also uses the Citizen CERT to provide a free warning and information service. This is currently being used by 102,137 subscribers in order to gain fast and reliable information about weaknesses, vulnerabilities and other risks. BSI experts analyse the security situation on the Internet around the clock and dispatch warning notifications and security information via email if action needs to be taken.

Internet users also have the option of finding out about current topics and issues in IT security and entering into dialogue with the BSI via the Facebook page (*www.facebook.com/bsi.fuer.buerger*) and the Twitter channel (*www.twitter.com/BSI_Presse*) which has been active since March 2016. As at the reporting date of 30th June 2016, 25,983 Facebook fans had been doing so, as had 1,871 Twitter followers. The BSI can also be contacted by telephone or email for citizen questions relating to IT and Internet security. The BSI service centre receives an average of approximately 400 enquiries from private users each month.

4.3.3 Collaborative approach for increased IT security

Nobody can solve challenges of cyber security alone. The BSI therefore also takes a collaborative approach to building public awareness of the risks and opportunities of information technology and collaborates with a range of institutions. An ongoing collaboration has been established, for example, with 'Germany – safe on the net' and with the European Network and Information Security Agency (ENISA) for citizen-related activities. Activities for specific purposes also exist with institutions such as the Regional and National Police Criminal Prevention Agency, the Federal Criminal Police Office, klicksafe or the consumer centres. These cooperative arrangements will be stepped up and developed further in the future.

In October 2015, the BSI was involved as a key national player in the organisation of European Cyber Security Month (ECSM) which included wide-ranging awareness and information programmes for citizens and SMEs. The BSI acts as both the national coordination office for acquiring partners to support the month of action and is also a stakeholder with its own activities and offers. At the BSI's initiative, 20 partners were involved in ECSM Germany with awareness activities in 2015. The BSI prepared a quiz through which users on *www.bsi-fuer-buerger.de* were able to test their knowledge about IT security, and also launched an advisory service on its Facebook page, where specialists were on hand to answer questions from private users. The BSI jointly conducted an online survey with the Regional and National Police Criminal Prevention Agency (ProPK) during the action month, which surveys aspects such as protection measures used by private users and their experience with cyber criminality.

4.3.4 Encryption creates confidence

The 'Charter for Strengthening Secure Communication' – an initiative run by the Federal Ministry of the Interior – was presented as part of the 2015 National IT Summit. In addition to the Federal Ministry of the Interior and a number of well-known corporations and institutions, the BSI is also one of the signatories to the charter. The signatories' declared aim is to strengthen secure communication in particular by means of supporting and implementing end-to-end encryption. The charter contains a series of relevant declarations and may thereby help to formulate framework conditions which bring together and focus a large number of activities that already exist.

The stated aim of the digital agenda adopted by the Federal Government is for Germany to become the number one encryption location for protecting its citizens, the economy and administrative bodies. The BSI is therefore pressing ahead with the use of encryption solutions to support secure communications on the Internet. In accordance with the digital agenda, the BSI recommends that both citizens and commercial enterprises use encryption to protect privacy and protect commercially relevant information from being spied on. From an information technology perspective, the development, provision and consistent use of secure crypto and cyber technologies for companies, administrations and citizens is, in particular, of key importance for minimising the risks resulting from the critical exposure. Effective and trustworthy security mechanisms are a basic requirement for ensuring information security at a technical level.

4.3.5 Secure email transport across the board

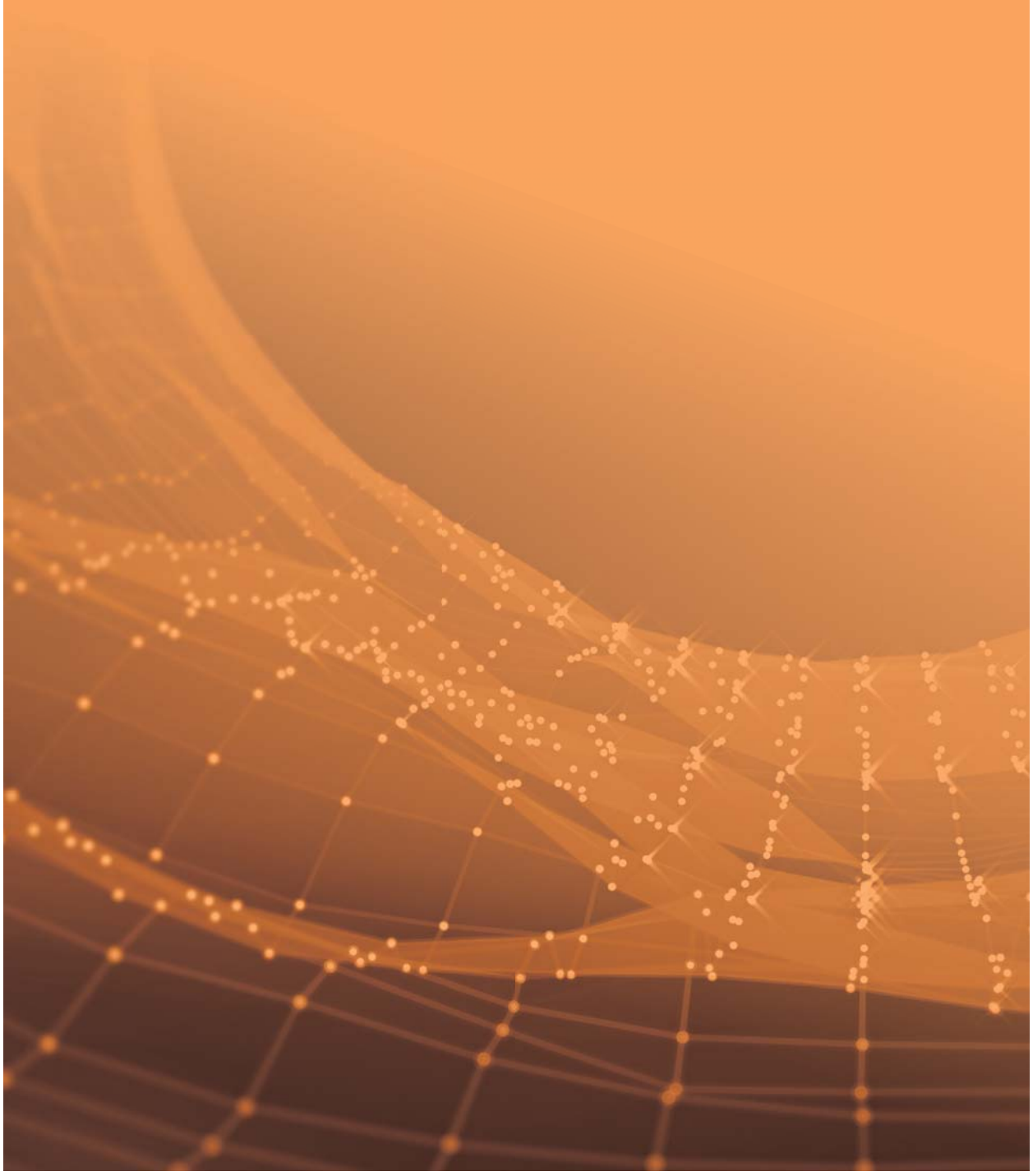
A large amount of digital communication today still occurs quickly and conveniently via email. However, in practice, consistent application of IT security is often neglected. In response to this, the BSI has defined a uniform standard in the form of the Technical Guideline 'Secure E-Mail Transport (BSI TR-03108)', which acts as a blueprint for the safe operation of email services for email service providers. The Technical Guideline's requirements focus in particular on functionally and cryptographically secure configurations of communication interfaces in order to ensure a high level of transport security. This relies on up-to-date standards such as DANE which have already been tested in practice. Requirements are implemented solely by email service providers. Users of email services therefore benefit from a high level of IT security without any additional workload for them.

Market-proven requirements and a collaborative solution

The draft of the Technical Guideline which was published back in 2015, was prepared in discussion with email service providers operating in the market. The concept on which the draft was based underwent ongoing development in which focus was placed on IT security, practicality and user acceptance. The core of the concept is that no new self-contained systems will be created as a result of the Technical Guideline, but that the IT security of the existing open email infrastructure will be increased. The draft was further developed and finalised in a working group formed by the BSI with over 20 members. It is worth noting that the Technical Guideline requirements were not only defined more precisely, but were also increased in agreement with the working group in such a way that the requirements previously indicated as optional have become obligatory in the final version. In addition to the use of high-quality crypto algorithms, the Technical Guideline requirements involve signed DNS queries, obligatory encryption and trusted certificates.

The Technical Guideline has already enjoyed positive reception; initial providers are indicating that the Technical Guideline requirements are already being implemented. The BSI is currently developing a certification procedure for the Technical Guideline in order that such statements in future could also be verified for third parties. The aim is that, in future, the Technical Guideline will also be accepted and implemented in sectors where email distribution is not part of the core business, but is part of everyday business, for example in the case of insurance companies, banks and authorities. The BSI has already received expressions of interest from a range of areas and the Technical Guideline is being followed with huge interest internationally.

5 Overall assessment and summary



5 Overall assessment and summary

This status report from the Federal Office for Information Security very clearly shows increasing complexity in the level of threat as well as in the associated risks for advancing digitalisation. The question of the security of the information technology used is therefore no longer simply a side issue. It is also no longer a question relevant to just a select group of IT specialists. Instead, information security has become an essential precondition for the success of digitalisation in Germany.

The level of exposure continues to present cause for concern. In addition to those phenomena which are already known, the BSI identified a new quality to the nature of the threat. The main gateways for cyber attacks are unchanged and remain critical:

- vulnerabilities exist in software, and in some cases also hardware products, which are used most often. These vulnerabilities enable attackers to remove information or gain control over systems.
- Attackers have botnets available which have been developed and are executed in an organised manner for distributing malicious software or spam emails on a mass scale. These botnets can also be used successfully for attacks on the availability of services.
- Users also often either fail to apply conventional and straightforward security measures, or do so inadequately.
- Opportunities are arising for cyber criminals in the marketing of attack tools, but also for extortion due to anonymous payment methods such as Bitcoin.

A sudden rise in cases of ransomware illustrates very clearly how vulnerable everyday life is to cyber attacks. Access to one's own data is becoming increasingly essential – not only for companies but also for individual citizens. Cyber criminals are exploiting this fact and are holding the victim's data and digital identity hostage. The fact that even hospitals with networked systems are affected and that, as a result, the running of these institutions is compromised, shows that cyber attacks have finally arrived in the real world.

The BSI has also identified that the threat to state and the economy as a result of professional and presumably state-controlled groups of attackers continues to be high. Relevant examples, such as the attack on German Bundestag IT systems in 2015, or current attacks on parties represented in the Bundestag, illustrate the political dimension and emphasis of cyber attacks.

Cyber security: Requirement for successful digitalisation

A self-driving vehicle would never be able to drive on its own without the highest level of safety guaranteed. Responsibility for supplying the population with essential goods cannot be handed over to industrial control systems without functioning protection. The German economy's added value that arises from advantages gained in expertise and technology must not be put at risk as a result of industrial espionage. Each of us wants to enjoy the benefits of what increasingly complex information technology may bring – whether that is as a result of unlimited access to information, controlling IT at home or simply for entertainment. The security of the IT systems used for these purposes must be ensured from the outset.

In their daily work, BSI employees confront the major challenges which emerge from this in collaboration with many other partners. Over the reporting period from July 2015 to June 2016, the BSI has demonstrated that it has the capacity to act in the face of this task and is able to tackle the threat effectively.

- The BSI has successfully protected government networks. It has also been possible to detect and defend against even highly specialised attacks at an early stage. Malicious software infections on Federal Government systems, which had actually been successful initially, were detected and cleared at an early stage as a result of numerous defensive and detection measures.
- Affected parties outside government networks were warned of current threats by the BSI and supported in adopting countermeasures. The BSI has provided support locally in cases where successful attacks have occurred – in view of the small size of the BSI, which has approximately 660 employees, this service merely represents the start of future efforts.
- The BSI takes a prominent role in the internationally important area of standardisation and certification. The BSI is a leading authority globally for IT security certification.

- As a result of the IT Security Act, the BSI has been assigned a new responsibility for the security of critical infrastructures in Germany. Effective and viable measures are being developed in close collaboration with those sectors and companies which are currently the focus of attention in order to ensure the supply of services for the population. The BSI is ready to fulfil its role as the supervisory authority for this area of the economy.

Over the reporting period that has just ended, the BSI has also laid essential foundations for further developments anticipated in the future. Justifiably, the BSI is increasingly expected to open up and provide services for administration, companies and citizens over and above merely an understanding of its responsibilities. The BSI has incorporated this into its mission statement: 'As the national cyber security agency, the Federal Office for Information Security organises and develops information security in digitalisation on behalf of the state, business and society'. In the reporting period, the BSI has already been able to set down initial foundations for implementing this requirement.

The BSI has, for example, increased its collaboration with state and business. Efforts to support this extended beyond the expansion and consolidation of cooperation platforms such as UP KRITIS and the Alliance for Cyber Security which already existed. Moreover, the BSI influences key information security standards with particular attention paid to viability in the economy – from the reorganisation of IT baseline protection through to particular standards for Industry 4.0. The BSI continues to provide security certification which the economy can use in the market to provide evidence of security standards which have been implemented.

The BSI is increasingly involved in major digitalisation projects in Germany and acts in an overarching sense on behalf of state and private stakeholders in the interest of guaranteeing security. In this way, the BSI is contributing to the success of the 'energy revolution' – Germany's move towards alternative energy – by developing security criteria for electric smart meters infrastructure and in supporting the development of security aspects for traffic infrastructure in which autonomous or highly automated vehicles are becoming a reality. The BSI has also been involved in the design and certification of the key security anchor in the electronic health card and the systems necessary for this. At the same time, the BSI has also been able to publish standards and recommendations for business such as recommendations for secure email infrastructure which have already been adopted.

In addition to this, the BSI continues to provide information for citizens, and this information is constantly being updated. The information ranges from advice and tips on managing IT, through to configuration instructions for domestic PCs. Citizen services have been supplemented with offerings for developing awareness and providing assistance. We shall further consolidate this area in the future.

Implementation of the IT Security Act

The IT Security Act has been in force since July 2015. Regulations which specify the areas of critical infrastructure covered by the act are needed for its implementation. An initial regulation relating to this entered into force in May 2016. It covers the KRITIS sectors of energy information technology and telecommunications, as well as water and food. The next regulation is expected in spring 2017 and will cover finance, transport and traffic, as well as health sectors. In each case, the sectors affected must fulfil their obligations under the law six months after the regulations have entered into force – i.e. initially from November 2016.

Initial effects are already being seen as a result of the enactment of the IT Security Act. For example, individual companies in the areas covered are already meeting their statutory obligations for reporting IT security incidents and for protecting IT systems in accordance with state-of-the-art technology ahead of the deadline. Sector-specific working groups have also already been formed under UP KRITIS. The number of organisations participating in UP KRITIS has now doubled to 380 organisations.

The BSI organises and develops information security in digitalisation

Groups which are particularly affected by cyber attacks and other IT security incidents must better adapt in order to cope with the challenges which lie ahead. The BSI is expanding provision of IT support for this purpose across the board.

However, this does not release businesses from their responsibility to also develop their own measures for prevention and to build awareness. The BSI is available to provide support in the designing and organisation of individual measures. There is also a huge demand for enhanced detection and response capability in the economy. The BSI will support initiatives for this purpose and will take action itself when it is sensible to do so. An urgent need for this can be seen in the area of critical infrastructures, however action is also needed across the board among small and medium-sized enterprises. The BSI shall continue with the changes already made in this respect over the reporting period. Initial steps for more direct collaboration with business have already been taken. For example, an individual collaboration agreement has recently been concluded with Volkswagen AG, and a similar agreement is already planned with Continental AG. The BSI is similarly approaching all DAX and MDAX companies in order to further develop cooperation. The initial outcomes from these collaborative arrangements are very promising.

The functioning of state information technology is in the particular interest of society at large. The BSI therefore continually adapts protection measures for the government network to the changing level of threat. The BSI is also increasingly collaborating with the federal states and expanding its provision of support. As a result of continual improvement in information relating to the state of IT security, the BSI is able to quickly acquire necessary information and fulfil its role. In order to improve the responsiveness of the BSI in the case of particular cyber situations, mobile incident response teams (MIRT) have been set up to support sites which have been acutely affected.

The BSI has most recently observed attacks on parties, media and state organisations which are grounds for concern regarding the targeted manipulation of public opinion by third parties. The BSI is closely monitoring the situation in this regard in particular during elections for the Bundestag, and will make particular arrangements to ensure that potential cyber attacks can be dealt with.

The BSI is also facing the challenges posed by digitalisation in conjunction with its international partners. As the attacks mostly have an international element, this is an essential source of information for the BSI which will be further developed.

Digitalisation is well underway, as are the risks and opportunities it entails. Sweeping changes have been triggered as a result and these will change Germany. The BSI continues to address the task of designing and organising information security and thereby contributes to the success of digitalisation in the state, business and society. Successful digitalisation of state, business, and society will not occur without cyber security.

6 Glossary

Advanced persistent threats
Advanced persistent threats (APT) are targeted cyber attacks on selected institutions and organisations, in which attackers gain long-term access to a network and then spread the attack to additional systems. The attacks are characterised by a high level of resource deployment and considerable technical capability on the part of the attackers; the attacks are generally difficult to detect.

Attack vector
An attack vector denotes the combination of attack routes and techniques through which the attackers gain access to IT systems.

Application/app
An application, or app for short, is a piece of user software. The term 'app' is often used in relation to applications used on smartphones or tablets.

Adware
Adware refers to programs that are financed by advertising. Malicious programs that generate advertising for their creator also fall under this category.

Bot/botnet
A botnet is a collection of computers (systems) that have been attacked by a remotely controllable malware program ('bot'). The affected systems are controlled by the botnet operator by means of a command-and-control server (C&C server).

Blinding
Blinding is a procedure generally used to protect against side-channel attacks in cryptography. Blinding can help to disguise the secret key (or parts of it) during an encryption operation so that no information can be extracted in relation to this key. A random number is generally added to the secret value which does not influence the crypto operation, but protects the genuine key.

CERT/Computer Emergency Response Team
A computer emergency response team is made up of IT specialists. Many companies and institutions have now established CERTs to handle defence against cyber attacks, respond to IT security incidents and implement preventive measures.

CERT-Bund
CERT-Bund (Computer Emergency Response Team of the Federal Government) is located within the BSI and functions as the central coordinating body for government authorities for both preventive and reactive measures in the event of security-related incidents affecting computer systems.

Cloud/cloud computing
Cloud computing denotes the provision, use and billing of IT services via a network, where these services are dynamically adapted to demand. These services are offered and used exclusively in accordance with defined technical interfaces and protocols. The range of services offered within cloud computing covers the entire range of information technology, including infrastructure (such as computing power and memory), platforms and software.

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

DoS/DDoS Attacks
Denial-of-service (DoS) attacks target the availability of services, websites, individual systems or whole networks. When these attacks are carried out simultaneously, they are referred to as a distributed DoS or DDoS attack (DDoS = distributed denial-of-service). DDoS attacks are often performed by a very large number of computers or servers.

Drive-by exploits/drive-by downloads
The term 'drive-by exploits' refers to the automated exploitation of security vulnerabilities on a PC. The act of viewing a website, without any further user interaction, is sufficient to open up a vulnerability in the web browser, additional browser programs (plug-ins) or the operating system which can then be exploited, thereby enabling malware to be installed on the PC unnoticed.

DNSSEC
DNSSEC is a security extension for the Domain Name System (DNS). Entries in the DNS can be cryptographically signed by means of DNSSEC. Manipulation of these entries is then easier to detect.

DANE
DNS-based Authentication of Named Entities (DANE) is a protocol which allows certificates to be bound to DNS names. A typical case is the storage of a TLS certificate. A DNS entry with the name TLSA is generated for this purpose. DNSSEC is necessary in order to protect these entries from manipulation.

Exploit Kit
Exploit kits or 'exploit packs' are tools for cyber attacks that are placed on legitimate websites. A variety of exploits are used in an automated way to try to find vulnerabilities in the web browser or its plug-ins and to exploit these for installing malware.

Firmware
Firmware denotes software that is embedded into electronic devices. Depending on the device, firmware can either have the functionality of, for example, a BIOS, an operating system or application software. Firmware is specifically adapted to the respective hardware and is not interchangeable.

Nonce
Nonce stands for 'number used only once' and in cryptography represents a unique number, i.e. a number which is only used once in a context. Nonces are often generated by means of a random number generator and then used, for example, for creating an electronic signature and deleted thereafter so that the same number cannot be used again for a different electronic signature. Nonces are also necessary for establishing the TLS connection.

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

Patch/patch management
A patch is a software package which software manufacturers use to resolve security vulnerabilities in their programs or to implement other improvements. Many programs offer an automated update function to make the installation of these updates easier. Patch management denotes the processes and procedures that enable an IT system to obtain, manage and install available patches as quickly as possible.

Phishing
The term 'phishing' is a combination of the words 'password' and 'fishing', i.e. 'fishing for passwords'. Here, the attackers attempt to extract the personal data of an Internet user via bogus websites, emails or messages in order to misuse this data for their purposes, generally at the expense of the victim.

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

Padding
Padding is used in cryptography for encryption procedures in order to extend data ranges. In a block cipher, for example, the data to be encrypted is stored in blocks of a set size. Padding may be used to extend the final bytes so that the last block is also full.

Ransomware
Ransomware is defined as malicious programs which restrict or prevent access to data and systems and only release these resources upon payment of ransom money. This involves an attack on the availability of a security target and constitutes a form of digital extortion.

RPKI
The Resource Public Key Infrastructure is a certificate infrastructure specifically used for protecting Internet routing.

Root Zone
The root zone is the top-level zone in the hierarchical Domain Name System (DNS):

.	Root Zone
.de	Top-Level Domain 'de'
.bund.de	Domain of Federal Government

Social Engineering
In cyber attacks involving social engineering, criminals attempt to mislead their victims into voluntarily disclosing data, bypassing security measures, or willingly installing malware on their own systems. Just as in the field of espionage, cyber criminals are adept at exploiting perceived human weaknesses, such as curiosity or fear, in order to gain access to sensitive data and information.

Spam
Spam is defined as unsolicited messages sent by email or using other communication services to a large number of people in a non-targeted way. Harmless spam messages generally contain unsolicited advertising. However, spam frequently also comes with attachments containing malware, links to infected websites, or is used for phishing attacks.

SSL/TLS
TLS stands for Transport Layer Security and is an encryption protocol for the secure transmission of data on the Internet. Its predecessor SSL (Secure Sockets Layer) is another such protocol.

Sinkhole
Sinkholes are defined as computer systems to which queries from botnet-infected systems are diverted. Sinkhole systems are typically operated by security researchers for detecting botnet infections and informing users who are affected.

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

Legal Notice

Published by
Federal Office for Information Security (BSI)

Source
Federal Office for Information Security (BSI)
Godesberger Allee 185–189
53175 Bonn

Email
bsi@bsi.bund.de

Telephone
+49 (0) 22899 9582-0

Telefax
+49 (0) 22899 9582-5400

Version
October 2016

Print
Druck- und Verlagshaus Zarbock, Frankfurt am Main

Content and editing
Federal Office for Information Security (BSI)

Image credits
all images: iStock.com/jm1366

Graphics
BSI

Item number
BSI-LB16/505e

www.bsi.bund.de