Federal Office
for Information Security

The State of IT Security in Germany 2015

Content

FOREWORD

The report by the Federal Office for Information Security in Germany (BSI) on the current state of IT security in Germany in 2015 provides information on the type and extent of key IT threats and resulting risks. The report is based on information analysed by the BSI relating to weaknesses and vulnerabilities in currently used information technology, as well as to attacks on IT systems and networks.

The report shows that the number of weaknesses and vulnerabilities in IT systems is continuing to run at a high level. Some of these vulnerabilities expose serious security gaps. The asymmetric threat level in cyberspace continues to escalate, meaning that users' protection of IT systems cannot always keep pace with the often highly developed tools for exploiting gaps in security.

The following trends are especially clear on reading the report:

Firstly, in view of the high number of identified vulnerabilities, some IT manufacturers tend to no longer provide security updates for their products' security gaps where they believe that those gaps are less serious. This unnecessarily worsens the current level of exposure.

Secondly, the number of attacks on industrial production facilities is rising, generating new commercial and economic risks.

And thirdly, aspects of IT security are not always properly considered during digitisation, even if the failure of the relevant systems can result in far-reaching individual or societal consequences.

The IT Security Act, which entered into force at the end of July 2015, is a key first step in improving the protection of IT systems and digital infrastructure in our country: we want them to be among the world's most secure. Germany is well prepared for the task with the BSI acting as the statutory centre of expertise for IT security matters.

However, neither the Government nor economy alone is able to guarantee IT security in our country. Everyone has a contribution to make. We must therefore strengthen collaboration between Government and commerce, as well as finding new ways to collaborate. We must work together to help make citizens aware of the risks and to show them how to work securely online. The more securely each individual can navigate the internet, the better the protection for the state and society online.

The digital vulnerabilities of our society will continue to place demands on us over the coming years. This BSI report on the current state of IT security in Germany provides the basis to enable decision-makers in Government, commerce and society to properly address the risks to our country that are associated with digitisation. Therefore, I hope this report will be widely read by people who can then identify the areas that affect them, and take action.

Dr. Thomas de Maizière
Federal Minister of the Interior

1 IT security between the conflicting priorities of innovation, globalisation and complexity

1 IT security between the conflicting priorities of innovation, globalisation and complexity

The continuously high rate of innovation in information technology is expressed by its huge force for change and rapid penetration of all areas of life and business. The saturation point of the potential use of IT has not yet been reached. Quite the opposite in fact: significantly higher growth rates can be expected in the miniaturisation and networking of intelligent systems. Developments such as the 'internet of things' and 'Industry 4.0' are just two examples of this. In a phase in which companies are developing their business models further, or even establishing new ones, industry and commerce as well as consumers are affected by the onward march of digitisation. For Germany, this creates economic and social perspectives. It is increasingly clear, however, that continued digitisation is essentially determined by functional and economic factors. Ongoing globalisation increases the financial pressure on all parties to succeed. Against this backdrop, IT security is often overlooked.

Providers who lag behind with respect to innovation and competitiveness run the risk of being very quickly forced out of the market. This results in pressure to service the needs of a growing global customer base more quickly and functionally better than the competition. Aspects of IT security are often considered of equal priority neither by users nor providers. It is therefore unsurprising that requirements with respect to the security of IT systems, applications and software take second place to economic considerations. As long as users of suppliers, service providers and manufacturers do not demand security as well as functionality, no material changes will be made to enhance IT security. Therefore, apart from special markets in upscaling business fields, especially the end customer sector, IT security is of little importance as a distinguishing feature. As a result, the necessary level of security is not produced.

This has serious consequences for the security of the IT deployed, which are evident from the number of disclosed weaknesses, vulnerabilities and attacks. This means that current level of IT risk remains acute. The regulation of critical infrastructures by the IT Security Act is therefore a step in the right direction. It remains to be seen how the current level of IT risk will develop in other areas of use outside critical infrastructures. Further IT security legislation may also be useful here if no adequate IT security level is established by market mechanisms.

A number of technological changes and their significance to IT security are described below. This will illustrate how quickly manufacturers and users will find themselves in the field of conflict described above.

Software-defined Everything versus Separation

The current trend toward software-defined everything illustrates the conflict between functionality and IT security. The term describes the trend toward architectures in which systems, networks, storage and – depending on design – also other elements of information processing are no longer defined statically by the hardware used, but can be configured dynamically (for example, Software-defined Network, Software-defined Data Centre, or Software-defined Storage). The benefits are clear: resources can be moved to where they are needed more quickly and at lower cost. Organisational changes can be mapped more easily, such as during mergers or acquisitions. Software-defined Everything however competes with the basic requirement of information security based on the separation of key processes and systems. The separation of different customer data, operational and technical processes as well as systems and networks with different security levels is an established and proven strategy for ensuring adequate IT security. In a dynamic, software-configured environment, this separation cannot be effected to the same technical depth as in traditional architectures. It is essential here to underpin the required separation on a virtual level and also to use secure platforms in order that virtual separation cannot be undermined.

Mobile computing versus protection of business-critical information

The trend toward the use of mobile IT continues apace. In the private user sector, new device classes are already launching on the market, e.g. as wrist watches and glasses ('wearable computing') alongside established smartphones and tablets. Smartphones and tablets already form part of standard business equipment. As a result, the demand for processing business-critical information on this type of device is growing. However, in view of the increasing risk of cyber-espionage, many institutions have recognised that they must pay particular attention to protecting specific information. The reason for this process is that it is mostly costly and impractical to establish the same high level of security for the entire institution. Instead of this, business-critical data, the 'crown jewels' are heavily protected, while proven standard security measures are implemented in all other areas. For many institutions, the question therefore arises of whether – and if yes, how – business-critical data can be accessed from mobile devices. Here, the available modern security solutions as well as individual risks should be considered.

Operational reliability versus protection against attacks

Security is an essential basic requirement in industrial controls and automation. In the event of malfunctions and deviating operating conditions, no unacceptable risk to people or the environment may be posed by machines and equipment. Requirements of this operational reliability, known as 'safety' have been defined for many years in norms and standards that are constantly updated and developed. In contrast to operational reliability, protection against attacks, against intentional malicious acts, is known as 'security'.

Organisational and technical interactions between safety and security arise against the background of increasing digitisation. On the one hand there are a number of synergies, for example in the clear structuring of networks and monitoring of components.

Encryption and filter mechanisms can also affect the propagation delay and in some circumstances safety features of the system. Such potential interactions must be systematically considered when planning safety and security measures.

Compatibility versus information security

When introducing modern and secure solutions, the justified demand for compatibility with existing solutions can become a barrier. It often takes time before improved security-related technologies become established and obsolete, insecure solutions can be retired. One example of this is the TLS/SSL protocol which is used in the internet and in other networks for the encryption of data traffic. Many online servers are configured in such a way that older, insecure cryptographic methods are approved, for internet users to be able to access the relevant website using older browsers. Another example is the use of older operating systems for which the manufacturer no longer provides security updates. In the field of industrial controls and automation, IT systems can often simply be upgraded to a new operating system, sometimes because the manufacturer does not support it or because there is no compatibility.

2 Current exposure

2 Current exposure

Chapter 2 describes the current exposure situation with the help of determining factors, causes and attack methods. In doing so, graphs are used to provide an analysis of the individual threats in the reporting period.

(low, average, high)

2.1 Causes and determining factors

2.1.1 Cloud computing

Introduction

Cloud computing is a continuing trend which is transforming the entire ICT sector and has a major impact on IT security. The fundamental change in the ICT sector due to cloud computing is the leasing of cloud services instead of buying software products. This increases dependence on cloud service providers, to the point at which process and data ownership may be lost. The use of cloud solutions requires greater confidence in the providers on the market. There is a crucial difference as to whether software is purchased in the traditional way from a provider and is operated in-house, or whether all data is transferred to the provider and the software is made available merely as a service of the provider. If the IT system is operated in-house, the operator itself determines which method of IT security management is used. If cloud solutions are used, the responsibility for IT operations lies with the provider and only specific Service Level Agreements (SLA) are negotiable with the provider. The secure use of cloud applications continues to pose a major challenge to IT security experts.

Current situation

Cloud computing and cloud security generate numerous requirements for application scenarios which mean those responsible face new challenges every day. The following aspects are relevant with respect to IT security.

- **Confidentiality of customer data:** multi-level safeguards to separate customer areas from one another are a requirement of secure cloud computing, but often involve high costs. If these measures fail, it generally affects many customers. The financial losses due to lost customer data are difficult to quantify. It is particularly difficult to provide for reasonable compensation in the contract in advance. The problem does not yet seem to have been addressed consistently in cloud contracts.

- **Cloud service provider as a target of attacks:** Cloud service providers present a lucrative target for attackers in many respects. On the one hand, the details of several customers can be accessed by a successful attack on a service provider. On the other hand, a cloud infrastructure itself is of interest to attackers since it provides a wealth of resources (processing power, storage capacity) which can be used to crack passwords or to perpetrate DoS attacks on third parties. This trend will continue to rise with increasing cloud use. In future, cloud service providers will have to devote even more time and effort to protecting their own systems – and with it the data and operational capacity of their customers.

- **Handling of security incidents:** cloud service providers often work with subcontractors or complete supply chains. If an incident occurs, measures must be taken promptly across a number of service providers and all customers must be integrated into the incident management. It has not yet been possible to resolve the conflict between the concern of the cloud provider not to unduly worry his client and the concern of the client to be informed quickly and precisely of incidents. From an IT security viewpoint, the cloud service provider must define and implement procedures to this effect.

- **Benefits of cloud computing for IT security:** the clear benefits of cloud technology currently face challenges. A cloud provider can – if it has a lot of customers – implement security measures more cost-effectively for all customers than a company could for itself. This applies to traditional information security measures, e.g. backup and geo-redundant data mirroring, but also in the field of cyber-security, since a cloud service provider normally has more resources at its disposal to protect against DDoS attacks. This can be of particular benefit to small and medium-sized businesses.

Assessment

At present, the awareness of process owners of the opportunities and risks posed by cloud computing in the field of information security remains low. Due to the customer's low level of demand for IT security measures in cloud solutions, providers have invested too little in this field to date. Customers must also demand a high level of IT security to help make security a key distinguishing feature on the cloud service market.

2015 danger

2.1.2 Software vulnerabilities

Introduction

Software contains vulnerabilities which create the perfect conditions for successful cyber-attacks. In view of the increasing size, measured in lines of code, and the complexity of today's software, it is inevitable that bugs will creep in during development. The exploitation of architecture, implementation and configuration bugs allows the system status to be changed against the will of the user. Examples of this are the automatic execution of regularly embedded malicious code when opening a document (architecture bug), the possibility of bypassing a password prompt (implementation bug) or the use of publicly disclosed standard passwords (configuration bug).

Current situation

- The number of critical vulnerabilities in standard IT products in 2015 has increased massively in comparison to figures from the previous year, which were already high (Fig. 1). In 2015, 847 critical vulnerabilities were identified by the end of September for just the 11 software products (Fig. 2) which appear most frequently in the BSI traffic light system for vulnerabilities.

- From the viewpoint of the attacker, web browsers and the plug-ins contained within them are the most exposed software. Vulnerabilities in these applications are therefore the preferred targets of attacks. In respect to the Microsoft products included in the vulnerability traffic light system, more than 45% of vulnerabilities up to July 2015 affected the web browser. The browser plug-in Adobe Flash Player had the highest number of critical vulnerabilities by some distance.

- Development methods which consider security aspects throughout the entire lifecycle of a software make a key contribution towards reducing the number of vulnerabilities and by doing so improve the security of software (for example source code analysis tools or tests by fuzzing).

- Techniques for containing the exploitability and/or the impacts of vulnerabilities, such as ASLR (Address Space Layout Randomization) and NX/DEP (No eXecute / Data Execution Prevention) are also of major importance. ASLR and NX/DEP are used throughout current software, provided that the mechanisms are supported by the hardware. Sandbox mechanisms, i.e. isolation of individual program components are also prominent in defending against viruses. Browsers with sandbox technology isolate the content of a website from the rest of the browser and from the operating system and by doing so reduce the impact of an attack if an infected website is visited.

- The patch management policy is also gaining in significance. Manufacturers are responsible for implementing an effective patch management policy with short response times. Some manufacturers however have already begun to provide fewer patches for fewer critical vulnerabilities, mostly due to lack of resources. As a result, this can lead to vulnerabilities only being removed weeks or months late or even not removed at all.

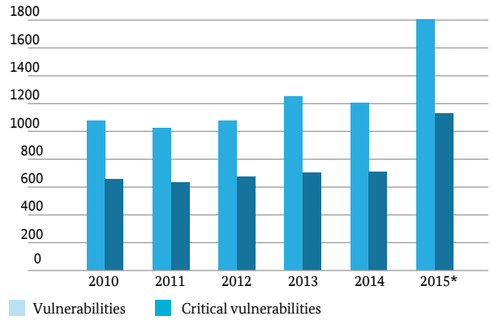

Figure 1: Number of all vulnerabilities in software products recorded in the BSI traffic light system for vulnerabilities. * The numbers for 2015 have been projected from the vulnerabilities discovered up to the end of September 2015

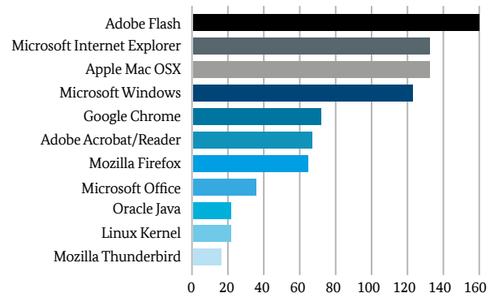

Figure 2: Critical vulnerabilities of the software products logged in the BSI vulnerability traffic light system by September 2015

Blackmail attempt after the web server was compromised

Circumstances: A company receives a blackmail letter by email demanding the payment of two Bitcoins within 24 hours. If the company did not meet the demand, the blackmailer threatened the publication of customer data already spied out after the website of the company was compromised. As proof that the website had been compromised, the database structure of the web application as well as screenshots had been attached to the blackmail letter.

Cause/trigger: The compromising of the company's website was made possible by the exploitation of a known vulnerability in the Content Management System (CMS) used. After receipt of the blackmail letter, an already available security update for the CMS was installed.

Method: In order to compromise a large number of web applications, attackers look for known vulnerabilities in common web applications. This is largely automated by using specific search machine parameters (e.g. known paths and/or web application files) and prepared attack scripts to exploit vulnerabilities. The use of cryptocurrencies such as Bitcoin for the ransom demands has been increasingly in evidence in DDoS blackmail attacks and crypto ransomware in 2015 as well as the case highlighted above.

The effect of the damage: The company initially suffered a loss of reputation following the cyber-attack due to the publication of confidential customer data. The secure restoration of the website also entailed financial and labour costs. The use of the exposed information for further cyber-attacks, e.g. against the customers of the company, is conceivable but was not identified in this case. In general, the compromising of websites can cause various damage. Alongside the exposure of sensitive information described here and the use of this for the blackmail scenario, the attacker can also spread malware through the website or misuse the web server for e.g. DoS attacks or sending spam.

Target groups: In 2015, predominantly small and medium-sized businesses reported compromised websites and similarly based blackmail scenarios to the BSI.

Technical abilities: Known vulnerabilities in common web applications can be exploited by attackers who do not have any great depth of IT security knowledge. Even unidentified vulnerabilities in web applications can be detected using vulnerability scanners and then exploited.

- Essentially, security updates must be programmed immediately following availability in order to keep the time-frame in which the systems are vulnerable as short as possible. If detailed information or even exploits for a specific weakness are disclosed before a security update is provided, the use of the affected software should be avoided, or it should only be used with extreme caution. In 2015, there have been nine published incidents by the end of September alone in which zero day exploits were used. The cyber-security survey 2015[1] also showed that successful attacks could often be traced back to attacks through unidentified vulnerabilities and to a lack of patch management.

Assessment

The threat level due to vulnerabilities remains high. There are signs however of a partial rethink in the software industry which could lead to a long-term enhancement of IT security through improved software development, enhanced mitigation of vulnerabilities and shorter reaction times. The manufacturers must meet their special responsibility throughout the lifecycle of a product, which includes the regular and rapid removal of vulnerabilities as well as the use of the available protection measures and current software development processes. In order to enhance the security of purchased hardware and software in this context, major clients could demand binding periods during the negotiation of delivery contracts with the manufacturers, within which a manufacturer must remove a vulnerability for products in the framework contract after the vulnerability has been disclosed. The BSI has already started to implement this in some framework contracts for IT procurement by the Federal Government.

The BSI believes that the correct way to remove vulnerabilities is through close collaboration between the identifier of a vulnerability and the manufacturer of the affected software. This process, known as Coordinated or Responsible Disclosure, allows the manufacturer to provide security updates without disclosing details in advance which can be used to exploit a vulnerability and which can be exploited for attacks.

[1] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/Umfrage/ umfrage2015.html

In spite of this, the identifier frequently discloses information on a vulnerability even if the manufacturer has not yet removed the vulnerability. A common reason for this is that in the opinion of the identifier, the manufacturer either needs too much time to remove a vulnerability or does not want to remove it.

The BSI has published information for manufacturers on dealing with vulnerabilities[2].

2015 danger

IT security certification: Confidentiality and security design

Since Germany and Europe are significant demand markets in the global information and communication technology sector and significant provider markets for software and hardware products in subsegments only, IT security certification plays a key role: From a user point of view, security standardisation and IT security certification provide effective instruments to enhance the transparency of information security, to assess the confidentiality of products and also to establish a high level of information security on the market in the interests of the user. The 'high assurance' approach in particular is not always in the interests of manufacturers and distributors who are tied to the short lifecycles which prevail in the IT sector and want to save on (time-consuming and) expensive certification processes. Due to the globality of the market, only IT security standards and IT security certifications based on international standards ("common criteria") are suitable for guaranteeing security and thus confidentiality in hardware and software products. The global players in the ICT sector are only prepared to invest in testing and certification on the basis of international standards.

The challenge posed by vulnerabilities in IT products is to develop products more securely as well as to perform evaluations with vulnerability analyses through independent certification bodies. In Germany, nine evaluation bodies are recognised by the BSI in the field of common criteria certification.
A key basis for the certification is formed by technical guidelines and protection profiles with which security requirements can be met for specific product groups or technical systems, the compliance with which is ensured by the certification. In recent years, a large number of protection profiles have been created, in part by the BSI. These protection profiles create reproducibility for the user in the various product classes. The differing testing rigours in particular show transparently whether and how the product has been analysed in the course of the evaluation for vulnerabilities.

In the course of 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 looks at security issues and solutions which result from the product testing and analyses. This often concerns issues from areas such as

» implementation of security-critical product changes
» actual integration of encryption methods into IT security products
» integration of new production and development locations at manufacturers
» individual issues in the context of correctness testing for security functions
» Handling and consideration of information on product-related IT vulnerabilities provided by test laboratories and manufacturers, e.g. after simulating side channel attacks

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 proves that the tested product actually includes the promised features.
Protection profiles and "high assurance" certificates are key security-related 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 future intelligent metering systems such as electric meters. Only through certification can we guarantee that the security level specified by the legislation is actually reflected in the products used. The BSI represents the view that a high test level is vital for the assessment of the security of modern and normally complex IT. A comprehensive, in-depth security certification is absolutely essential in view of the risks involved, especially if IT systems are used at key interfaces of critical infrastructures.

At present, we see that states outside Europe in particular have a tendency not to share this view. There are many voices demanding quick, easy testing and certification. Even in international trade agreements (TTIP, TiSA etc.) currently in negotiation, there is a real risk that IT security interests are not being properly considered. It is important here that the high standards established in Germany and Europe are not put at risk.

[2] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/programmierung/BSI-CS_019.pdf

2.1.3 Hardware vulnerabilities

Introduction

The threat presented by hardware vulnerabilities in electronic equipment has long been the subject of many IT security studies in professional circles. Hardware manipulation can take place on various levels. In general, we can distinguish between the following attack vectors:

- Modifications through additional modules
- Changes to existing circuitry
- Manipulation on a chip level
- Software modifications on a firmware level

With the exception of firmware manipulation from the operating system, physical access to the equipment is required for this type of attack. In view of the production plants and global supply chains distributed throughout the industry, the components pass through many hands which significantly increases the opportunities for manipulation.

Current situation

- Hardware manipulation can be perpetrated through the integration of components in equipment or through the weakening of existing electronic circuitry (thinning of wires, irradiation of components). For example, the integration of additional modules can enable a keyboard to send data via radio frequencies alongside its actual function. Any USB devices can be manipulated in a similar way and by doing so bring about the desired side effects. The detection of additional components is essentially possible but is often a laborious process.

- Manipulation on a chip level is practically impossible to detect. The target of these attacks is, e.g. the random number generator in the processor which is a crucial element in cryptographic methods. This random number generator can be weakened by doping changes to the semiconductor material so that the random numbers become predictable. The effects on encryption methods are serious: An encryption can be cancelled and/or broken easily many times over[3]. Such a manipulation is very difficult to detect since the internal structure and the components of the chip do not change. Neither would a function test reveal the predictability of the random numbers.

- Modern hardware is often intrinsically linked to software components. Publications on the NSA spying affair refer to back doors which are permanently implanted in the BIOS or in firmware[4]. Since these programs are beyond the control of the operating system, they are often attributed to hardware Trojans. The risk from such implants is based on the fact that they run in the system management mode (SMM) of x86 processors or in the underlying management engine (Intel ME, Apple SMC) and thus have full access to the main drive and/or other key components of the system. In this way, the attacker can completely take over the computer or at least damage it. Finding such malware is also a very laborious process.

- Many cyber-attack methods for hardware have become generally available in their basic form and can be implemented at little cost. This includes side channel analyses and the intentional creation of bugs or glitches. These technologies enable internal information to be obtained, e.g. keys for protection of communication, without damaging the equipment or accessing the debug interfaces.

Assessment

The specific threat from hardware attacks lies in the fact that they can only be detected with great difficulty. The same applies to hardware Trojans which are mostly passive and only execute their malware function after activation. Existing test methods are inadequate or too laborious, with the short product innovation cycles in information technology also making analyses difficult or obsolete. Effective protection against manipulation can only be achieved by producing components in a confidential environment and distributing them by means of a secure supply chain.

[3] http://people.umass.edu/gbecker/BeckerChes13.pdf
[4] http://mjg59.dreamwidth.org/35110.html

Vulnerability of Intel Management Systems

Issue
Intel offers a remote maintenance function for PCs with the implemented AMT management solution (also marketed as vPro) in the chip set of the mainboard, which enables computers to power themselves on when switched off and to fully configure themselves. AMT is part of the Intel Management Engine. The system is typically unconfigured when delivered and is supplied with a standard password. If this function is not used, this unconfigured condition normally remains in place.

In July 2015, a vulnerability was identified on several device types from various manufacturers: attackers have the opportunity to reconfigure an unconfigured computer with a specially prepared USB stick by using the manufacturer-specific standard AMT password, regardless of any security measures which may have been set up. Only business systems of various manufacturers are normally affected by the vulnerability.

Assessment
If the attacker has just a few seconds of physical access to a vulnerable system and connects a prepared USB stick, he can then fully remotely control the computer and read and modify data. Protection mechanisms on an operating system level cannot prevent the attack, but only detect it under specific conditions. At particular risk are mobile systems since normally they are not constantly under the control of the owner.

Measures
The AMT subsystem should be provided with a new, device-specific secure AMT password before use, irrespective of the subsequent use of AMT. The AMT subsystem can then be deactivated in the BIOS settings. Simply deactivating AMT in the BIOS settings alone is not sufficient.

2.1.4 User behaviour and manufacturer responsibility

Introduction

The growing spread of information technology puts people firmly back at the heart of IT security issues. People are responsible for IT and information security, but are also often the weakest link in the defence chain. Alongside technical and organisational measures, sensitisation, awareness and a healthy degree of mistrust on the part of the user is essential for IT security.

Current situation

- Digitisation touches many areas of everyday life. For example, at present so-called fitness trackers which can measure various physical functions and training units are enjoying a rise in popularity[5]. The digital assistants also transfer sensitive health data to central service providers for storage or analysis. The presumption is that scant heed is paid to the vulnerability of the technology or the use of the data by the operator. Existing and new services on the social web promote apparently free or low-cost social networking and affiliation and lead to ever growing membership figures[6].
- Personal data or digital identities are vulnerable if a lack of technical understanding compounds the inadequate transparency of the services. Disinterest and the excessive demands cause the user to act carelessly in the digital world.
- Awareness campaigns and the increasing number of media reports contribute to an increased awareness of the risks when using IT and the internet. Many users however go for certain devices, services and applications for reasons of comfort and user friendliness, whilst IT security aspects frequently play no role in their choice.
- According to an IBM study, over half of all successful cyber-attacks are related to the user. Regardless of cyber-attacks by external attackers, (former) employees or service providers can cause serious security problems intentionally or through inexperience[7, 8]. Examples include preventable user error, use of social web services as well as increasing connection of mobile devices – including private devices – to the company network. Unauthorised access headed the list of security incidents in the study, in previous years detected attacks through malicious code and spying on systems by external attackers came out on top.

[5] http://www.connect.de/news/smartwatch-fitness-armbaender-wearables- apple-watch-verkaufszahlen-2897622.html
[6] WhatsApp with 800 million active users: http://www.heise.de/newsticker/meldung/WhatsApp-mit-800- Millionen-aktiven-Nutzern-2612236.html
[7] http://www.heise.de/ix/meldung/IBM-Sicherheitsstudien- Cyber-attacken-aus-den-eigenen-Reihen-am-haeufigsten-2715977.html
[8] 2015 Cyber Security Intelligence Index; http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03073USEN&attachment=SEW03073USEN.PDF

Assessment

The road from digital carelessness to responsible digital behaviour is not one that the individual user should walk alone. The responsibility for digital security is borne by all those involved: Users, company management and authorities, manufacturers, providers and service providers. Management carries the main responsibility for a high level of IT security in a company. IT security concepts must be addressed to directors or board members who then take the decisions and communicate them within the organisation. By doing so, they create the necessary basis on which users can act responsibly.

Manufacturers should integrate IT security concepts into production development at an early stage and also consider intuitive usability as well as the manageability of software and processes for less technically gifted users (security ergonomics). Manufacturers should also follow the security by design approach during product development. In their development of secure IT products, manufacturers can create a solid basis on which administrators and employees in companies can build.

Due to their central and upstream position, providers can make a key contribution towards more IT security by structuring their workforce and facilities with respect to IT security aspects, in such a way that they can detect and analyse anomalies or security incidents at an early stage and inform their customers promptly of IT security incidents and efficiently provide support and information. Warning services as well as provision of security tools provide material assistance.

In spite of the responsibility shouldered by the manufacturers and providers, a key role is also played by the user. Demand generates supply, even in relation to IT security. It remains to be seen whether users will demand more information and transparency from providers in future – for example after the new EU data protection regulation enters into force – claim their "right to forget" and as a result digital responsibility can replace digital carelessness.

2015 danger

2.1.5 Cryptography

Introduction

Mathematical cryptography is the central and strongest pillar of IT security mechanisms for the protection of confidentiality, integrity and authenticity of digital information. It is also used for the authentication and protection of the integrity of software and for the protection of physical systems, e.g. locking systems. Cryptography is also an important and dynamic research field which frequently sets new challenges for experts which arise for example from new applications such as cloud computing. The number of potential uses of cryptographic methods is very high and the potential for cryptography is nowhere near exhausted.

Current situation

- In recent years/decades, numerous cryptographic methods have been developed: Block ciphers and stream ciphers for encryption, methods for exchanging keys or for creating digital signatures as well as hash functions and random number generators.
- These methods are used as building blocks in cryptographic protocols such as the Transport Layer Security (TLS) protocol, which are used, for example, to protect mobile communication as well as transactions in online shopping.
- Current cryptographic algorithms can – apart from RC4 – be viewed as secure based on current information. The prerequisite for this is a reasonable choice of parameter and key lengths (cf. BSI Technical Directive TR-02102).
- In research, the development of quantum computer resistant methods is a key issue. Many current methods are no longer secure where a sufficiently capable quantum computer exists. This development is especially significant for the transfer of information with a high and long-term protection requirement.
- Security problems sometimes result from the incorrect application of cryptographic methods in cryptographic protocols and/or errors in implementing cryptographic protocols.
- Side channel attacks allow implementations of secure algorithms to be attacked. These exploit, for example, timing information or power consumption of devices to obtain information on secret keys.

Current attacks on encryption methods

Since December 2014, there have been two new serious attacks on the TLS protocol: the FREAK attacks and the logjam attacks. Both attacks exploit the existence of weak TLS parameters (so-called export grade). Whilst the FREAK attacks are based on an implementation bug in OpenSSL, in Logjam a vulnerability in the protocol enables an attacker to act as a man-in-the-middle between the two communication parties. The Logjam attack is directed against a method of key exchange which forms the basis of the discrete logarithm problem (DLP). In relation to the Logjam attack[9], researchers from the French INRIA have made use of the fact that the DLP can be relatively easily broken with the help of precomputations if the export grade is weak. By doing so, they were able calculate the secret key exchanged when establishing a TLS connection, virtually in real time. The results are transferable to other applications of this key exchange method. With more time taken for precomputations, DLP cases which are more state of the art could also potentially be solved. For example, the French researchers argue that the NSA is in a position to quickly solve the DLP for selected groups of 1024 bit primes.

Vulnerabilities in RC4

The stream cipher RC4 remains widespread in spite of known vulnerabilities. In recent months, more effective attacks have again been reported, targeting in particular the use of RC4 in TLS. To date, these attacks have only been possible in theory, yet the Internet Engineering Task Force which is responsible for internet standards have now prohibited the use of RC4 for TLS[10].

Assessment

Cryptography is a very active and important field of research. The BSI evaluates cryptographic algorithms and/or standards, tests the implementation of these algorithms and analyses the tests for side channel resistance of implementations. Due to the high potential of cryptographic solutions, it is expected that they will continue to be deployed in numerous everyday applications and contribute to the protection of data there.

2015 danger →

2.1.6 Internet protocols

Introduction

A basic premise of the internet is its openness which allows all users to use the internet for information and the exchange of data. At the same time, the internet has a highly complex structure. Numerous components and protocols are involved, even in the case of simple actions such as opening a website. For many users, openness and anonymity are desirable attributes of the internet. However, together with the technical complexity they can also be the cause of misuse of the internet as an attack platform.

Current situation

- When the internet was designed, the expectation was of a group of cooperative users in a confidential environment. Accordingly, security was not a criterion in the development of protocols. The protocols originally used, e.g. IP, UDP, TCP, DNS, SMTP, HTTP, SSL and BGP are however still used today.
- Since the internet is an elementary component of today's communication, vulnerabilities in the protocols or the reference implementations used have serious consequences. Billions of devices support these and so in principle they are vulnerable to attack.
- Protocol extensions which have previously complemented missing protection mechanisms often take time to become established.
- As a result, following a joint testbed initiative by BSI, DENIC and the eco association, the DNSSEC suite has been available to the DNS directory service since 2010 for .de, the standard top level domain for Germany. The second level domain .bund.de has since been signed with DNSSEC. Various BSI publications on internet security issues reference and recommend this. However, by the start of 2015, only 0.25% of registered .de domains were signed with DNSSEC. Consequently, security protocols based on DNSSEC, e.g. DNS-DANE cannot be introduced.
- When communicating by email, the secured exchange of emails, as well as the validation of sender authenticity is a challenge. A standardised procedure for mutual authentication of the respective email server uses signatures stored in DNS for validation (DNS-DANE). One barrier to implementation here is the hitherto lack of acceptance of DNSSEC, with the result that the majority of emails are still sent unencrypted.
- In many areas of internet communication, the current trend is to encrypt protocols (e.g. HTTP) with TLS. In doing so however, obsolete algorithms are often used. Vulnerabilities in implementations, such as the Heartbleed vulnerability reported in 2014, also allow attackers to read encrypted communication.
- The internet is a combination of many individual systems. The reachabilities – or 'routing prefixes' – are exchanged between the individual systems via the Border Gateway Protocol (BGP). Prefix hijacking allows entire IP address ranges to be re-routed in the internet with the result that communication is disrupted or that data espionage can take place. The cause of these attacks on internet routing are vulnerabilities in the BGP routing protocol. The Resource Public Key Infrastructure (RPKI) provides a security mechanism which will only become fully effective with its widespread adoption.
- Alongside the exploitation of protocol vulnerabilities, attacks are also increasingly detected on devices and components used for exchange of data. These include billions of internet user devices, as well as routers, DNS resolvers, DNS server or web servers. The detection of vulnerabilities, in particular in routers, and attacks on these and similar components has risen sharply. The manufacturers of these components bear a heavy responsibility here to identify vulnerabilities and provide security updates as quickly as possible. Unfortunately, this responsibility is often met with a slow reaction or none at all. This only makes it difficult for users and operators to meet their responsibility to keep their network components up to date from a security perspective.

Assessment

In many cases, the structural vulnerabilities of internet architecture are based on past design decisions, which have been made without regard to security aspects, but which cannot easily be reversed. Therefore, to improve security it is necessary to at least put the available enhancements into practice, for example in the area of protocol extensions, as quickly as possible. Component manufacturers today are required more than ever to focus on the after-sale service of the devices and to quickly provide software updates where vulnerabilities are identified.

2015 danger →

2.1.7 Mobile communication

Introduction

Mobile devices such as smartphones and tablets, as well as – increasingly – smartwatches, have become constant companions in both our professional and personal lives. Many users store personal information on these devices, or use them to process sensitive transactions. This makes the devices a profitable target for criminals.

Current situation

- Mobile products are continuing to be developed very quickly. This creates a very diverse range of device types, both at hardware and software level. The fast and smooth provision of software updates for closing security gaps is not guaranteed under these conditions: updates are sometimes not made available at all, and often only for a short period of time after purchase or only after a significant delay.
- Much of the personal information that we manage using mobile devices is stored in a cloud. The user is therefore entrusting its data to the supplier. If access to the cloud is not sufficiently protected, both user data and access data for the cloud itself – such as passwords – can quickly get into the wrong hands.
- Mobile devices can automatically connect to public hotspots. These are often open, meaning that the data can be transferred unencrypted, and therefore can also be read by unauthorised third parties.

[9] Imperfect Forward Secrecy: How Diffie-Hellman Fail in Practice, D. Adrian et. al., accessible from weakdh.org
[10] RFC 7465: Prohibiting RC4 Cipher Suites, A. Popov, February 2015

- It is possible for the operator of the mobile network and app suppliers, but also cyber-criminals who have access to the device, to locate mobile devices and therefore also their owners at any time. In combination with other information that is spied out, attackers can create a comprehensive profile of the victim's movements.

- Telephone calls that are made using second-generation mobile network technology (2G/GSM) can 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 factors described above combined with the unmanageably large quantity of available apps, some of which include malicious code, will also continue to represent a high potential for risk in the area of mobile communication for the foreseeable future.

In relation to the example of mobile communication, the influence certain business models can have on information security is clear when looking at the example of mobile communication. Apple takes great care to keep its operating system closed and to retain control over which software can be installed on mobile Apple devices. Exceptions only exists for software distribution within institutions.

Google, however, also enables Android apps to be installed from third-party sources: a function that is often utilised by users. From the perspective of information security, both approaches have advantages and disadvantages: while there are now several million different malicious program versions for Android, relatively few are known for iOS. On the other hand, iOS users have significantly less control over which programs run on their devices and what actually happens to their information. At least in the context of companies and authorities, both dangers – malicious programs and loss of control – must be taken into account within risk analysis.

2015 danger

Stagefright gap in Android: careless update behaviour on the part of manufacturers

Dealing with stagefright gaps in Android is a prominent example of slow, partly careless, update behaviour on the part of device manufacturers. According to discoverer zLabs, at the time of discovery the gap existed on 95% of all Android devices[11]. Stagefright is the designation for the multimedia interface integrated into the Android operating system (Media Playback Engine). The Android operating system as well as installed apps can use the interface to process audio and video content. A total of seven different vulnerabilities, which could be used to increase authorisation and to execute code, were discovered in this interface. For example, an MMS with multimedia content received by a smartphone, or visiting a prepared website, can be used for an attack that is not noticed by the user.

New versions of Android, which generally close various security vulnerabilities, are often delivered to smartphones by the various device manufacturers with a delay lasting months. Some older devices are no longer supplied with any updates, meaning that security vulnerabilities remain open. According to an investigation performed by the Heise[12] online portal, both the update frequency and the update speed are very different. Google's own Nexus devices are supplied most quickly. However, there is an update delay of up to 10 months with other manufacturers. The device price also plays a role when it comes to supplying updates. Premium, expensive smartphones are generally updated more frequently than cheap devices.

2.1.8 App security

Introduction

For many people, smartphones and tablets have become the linchpin and pivotal point of their digital existence. Meanwhile, users are provided with millions of applications – apps –, with which they can organise and design their professional and personal day-to-day lives. Most apps, however, also record and exploit information about the user himself in the background. Preferences, location data, search history, and also personal data about health and the duration and intensity of training or heart rate are processed, with apps collaborating with the cloud to create comprehensive user profiles and possibly comparing and linking with additional data sources. The combined usage of many smartphones and tablets, both privately and commercially, also makes it more difficult for the user to have an overview and control over the data flows.

[11] http://blog.zimperium.com/experts-found-a-unicorn-in-the-last-heart-of-android/
[12] http://heise.de/-2237972

Current situation

- App stores operated by large companies such as Google, Apple and Microsoft serve a global audience. However, security and data protection mostly play a secondary role in the selection of apps. Competition is instead based on 'user experience': the combination of utility and convenience, as well as the costs of an app.

- Mobile operating and ecosystems[13] are equipped with different security mechanisms: Google's Android has different rights management than Apple's iOS. App developers are dependent on the company's ecosystems, and must also act in a very dynamic environment in which the products need to be constantly updated to new versions and end device types, while users constantly demand greater and more sophisticated functionality. App security and data protection are therefore often not given the consideration required; security features for an app may differ depending on the operating system.

- An app's security depends on how the app deals with sensitive information. Apps requiring rights that are unnecessary for actual use are not uncommon. It is very difficult for users to restrict the required rights manually and individually to be able to use the app. Users therefore frequently grant the app these rights, which are in fact not required to be able to use the app.

- Many apps integrate advertising networks to enable personalised advertising, either in the app itself or elsewhere. This extends the possible area of attack.

- The traditional PC virus scanner methods cannot be directly adopted due to the fact that apps are isolated from one another (sandboxing). Instead, basic rules and criteria for assessing app security are defined, and specialised companies subject apps to different test procedures. These are only partly automated and important parts of the investigation have to be performed manually; this has a negative impact on costs and the scalability of these tests.

- Since 2014, the BSI has had around 100 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. There was not a single app that came through the test without any findings. A large range of potential problems became clear in this process. While some apps only breach a few of the defined security criteria, others handle the data entrusted to them very carelessly. In the tests to date, integration into 'tracking networks' that cannot be switched off, the recording of geodata and the lack of appropriate data protection statements were found particularly frequently. In areas with high security requirements, it is necessary to review all apps used and to provide approval before use.

- Mobile Device Management (MDM) systems have developed further over recent months. In collaboration with manufacturers of mobile operating systems, solutions are now offered that make it possible to define basic rules with which mobile devices that are used commercially can be centrally managed and restricted. Within this, which apps may be installed can also be specified. Scenarios with combined private and commercial use are also addressed by MDM systems.

Assessment

For private use, users must often also weigh up aspects of an app's utility and convenience with the functions provided for data security and data protection. Most apps can only be used once all the required rights have been accepted, even if these have nothing to do with the actual function of the app. Here, app developers and app store operators are asked to give greater attention to security aspects and at least give the user the option of which rights he wishes to accept. For commercial use, initiatives are becoming apparent that integrate MDM systems more greatly with app tests. The market is still young: cross-system standards for tests as well as for the systematic recording of apps' security features, including regarding subjects such as mobile payment, home automation and mobile health management, still need to establish themselves.

A well-prepared integration of an MDM system, combined with constant monitoring and maintenance, can bring with it decisive advantages in the area of security of mobile devices.

[13] In this context, the close linking of devices, operating systems and service offers from a manufacturer is designated as an ecosystem.

It is, however, improbable that one individual solution for separating commercial and private use of mobile devices (Bring Your Own Device – BYOD) will become prevalent in the foreseeable future. Individual companies' approaches to problems are offered in a wide range of formats depending on need, in order to satisfy the complexity of the environment. Tension between the private and commercial use of devices therefore continues to pose the economy and authorities the challenge of adapting appropriate solutions specifically for the respective conditions. The BSI will continue to face this challenge over the next few years.

2015 danger

2.1.9 Industrial control system security

Introduction

Industrial control systems (ICS) are not only an elementary component of many critical infrastructures. Their availability and integrity is also essential for controlling the physical processes that take place in many other areas of use in factory automation and process control. This represents a significant challenge if the future vision of Industry 4.0 is actually to become reality with comprehensive networking, including across company boundaries. In contrast to the public perception, security risks and ICS are not due to the lack of security in individual components. Alongside suitable components, sufficiently secure factory automation or process control requires a machine and system that is designed and integrated in accordance with the security concept, as well as suitable measures in the operating phase, as part of security management. Therefore, alongside manufacturers of components as well as machine builders and integrators, the operators also face demands.

Current situation

- With the increasing use of components from standard IT in the industrial environment, production failures have often occurred in the past due to non-targeted malware. This collateral damage has included, for example, the infection of control components or operating terminals with general malware, and subsequent crashes. Within this, it was not individual computers but entire production locations that were affected in many cases. Cases of ransomware or spyware have also been seen in the industrial environment. In cases with ransomware, malware not only encrypted local data on the PC affected, but also data on accessible central file repositories. One reason for this is ICS systems which have not been supplied with updates, and therefore can include open weak points that have already been known for several years. Infection may come for example through office IT, which has not been sufficiently separated from the production network, through ICS components connected directly with the Internet, or through USB sticks (which, for example, are used for updates), and which contained malware.
- Targeted attacks mostly start through office IT or on engineering workstations, where infection comes via spear phishing or manipulated websites. Often, in the industrial environment, attackers are not sufficiently prevented from spreading through the company all the way into production networks.

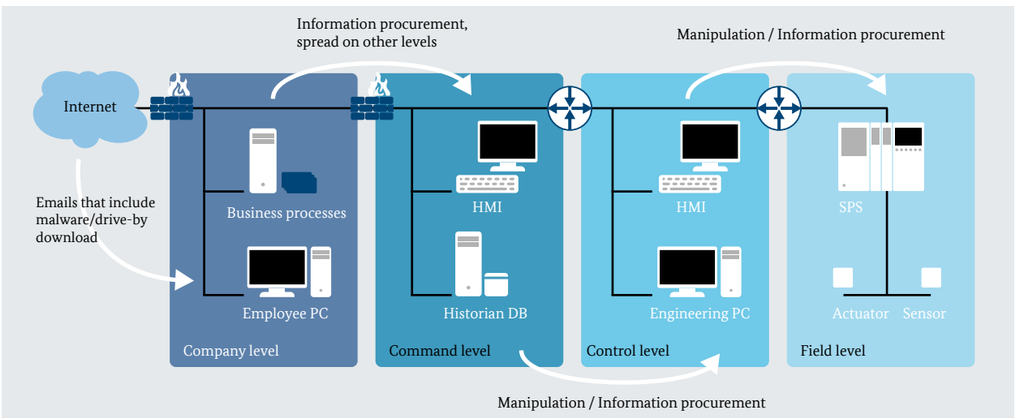

Figure 3: The process of multi-staged attacks on a typical ICS infrastructure

In this way, it is possible to steal critical data or manipulate production systems in such cases – i.e. access the company's crown jewels – with little effort. The causes are a lack of awareness of risks, lacking organisational processes and technical implementation that is insufficient from an IT security perspective. In particular, targeted attacks are still much less reported in the industrial environment than in classic IT. In such cases, the BSI assures a maximum level of confidentiality; for this reason, no attacks of this type in German companies have been specifically named at this juncture.

- There is also the question of the cyber-security components of functional security, which are intended to protect people and the environment in the event of the machine or system malfunctioning. It should be noted that these components additionally communicate via the general production networks and with operational control components. This means that attacks are possible, in which all protective functions could be bypassed.

Assessment

Increasing sensitivity for the subject of IT security can be seen in ICS in 2015. In individual companies this is resulting in substantial advances in IT security. This trend must be continued and significantly increased in order to be able to counter existing and new dangers a little. Both manufacturers of components and machine builders and integrators, as well as operators, have responsibility in this respect.

Manufacturers must understand security as an integral component and objective, and implement this by means of development guidelines or security-specific tests, among other measures. The prompt provision of information regarding weak points is particularly important.

Comparable requirements apply for machine builders and integrators, as the machine and system designed needs to be understood as a separate product, and its security must be implemented in an integrated way. A sufficient flow of information between manufacturers and operators is particularly important here.

Operators must see security as an ongoing process, and implement this in a security management system. This includes not only organisational processes, but also technical measures such as the segmentation of networks.

The tried and tested best practices in this area must urgently be implemented in the industrial environment. Functional security must also be taken into account in this process. As is the case today in conventional IT, the paradigm of 'assume the breach' must apply in the industrial environment, and be taken into account within integrated security management. A purely preventive approach at the gateway (perimeter) is therefore no longer productive. Instead, it is necessary to detect attackers in the distinct production environment, and react promptly.

2015 danger

US researchers hack all-terrain vehicles

In summer 2015, US computer experts used the Internet to wirelessly penetrate the infotainment system of an off-road vehicle via a vulnerability. Researchers were able to extend access from the infotainment system to the CAN bus system of the vehicle, thereby taking over control of the connected electronic control devices, including gas and brake control. Therefore, it was possible to encroach upon the vehicle's mechanical systems by manipulating the digital systems. In the test scenario, the driver lost control over the car while striving, and the would be attackers manoeuvred the all-terrain vehicle into a ditch. At the time of the attack, the attackers were at a distance of several kilometres from the vehicle. The infotainment system of the affected vehicle bundled numerous important functions, and is generally the interface to smartphones or tablets of the occupants, acting as a mobile Wi-Fi hotspot. Alongside this attack on vehicles technology, which in case of an emergency could have serious consequences for safety on the streets, there were also additional tests in which researchers were able to prove vulnerabilities in vehicles' on-board electronics. Among other examples, the locking system supplied by a German car manufacturer was made ineffective using mobile communications.

The tests provide an impressive account of the possibilities and gateways that attackers already find today in the area of vehicle technology, and which could have significant impact on security in road transport. Car manufacturers and suppliers must therefore protect digital components of a control device against unauthorised access or change, and to also take into account IT security within the production process. The digitisation of vehicles means that car manufacturers and traditional software producers will continue to be confronted with challenges in the areas of software development, responding to vulnerabilities and patch processes. In order to set up and operate vehicle technology that has maximum security, security standards will in future have to be developed in a way that is comparable with the protection profiles or technical guidelines tried and tested in other areas. Car manufacturers would therefore be able to provide an important proof of the security of their IT systems in vehicles.

2.2 Methods and means of attack

2.2.1 Malware

Introduction

Computer programs that execute unsolicited or damaging functions on an infected computer are designated as malicious software, malicious programs or malware. The clear classification of malware that was previously widely used is no longer possible today, as advanced malicious programs mostly consist of several components that have different functions, and additional modules with other functions can be downloaded where necessary. Email attachments and infection unnoticed by the user when visiting websites are two of the most frequent paths of infection.

Current situation

- The total number of malicious program versions for PCs is currently estimated to be over 439 million with an increase in the individual prevalence of malicious program versions that are always new, and automatically generated. It is primarily the Windows operating system that is affected due to its large market share.
- The number of versions of malware for mobile platforms is continuing to rise at great speed. Around 96% of malware affects the Android operating system due to its level of prevalence. Malicious programs are predominantly camouflaged as legitimate apps or updates on mobile computers; when these are installed, the user unwittingly causes infection. The greatest danger comes from software in app stores, which are not provided by the large operators such as Apple, Microsoft Google, and do not include any review of apps.
- 59% of the malicious Android apps detected by AV products up to September 2015 are Trojan Horses. In 2014, it was 51%. In contrast, the number of adware detections decreased from 26% to 10% in the same period.
- Ransomware spread more in 2015 than in 2014. This type of malicious program encrypts files or prevents access to the computer in order to extort ransom money, which is often to be paid in crypto-currencies such as Bitcoin. Newer versions such as 'Cryptowall 3.0' spread via drive-by exploits and exploit kits. In this process, advanced cryptographic procedures are used to encrypt documents on the infected computer. Backups performed before infection are often the only way to recreate the data.
- The high number of automatically generated malicious program versions means that the traditional, signature-based AV approach offers a decreasing level of protection because the new versions can be created more quickly than they can be analysed, or the duration of the malicious program distribution rounds (spam) is no longer sufficient to create/supply appropriate defence measures (AV signatures). This makes it more difficult to detect and defend against such malicious programs and results in a larger time window in which the user is unprotected. The analysis of malicious programs is often also made more difficult by detection of analysis tools and virtual machines, or due to delayed execution. In order to make the discovery of a malicious program's communication more difficult, compromised websites are increasingly being misused as control servers and means of distribution. In this process, the good reputation of a website that already exists is exploited in order to circumvent potential URL filters.
- In the 2015[14] cyber-security survey undertaken by the Alliance for Cyber-Security, malware infections following non-targeted attacks were also named as the type of attack that occurs most frequently.
- The distribution paths for malicious programs are varied: drive-by exploits, spam emails, links to malicious programs. Malware increasingly installs root certificates from separate certification offices, in order to execute men-in-the-middle attacks.
- The trend seen in 2014 of using macro viruses for Microsoft Office products is continuing. Here, malicious code is increasingly disguised in order to make its detection and analysis more difficult. It is suggested to the user that the intended document can only be displayed correctly if he enables the macro functions, thereby enabling the malicious program to run.

Assessment

Malicious programs are also one of the greatest threats both for private users and companies and authorities. Malicious programs have developed further compared with 2014, and the traditional defence measures are increasingly being circumvented. Attackers are focusing increasingly on mobile and alternative platforms.

[14] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/Umfrage/umfrage2015.html

Ransomware in hospitals

Circumstances: Criminals infect computers and encrypt data stored on them using the malicious Cryptowall (ransomware/cryptoware) software. The attackers then extort ransom money from the victim; when this ransom money is paid, the encryption is meant to be reversed. In April 2015, a system in a consortium of hospitals was affected by ransomware, which encrypted health data as well as medical reports and accounts.

The cause: Infection with malware is probably due to application software which did not have the current security updates.

Method: The precise attack vector has not been determined in this case. Infection with malware was probably due to a drive-by exploit on a website, after a link in an email was accessed.

The effect of the damage: After detection, it was possible to Install a backup; this meant that the data loss was limited to a period of twelve hours. However, it was not possible to exclude further financial damage as a possibility, as it was no longer possible to track financial accounts, and the re-creation of medical records and updating medical documentation generates additional expense.

Target groups: Cryptowall is malware that is used by cyber-criminals in a non-targeted way in order to extort money. As a result, all user groups could be affected by it. The fact that a company from the critical infrastructure sector of health was affected in this specific case shows that critical infrastructure companies are also susceptible to day-to-day attacks from cyber-criminals.

Technical abilities: Cyber-attacks with ransomware to exploit money are now day-to-day occurrences, and part of the typical range of attacks performed by cyber-criminals.

Malicious programs are often installed with the collaboration of the user, meaning that technical protective measures are circumvented and attackers are able to penetrate secured networks. Traditional AV solutions and firewalls are no longer sufficient for protection; instead, IT security must be seen and implemented as an overall concept, including the integration of the user.

2015 danger

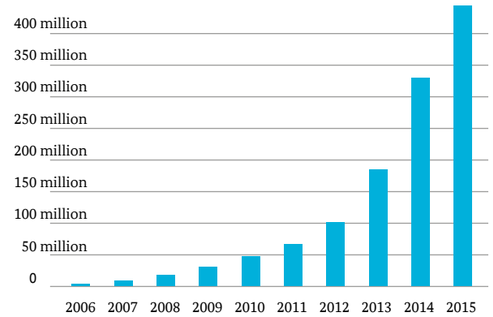

Figure 4: Number of known versions of malicious programs for Windows

2.2.2 Social Engineering

Introduction

'Human vulnerability' is targeted and exploited in social engineering. Attackers mislead their victims into circumventing protective mechanisms, or installing malicious programs unwittingly, in order to access data and information that is worthy of protection. To this end, perpetrators spy out the victim's personal environment, and use this knowledge about the victim to gain his trust. When doing so, they use human weaknesses such as trust, curiosity, respect for authority, a feeling of belonging or a willingness to help. The victims mostly act in ignorance, due to a situation of stress or out of politeness, and in this way become a tool for the attacker. Attacks through social engineering often have multiple stages, whereby the results of individual stages are used successively in the ongoing attack operations.

Figure 5: Apple ID Phishing website

Current situation

- Over one billion people are connected to each other on social networks. This large collection of data means that attackers have the opportunity to quickly and anonymously obtain the personal data of specific people for their attacks. The more personal information each user reveals, the easier it is for the attackers. They search social networks in a targeted way for people in a specific organisation, and use the information they have obtained to attack the company through these target persons.

- Phishing attacks happen almost every day; these are sent as mass emails, apparently from known and trustworthy organisations such as banks, phone companies or online shops. Users are misled into entering personal information such as access data, their account or credit card numbers or other customer data in fake websites by means of fictitious security problems, high invoice amounts or status messages regarding orders; this information is then transferred to the attackers.

- In the same way, users are misled into opening emails or accessing links in emails, which in both cases can result in the installation of a malicious program.

- In the event of targeted attacks, social engineering is used in the first phase of the attack. The attacker first collects information about his victim and uses this information to develop opportunities for attack:

  - He can guess the victim's password using profile data, if the password has been poorly selected (brute force attack)

  - Using information about the victim, he can build trust in order to gain confidential information (social hacking)

  - By sending a personalised email (spear phishing attack), he can install and execute a malicious program on the victim's computer.

- Since the beginning of 2015,there have been an increasing number of calls, apparently from Microsoft employees, who inform the victim about an alleged malicious program infection of the computer, or about problems with the Windows license. The callers offer to purge the affected peoples' systems, and mislead the victim into installing remote maintenance software through which malware can be downloaded, or sensitive data can be stolen.

- The 'fake President attack' is lucrative in the commercial environment. In this type of attack, an 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 flanked with authentic-looking emails from the supposed manager. Alternatively, phone numbers are shared by apparently 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. All fake president attacks have the common feature that the scammers have spied out many details about their victims in advance, meaning that – among other things – the company's style of communication can be authentically reproduced.

- In consideration of the risk that arises through social engineering, the protective measures are rather moderate: The 2015[15] cyber-security survey from the BSI states that only 50% of the companies asked regularly perform sensitisation measures. In many instances, there is a lack of awareness at all levels of the hierarchy.

Assessment

Social engineering is still a popular way of successfully conducting or supporting cyber-attacks. Even very high levels of technical safeguards can be circumvented by the 'human' vulnerability. It is easier for attackers to attack the weakest link – the person – instead of circumventing complex technical security measures with a great deal of effort. Training and sensitisation measures are therefore required on a regular basis to steel users against these methods of attack. The more security consciousness and digital training there is among users at all hierarchy levels, the more difficult it will be for attackers to exploit human vulnerabilities.

2015 danger

Social engineering by phone

Circumstances: As was the case in the previous year, there continued to be wave after wave of social engineering attacks in the current reporting period. Within these, criminals impersonated Microsoft support employees on the telephone and, by pretending that there were license problems or malware infections, tried to move those called to disclose personal data or make it possible for the caller to access their computer.

Method: The perpetrators call up and impersonate Microsoft support employees, who have found an apparent problem with the victim's operating system license or a malware infection, and wish to remedy this in collaboration with the customer. During the course of the conversation, the victims are convinced to install a piece of remote maintenance software so that the supposed support employee receives access to the system in order to directly resolve the alleged problem. With the aid of this software, the attacker has full access to the system and all data stored on it. In some cases, the customer's credit card details are also asked for on the phone, in order to pay for the support apparently provided.

The effect of the damage: Accessing the system and victim's data remotely makes it possible for the attackers to run malicious programs of their choice on the computer, or to directly search for information that could be used for criminal purposes. This type of attack represents a breach of privacy. If the attacker is successful in eliciting account or credit card details from the victim, the victim is then subject to direct financial damage due to withdrawals.

Target groups: The phone calls are primarily made on a random basis. Due to the very high prevalence of Windows operating systems and other Microsoft software, and the associated probability of success in reaching a Microsoft customer on the phone, attackers impersonate Microsoft employees. Private users are victims of these attempts at deception particularly often, as many people do not have awareness of this type of attack and often assume that there is an actual problem.

Technical abilities: No particular technical abilities are applied in this attack. Instead, the level of organisation of the perpetrators is much more important; they presumably have entire call centres set up for this type of social engineering.

[15] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/Umfrage/umfrage2015.html

2.2.3 Targeted attacks – APT

Introduction

In contrast to normal cyber-attacks, an Advanced Persistent Threat (APT) attack is mostly distinguished by the fact that the attacker has both a large quantity of time as well as means in the form of money, information and development capacities. An APT pursues long-term targets. The attackers use individually tailored attack vectors for infection and ensure that they have ongoing options for accessing the infected systems. A network being compromised is therefore not classified as an APT due to the use of complex malware. Instead, this type of assessment is mostly based on the attack vector used and the fact that the perpetrators establish themselves in the internal network and have spread to several systems, typically central servers.

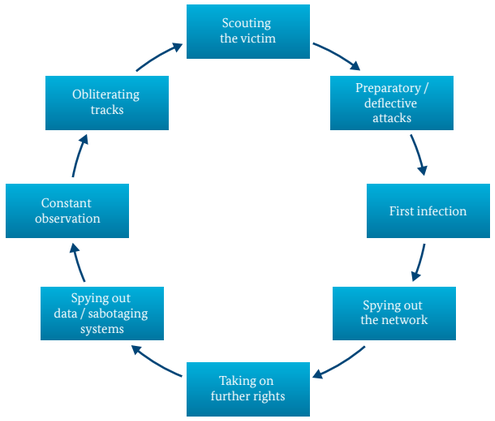

Figure 6: The procedure for an APT attack

Current situation

- Not many APT attacks become publicly known; there are hardly any valid numbers and statistics, and those that there are only provide a snippet of the overall situation. The estimated number of unknown cases is high, because most victims do not disclose that they have been attacked.
- In most cases, the period between infection with and the discovery of an APT attack is several months. This is a lot of time in which attackers move unhindered in the victim's network and are able to spy out information.

A cyber-attack on the German Bundestag

At the beginning of May 2015, the Federal Office for the Protection of the Constitution informed the German Bundestag and the BSI of indications that at least two computers from the German Bundestag network had been compromised. The BSI then contacted the German Bundestag, where anomalies had also already been found in the network. These abnormalities in the German Bundestag network indicated at this point that central systems in the internal Bundestag network had been compromised. Then, on behalf of the German Bundestag and together with an external service provider, the BSI tried to find out more detail about what had happened, in order to determine the extent of compromising.

It became apparent that the perpetrators had proceeded using the classic APT method, in which individual workplace computers are initially infected with a piece of malware. This first infection typically enables files to be uploaded and downloaded. It was not possible to precisely analyse the first infection in the log files due to the short storage period of a maximum of seven days. The perpetrators used this functionality to download additional tools into the infected system, including tools that are publicly available and used by many groups of perpetrators. The reloaded software was used, among other things, for ascertaining access data for a system account for software distribution, and using this to spread further in the internal network. The analysis showed that a malicious back-door program had been installed on individual systems, which enabled the attackers to access the system at any time. As well as this, additional attack tools and malicious programs such as Keylogger, which record keyboard input and create screenshots, were found, as well as self-written scripts for collecting documents of particular file types. Based on the analysis of the incident, it is to be assumed that the perpetrators had focused on selected email inboxes.

The attack corresponds with the classic APT template, which is used by almost all known groups of cyber-espionage groups. When spreading in the internal network ('lateral movement'), the attackers relied on traditional methods and publicly available tools, in ways that are also used by a small number of professional perpetrators. This may be due to the attackers trying to make it more difficult to correlate the attack. However, a few mistakes made by the attackers meant that their activities in the network could be followed and detected.

- As was the case in 2014, it was also true in 2015 that in particular the armament and high-tech (cars, shipping, space travel) industries, research institutions and public administration were the target of APT attacks.
- First infection continues to often be 'watering hole' attacks as well as sending emails with a prepared attached document and some additional text with good social engineering, meaning that the victim opens the malicious document. The email is often designed so that it almost impossible for the victim to detect that it is fake.
- The attackers mostly anchor themselves deep in the victim's system and use all conceivable technical options to make it very difficult for the victim to remove the attack from the network again. Alongside the spying activities already performed, in individual cases the attackers also switch over to misusing the acquired privileges to disrupt operation or for propaganda purposes. Cleaning up the network is associated with high personnel-related and financial costs for the victim.
- By combining what are for the most part inadequate protective measures – often no underlying IT security measures at all are put in place – and the significant persistence of the attackers, APT attacks often cause substantial damage. This includes not only costs to remove the attack tools and the required clean-up work, but also costs due to data that has been lost as well as potential commercial injury due to data leak.
- High-end attacks are no longer only performed by intelligence services, but increasing also by criminal organisations.
- Due to the increasing number of APT stakeholders and attacks, a market has now formed for the defence against and analysis of these attacks. Publications issued on this subject by service providers and security firms are always to be read with the awareness that such publications are also to do with positioning themselves in relation to the competition. However, publications regarding large APT campaigns should not be dismissed as hype as they document that these attacks are more widespread than generally accepted.

Dealing with an APT attack

APT attacks are targeted cyber-attacks on very localised systems and networks. The attackers generally have high levels of resources, both financially and in terms of personnel. APT attacks can be prevented, but this is very hard to achieve as they have been often been designed – with a high level of expense – in such a way that standard protective measures can be circumvented. A whole range of measures need to be implemented as quickly as possible in the event of an APT attack. These are not only used to limit the attacker's radius of action, but also must not alarm the attacker too early; this means that the attacker is not able to obliterate any tracks, which would make finding out more detail about what has happened more difficult or even impossible. The following basic steps must be adhered to:

1. Analysis: attack tools used, recognisable attack pattern, scope of attack
2. Control: keeping activities undertaken by the attacker under control, restricting the attacker's radius of action
3. Clean-up: cleaning up infected systems and networks, rebuilding if applicable
4. Hardening the system: using experience and lessons from the current APT attack to better partition the system and be able to defend better against future attacks.

Assessment

APT attacks are currently a high threat for companies and administrative bodies, and are likely to remain so. APT attacks for the purposes of industrial espionage or spying on competitors will continue to be carried out by various groups in the future. In particular, companies that are active and prominent internationally should incorporate APT attacks into their corporate risk management processes and implement IT security measures in the areas of detection and monitoring, as well as in relation to incident processing.

2015 danger

2.2.4 Spam

Introduction

Sent but unsolicited emails are generally designated as spam. This term can be subdivided into traditional spam, malicious program spam and phishing messages. Span is generally sent either via compromised servers, infected client systems or with the aid of access data that has been spied out, via legitimate email accounts. Often, the systems sending the spam are connected to a botnet, making it possible 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 want 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 refers to the malware or a page with drive-by exploits.

Current situation

Following an increase in 2014, spam activity decreased to approximately 30% of the volume of the previous year in 2015 (Figure 7). This decline was mainly in the area of traditional spam. To date, the most popular topics in 2015 have been dating agencies, medications and dubious job offers.

- The number of spam messages with malware in the attachment decreased to around 75% of the previous year's level.

- The proportion of malware spam, for which current email addresses collected on other infected systems were used, increased. Often, pieces of malware from the Geodo family were responsible for this.

- In spam messages, recipients are often addressed with their correct name, increasing the probability that the malicious contents will be clicked.

- Office documents sent since the middle of 2014, which include macros for downloading malware automatically, continue to occur and have been further developed by the perpetrators. To do so, they increasingly disguise and vary the macro code. In some instances, pieces of malware were coded and embedded into the document as invisible text, meaning that it was not necessary to perform any additional downloads. In individual instances, embedded download scripts were also worked with, which are executed when the victim double-clicks in the document.

- Instead of a malicious attachment, attackers often send a link to download the malware. This is disguised as a link to invoices, warnings, package shipment notices or similar in the relevant email cover note. Criminals imitate email templates used by renowned and well-known companies to this end. In a few instances, the links are sent in attached documents, presumably with the objective of making detection more difficult.

- The volume of malware sent differs greatly depending on the time (Figure 8). Compared to last year, incidents of malware being sent on Thursdays and Fridays increased, and overall the focus shifted slightly to the morning hours. This time-based control is probably effected by the attackers with the intention of as many spam messages as possible being opened directly during normal working hours.

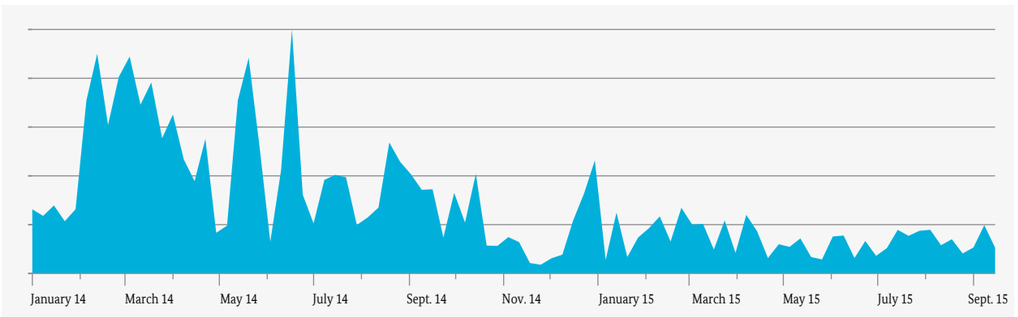

Figure 7: Spam overview per week in Germany since January 1, 2014

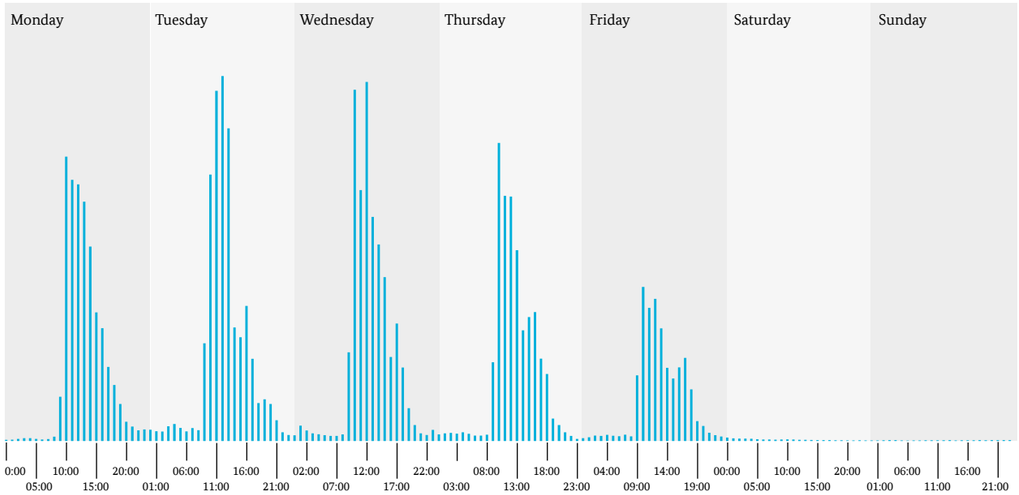

Figure 8: Distribution of malware being sent on weekdays since the start of 2015

Assessment

The spam emails distributed increasingly professionally by attackers – in accordance with templates used by well-known companies and with relevant subjects – are misleading more and more users to execute malware from spam messages. Advanced deception techniques, 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.

Today, traditional spam has hardly any impact on the availability of email systems. Malware spam continues to be the main source of infections. In terms of countermeasures, above all the user is asked to treat emails with healthy distrust when they come from unknown senders, or if anything seems not to be right. One good technical countermeasure is 'whitelisting' directories from which executable files can be started.

2015 danger

2.2.5 Botnets

Introduction

A botnet is a collection of systems that have been attacked by a remotely controllable malware program. This may be computer systems, but also mobile devices such as smartphones or tablet computers. Due to their high level of availability and broadband connection, webservers are also increasingly being compromised or targeted and hired via cloud services. Botnets consisting of internet routers indicate that any internet-enabled system can become part of a botnet.

All attacked systems in a specific version of a malicious program are controlled by one or several overriding units, which are controlled by the botnet operator. In many cases, this takes the form of servers, which are also referred to as command and control servers (C&C Servers).

Current situation

- In the reporting period, two botnets were switched off, which were also active in Germany. The Dropperbot botnet consisted of around 11,000 bots and was deactivated in December 2014; the Ramnit botnet with approximately 3.2 million infections worldwide was deactivated in February 2015. Affected users were informed by the internet provider and the BSI.
- In the first half of 2015, up to 60,000 infections were registered by security researchers every day, and reported to the German internet suppliers via the BSI. They then inform their customers, and some also offer support in clean-up processes.
- Due to the high market share, it is predominantly Windows systems that are affected by bot infections. But cyber-criminals are increasingly focusing on Mac OS X and Android devices. The trend of misusing compromised webservers to operate C&C servers continues to persist.
- It is to be assumed that several hundred C&C Servers are active in Germany per day, on average. Due to countermeasures taken by the operators, there is significant fluctuation in the systems.

Assessment

Botnets are used by criminals on a massive scale, to steal information, commit online banking fraud, attack the availability of computer systems and send spam. Current malicious programs can be used flexibly due to their download functionality. Botnet infrastructures offer cyber-criminals access to large-scale resources in terms of computer capacity and bandwidth, which they can use for their criminal actions. Due to the professionalisation and criminalisation of cyber-crime, operating a botnet is also comparatively easy and cheap for technical laypeople. The current level of threat due to botnets continues to be critical in comparison with the previous year, and the trend is rising. This results not only from the high number of vulnerable internet systems, which can be used as potential bots, but also from the low barriers to entry for cyber-criminals.

2015 danger ↑

2.2.6 Distributed Denial of Service (DDoS) attacks

Introduction

Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks are mainly performed by attackers whose motivation is in the area of extortion, but hacktivism is also a factor here. Attacks on the availability of services or systems can cause victims immediate damage, such as due to business-critical processes no longer functioning or it no longer being possible to offer services. DDoS attacks or a threat in this respect can also move the victim to react to specific demands made by attackers.

Reflection attacks are a common type of attack. In these attacks, publicly accessible servers (e.g. NTP servers) are misused to strengthen an attack. This makes operators of this type of server co-perpetrators. An effect comparable with that of an attack via a traditional botnet can be achieved with this type of attack.

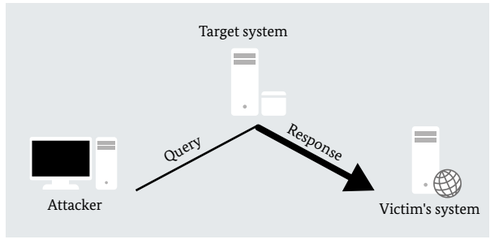

Figure 9: Illustration of a reflection attack

Current situation

- It happens time and time again that websites cannot be reached due to DDoS attacks. Websites within the Federal Government are also occasionally targeted by attackers.
- In the first half of 2015, 29,437 attacks were registered in Germany. In the first half of 2014, it was 25,113 attacks. This corresponds to an increase of around 17%. At the same time, the average attack bandwidth in Germany has increased from 1,315 to 1,435 Gbps, and the average packet rate for attacks increased from 469,889 to 665,691 Kpps (42%). This increase is due to the greatly increased average packet rate in the second quarter of 2015. Here, it was around 919 Kpps – in comparison to around 486 Kpps in the first quarter of 2015.
- The reflection attacks via NTP observed in 2013 and at the start of 2014 have decreased proportionately during 2014, while reflection attacks via SSDP (Simple Service Discovery Protocol) have increased. Taken as a whole, the proportion of reflection attacks in the overall number of DDoS attacks has increased. Significantly fewer systems are needed to achieve a comparable result for this type of attack than for an attack using a traditional botnet.

Assessment

- Although Germany is not a particularly noticeable source or target of attacks. the greatly increased average packet rates for attacks in the second quarter of 2015 is noticeable. The average packet rate has therefore again reached a level comparable with 2013, after a 'quiet' 2014. Upstream components such as load balancers or firewalls can become bottlenecks in attacks with high packet rates.
- Germany is still in the top 10 of countries with the highest numbers of open NTP servers. Because the number of open NTP servers in Germany is declining, attackers will switch to other protocols, such as SSDP, meaning that the overall situation will remain predominantly unchanged.

2015 danger →

! DDoS attacks on Federal Government and the German Bundestag websites

Circumstances: On Wednesday, January 7, 2015, the www.bundeskanzlerin.de, www.bundesregierung.de and www.bundestag.de websites could no longer be accessed from around 10am. The outage was initially noticed in the Situation Centre of the BSI. The Federal Foreign Office website, www.auswaertiges-amt.de, was also temporarily unavailable from around 2pm.

The cause: The triggering incident was a DDoS attack that the politically-motivated 'CyberBerkut' group stated they had initiated. In a claim of responsibility, the group stated that the reason for the attack was a visit that the Ukrainian Prime Minister Arseni Jazenjuk made to Germany at that time. Whether the group was actually responsible for the attack is not known.

Method: The attack was made up of different types of DDoS attacks, varied by the attacker. The types included TCP SYN flood, UDP reflection and attacks on web application level, with a significant bandwidth that overloaded the internet connection. Thousands of botnet clients all over the world were temporarily involved in the attack.

The effect of the damage: The availability of the www.bundeskanzlerin.de website was temporarily recreated using filter rules and the connection to a dedicated internet service. As it progressed, the attack extended to German Bundestag website, www.bundestag.de, and from around 6pm the www.bundesregierung.de website was also restricted. The DDoS attack continued overnight, but the initiated countermeasures meant that there were no effects that were visible externally. The DDoS attack continued well into the next day. Other websites owned by the Federal Government were not affected by the attack.

Target groups: The claimed authorship of the attack, as well as the time correlation with political discussions in Berlin, support this DDoS attack being explicitly aimed at the Federal Government.

Technical abilities: In contrast with other, regularly occurring DDoS attacks with low impact, the attackers showed advanced technical abilities in this instance. In particular, this included an immediate response to the countermeasures initiated. As soon as an attack vector was closed by a filter, the attackers switched to a new vector.

2.2.7 Drive-by exploits and exploit kits

Introduction

Drive-by exploits are an insidious means of attack, as they function without the internet user's co-operation. Accessing a correspondingly prepared website is sufficient to enable the exploitation of vulnerabilities in web browsers, browser plug-ins or in the operating system, and install malicious programs. Drive-by exploits are used individually or cumulatively in 'exploit kits'. They are generally distributed using manipulated advertising banners or compromised web servers. Drive-by exploits or exploit kits, which are integrated into a popular website that get lots of hits, can infect a large number of vulnerable systems with malware in a very short space of time. While exploit kits are primarily used in broad, non-targeted attacks, individual drive-by exploits are used both in targeted campaigns and also in non-targeted attacks.

Current situation

- Drive-by exploits and exploit kits are currently used not only on dubious websites, but often also on unsuspicious, legitimate websites. Google[16] website indexing analysis shows that between one and two percent of all websites in Germany will execute or point to drive-by attacks in 2015. In July 2015, an attack campaign performed using an exploit kit and affecting approximately 5,000 websites in Germany alone was successfully stopped.
- Malicious ad banners are a key source of infection, as the ad banners are provided by third parties and are integrated into many pages. Integrating manipulated ad banners is sufficient for starting an attack. Both large and small ad networks were the starting point for attacks via ad banners in 2015.
- 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. In 2015, this method was used by compromising a website belonging to the President of Myanmar, in order to attack organisations with political or commercial relationships with Myanmar[17].
- Furthermore, targeted attacks by means of drive-by exploit are undertaken in emails, tailored to the recipient and his area of activity or interest, that contain links to prepared websites. A group or perpetrators used this method of link distribution by email in June 2015 against companies in several industries such as air and space travel, the armament industry and telecommunications and logistics[18].
- Since the beginning of 2015, the new vulnerabilities shown in Figure 10 have been used first time in drive-by attacks, or integrated in exploit kits. The attack targets were mainly new vulnerabilities in Adobe Flash Player.

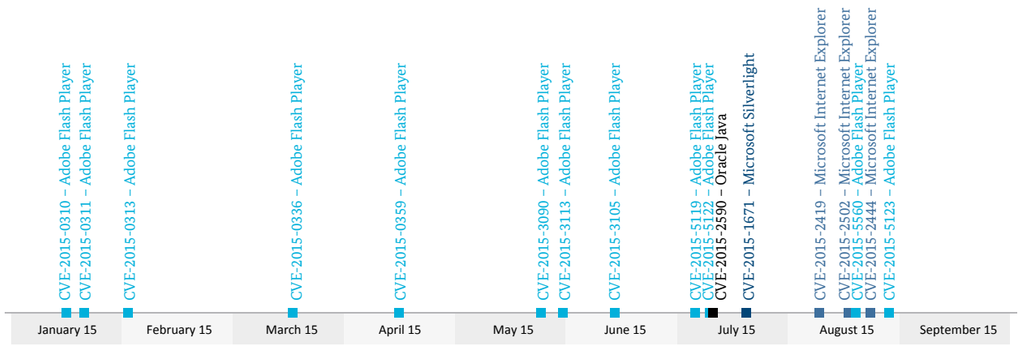

Figure 10: Exploitation of new vulnerabilities in drive-by attacks and exploit kits in 2015

[16] https://www.google.com/transparencyreport/safebrowsing/malware/?hl=de
[17] http://researchcenter.paloaltonetworks.com/2015/06/evilgrab-delivered-by-watering-hole-attack-on-president-of-myanmars-website
[18] https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html

- The situation with respect to exploit kits has changed in comparison to 2014: the main attack target for 2015 is Adobe Flash Player. In the first half of 2015 alone, eight new exploits targeted at vulnerabilities were integrated in Adobe Flash Player in exploit kits, or used in one instance by an individual drive-by exploit. Five of these exploits were 0-day vulnerabilities, which were actively used for attacks before the provision of a security update by the manufacturer. Some of the other exploits were also integrated in exploit kits a few days after the security update was provided.
- The malware installed after an attack varies and can be adapted at any time. In non-targeted attack campaigns, victims are infected – among other things – with different ransomware versions such as CryptoWall 3.0 or TeslaCrypt/AlphaCrypt, malware for click fraud such as Kovter or Bedep, and generic droppers such as Pony Loader.

Assessment

In comparison to the previous year, the level of threat has worsened due to drive-by exploits and, above all, exploit kits: new vulnerabilities such as 0-day vulnerabilities are integrated in exploit kits regularly and within a very short period of time. The current situation shows that investments are being made in new exploits and the search for unknown vulnerabilities, to exploit the potential of drive-by exploit attacks. Alongside the immediate installation of security updates, the at least temporary deactivation of affected programs or plugins may be necessary to protect against these attacks.

2015 danger

Thousands of websites direct users to an exploit kit

Circumstances: In July 2015, an attack campaign affecting around 5,000 websites in Germany alone was stopped using the 'Angler' exploit kit, by means of collaboration between the international CERT Community.

Method: More than 150,000 websites worldwide were compromised for the attack. It was mainly websites that use the content management system WordPress that were affected. The attackers manipulated the sites such that visitors to the websites were redirected to the exploit kit in the background. The exploit kit then tried, using different exploits, to take advantage of vulnerabilities on the website visitor's PC to install malware.

The effect of the damage: Around 5,000 websites were compromised in Germany alone. 68 million page impressions from four million IP addresses worldwide were redirected to the exploit kit. Just five percent of the page impressions came from Germany. After a successful attack, the victims' systems were infected with the Cryptoware ransomware in order to extort money. The proportion of attacks that are actually successful and therefore also the number of associated malware infections is unknown. As exploit kits have increasingly been exploiting zero-day vulnerabilities or vulnerabilities immediately following the publication of a security update in Adobe Flash Player since the beginning of 2015, it should be assumed that a high number of attacks have been successful.

Target groups: Attacks using exploit kits are non-targeted. Those affected are often private users, but also companies whose systems do not have the most recent security updates.

Technical abilities: No particular technical abilities were applied in this attack. In fact, attacks using exploit kits and a criminal background are now an everyday occurrence. The mass of websites compromised in advance and the high number of redirected users show the potential of this type of attack.

2.2.8 Identity theft

Introduction

The identity of a natural person is defined by a high number of different features, for example his name, date of birth, address, social insurance number or tax number. In the context of the internet, the identity is restricted in many cases to identification and authentication data, mostly to the combination of username and password, bank or credit card information and email addresses. The term 'identity theft' has come into common usage for if an unauthorised party gains access to data of this type. Identity theft is conducted chiefly using social engineering, by installing malware on end devices or by removing data after attacks on websites. For the most part, the attacker has no interest in taking on the real identity of the natural person, instead using this data to his own advantage, for example for achieving profits. If an attacker uses stolen digital identities, this is referred to as identity fraud. This is generally performed on a collaborative basis: while digital identities are stolen by one criminal, another misuses those identities for his criminal purposes. In the meantime, there is active online trade in digital identities.

Current situation

- At any given time, the BSI is aware of around 100,000 infections in Germany with an identity theft function. These are from several families of malware. It is to be assumed that the total number of infections by these malware families is much higher again, because it is likely that only a fraction of infections is detected with the measuring method used.

- Beyond the malware families recorded in the count above, there is also a far greater number of malicious programs with a theft identity function: from December 2014 to September 2015, the BSI analysed around 168,000 new pieces of malware that bear reference to identity theft in Germany.

- In the course of the year, only one breach of servers used to steal usernames and passwords was publicly announced in Germany. On an international level, no noteworthy password thefts from servers became publicly known in 2015. It is however to be assumed that there is a high number of unknown cases here, because an affected operator generally has no interest in a successful attack becoming known to the public. In addition, in some instances, an attack may not be noticed by the operator. Just one individual successful attack can affect millions: we already know, from the distant past, that significantly more identities are stolen from servers than from end devices.

- It is not only usernames and passwords that can be used for the abuse of digital identities, but stolen personal data too. In the reporting period, outstanding examples of this type of attack include a cyber-attack on the US Government personnel data management, in which the personal data of around 21.5 million Government officials and applicants[19] was taken, as well as an attack on the US tax authority, in which stolen taxpayer data was used to obtain 39 million US Dollars (state of investigations: July 2015)[20].

- As there is a high number of unknown cases of theft, the damage caused by identity fraud cannot be reliably determined.

Assessment

Attackers can make a direct financial profit by selling stolen identities. As the installation of malware on the other hand is accomplished with relatively little effort and cost, the profit margins can be high. It is therefore to be assumed that any identity data theft of any type will remain at the currently high level.

2015 danger ↑

[19] https://www.opm.gov/cybersecurity
[20] http://www.irs.gov/uac/Written-Testimony-of-Commissioner-Koskinen-on-Unauthorized-Attempts-to-Access-Taxpayer-Data-before-Senate-Finance-Committee

2.3 Cyber-attacks: Motivation and goals

Intelligence services, cyber-criminals and hacktivists have considerable influence on technical cyber-security. Their motives differ greatly and their intentions may be related to geostrategy, political ideology, religious ideology, intelligence services, or economic or destructive goals.

2.3.1 Intelligence-related cyber-attacks:

Many states have now recognised the potential of cyber-attacks. Germany is constantly exposed to cyber-attacks, the intention of which is to gain informational and financial advantages. The constantly improving sensor technology of the BSI in Government networks, sharing of knowledge in the cyber-defence centre with other authorities, and additional publications from the Edward Snowden document stock and through Wikileaks mean that the number of specific detections, technical findings and the general knowledge of the BSI about intelligence-related cyber-attacks as well as cyber-attack methods have again been extended since the last annual report in December 2014.

In the 2014/2015 period, chiefly the attacks with the designation 'APT28'[21] and the spyware Regin[22] should be named among the internationally detected cyber-attacks that prompt suspicion of an intelligence background. With upgraded detection options in the Federal Government as defined by Section 5 of the IT Security Act (IT-SiG), as well as through the future message rates from critical-infrastructure companies as defined by Section 8b IT-SiG, the BSI will again expand its capabilities over the next two years, enabling it to make an improved statement on current cyber-security, including in relation to intelligence attacks in German cyber-space.

The analysis of the new BSI findings named above regarding intelligence attacks confirms and deepens the statements made in the annual report from 2014 regarding the four main attack vectors used by intelligence services:

1st attack vector: gaining strategic information All data accruing at internet and communication nodes can be tapped, stored and analysed. In particular, the (movement) data of any internet user is affected. Unencrypted data can be listened in on or additionally read. All of these processes generally happen automatically and are able to process very large quantities of data.

2nd attack vector: individual attacks in the communication- and cyber-space These attacks are targeted at IT systems belonging to interesting persons and institutions. IT systems identified during the strategic gathering of data are attacked and controlled with specifically adapted cyber-attacks using technical as well as social information about the user, which is collected in advance. If for example the target person uses mobile IT in 'always on' mode, the place that the device owner is staying can be constantly tracked using the location data determined by the IT system.

3rd attack vector: influencing standards and implementations In this process, IT standards, and above all cryptographic standards, are manipulated in advance of technical information gathering. The implementations of inherently stronger security mechanisms and the associated confidentiality are systematically weakened in this way, and therefore no longer offer sufficient protection of confidentiality.

4th attack vector: targeted manipulation of IT equipment In this process, the order, delivery or service chains are encroached upon in order to undertake manipulations. This includes for example inserting back-doors or weakening technical security features, which can then be exploited again within the strategic gathering of information detailed above, or in individual attacks.

As is the case with APT attacks in general, intelligence cyber-attacks are the cyber-attacks that are the most difficult to assign to one attacker. Precisely these attacks use perfect methods of concealment to disguise both the attack paths (and therefore the author) and the attack in the relevant IT system itself. Given the fast-paced trend toward increasingly high-end methods of attack, the BSI believes that collaborating with other authorities and IT forensics companies to further develop its technical methods of analysis is a key responsibility over the next few years in the qualified detection and assignment of cyber-attacks. All of the options detailed for compromising ICT systems for the purpose of technical or cyber-espionage can also be used in the same or a similar way to commit cyber-sabotage.

[21] https://www2.fireeye.com/apt28.html
[22] http://www.symantec.com/connect/blogs/regin-top-tier-espionage- tool-enables-stealthy-surveillance

This is particularly true for the information and communication technology used in critical infrastructures, as proven specifically by the cyber-attack on the French television broadcaster TV5MONDE – an attack that is also assigned to type APT28.

2.3.2 Cyber-crime

One side-effect of the publications issued by Edward Snowden is the information – some of which is very detailed – about attack targets, paths, tools and methods, which could lead to a proliferation, i.e. further spread, of this knowledge and the associated blue phase for new attackers, including on the cyber-crime scene. The methods used by cyber-criminals are based both on technical progress and existing defence measures. In this process, the attackers use the entire bandwidth of technical options: for private users, this is spam and phishing emails, malware used for identity theft or manipulating online banking, and the use of ransomware. Companies face different forms of extortion, server hacking or malware for till systems (point of sale, POS).

Those who took part in the 2015 cyber-security survey[23] conducted by the Alliance for Cyber-Security also specified organised crime and economic crime as the attacker group with the highest threat potential over the coming years.

The existing market on which the vulnerabilities, attack methods and performance of cyber-attacks are offered makes the risk level in the situation more complex. Organisations also offer their capabilities and services to other interested circles in the form of contract work ('cyber-crime as a service'). This means that high-end attacks are also available for organisations and states which to date have not been able to build up this expertise themselves, or which are in principle not able to do so due to a lack of capabilities.

An attack on the Hacking Team company

In July 2015, a high number of internal documents belonging to the Italian company Hacking Team were published following a cyber-attack. The company itself states that it sells attack tools and monitoring technology to law enforcement agencies and Government institutions worldwide. The publications resulted in several previously unknown vulnerabilities in widely-used applications being discovered, which the company had bought in or developed itself. With the publication of the vulnerabilities withheld from the manufacturers, the threat to affected users increased as the vulnerabilities were taken on and exploited in distinct attack campaigns shortly after publication, both by APT groups and cyber-criminals.

The publications prove that, today, there is an active and financially lucrative market for cyber-attack resources and vulnerabilities. The incident also illustrates that the capabilities for developing exploits and malware, and therefore for conducting cyber-espionage, are not restricted to intelligence services. This market increases the current level of threat, as the capabilities of Hacking Team or comparable companies could also be bought in and respectively used by market competitors or intelligence services, who themselves do not have sufficient IT expertise.

[23] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/Umfrage/umfrage2015.html

3 Current exposure: Federal Government

3 Current exposure: Federal Government

Since 2010, the BSI Situation Centre has been the central reporting point for IT security incidents in the Federal Government. Findings from the protection of Government networks also come together in the BSI Situation Centre. This means that, as well as responding immediately to an incident, the BSI can also deduce trends and developments regarding the current threat for information technology and the Federal Government's networks, and promptly undertake measures as appropriate.

3.1 Defending against attacks on Government networks

The Federal Government's networks have again been constantly exposed to cyber-attacks in 2015. These include both non-targeted mass attacks and targeted attack campaigns. A multi-level security model is used to prevent IT systems and networks from being compromised, and to detect such compromising quickly. Adapted security measures are effective at different interfaces, as well as traditional virus protection programs.

With regard to defending against unsolicited emails: an average of approximately 11,000 infected emails were intercepted in Government networks per month in real time in the first half of 2015, before they reached the recipients' inboxes. Commercial virus protection programs were used to this end, and supplemented with separate signatures, which for example took into account the specific day's current level of spam. The number of detections fluctuates depending on the level of spam and the efficacy of pre-filtering (recipient check/greylisting). An average of 15 attacks per day on Government networks were also discovered, which could not have been detected with normal protective measures. On average, there was a targeted attack with an intelligence service background every two days.

Another protective component blocks outgoing network connections on infected websites that distribute malware, or 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 commercial IT security products used have not taken effect. To date in 2015, around 5,000 attempts to connect to malicious code servers have been blocked per day with this method. By September 2015, active pieces of malware that have circumvented commercial protection systems have already been found 152 times.

Tiered protective measures in Government networks against email-based attacks

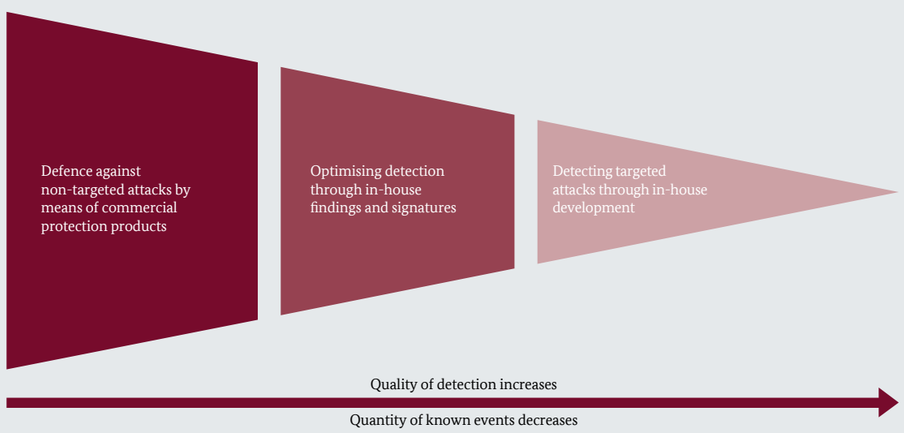

Figure 11: Tiered protective measures in Government networks against email-based attacks

The largest proportion was made up of campaigns that sent the banking Trojan Feodo in fake invoice attachments. No vulnerabilities are exploited in this process; instead, the recipient is deceived into independently executing the malware by opening the attachment, which installs it.

3.2 Notifications from the Federal Administration

As stated by Section 4 BSI Law (Law 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.

By September 2015, more than 2,300 malware infections had been detected in the Federal Government by commercial protection products. The number of malicious programs successfully defended against was just 500,000 in the same period.

On average, the BSI records a denial of service (DoS) attack on individual Federal Authority websites three to four times per month. The number of attacks in which the authority affected in each case asks the BSI for immediate support has increased from two in 2013 to 16 in the period from January to September 2015.

Information security in authorities

IT security checks such as audits, IT penetration tests or web checks are part of the BSI's advisory mandate and are conducted at the request of an authority. In tests, the BSI monitors regularly underlying security defects such as out-of-date patch statuses for operating systems and applications, as well as deactivated security mechanisms, a lack of network monitoring and network access controls, or insufficient or non-obligatory log data analysis. The lack of interface control and the use of unencrypted mobile devices still represent challenges for those responsible for IT security. There are substantial risks associated with insufficient training and sensitisation measures, incomplete and inconsistent security concepts, and a lack of clarity regarding responsibilities for information security. The BSI believes that information security within authorities can be significantly improved if the staff in IT security teams constantly engage with IT risks and the increasing complexity of applications. This includes appropriate set-up in terms of personnel, technology and organisation, in order to be able to overcome extensive and changing responsibilities.

4 Protection of critical infrastructures: IT security for public welfare

Power, water, finances and food: the failure or restriction of critical supply services would have dramatic consequences for Germany's economy, state and society. Operational responsibility for critical infrastructures is held by the respective operators; for the most part, these are commercial companies. Due to its importance for the entire community, the state has also – within its public services – taken on a duty of care with respect to its citizens and therefore a guarantee responsibility for critical infrastructures. A special responsibility therefore falls upon the state and operators of critical infrastructure to protect systems against failure and restrictions. The state and critical infrastructure operators have already been working together successfully for some years to protect critical infrastructures. The UP KRITIS public-private cooperation, which was set up in 2007, forms the framework for this collaboration. Since its founding, UP KRITIS has grown constantly and has developed and implemented many measures for protecting critical infrastructures. It has however become clear that, in IT security, the purely voluntary approach of UP KRITIS is not sufficient to achieve an appropriate level of IT security in all critical infrastructure sectors.

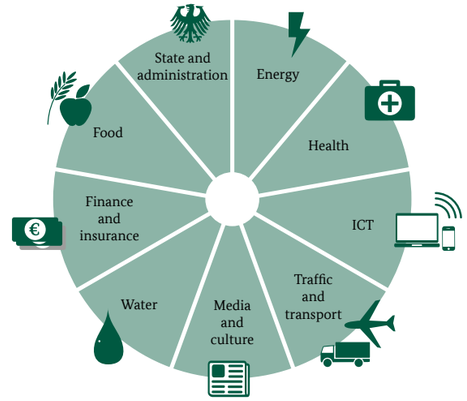

Figure 12: Critical infrastructure sectors in Germany

Targeted attacks on the infrastructure of financial institutions

Circumstances: In 2014, targeted cyber-attacks were performed on the internal networks of various Eastern European banks under the name Carbanak/Anunak. This became publicly known by means of a publication issued by the Kaspersky Labs company[24] in February 2015.

Method: The first infection of bank employee's computers is suspected to have been via spear-phishing emails. By running file attachments, the systems were infected with Carbanak malware, a piece of malicious software based on the banking Trojan Caberp. After infection, the spear phishing emails were sent to additional recipients from the victim's address book. In some instances, the attackers deceived their victims into accessing compromised websites and infected their computers using drive-by exploits.

The effect of the damage: Through the infected systems, the attackers received access to the SWIFT payment system, bank customers' accounts, and the control systems for cash machines. As a result, cash transactions were initiated and cash payouts from cash machines were triggered. The banks' fraud detection systems did not detect the manipulation as they are not aligned to discover fraud committed by the end user. Overall, the networks of hundreds of victims, including over 50 Russian banks, were successfully attacked, and two Russian banks had their license revoked as a result. The total damage is estimated at around two million US dollars per incident. Following these estimates, Carbanak/Anunak may have caused damage of 500 million to one billion US dollars worldwide.

Target groups: Financial institutes in Eastern Europe, in particular former Soviet Union countries. Despite reports to the contrary and a large-scale search for known indicators of an incident, no specific cases are known in Western Europe and the US.

Technical abilities: The effort involved for planning and researching an attack of this type in an environment characterised by specialist systems is high. Targeted compromising of target systems in the network also indicate strong technical capabilities which, before that point, were instead associated with intelligence services. The group's ability to adapt – illustrated on the attack path from customer systems into internal bank transaction systems and other payment systems – indicates a high level of organisation and a professional cost-benefit reckoning.

[24] https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/

4.1 Critical infrastructures depend on functioning IT

Advancing digitisation and networking also affect the critical infrastructures sector. The provision of critical services therefore increasingly depends on the information and communication technology (ICT) used functioning correctly. A failure or restriction of ICT components in the operator's critical processes may under some circumstances result in a restriction of service provisions and, in a worst-case scenario, to a complete interruption of supply. Dependencies between individual sectors or industries increase the risk of failures even further. Failures in one sector may lead to failures in other sectors, triggering a domino effect.

- Availabilities of transport, storage or transaction capacities impact logistics chains and therefore also the availability of goods or bought-in parts in trade and industry.
- Restrictions in telecommunication impact the complex communication and coordination processes of many companies and critical infrastructures.
- Power supply failure would substantially impact all commercial and social sectors.

Many industries are aware of these dependencies among critical infrastructures and are well positioned. Redundancies are often kept available for supply bottlenecks, mitigation plans are created or, if the worst comes to the worst, substitutes are used. This means that restrictions are often within the bounds of what is manageable. Nevertheless, every IT security incident reduces the available safety margin for a certain period of time. Knowledge obtainable from those affected about IT security incidents is an important building block in evaluating the current level of IT security in critical infrastructures. Early warnings and trend predictions are important instruments in being able to increase the available safety margin in the short-term for an expected attack.

4.2 The IT Security Act

To date, not all critical infrastructure sectors have engaged equally with UP KRITIS. At the same time, the level of IT security among critical infrastructure operators is very inconsistent. Some operators are very well positioned in terms of their IT security, and are making substantial investments in the efficacy of the measures they employ. For other operators, there is still need for improvement in this area. Considering critical infrastructure operators' particular responsibility for public welfare, and the far-reaching societal consequences that a failure or restriction of critical infrastructures could have, the 'Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme' ('Law for Increasing the Security of Information Technology Systems', 'IT Security Act') came into effect in July 2015. Work is currently under way on a regulation with which, among other aspects, the critical infrastructure operators that are subject to the law will be specifically identified.

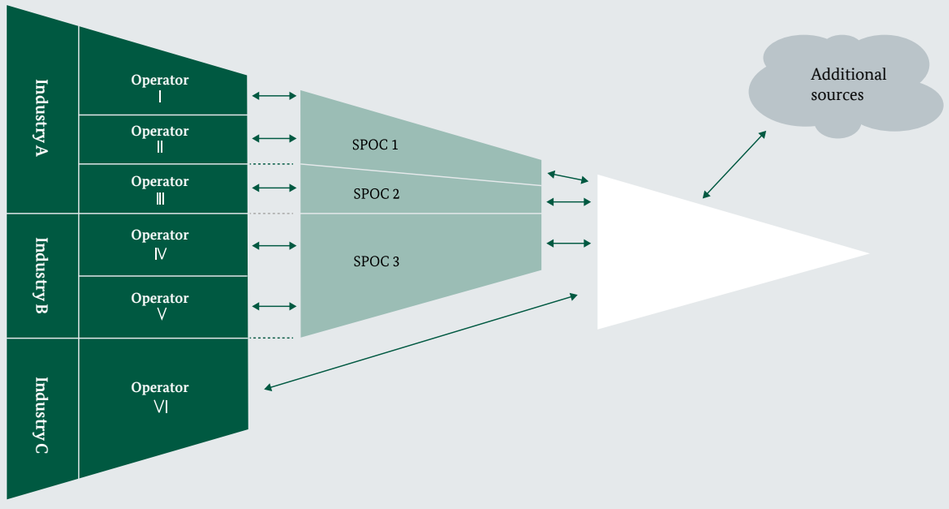

Figure 13: The communication structure in UP KRITIS

The goal of the act is, among other aspects, to increase companies' security, and in particular that of operators of critical infrastructures. Critical infrastructure operators are required to adhere to a minimum level of IT security as well as to report any IT security incidents to the BSI. The BSI analyses the reported information and uses it to create an overview of the current situation on an ongoing basis; this overview is made available to critical infrastructure operators as well as the relevant authorities. This means that operators regain information and expertise and are able to benefit from the analysis of reports from all operators and many other sources through the BSI.

It is intended that the act will be implemented together with the relevant specialist authority and operators of critical infrastructures. The collaborative approach and UP KRITIS structures are used and further developed as an established collaboration platform between operators and the state, and existing communication structures are further built out. The IT Security Act states that critical infrastructure operators must specify a point of contact through which they can be reached at any time. 'Single Points of Contact' (SPOC) can also be used here, which function as a shared, higher-level point of contact for operators in a sector (see Figure 13) and make it possible to report anonymously. Industry-specific IT security standards are also compiled on a collaborative basis to guarantee a minimum level of IT security that is appropriate to the current level of threat. The standards are compiled by the operators and their associations, and recognised by BSI. The implementation and efficacy of the measures compiled are reviewed in audits.

Cyber-attack on the French television broadcaster TV5MONDE

Circumstances: The French television broadcaster TV5MONDE became the victim of a massive cyber-attack in April 2015. The perpetrators sabotaged essential production and broadcast servers so that, for several hours, it was not possible to broadcast television programs. In parallel, the broadcaster's Twitter, Facebook and YouTube accounts were also taken over and misused to distribute propaganda messages for 'Islamic State'. A sustained DDoS attack also resulted in the broadcaster's website being unavailable for several hours.

Method: It is as yet unclear how the perpetrators gained access to the internal network of TV5MONDE. The visible impact in April may however be the result of a network having already been compromised for some time. The perpetrators must have had profound knowledge of the broadcaster's internal network and processes to sabotage television broadcasting and internal servers. It is to be assumed that the perpetrators had appropriated this knowledge over a longer period of time, by having first compromised the network and then gathered more information. Access data for the social media channels may also have been collected during this information-gathering phase. This approach is in line with a traditional APT attack, in which an individual system is initially infected with malware, in order to spread further in the internal network from this entry point. Publications in the aftermath of the incident show that the malicious programs found are widely used in the Middle East[25].

The effect of the damage: A cyber-attack resulted in the failure of central functions of a TV broadcaster for the first time. Lost advertising income and the work to recreate the infrastructure meant that the broadcaster had to bear financial losses, as well as enormous reputational damage.

Target groups: The incident is a good example of the fact that the critical infrastructure sector of media is also vulnerable to cyber-attacks. Media and cultural institutions – specifically television broadcasters whose schedule is broadcast worldwide as was the case here – are worthwhile targets for spreading distinct political messages or manipulating or sabotaging information spread via these channels. The method used in the TV5MONDE attack is however also typical for espionage attacks on companies and authorities.

Technical abilities: The attacker or attackers had the ability to spread unnoticed in an internal network for a considerable period of time. This indicates that they are experienced perpetrators. As well as the ability to spread, the perpetrators also had the expertise to understand internal work processes through observation, and identify the critical points in broadcast operation. The coordinated approach of sabotaging broadcast, defacing social media channels and conducting sustained DDoS attacks also indicates a disciplined work organisation that functions in a coordinated way.

[25] http://blog.trendmicro.com/trendlabs-security-intelligence/vbs-malware-tied-to-media-attacks

Extortion: DDoS attacks on critical infrastructure companies

Circumstances: An internationally operational group called DD4BC ('DDoS for Bitcoins') extorts companies with the threat and performance of DDoS attacks.

The cause: The cause is in the area of cyber-crime. The attacker's intention is to extort money. Aims going beyond this, such as reputational damage to the attacked company or suppressing the victims' markets, cannot currently be identified.

Method: With DDoS attacks (reflection/amplification attacks), the extortionists target companies with a bandwidth of up to 25 Gbit/s over a period of up to 60 minutes. Thereafter, the companies receive a letter from the extortionist, in which a payment of several hundred Bitcoins is demanded. If the payment is not made, another attack of up to 500 Gbit/s is threatened.

Damaging effect: The impact of the initial attacks of up to 25 Gbit/s differ greatly. In some companies, the attack was mitigated immediately and there was no damaging effect; in others, there were failures in the internet connection and associated services. Collateral damage was also observed, such as failures of services that are located on the same server infrastructure as the actual victim, but which have nothing to do with the extortion. An attack with a bandwidth of up to 500 Gbit/s, as threatened in the extortion letter, seems not to have happened to date, but is possible from a technical perspective. To date, bandwidths of 40 to 60 Gbit/s have been publicly disclosed for the main attack.

Target groups: In Germany and internationally, the BSI is aware of concerns from the finance and insurance sector. The BSI has collaborated on case-handling within various cross-organisation and -authority working groups, for example within UP KRITIS or in national and international CERT working groups. A working group has been set up on this subject at the National Cyber-Defence Centre.

Technical abilities: No reliable statements can be made about attackers' technical capabilities based on present knowledge. Capacities for performing DDoS attacks in the context described could also have sometimes been bought in via third parties. This means the extortionists could also operate the extortion campaign without having technical capabilities themselves.

4.3 The threat level for critical infrastructures

- In principle, there is the same level of threat for critical infrastructures as there is for other commercial enterprises. Threats due to cyber-sabotage or terrorism are however distinct for critical infrastructures as the attackers' goal is disruption to availability or societal damage that is as great as possible.
- The threat due to cyber-crime is particularly relevant for the finance and insurance sector. The crimes perpetrated range from identity theft to cyber-attacks on the infrastructure of banking institutions to extortion.
- Attacks performed by politically motivated hacktivists are observed in companies in the critical infrastructure sectors of media (defacements or placing of incorrect information on hijacked media websites), energy and the banking industry.
- The threat from cyber-sabotage is concerning. Since Stuxnet, it has been known that the sabotage of machines and institutions by means of cyber-attacks is not only conceivable, but is actually undertaken. The attack on the French broadcasting group TV5MONDE is a current example of successful cyber-sabotage.
- The potential for cyber-attacks performed by other states represents a threat for the Germany economy. In addition, companies in Germany are in many instances not sufficiently equipped against cyber-attacks. This is also true of critical infrastructures.
- It is not only targeted attacks that represent a threat for critical infrastructures. Non-targeted attacks, for example with malware, can also disrupt critical infrastructures and the normal flow of processes (see the 'Ransomware in the hospital' incident). The challenge for many critical infrastructures is that technical devices and software products are used, or have to be used, that either cannot be patched at all or can only be patched with a great deal of effort. This offers trillions of malicious programs that are circulating online many opportunities for attack. In this context, 'Bring Your Own Device' is one of the greatest sources of danger because malware from employee's own private networks is able to gain direct access to the companies' networks.
- The increasing networking taking place within critical infrastructures means the number of possible sources of errors is rising constantly. The reasons for this are the increasing complexity of networks themselves and the use of standard software and standard protocols for networking. This means that the incorrect configuration of devices and software in a test on a gas grid operator's control system resulted in substantial issues in power networks' control systems.
- It is very difficult to comment on which sector is particularly affected by which threat. A targeted attack on sector X may also inadvertently also affect sector Y, because they both use the same protocols and the same software. Nonetheless, the type and size of the impact may be very different in the two sectors. If sector X deals with a specific type of attack more often, and has protected itself accordingly, the attack may be entirely new for sector Y and could cause significant disruption.

Assessment

Due to advancing digitisation and networking, companies are more dependent than ever on information technology functioning correctly. This is particularly true for critical infrastructures, the failure of which may have substantial consequences not only for the company affected, but also for the economy, state and society. This means that operators, as well as the state, bear a special responsibility that must be met by both sides. The incidents that took place in 2015 clearly show that cyber-attacks do not spare critical infrastructures. Although it has not yet achieved the desired success in all areas, it is the responsibility and objective of UP KRITIS to improve critical infrastructures' IT and cyber-security. The IT Security Act that came into effect in July 2015 requires operators of critical infrastructures to adhere to a minimum level of IT security and also to be able to prove that they are doing so.

Spear phishing targeted at critical infrastructure companies in the energy sector

Circumstances: An employee in the financial accounting department of a critical infrastructure company from the energy sector received a very well put together phishing email, in which he was requested to contact an email address at a law office in order to receive data for a financial transaction. The email seemed strange to the employee and he informed his company of it.

Method: An existing management employee is stated as the apparent sender in the phishing email, in order to legitimise the instruction for payment. In fact, the identity of the employee was faked and his email address was misused.

The effect of the damage: No damage occurred.

Technical abilities: The phishing email was very well put together. The sender's email address was authentic and the specific law office actually existed. The text was written in flawless German [translation provided here]:

VFrom: <Management Employee>
To: <Financial Accounting Employee>
Subject: <Project name/code>

Dear Mr <Financial Accounting Employee>,
I am writing to inform you that I am currently processing a confidential financial transaction that needs to be finalised today with the aid of the lawyer Mr <Law Office Employee>, whose information is detailed below.
Please contact him immediately by emailing <Law Office Employee email address> or calling +XXX XX XXX XXX. Your point of contact will send you the bank details so that you can make the first prepayment for this operation. Please follow his instructions precisely. The reference is <Project name/Code>; please state this in your message or when you call.
I ask that you exercise the required discretion and confidentiality regarding this dossier, as you will be the only contact between our group and the law office until the time of official disclosure, which will be very soon. All of our future communication regarding this dossier will take place via the email address of Mr <Law Office Employee>. I am relying on your willingness to respond as the law office needs to keep me updated about the development of this dossier, which is particularly important to me.

Kind regards,
<Management Employee>
'Sent from my mobile'

5 Overall assessment and summary

5 Overall assessment and summary

The highly complex nature of information technology is also evident with regard to current IT security in Germany. The threat presented by a single malware program, for example, is negligible within the context of the variety of causes, methods and underlying circumstances that shape the level of threat in the period covered by this report. Dependencies between individual factors, as well as their combined effect and mutual influence on each other, are more significant for determining the overall level of threat. Consequently, solutions cannot be directed at individual causes but must, wherever possible, have a positive impact on the overall state of IT security more broadly.

5.1 Causes of threats

The level of threat facing IT security in Germany in 2015 is rated as 'high' in many areas:

Threat	2014	2015
Cloud computing		→
Software vulnerabilities	→	↑
Hardware vulnerabilities		→
User behaviour and manufacturer responsibility		↑
Cryptography		→
Internet protocols		↑
Mobile communication		↑
App security		↑
Industrial control system security		↑
Malware	↑	↑
Social engineering	↑	→
Targeted attacks – APT	→	↑
Spam	↑	↑
Botnets	→	↑
Distributed denial of service (DDoS) attacks	→	→
Drive-by exploits and exploit kits	→	↑
Identity theft	↑	↑

Key
Level of threat in 2015 (low, average, high) ↓ → ↑

Considering individual aspects in isolation, however, would not accurately reflect the overall assessment. The current level of threat is far more the product of the causes and complexity of its individual aspects. Figure 14 provides an illustrative example of how the causes, methods and underlying circumstances outlines in the report are in part connected and have a mutual influence on each other:

- Inadequate patch management and the associated use of out-of-date software on computers, mobile devices or central server systems remains a significant technical challenge for users and is the cause of many successful attacks. The many zero-day vulnerabilities that became known during 2015 and the rapid exploitation of new vulnerabilities by, for example, exploit kits make clear the necessity of implementing thorough and rapid patch management, which is the basis of sustainable information security.

- In many cases, users lack awareness of the social engineering and attempted manipulation that often accompany cyber-attacks. It is necessary to adopt a healthy level mistrust regarding unexpected approaches in both private and business contexts. This applies equally to supposed telephone bills, unsolicited offers of support on the phone or supposed secret projects in companies, which lead to the submission of confidential information or even to financial transactions.

- Manufacturers and service providers are responsible for their products and services. Once a vulnerability has been reported, or has become apparent, they are obliged to close it down as quickly as possible, and to provide users with security updates. Service providers should have a strong vested interest in maintaining a reliable security level to protect company and client data.

- APT attacks currently pose a substantial threat for companies and administrative bodies, and will continue to do so. APT attacks for the purposes of industrial espionage or spying on competitors will continue to be carried out by various groups in the future. In particular, companies that are active and prominent internationally should incorporate APT attacks into their corporate risk management processes and implement IT security measures in the areas of detection and monitoring, as well as in relation to incident processing.

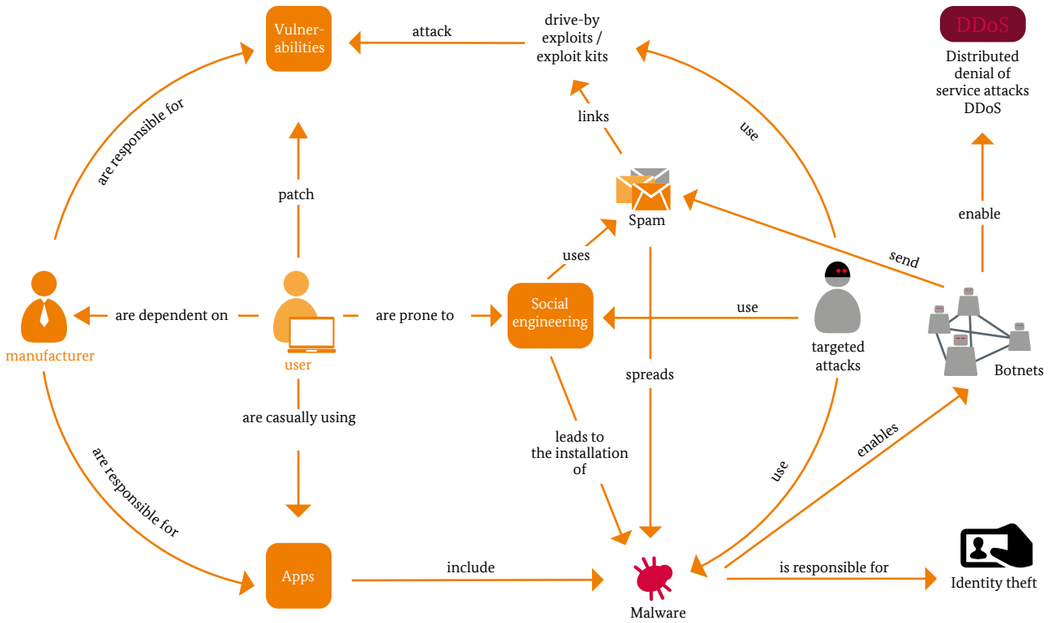

Figure 14: Causes of current security threats

- IT in the industrial environment and the networking of industrial operating systems will remain a significant challenge beyond 2015, particularly in the area of critical infrastructure.
  Networks are not currently extensively segmented, meaning that any attacks on office networks could also have an impact on control and production.

- The number of detected malware programs is increasing, both for stationary and in particular mobile platforms. Combined with the fact that attackers' distribution cycles are getting shorter, this means that the signature-based approaches of security components are subject to increasing pressure. Spam messages remain a key source of malware infections.

- Increasingly, management teams of organisations are having to ask themselves what economic impact a successful cyber-attack would have on the affected organisation itself (internal costs) or on its clients, service providers and suppliers (external costs). According to the Cyber-Security Questionnaire 2015[26] by the Alliance for Cyber-Security, the most common types of damage following successful attacks include production or operation failures and the often significant financial and personnel expense incurred for restoring affected systems and investigating incidents.

- The technical development of the level of threat also suggests an increasing professionalisation of the attackers, regardless whether they are attacking the state, businesses, the scientific community, or citizens and society. The availability of tools, and the provision of services and complete infrastructure for carrying out cyber-attacks, mean that the entry-level requirements needed to carry them out are getting even lower, and at the same time new stakeholders are becoming available.

- There is a lucrative business model, and an associated additional danger for IT security, arising from the difficulties of prosecuting offences (attribution and anonymisation).

- The practical impact is clear from the incidents presented in the above status report. This impacts affects all user groups in Germany. Here, too, it is not isolated individual aspects but rather the interaction of different characteristics that make an attack successful.

[26] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/Umfrage/umfrage2015.html

5.2 Collective responsibility for IT security in Germany

In a world where digitisation affects every area of life and all user groups, responsibility for IT security must become something that is undertaken by all members of society, collectively borne by citizens, businesses, research institutions and politicians. Prevention, reaction and sustainability still remain the areas in which the BSI is active.

Assume the Breach: Responsibility for prevention, detection and reaction in business

The business world must accept that IT security is a part of risk management, and therefore is a management task that needs to be embedded within the responsibilities of the company's leadership team. A lack of resolve on the part of the company's leadership team will lead to inadequate IT security. However, IT security can be implemented in business according to the Pareto principle. Namely, investment in reliable basic measures in the fields of technology, personnel and organisation is economically feasible and alone protects against the majority of current attacks. Further security measures can be selectively used to supplement these. The BSI's own basic IT security is currently being developed in line with this model. Alongside this, the Alliance for Cyber-Security provides a platform for sharing information and experience. An investment in prevention itself constitutes an act of counter-espionage with respect to the current level of threat.

As well as improving prevention, detection capabilities must also be strengthened. The quicker an attack can be detected and responded to, the less damage there will be, e.g. for cleaning up the affected systems or through data that has actually been leaked. Having said that, data protection is not an impediment to effective detection measures. Today it is possible to undertake measures conforming with data protection requirements in consultation with staff representatives and/or those responsible for data protection. Existing detection measures can be supplemented by the purchase of 'early warnings' (or 'indicators of compromise') in order to increase the likelihood of also recognising targeted and novel attacks. In the same way, the BSI will pass onto companies a collection of its future insights arising from reports submitted by operators of critical infrastructure, in keeping with the IT Security Act.

Nevertheless, prevention and detection are no longer sufficient to deal with the current level of threat. Rather than simply defending against attacks, it should be part of an organisation's risk management activities to prepare itself for an IT security incident or a successful cyber-attack (the 'Assume the Breach' paradigm). In order to accomplish this, structures must be put in place, responsibilities must be allocated, and procedures for dealing with an anticipated incident must be practised. A professional response to an incident can effectively minimise the consequent damages. Service providers who specialise in responses to cyber-attacks, and who can support companies in their management of incidents, already exist.

Development of cryptography and the IT security economy

The development and use of stronger and more reliable cryptography is a pre-requisite for the encrypting, authenticating and integrity assurance of electronic communication. Without these there is no trust in the communication technology of today. However, the potential of cryptography has not yet been exhausted, in part due to insufficient demand, which means that the BSI is still engaged in supporting the development of research and deployment of cryptography in Germany. The same applies to the IT security economy and the development of cyber-defence measures in Germany, which has not yet been able to develop into an independent market segment. Both areas need to constantly adapt to demand and the current level of threat. In order to protect technical sovereignty, companies and investments in cryptography and IT security must remain within Germany and be protected from foreign takeovers in the face of emerging corporate success.

The exceptionally high rate of innovation in the field of information technology will pose new challenges regarding IT security in the coming years. It is foreseeable that there will be a further increase in the number of successful attacks on the systems and services of all user groups. The underlying circumstances and measures of prevention, detection and reaction must also develop at the same rate. Each user already has a responsibility to ensure their behaviour supports IT security in Germany.

6 Glossary

Advanced Persistent Threats/APT
Advanced persistent threats (APT) are targeted cyber-attacks on selected institutions and organisations, in which attackers gain persistent (long-term) access to a victim's 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 attackers' part and are generally difficult to detect.

Adware
Adware refers to programs that are financed by advertising. Malicious programs that generate advertising income for their creator are also referred to as adware.

Attack vector
Attack vector denotes the combination of attack routes and techniques through which the attacker gains 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 smart phones or tablets.

BIOS
The BIOS (Basic Input Output System) on PC systems is the program code that is first to be implemented following system start-up. BIOS offers standardised access opportunities to the operating system on the hardware.

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

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

CERT/Computer Emergency Response Team
Computer emergency team made up of IT specialists. Many companies and institutions have now established CERTs to take care of defending against cyber-attacks and the prevention of and reaction to IT security incidents.

CERT-Bund
The 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 preventative and reactive measures in the event of security-related incidents affecting computer systems.

Cloud/Cloud computing
Cloud computing denotes the offering and use of, and charging for, 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 (e.g. computer power, 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 in parallel they are referred to as a distributed DoS or DDoS attack (DDoS = Distributed Denial of Service). DDoS attacks are often made by a very large number of computers or servers.

Drive-by download / Drive-by exploits
The term 'drive-by exploits' refers to the automated exploitation of security gaps on a PC. The act of viewing a website, without any further user-interaction, is sufficient for a vulnerability in the web browser, or in additional browser programs (plug-ins) or the operating system to be exploited, and for malware to be installed on the PC unnoticed.

Exploit kit
Exploit kits (also referred to as '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 use 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 adapted especially for a particular type of hardware and is not interchangeable.

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

NTP
The Network Time Protocol provides the time synchronisation of IT systems in networks.

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 close security loopholes 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. 'going fishing for passwords'. The attacker attempts to extract personal data of an internet user via bogus websites, emails or messages, in order to use this to commit identity theft.

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.

Ransomware
Ransomware is a type of malware that is used by an intruder to prevent access to, or use of, data or entire computer systems. The purpose of this is generally to extort money (the 'ransom').

Reflection attack
A 'reflection attack' is a special kind of DDoS attack. In this type of attack, the victim's system is not directly attacked. Instead, the attacker operates indirectly (by 'reflection'). To do so, he sends a query with a fake sender address (victim's system) to a target system (reflection). The response to the attacker's query is not then sent to the attacker, but rather to the victim's system, because of the fake address. The response packets are frequently considerably larger than the queries. This makes it possible for the attacker to generate a lot of attack bandwidth without using much of their own bandwidth. This is referred to as an amplification of the bandwidth used.

Social engineering
In cyber-attacks using 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 skilful 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 also known.

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

Watering hole attacks
The analogy refers to a watering hole that attracts animals of prey and is therefore also a favourite spot for their hunters. This type of attack initially involves the hacking of websites that are likely to be visited by the targeted person, and the infection of these websites with malicious code. If one of these infected sites is visited then malware is automatically installed (such as via drive-by download).

Web browser
Web browsers are specialised computer programmes for displaying websites online, or documents and data generally.

Legal Notice

Published by
Federal Office for Information Security (BSI)

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

Email
bsi@bsi.bund.de

Phone
+49 (0) 22899 9582-0

Fax
+49 (0) 22899 9582-5400

Date
November 2015

Printing
Zarbock Printing and Publishing House, Frankfurt am Main

Content and editing
Federal Office for Information Security (BSI)

Picture credit for cover picture
Fotolia

Graphics
BSI

Item number
BSI-LB15/504e

www.bsi.bund.de