COURSEBOOK



## Cyberattack scenarios and incident response

DLMIMWCK01



Main learning objectives

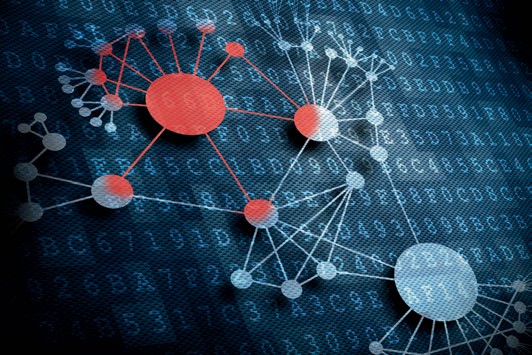
##### Preface 9



This course, *Cyberattack scenarios and incident response*, aims to first provide an overview of the most important principles in this field of study. You will learn, for example, about the possible attack vectors on computer systems. You will then become familiar with preventative actions and responses to prevent or mitigate potential attacks. Furthermore, you will come to understand the importance of IT forensics in being able to find and use electronic evidence.

Building on this knowledge, the course will present sources on the current state of IT security for your critical analysis.

[www.iubh.de](http://www.iubh.de/)



# Unit 1

## Introduction

#### LEARNING OBJECTIVES

After completing this unit, you will know ...

#### ... what computer crime is.

#### ... what types of vulnerabilities there are in IT systems.

#### ... how to assess a vulnerability.

#### ... what types of malware there are.

#### ... what impact the human factor has on computer crime.

DL-D-DLMIMWCK01-L01

1. Introduction

### Introduction

Emails from an odd sender or with a suspicious attachment or link to a harmful website can be found both in the professional and private spheres. Opening a suspicious attachment can, for example, lead to the computer being infected with malware due to the exploitation of a vulnerability. One scenario is the disclosure of bank account details to the attacker, which is a clear example of cybercrime. But would this attack still be considered cybercrime if the bank account details were stolen from the person’s desk? What types of vulnerabilities and malware are there? The following introduction will address these and other questions.

### Differentiating cybercrime from other offenses

The importance of digitization has risen steadily since the start of the 20th century. The number of internet-based services used by private individuals and businesses – such as email, messenger, e-payment, and cloud computing services – is rising. While these technologies offer many benefits, they also present risks for the business world, government, and private individuals.

Internet of Things

(IoT)

The “Internet of Things” describes the trend of connecting internet-capable objects in a network.

Computer Crime

Computer crime refers to any offense targeting and/or originating from an IT system.

Alongside internet-based services, the number of internet-capable devices is also rising. Laptops and desktop computers constitute a standard part of our business and personal landscapes. What is new, however, are the everyday objects that have transformed into internet-capable devices thanks to IT – devices like smartwatches, voice assistants, and smart fridges. This trend is encompassed by the term **Internet of Things (IoT)**. IoT describes a concept where a number of everyday objects are connected to each other in a network and to the internet (cf. Horten & Gräber, 2020).

As the number of the services and devices described has grown consistently, criminals have spotted the potential for computers and networked devices to be used for illicit purposes. Cybercrime, also known as computer crime and internet crime, has developed from this.

The terms computer crime and internet crime do not have a standard definition. **Computer crime** is generally used to mean any criminal offense that targets IT systems or for which an IT system is used as a tool. **Internet crime**, in turn, encompasses any criminal offense for which the internet is used as a tool for committing the act (cf. Huber, 2019). Since internet crime always involves the use of a computer or modern information and communications technology, these two terms overlap and are often simply referred to under the umbrella term “cybercrime.”

Introduction

Within policing, cybercrime is defined in both narrow and broad terms. In the narrower sense of the term, cybercrime refers to any offense that is only possible to commit using IT systems or the internet. For example, stealing someone’s identity through their email account and making an illegal transfer of cryptocurrency would be considered cybercrime in the narrower sense of the word. Without the internet, neither the identity through the email address nor the cryptocurrency would be accessible. The offense, therefore, relies on internet or computer use (“cyber-dependent crime”).

Within its broader meaning, cybercrime covers offenses that would be possible even without the use of the internet or IT systems, such as credit card fraud. One version of this offense might be pickpocketing someone and then using the victim’s credit card. Another version might be stealing a person’s login details to a credit card portal in order to view the credit card data and use it for one’s own purposes – this is an example of cybercrime. This type of credit card fraud can be carried out efficiently via the internet (cf. Horten & Gräber, 2020). The following table lists a few examples of cybercrime:

|  |  |
| --- | --- |
| Examples of cybercrime in the narrower and broader sense | |
| Cybercrime (narrower definition) | Cybercrime (broader definition) |
| Hacking | Cyberbullying |
| DoS attacks | Cyberstalking |
| Phishing | Child pornography |
| Ransomware | Fraud |

In addition to categorizing offenses within these two definitions, German case law also describes multiple elements of offenses that address computer crime (Criminal Code, or StGB, version as amended on 17 July 2020):

* § 202a StGB, Data espionage: this section covers unauthorised data spying.
* § 202b StGB, Phishing: when someone intercepts data by data transmission or electromagnetic broadcasts.
* § 202c StGB, Acts preparatory to data espionage and phishing: this section covers acts carried out in preparation to commit the acts specified in § 202a StGB and § 202b StGB.
* § 263a StGB, Computer fraud: this section refers to the manipulation of data processing operations or programs.
* § 269 StGB, Forgery of data with probative value: this section applies to identity theft on the internet, for example.

Internet Crime Internet crime refers to any offense committed with the aid of the internet.

DoS Attacks   
A denial-of-service attack aims to make a service inaccessible to other users. A barrage of queries is sent to the service or system in order to achieve this.

Vulnerability   
The term vulnerability refers to the weakness in, among other things, an IT system, an organisation, a building, or a human being.

.

* § 270 StGB, Deception in relation to data processing in legal commerce: this section applies the regulations set forth for deception in analogue legal commerce to deception involving data processing operations.
* § 303a StGB, Data manipulation: this section covers the illegal manipulation of data in general, which includes deleting data or rendering it unusable.
* § 303b StGB, Computer sabotage: this section penalizes interference in data processing operations using **DoS attacks**, for example.

The spectrum of cybercrime offenses ranges from identity theft and cyberstalking to economic crime. Offenses that involve the use of the internet or an IT system fall into this category. The example of bank account misuse described previously also falls into this category; however, the lines here are blurred. Bank accounts have been targeted by criminals even prior to the age of the internet. Before criminals began using IT systems for this type of offense, they forged signatures or stole other means of identification, such as savings books, certificates, and contracts.

An example of an offense that would count as cybercrime in the future is a break-in. If a homeowner has a “smart” lock, this can be exploited by a cyber attacker. The lock can be accessed via the internet to open the door remotely, for instance, to receive a delivery. If the lock has a technical vulnerability or the owner is careless with their access details, a hacker can open the door without picking the lock or physically forcing it open.

### Vulnerabilities in computers and mobile devices

The term vulnerability does not have a uniform deﬁnition. The German Federal Office for Information Security (BSI) defines a vulnerability in the IT-Grundschutz Compendium as a security-relevant flaw in an organisation's IT system (cf. BSI 2019a).

Vulnerabilities in computers, mobile devices, and any other type of information and communication technology enable successful attacks on computer systems in the first place. From an attack vector perspective, vulnerabilities can be divided into five categories:

* Chip or firmware vulnerabilities,
* Operating system vulnerabilities,
* Network and server vulnerabilities,
* Application vulnerabilities, and
* Organisational vulnerabilities.

Introduction

The impact of vulnerabilities varies depending on the category. For example, a firmware or chip vulnerability may be present directly at the hardware level, making an update either not possible at all or too consequential. The consequences of such a vulnerability would be negative, since removing the vulnerability is costly. One such vulnerability was "Meltdown" in 2017. By exploiting this vulnerability, it was possible to read the memory area inside a chip without authorisation by way of time measurement. "Meltdown" exploited the "out-of-order execution" of modern processors, i.e., the calculation of process steps in an order different from the one than was intended. The procedure is supposed to lead to an increase in throughput speed. However, by measuring the time, it was possible to determine the result of this calculation and thus read memory areas that the current process is not authorised to read (cf. Lipp et al. 2018).

Operating system vulnerabilities overlap with the previous category, since firmware and operating systems on mobile or IoT devices are sometimes identical. The operating system refers to the programs that manage the computer's system resources and provide applications. System resources are, for example, the main memory, the hard disk, and the processor. Vulnerabilities at the operating system level can affect a wide range of devices and result, amongst other things, from programming or conﬁguration errors. Programming errors are usually fixed through manufacturer's security updates. Regular updates are indispensable when it comes to vulnerabilities in operating systems.

The first two categories of vulnerabilities affect individual computers or mobile devices. Vulnerabilities at the network or server level, however, affect communication between individual systems such as server systems. One example of a vulnerability in this category would be servers that are accessible from the public internet and that do not perform any filtering of incoming connections. In this case, it is possible for an attacker to send a large number of domain name system (DNS) queries to the server in question, causing this server to be overloaded and no longer capable to accept any queries. This type of attack is called "DNS Ampliﬁcation Attack" and constitutes a DoS (cf. Mahjabin/Yiao 2019). Another well-known example at the network protocol level was the Eternalblue vulnerability, which enabled attackers to infect computers via an SMB share. This vulnerability was leveraged via the internal network and the internet and caused a high level of damage.

Vulnerabilities at the application level are very diverse. Applications include programs for accounting, production, and human resources management. Despite the diversity of applications at this level, the vulnerabilities are always similar. Applications should have some form of authentication and access control to prevent unauthorised access. The absence of these measures or faulty implementation makes this a vulnerability (cf. BSI 2019a).

Firmware

Firmware is the software embedded in computer systems and thus functionally connected to the hardware.

Operating System

An operating system manages the hardware of a computer and makes it available to application programs.

CEO  
Fraud  
CEO Fraud refers to the impersonation of an organisation's senior management for the purpose of causing wrongdoing.

Information Security Management System

(ISMS)

An ISMS aims to permanently deﬁne, control, maintain, and continuously improve information security.

Common

Vulnerability Scoring System

(CVSS)

The Common Vulnerability

Scoring

System is a method to assess vulnerabilities in computer systems.

The previous vulnerabilities referred to the hardware or software of a computer system. Vulnerabilities at the organisational level, on the other hand, are embedded in the structure of an organisation and therefore are not necessarily linked to a computer system. One example is the so-called CEO Fraud or President Fraud. In such cases, individuals within an organisation's accounting department, for example, are contacted by a caller who pretends to be the boss. The fraudulent caller usually stresses out urgency. For business reasons, it is supposedly imperative to transfer money to a certain bank account within the shortest time possible. By combining time pressure and high authority, the person is driven to take incorrect action. In the process, the deﬁned policies and processes are disregarded. In such cases, it is the fraudster who owns the bank account.

The vulnerability, in this case, is the employee who does not comply with the usual control mechanisms, such as the four-eyes principle or signed transfer instructions. This category of vulnerability forms a special case, as it does not lie in a computer system, but exclusively in the organisational structure. Other examples of this category are a lack of security guards or insufficient employee awareness.

Following the overview of vulnerability categories, the question arises of how to assess the criticality of vulnerabilities. This is essential for planning and implementing countermeasures.

In principle, the criticality degree of a vulnerability is measured by the risk it imposes on the organisation. An information security management system (ISMS) can be useful for structured risk handling within an organisation. This is based on various standards, such as the BSI's IT-Grundschutz or ISO 27001. A central component of the ISMS is the analysis and evaluation of risks within an organisation. Risk handling thus contributes to the deﬁnition of corrective, detective, and preventive measures (cf. BSI 2017).

Once a new vulnerability has been discovered, the criticality can be determined via a generic vulnerability assessment. Various systems are used for this assessment. One of them is the Common Vulnerability Scoring System (CVSS). Using speciﬁc criteria, this methodology results in a numerical value for the criticality of a vulnerability. Such criteria are divided into the metric groups Base, Temporal, and Environmental, and are composed as follows:

The Base group (characteristics of the vulnerability without temporal and environmental influences):

* Exploitability Metrics
  + Attack vector: What type of access (including network, local, or physical) does the attacker require?
  + Attack complexity: How complex (low, high) is the exploitation of the vulnerability?

Introduction

* + - Privileges: What privileges/rights (none, low, high) are required for the attack?
    - User interaction: To what extent is a user action (none, required) required?
* Scope metrics: To what extent does the exploitation of the vulnerability impact components (constant, changed) outside the security perimeter?
* Impact metrics:
  + Confidentiality: What is the level (none, low, high) of data confidentiality breach?
  + Integrity: To what extent is the integrity of data violated? To what extent can data be changed and how much damage is caused by this change (none, low, high)? For example, can payments be manipulated?
  + Availability: To what extent is the availability of data affected (not at all, low, high)? To what extent is the performance or functionality of systems restricted? Can the system still be used for its intended purpose?

The Temporal group (characteristics of the vulnerability depending on the time course):

* Maturity of the exploit code: To what extent does such code exist (including proof-of-concept, functional, untested), and what is its impact on the vulnerability?
* Removal: To what extent are remedies (including non-availability, workaround, patch/update from vendor) available to address the vulnerability?
* Trust: What is the degree of trust in the existence of the vulnerability and the level of credibility surrounding the technical details (among others not deﬁned, confirmed, not known)?

The Environmental group (characteristics of the vulnerability depending on its "own" implemented user environment):

* Security requirements applicable to the affected IT system in the organisation
  + Confidentiality: What is the required confidentiality level (not deﬁned, low, medium, high)?
  + Integrity: What is the required integrity level (not deﬁned, low, medium, high)?
  + Availability: What is the required availability level (not deﬁned, low, medium, high)?
* Modiﬁcation of values in the Base group due to the organisational environment: To what extent are Base group assessments subject to change in one’s own organisation?

A sample explanation on how to use the framework is described below. The impact in case of integrity violation (Base group) depends on the data volume which an attacker is able to change, and how critical this data is. Presuming that a vulnerability grants an attacker access to a web server database storing customer data, allowing it to change all data fields of all customers, this criterion comes with a high score.

The criticality degree is lower if the attacker is only able to change one field, such as the country code. However, the criticality is higher if that field contains, for example, the IBAN.

The calculation of the CVSS score results from the ratings of Base, Temporal, and Environmental group criteria. While Base criteria are always included in the calculation, the other two groups of metrics are optional. The resulting CVSS score is calculated using a formula and ranges from zero to ten (cf. FIRST 2017). In doing so, the following value ranges are deﬁned for the vulnerability criticality degree:

* CVSS Score 0.0: "no criticality",
* CVSS Score 0.1-3.9: "low criticality",
* CVSS Score 4.0-6.9: "medium criticality",
* CVSS Score 7.0-8.9: "high criticality", and
* CVSS Score 9.0-10.0: "critical criticality".

Protection goals Confidentiality, integrity, and availability are the basic protection goals of information security.

There may be vulnerabilities that have been reported by various security researchers and deemed to have a low impact, even though they pose a serious threat to the organisation. A vulnerability can have a large impact on the availability and no impact on confidentiality and integrity, resulting in an average CVSS score. By adding the Environmental group, for example, the requirement for one's own organisation with regard to availability can constitute the most critical protection goal. This increases the CVSS score in relation to the implementation within the organisation.

Potential for vulnerabilities is rooted in the programming of software. In this process, errors may be made, or certain principles may not be adhered to. Buffer overflows constitute an example of vulnerabilities that occur in programs. They can occur if the size of the value is not queried when assigning a value to a variable. Unless this is secured, an attacker with a large value can overwrite memory areas that are not allocated to the program, thus allowing arbitrary malicious code to be executed. In some cases, it takes years to discover such vulnerabilities in the program code (cf. Barrientes et al. 2018).

### An overview of malware

Malware is a type of code or program that is intended to cause damage to a system or to change its function in a harmful way. This also includes the modification or removal of existing code within a system (cf. Namanya et al. 2018).

Introduction

Accordingly, malware can be an additional program on a system that, for example, uses the system's computing capacity to mine cryptocurrencies. Malware also refers to the modification of an internal driver, thus sending all keyboard strokes to an attacker. Malware does not necessarily have to be a standalone program. Rather, the modification of another program is also classified as malware. Removing code can also be classiﬁed as malware. One example is the removal of a password prompt. Subsequently, an attacker can view, modiﬁy, or receive previously protected content without using a password.

Regardless of the program code design, several types of malware exist, and are explained in more detail below (cf. Namanya et al. 2018):

* Viruses,
* Worms,
* Trojan horses (Trojans),
* Spyware,
* Adware,
* Rootkits,
* Bots, and
* Ransomware.

Each malware has different characteristics and poses different threats. A virus is self-replicating malicious software that spreads on the infected system by itself. This spreading can happen via file transfers or shares. A virus, therefore, does not actively spread within a network. Typical effects of viruses are data theft, damage to computers or networks, and the spread of botnets.

A worm is also a self-replicating malware, however, it actively spreads. Once a worm has infected a system, it scans the adjacent network and searches for additional vulnerable systems. Subsequently, the worm attempts to infect these reachable systems with various attacks as well. Once the new system is found, this process is repeated, eliminating the need for user interaction to spread the worm. In addition, worms can also have the functionality of a virus and cause damage to the infected system. One example of a worm is "Stuxnet". The main aim of this malware was to disrupt the operation of Iranian enrichment plants. In the process, the worm spread independently over the Internet and across networks until the ultimate target was reached. Functionalities of a virus were only activated at this point, disrupting the operation of systems. Since the "Stuxnet" worm did not cause any damage to other computers, it was not noticed until very late.

A Trojan horse (Trojan) is malicious software hidden in legitimate software. As soon as a user starts the software, a program that appears to be useful launches. At the same time, the malicious component of the Trojan gets activated. This type of malware is passive and requires human interaction.

Malware

Malware refers to programs with specified functions hidden from the user, intended to cause damage.

Ransomware

Ransomware is malware with the aim of encrypting data in systems and subsequently demanding a ransom.

Virus

Viruses can have various damaging effects on networks and computers and do not actively spread.

Worm

Worms harm a computer similar to a virus while actively spreading throughout networks.

In most cases, the purpose of a Trojan horse is to provide attackers with access to a  
system to enable further malware to be loaded.

Spyware has similarities with Trojan horses regarding the way spyware is distributed: Most often, it is also hidden in legitimate programs. However, the functionality of spyware differs from Trojan horses. This is because spyware attempts to collect information on the user and send it to the attacker. This information includes user behavior, internet usage, or keyboard strokes. One example of spyware is the "GO Keyboard", which was available in the Google Play Store for a long time. This alternative keyboard sent data about the user's behavior to external servers.

Attackers use adware in conjunction with Trojan horses or spyware. The purpose of adware is to display advertisements to the victim while generating illegal advertising revenue.

A rootkit encompasses various tools. Rootkits are used to gain control of a system in a hidden manner. After compromising the system, the intruder's activities are covered. Examples include hiding malicious processes and files from the user or antivirus software. This way, automated defense against this type of malware becomes more difficult.

Bots A bot uses similar functionalities as a worm or virus, but its goal is to create a botnet.

DDoS Attack A DDoS attack is a coordinated DoS attack from multiple distributed computer systems.

Bots also combine some of the characteristics of malware mentioned so far. The term "bots" stems from "robots" and is also used for bots with benign uses, such as chatbots. In the context of malware, bots are described as a method that uses various techniques to attack as many systems as possible in order to form them into a botnet. Malware such as viruses, worms, or rootkits is used to set up and spread botnets and attack systems. The infected systems are called bots or zombies.

A botnet is controlled by a botmaster or a command & control server. In addition to the damage that the bots cause to the affected systems, a botnet is usually used for DDoS attacks. One example is "Zeus". This botnet was estimated to have infected over 3.6 million IT systems. "Zeus" was used by attackers to build botnets and then exploit various malicious functionalities. For example, "Zeus" botnets were used to distribute ransomware and launch DDoS attacks (Namanya et al. 2018). Another example of a botnet is "Mirai," a malware that first targeted and infected IoT devices such as cameras in 2016. Criminals used the infected devices to offer services such as "DDoS for hire". The infected devices were "leased" to launch DDoS attacks to cripple specific targets. On this occasion, paying criminals determined the target. This offering has, in this case, enabled the attack of the DNS service "DynDNS", rendering many other services, such as Twitter and Facebook, inaccessible.

Introduction

The last type of malware is ransomware. Ransomware spreads similarly to a virus or worm and aims to encrypt data on a system to extort a ransom from the victim. The first malware with this functionality was discovered in 2013. In 2017, the "WannaCry" ransomware made headlines, infecting over 300,000 computers in 150 countries. The criminals' goal was to deny victims access to their own data and systems and to only release access in exchange for a ransom. Data encryption served as the instrument to achieve this purpose. Without access to the key, the data and systems were no longer accessible to the victim (cf. Namanya et al. 2018).

Overlaps exist between all the above-mentioned types of malware. A virus can contain ransomware functionalities and adware can simultaneously send data about a user's behavior to the attacker. In addition, new malware is detected and thus assigned to new types of malware every year (cf. Fireeye Mandiant 2020).

### Social engineering and the human factor

The previous considerations have centered the technical component of computer criminality: vulnerabilities in soft- and hardware and malware that exploits these vulnerabilities. Merely mentioning of vulnerabilities at the organisational level was an indication that the human factor will play a role.

Until a few years ago, the defense against malware was realized solely by technical means. However, the human factor should be included when looking at vulnerabilities. Many technical measures can be undermined by way of human intervention. Both the human and the cultural factor within an organisation must be considered (cf. Stirni- mann 2018).

In 2020, the social network Twitter was hacked by attackers gaining access to an administration tool. Access was restricted to a specific group of Twitter's internal employees, and authentication measures were also in effect. However, the attackers succeeded in obtaining the authentication characteristics of Twitter's administrators via forged emails. This ensured that attackers had access to the administration tool, and fake tweets calling for the transfer of Bitcoins were posted from prominent Twitter accounts. In addition, the attackers had access to the personal data and private messages of the users (cf. Sokolov 2020).

This example illustrates the extent to which the human factor can undermine protective measures. Moreover, this exemplifies social engineering. This concept too is lacking a distinct deﬁnition due to ﬂowing demarcations. One cybersecurity deﬁnition is that social engineering includes all attacks that exploit human vulnerabilities via social interaction to circumvent security measures in computer systems.

Social Engineering Social engineering uses social interaction with humans to circumvent technical protection measures.

Baiting Baiting attempts to use physical devices such as USB sticks as lures to trick employees into using them on company hardware.

Phishing Phishing is an attempt to obtain user names and passwords from victims.

Spear Phishing Spear Phishing describes phishing targeting individuals or organisations.

Attackers do not necessarily have to be using computer systems themselves (cf. Wang/Sun/Zhu 2020).

One of the first attacks to be categorized as social engineering was dumpster diving. In this context, an organisation’s Recycle bin is searched for useful information. This includes header sheets, address directories, or notebooks with usernames and passwords. This type of attack does not require special technology or computers, but simply bypasses protective measures, such as the secure trash disposal of sensitive information. The vulnerability that gets exploited is the human misjudgment as to which data may go directly into the trash and which must be shredded beforehand. Dumpster diving thus corresponds to the above deﬁnition of social engineering.

The attacker may, for example, use a USB stick as bait, which is then grabbed by the victim and, out of curiosity, inserted into the victim's own workstation computer. If the attacker prepares the USB stick accordingly, malware is executed on the company computer. This technique exploits general human curiosity.

Somewhat similar in nature, but using a different technical approach, is phishing. Phishing is an artificial word made up of "password" and "fishing," as it involves "fishing" for a password. Attackers usually send masses of emails (e.g., via botnets) that call for passwords to be entered on prepared websites, from where these access data are then sent to the attacker. Here, too, the attackers exploit the curiosity and carelessness of their victims.

The specialized variants of phishing are spear-phishing and whaling. Unlike phishing, which attacks victims indiscriminately and en masse, spear-phishing targets specific organisations or individuals. Attackers start by gathering information on their victims from public sources, such as social networks or company websites, and then launch phishing attacks that are as authentic as possible. The described attack on Twitter began with spear-phishing on Twitter administrators. Whaling is similar in nature, focusing on high-value targets such as executives, board members, or government leaders, and has some proximity to President Fraud (CEO Fraud) (cf. Wang/Sun/Zhu 2020). To gain an insight into the world of a phishing attack one can, for example, clone any website with the "SEToolkit". The copied website is executed on one's own web server and contains an implemented "password collector". After sending emails with a link to the copied website to the target persons, the password data can be viewed by the attacker after it has been entered.

In principle, humans assess a situation using various indicators, such as body language, external appearance, or voice color, and then determine whether the situation is trustworthy or dangerous. Many of these indicators are missing in digital or online interactions. People therefore often draw the wrong conclusion.

Introduction

Attacks using social engineering rely on this vulnerability.

One mitigating measure to reduce this vulnerability are awareness and training measures (cf. Stirnimann 2018).

Summary

Computer crime is a highly elastic term that has gained a great deal of significance in recent years. Criminals are increasingly using computers and the internet for their offenses, which makes them part of computer crime in the narrower sense.

The types of vulnerabilities that exist in hardware, software, and at the organisational level, along with the way these vulnerabilities can be compared using risk analysis and the CVSS score, are important in gaining a basic understanding of computer crime. Coupled with these are the various types of malware exploiting these vulnerabilities to cause damage to systems. Viruses, worms, bots, and ransomware are examples of malware.

The final section examined the human factor. A purely technical assessment of computer crime omits this important aspect. The term social engineering was used to describe attack options that exploit human vulnerabilities and thus circumvent technical protective measures.



# Unit 2

## Criminal law bases

#### LEARNING OBJECTIVES

After completing this unit, you will know ...

... which criminal law principles sanction the misuse of identity.

... which sub-areas are covered by intellectual property law.

... which newly created paragraphs regarding computer crime have been implemented.

... how falsification of a document in the digital space is punishable.

... which actions are considered computer fraud.

DL-D-DLMIMWCK01-L02

1. Criminal law bases

### Introduction

Internet crimes are a relatively new phenomenon from a legal perspective, and actions by criminals need to be punished with a new basis in criminal law. If, for example, a private individual falls victim to a phishing email and discloses their access data, they may lose control of their online store account. The criminals can use this access to order the merchandise on the victim's account. The question arises as to what legal recourse a victim has to its availability in this case.

Appropriation of identity Appropriation of identity describes the use of another person's identity with malice.

§ 242 StGB

Section 242 of the StGB refers to the theft of movable property and thus does not apply to identity theft or appropriation of identity.

### Appropriation of identity

In order to deﬁne the terms appropriation of identity and identity theft, it is necessary to establish the concept of identity beforehand. In principle, identity is based on characteristics. To this end, identity comprises uniquely distinguishing characteristics that identify a person, an object, or an organisation. The verification of identities can be carried out, for example, through ID numbers, passwords, names, or electronic keys. Identity theft or appropriation of identity occurs when a victim's identity is exploited, damaged, or taken over during social contacts (cf. Huber 2019).

Section 242 of the StGB is the general basis of criminal law regulating the offense of theft. However, this section focuses on movable property belonging to third parties, making it inapplicable to identity theft or appropriation of identity. For this reason, this section does not apply to the example described above.

There is no separate paragraph with the designation "appropriation of identity" or "identity theft". The Scientific Service of the German Bundestag has already dealt with this requirement in 2014 and determined that no criminal liability gap is present (cf. Deutscher Bundestag/WD 2014). Various sections can become relevant to the appropriation of identity, e.g.:

* § StGB 263 Fraud,
* § StGB 253 Blackmail,
* § 202a StGB Data espionage,
* § 202b StGB Phishing,
* § 202c StGB Acts preparatory to data espionage and phishing,
* § StGB 238 Stalking, and
* § 42 BDSG Penal provisions.

Sections 263 and 253 of the StGB are more concerned with the consequences of the appropriation of identity and generally applicable, even if no computer crime is involved.

Criminal law basis

Sections 202a, 202b, and 202c target the aspect of identity theft in that unlawful access to data by an unauthorised person is punishable. The problem here is that those affected are usually unaware that their data has been spied on or phished. In this case, websites such as those of the Hasso Plattner Institute or "haveibeenpwned" (cf. Hunt 2020; Hasso Plattner Institute 2020) can help. These websites collect identity features from data thefts and make them searchable so that one can determine whether access data to one's own email address has already been stolen. On "haveibeenpwned", it is also possible to set a domain alert to ensure immediate notification upon data theft including the corresponding domain.

In the fall of 2009, a defendant obtained the passwords of various users of the instant messaging service ICQ. Using the victims' identities, he sent images containing an embedded virus to their contacts. The virus sent images from the victims' webcams to the attacker (Case No. Ls-80610 Js 644/10-275/10). This is an example of a conviction under Section 202a of the StGB.

However, Section 202a of the StGB requires sufficient access security. Copying unencrypted data on an EC card is therefore not covered by Section 202a of the StGB (Case No. 4 StR 93/09). Section 238 of the StGB deals directly with stalking and ordering goods using appropriated personal data. This legal text also applies to the example in the introduction.

Section 42 of the German Federal Data Protection Act is a supplementary penal provision targeting the disclosure of personal data in bulk and on a commercial basis, and the unauthorised publication of personal data. Accordingly, this section applies to the publication of identity data with malicious intent.

### Theft of intellectual property

The term "intellectual property" is controversial in Germany, and specialist literature tends to refer to “Immaterialgüterrecht“ which, in the literal sense of the word, means “law governing intangible assets”. However, both terms refer to intangible assets protected by copyright or competition law. Copyright law refers to literature, science, and art works, whereas competition law deals with patent and utility model protection, design rights, and e.g., trademark law (see Pierson/Ahrens/Fischer 2018).

From a criminal law perspective, these two areas contain supplementary penal provisions. The following sections are of particular relevance:

§ 202a StGB

Section 202a of the StGB penalises the spying on data while making sufficient access security a prerequisite in parts.

§ 42 BDSG

Section 42 of the German Federal Data Protection Act is a supplementary penal provision.

It penalises the mass disclosure of personal data.

Intellectual Property Law

Intellectual property law refers to the right to intangible assets and entails competition law and copyright law.

|  |  |
| --- | --- |
| Ancillary Criminal Laws on Intellectual Property | |
| Sections | Description |
| § 142 PatG | Penal provision in the German Patent Act |
| § 25 GebrMG | Penal provision in the German Utility Models Act |
| § 51 DesignG | Penalty provision in the German Act on the Legal Protection of Designs |
| §§ 143–144 MarkenG | Penal provision in the German Trade Mark Act |
| § 10 HalblSchG | Penal provision in the German Semiconductor Protection Act |
| § 39 SortSchG | Penal provision in the German Plant Variety Protection Act |
| §§ 106–108b UrhG, § 111a UrhG | Unauthorised exploitation and unauthorised interference with the German Copyright Act. Affects works such as music, videos, and books. |

Consequently, the criminal law consideration of intellectual property encompasses a variety of legal regulations. Some of these are not intended to apply to digital intangible assets. Thus, the requirements for legislation around intellectual property are at the center of international and national legislative initiatives (cf. Pierson/Ahrens/ Fischer 2018).

FilehosterFilehosters are internet providers that allow users to upload any data so that other users can download it.

The topic of intellectual property protection in connection with computer criminality first came to the public's attention through filehosters or file-sharing networks, such as Napster and Rapidshare. These services provide for digital content such as music, videos, e-books, and other documents to be downloaded, with the actual rights holders having no knowledge of the acivity (cf. Bonik/Schaale 2016).

As already described, the lawmakers did not have digital file-sharing environments in mind when creating copyright and competition law. For this reason, the position of file hosters is still the subject of current case law (file number I ZR 80/12). The main question here is whether the users of file hosts must be prosecuted under criminal law. The data is not distributed by the users, hence there is no reproduction. This does not constitute a criminal offense under copyright law. The impact of EU Directive 2019/790 on the activities of filehosters, intended to regulate copyright in the European digital single market, has not yet been clarified. This EU directive must be implemented into national legislation by June 2021.

Criminal law basis

Another controversial topic in the context of intellectual property theft is software. Computer programs are not patentable. This is laid down in Section 1 Subsection 4 PatG (German Patent Act) and Art. 52 EPC (European Patent Convention). "Computer-implemented inventions", on the other hand, are patentable. These are computer programs that solve concrete technical problems. However, the distinction between these two constructs under patent law is blurred. If one looks at software from a copyright law perspective, the source code itself enjoys protection, since it represents a copyrightable performance. Thus, in the case of source code or software theft, one must always check whether there is a patent for a computer-implemented invention or whether copyright in source code can be considered (cf. Brodowski/Freiling 2011).

### Forgery of data of probative value

This section was a legislative response to the inapplicability of Section 267 of the StGB to digital data. Section 267 of the StGB deals with the forgery of documents. However, it refers to a physical document, which means that it does not apply to digital data. In response to this, Section 269 of the StGB was introduced (cf. Singelnstein 2011). This section prohibits the storage or alteration of data of probative value to create a document that is perceived to be false or falsified for the purpose of deception.

To get the idea, imagine an attacker who creates an account on an auction platform under an arbitrary user name. The attacker uses false personal data to create this account. It then auction off various items and retains the money received in advance without ever sending any goods. A similar case was brought by the Berlin Appellate Court in connection with Section 269 of the StGB. In this case, the necessary data for registration constitute data of probative value. This data was stored on the platform, giving rise to the perception that a genuine document exists. In addition, the attacker obviously acted in such a way as to deceive future buyers (Case No. NRÜ 2011, 507).

Presumably, this example would also fall into the category of identity theft and involve some of the sections presented. However, a similar case has also been submitted to the Higher Regional Court of Hamm. In this instance, no criminal liability under Section 269 of the StGB was established. This applicability has therefore not yet been conclusively clarified (Case No. StV 2009, 475).

Under certain conditions, a phishing email, for example, could also fall within the scope of Section 269 of the StGB (forgery of data of probative value), insofar as the email is intended to create the impression of let’s say a contacting attempt from an ofﬁcial bank. This gives the impression that a contractual relationship exists between the victim and the attacker. Once the password has been sent to the attacker and the latter has logged on to online banking, the attacker can act in the name of the victim and initiate transfers

§ 269 StGB

Section 269 of the StGB describes document forgery in the digital space.

Data of Probative Value

Data are of probative value if they possess the characteristics of a document. The data must therefore provide the viewer with proof of identity.

or other banking transactions. The mere advertising of a product or service does not constitute forgery of data of probative value, as no forged data is used (cf. Singelnstein 2011).

An example of the legal proximity to the primary Section 267 of the StGB is the account number alteration on the magnetic stripe of a bank card. Having undergone this change of data, the perception of the account number on the magnetic stripe of the card would constitute a forged document.

### Computer fraud

Computer fraud is regulated in Section 263a of the StGB. This section was included in the StGB at the same time as the section on the forgery of data of probative value and also serves the purpose of closing a criminal liability gap in relation to computer crime. In this case, the gap was discovered through Section 263 of the StGB which regulates fraud. In electronic data traffic, this section ﬁnds no application. This is because there is no human recipient of the declaration since computer fraud is committed via data packets and these are received and processed by a data processing device and not by a human being. For this reason, Section 263a (Computer Fraud) was introduced (cf. Kraatz 2016).

263a StGB Section 263a of the StGB describes computer fraud. It refers to the act of influencing the result of a data processing operation with the intention of obtaining an unlawful pecuniary benefit.

Just like Section 263, Section 263a of the StGB on computer fraud is a pecuniary offense and aims at the unlawful pecuniary benefit of a third party or the pecuniary damage on the side of the victim. When committing an offense, the result of the data processing procedure is affected by the following actions (Section 263a subsection 1):

* Incorrect configuration of the computer program,
* Use of incorrect or incomplete data,
* Unauthorised use of data, or
* Unauthorised influence on the processing operation.

An example of the unauthorised use of data is a case tried before the Cologne Higher Regional Court: a person orders an airline ticket and provides their own account information. The person is aware that the account is not funded and that there is no overdraft facility. Thus, the payment cannot be processed successfully. Following the order process, the person prints out the airline ticket, goes to the airport, and takes the flight. According to the Court, Section 263a of the StGB was applicable here, as the person provided their own account data without authorisation (Case No. RBs1 172/15).

Another example of the possible applicability of Section 263a of the StGB is a scam where several people try to elicit the bank cards, including PINs, from elderly persons. This involves faking telephone calls in the name of the bank and requesting the PIN under the pretense of replacing the bank card.

Criminal law basis

Using this bank card, withdrawals are then made at the ATM. Whether this case falls under Section 263 or 263a of the StGB is controversial. The Federal Court of Justice ruled in favor of the applicability of Section 263a of the StGB (cf. Kraatz 2016).

The interpretation of Section 263a of the StGB proves to be extremely difficult in many judgments, as the wording "unauthorised" is criticized in the literature as being "too vague". Section 263a of the StGB has thus become one of the most controversial sections of the StGB (cf. Kraatz 2016).

With all the offenses presented in this unit, it is important to keep in mind that in many cases, the victim and the offender act in different countries, making German or European jurisdiction usually not the only relevant jurisdictions. This makes the assessment more complex. In these cases, the law of both locations, that of the perpetrator and that of the victim, is applicable. However, the characteristics of crimes involving computers or the internet give rise to other problems. These include, for example, pieces of evidence that, in the case of internet crimes, do not necessarily have to be situated in the perpetrator’s or the victim’s physical location. Evidence, such as connection data from servers or malware, can be distributed through cloud infrastructures not involved in the crime across many countries. Then there is the concealment of the attacker's actual location via remotely controlled servers or proxies. So, the first thing to do is to find out which jurisdictions apply at all. (cf. Kleijssen/Perri 2017).

Summary

In this unit, you have learned the criminal law basis related to computer criminality. Appropriation of identity does not have its own paragraph and is distributed among several criminal law paragraphs. Sections 202a, 202b and 202c of the StGB play an essential role. In summary, appropriation of identity is the theft of characteristics that clearly identify a person. In the context of computer crime, these can be passwords, email accounts, or digital keys. The misuse of these features constitutes the appropriation of identity. This offense is spread over several paragraphs in the German jurisprudence, although it is the opinion of the Scientific Service of the German Bundestag that there is no criminal liability gap.

Theft of intellectual property is also broadly defined. In German legal terminology, this is referred to as “law governing intangible assets” (intellectual property law). This complex issue is covered by ancillary criminal laws and divided into copyright law and competition law.

In contrast to the two previous areas, the forgery of data of probative value

is regulated in a separate criminal law section: Section 269 of the StGB, based on Section 267 of the StGB.

Computer fraud is similarly situated. It is defined in Section 263a of the StGB and emerged from the criminal liability gap under Section 263 of the StGB in relation to fraud. However, Section 263a of the StGB is worded differently in certain parts than Section 263 of the StGB, meaning that computer fraud can be applied in many cases.



# Unit 3

## Speciﬁc offenses

#### LEARNING OBJECTIVES

Upon completion of this unit, you will know ...

... what developments make data theft more likely.

... what attacks are used for digital blackmail.

... what a denial-of-service attack (DoS attack) is.

... how industrial espionage is distinguished from other crimes.

DL-D-DLMIMWCK01-L03

1. Speciﬁc offenses

### Introduction

Attacks involving IT systems and computers make it into the media time and again. Be it a misconﬁguration of servers that make millions of customer data openly accessible on the internet, as happened in the case of Buchbinder, or the hacker attack on the German Bundestag that presumably took years to prepare. These and other examples are explained in more detail below to demonstrate speciﬁc offenses surrounding computer criminality.

### Data theft

Data Theft

Data theft refers to the unauthorised acquisition of confidential or personal data by an attacker.

Cloud Storage Cloud storage describes a storage infrastructure that can be accessed via the internet.

Data theft occurs in various forms. Attacks on computers or IT systems are often preceded by data theft. The attack vectors for data theft have increased significantly in recent years, giving criminals much more opportunity. This is due to several technological developments in recent years. They include (cf. Marge/Iovan 2018):

* Internet-of-Things (IoT): The trend toward Internet-connected devices is leading to an increase in attacks on these potential targets. Medical devices, automotive control units, emergency call systems, and household appliances are now connected to the internet, with these types of devices accessing data from the public internet.
* Mobile devices: In addition, however, the smartphone is increasingly becoming a substitute for a desktop PC or laptop, resulting in some sensitive data, e.g. for payment transactions or access data for other services, being stored here. This makes the theft of this data all the more interesting for attackers.
* Cloud storage: The use of cloud storage results in the data being stored in a storage location that can be accessed via the internet. Cloud storage is used for current data, but also for back-up storage. The variety of storage locations increases the complexity of securing the data.
* Social networks: Social networks contain a large number of users. They are therefore interesting targets for attackers. Some of the data is publicly viewable. This allows an attacker to gather information. In addition, attackers can steal the data giving access social networks and then misuse them. This allows them to obtain further information or account data for other services.

For clarity, this section illustrates well-known examples of data theft that occurred in recent years. The data leak at the Buchbinder company in January 2020 has already been mentioned. This is an example of the increasing complexity of data storage and the associated effort to secure the data appropriately against unauthorised access. The Buchbinder company had rented a server from a service provider,

Speciﬁc offenses

on which ".bak" and ".log" files were periodically backed up. The file extensions suggest back-up files. The server or the associated firewall were incorrectly conﬁgured and port 445 of the TCP protocol was released to the public internet. This port is used for the Server Message Block (SMB) protocol and to transfer files, among other things. In addition, the SMB conﬁguration did not exhibit any authentication. Thus, access to the data was possible without overcoming this protective measure. A security researcher found the open port during routine scans of the public internet and published the data leak. The publicly available back-up files contained data on more than three million rental cars and their renters, including mobile phone numbers, email addresses, company correspondence, accident reports, and payment information. In addition, data on sensitive employers, ministries, embassies, or special task forces were included (cf. Heidrich et al. 2020).

In this example, the data leak was found by a security researcher and not by a criminal attacker. However, a different case was brought before the Berlin Regional Court. In this instance, an employee of an external IT service provider gained access to internal email accounts and passwords belonging to the Federal Ministry of Health. The defendant was the system administrator of the IT service provider who sold the email account data to the press spokesperson of the pharmacists' association, who intended to use the email correspondence to gain an information advantage. Both defendants were convicted under Section 202a of the StGB, and other provisions. (Case No. 39/13501).

The last example represents a series of hacker attacks on the German Bundestag and members of the German federal government. The German Bundestag was attacked several times, with the most extensive data appropriation having taken place in 2015. Over several months and years, a group of organised hackers had gained access to individual computers belonging to members of various parliamentary groups. They used manipulated emails, websites, and social networks. Access to individual computers was used to gain access to the Bundestag's internal network. Entire email correspondences and other internal data were accessed this way. The consequences of this data theft have not been conclusively clarified. The data could be used to blackmail members of parliament or to manipulate election campaigns (cf. Nicola 2019).

Protection against data theft is very diverse. Access, entry, and permission control is a start, but it must be implemented in conjunction with other measures.

### Digital blackmail

Digital blackmail is multifaceted and refers to an attack via the internet or other computer systems which is not terminated until a ransom is paid. One example is a DoS (Denial-of-service) attack on a corporate system. An attacker may, for example, restrict the accessibility of a company website through a large number of accesses (denial-of-service) to such an extent that customers are no longer able to call up the website.

TCP Protocol

The TCP protocol (Transmission Control Protocol) is used to exchange data. TCP establishes reliable connections.

Server Message Block Protocol (SMB)

The SMB protocol is used for file, print, and other server services.

Digital Blackmail Digital blackmail is an extortion carried out via computers or the internet. The attack only ends when a ransom is paid.

SMB Shares

An SMB share makes files available in networks. Permissions can be set up for individual users or groups.

The attacker then demands a ransom to restore accessibility. Effective defenses against DoS attacks are now in place, such as scrubbing centers, which pre-ﬁlter access and use patterns to filter out DoS attacks. According to the German Federal Criminal Police Office (BKA), ransomware has become an established method of digital blackmail. (cf. BKA 2020).

As soon as ransomware becomes active on an IT system, the malware starts to encrypt files on the system. This involves the use of cryptographic methods (e.g. AES256) making it impossible to decrypt the data without the corresponding key. After restarting the system, the victim is then presented with a screen that indicates the encrypted data and that the key will only be revealed if a ransom is paid.

Some variants of ransomware not only encrypt the initially infected system but also actively search the network for other accessible files. One example of this is the further encryption of SMB shares. In this process, ransomware is combined with the functionalities of a worm, as happened in "Petya". The "Petya" malware encrypts systems and at the same time spreads independently in the network. This makes the infection of further systems possible, provided that certain vulnerabilities are present in them. The ransomware thus moves through the network and encrypts the accessible data (cf. Oberly 2019).

In the immediate aftermath of the attack, the affected organisations are faced with IT systems not functioning properly and encrypted data. One solution, in this case, is to reinstall the infected systems and back up the data. However, the ability of worm-like ransomware causes online back-ups to be encrypted as well. Online back-ups are back-ups accessible via an organisation's network. These are accessible to ransomware and thus offer no protection against encryption. Effective protection against current ransomware is only provided by back-ups with the following properties (cf. Oberly 2019):

* Complete: All important data in the company must be backed up. As soon as a part is missing, it is lost after a ransomware infection.
* Up-to-date: Back-ups must be created at short, regular intervals. The data accumulating between back-up cycles is lost in the event of a ransomware attack.
* Ofﬂine: Back-ups must be kept separate from the corporate network.

Caution is advised when obtaining the key by paying the ransom. Often, the attackers do not hand over the key even after a ransom is paid. In addition, it should always be verified whether there is a decryptor for the ransomware. Some variants of ransomware exhibit vulnerabilities in their cryptograﬁphic methods, making it possible to find out the key with the help of a decryptor and an encrypted file. The "No more ransom!" project provides an overview of existing decryptors (cf. The No More Ransom Project 2020).

Speciﬁc offenses

There is now even a "division of labor" between the different types of malware. The "Emotet" malware in conjunction with "Ryuk" is an example of this phenomenon. "Emotet" spreads via forged emails and gives attackers access to infected IT systems. This access is sold to the criminal operators of another malware called "Ryuk." This is an encryption Trojan and thus belongs to ransomware. The operators of "Ryuk" use this access to manually gain an overview of the victim. If the infected IT system is part of a worthwhile corporate network, "Ryuk" is installed via the "Emotet" access and the encryption begins (cf. Adloff 2020).

### Computer sabotage

The act of computer sabotage is regulated in Section 303b of the StGB. Accordingly, computer sabotage includes interference with data processing operations which are of substantial importance to another. This can be done by altering data or by destroying or rendering the data processing system unusable. This section on computer sabotage, together with Section 303a of the StGB (data manipulation), is classified as virtual property damage and was enacted as part of the Act to Combat Economic Crime.

The previously described offenses require access by the attacker to the affected system to commit data theft or deactivation. Computer sabotage offenses are possibly committed when viruses, worms, or other malicious software are active on a system. Once ransomware has encrypted data, data processing operations may also be disrupted. Computer sabotage also includes the transmission of data with malicious intent. This does not require direct access to the system. This passage of the law is particularly aimed at DoS attacks, as they can be carried out without special access to a system. Servers that have fallen victim to an attack are usually accessible from the public internet, and data is transmitted to these servers. In a DoS attack, however, data is sent with malicious intent (cf. Koch 2008).

During a denial-of-service attack, the attacker deliberately creates the overload of a victim's system. A large number of requests is sent to the target system that cannot process this flood of requests. This works, for example, with websites or web applications accessible from the public internet. These services receive legitimate requests from the actual users of the services. The attacker does not need special access to the system (cf. Crelin 2020).

Simple DoS attacks are launched from a single computer. As a result, defending against an attack is relatively trivial, given that after a certain number of requests, the attacker's IP address is blocked and the system no longer processes the requests. The term distributed denial-of-service attack (DDoS attack) applies when DoS attacks are carried out by multiple computers.

Decryptor

A decryptor is used to decrypt data that has been encrypted by ransomware.

Computer Sabotage Computer sabotage describes the disruption of the functionality of IT systems.

This situation makes the defense considerably more difficult, as the requests of legitimate users are difficult to distinguish from DDoS requests. In the beginning, DDoS attacks were coordinated actions by activists who called for mass visits to a specific website. Nowadays, criminals build or rent botnets. These botnets consist of a large number of mostly infected computers that can be controlled by malware. As a result, all computers in a botnet can be used for DDoS attacks (cf. Crelin 2020).

One example of a DDoS attack that was tried before the Cologne Regional Court was an attempt by a defendant to exploit a gap in certain routers. The defendant was given the task of attacking a telecommunications company from Liberia via DDoS. In return, they were to receive a five-digit euro amount per month. Using the internet, they downloaded the source code of the "Mirai" malware and modiﬁed it. The modiﬁcation was designed for remote maintenance of the routers via port 7,547. Following contact with the routers and via manipulation of the timing information, the malware was to be installed. The corresponding vulnerability in the TR-069 protocol was published shortly before the attack was carried out (Case. No KLs118 4/17).

Remote Maintenance Remote maintenance functions enable the execution of device functions from a distance.

The botnet was to grow by infecting more routers starting from routers that had already been infected. The infected routers were then to launch regular DDoS attacks on the Liberian telecommunications company. Among the routers targeted were models from the "SpeedPort" series, which are issued to end customers by Telekom AG. However, these routers communicated with a special version of the TR-069 protocol. Specifically, a query was sent to a Telekom server for each remote maintenance request. These queries did not affect the Telekom routers. However, the volume of queries caused the routers to crash. As a result, the end customer's internet connection was blocked and telephony, internet, and IP-based television were no longer available. The defendant was convicted under Section 303b of the StGB (Cas No. KLs118 4/17).

Defense against DoS attacks always involves the differentiation between legitimate requests and malicious requests. This is usually easier with DoS attacks, since only one IP address sends the requests. In the case of DDoS attacks, there are products from various manufacturers that use pattern recognition to try to forward only legitimate requests to the system in question.

Computer sabotage not only includes DDoS attacks but was also used, for example, in the case of the "Sasser" worm. This spread via emails and caused infected computers to shut themselves down at irregular intervals. Among other things, this severely restricted the data processing operations of the affected banks. On 8 July 2005, the Verden Regional Court sentenced the defendant pursuant to Section 303b of the StGB.

Speciﬁc offenses

### Industrial espionage

Industrial espionage refers to the act of spying on an enterprise. This can be performed by a competitor or an individual. Industrial espionage comes in different forms, such as competitor espionage, company spying, or factory espionage. Industrial espionage has its criminal law basis in Section 17 of the German Act against Unfair Competition (UWG or Act against Unfair Competition), the Betrayal of Business or Company Secrecy, or the digital environment of Section 202a of the StGB, the act of data espionage.

The goal of companies or individuals engaged in industrial espionage is to increase or maintain their own competitiveness or market power. Information on innovations, cooperation efforts, or price calculations for tenders can be the target. Industrial espionage must be distinguished from economic espionage carried out by intelligence or secret services. This is usually directed or supported by the state and can also be punishable by law. Legit forms includes market research and competitive intelligence (cf. Hofer/Weiß 2016).

In a classic case of industrial espionage, a medium-sized company from Carinthia produced control software for wind turbines. The development took several years and after a short time, the software was found in the Chinese products of a competing company. A senior employee had sold the source code for 15,000 € and a work contract with the competitor. For the Carinthian company, this meant a loss of millions and the dismissal of a quarter of the workforce (cf. Hofer/White 2016).

Industrial espionage in relation to computer crime has been on the rise in recent years. In the “Bundeslagebild Cybercrime” (Federal Report on cybercrime) published by the German Federal Criminal Police Office (BKA), 68% of industrial companies stated that they had been victims of industrial espionage, sabotage, or data theft in the past two years (cf. BKA 2018).

An example of industrial espionage by means of computer crime is the attack on BMW in 2019. What is suspected to be a Vietnamese hacker group forged web pages that were modeled on the Thai website of BMW. By doing so, they succeeded in installing the "Cobalt Strike" software on some computers. This software is usually used to show the effects of malware infection and, accordingly, is not malware itself. The attack lasted for several months before BMW noticed the intruders. However, the systems were not shut down immediately, but rather a forensic investigation was launched. This aims at gathering information on the attackers and the appropriated data. According to the investigation, the attackers also targeted other carmakers, e.g., Hyundai (cf. Tanriverdi/Streule 2020).

Industrial espionage requires a much more discreet approach on the part of the attackers since data is to be collected over a long period of time. This also slows down movement within the network, since only few or no traces may be left behind.

Industrial Espionage Industrial espionage refers to espionage between companies. Confidential information is stolen in the process.

Competitive Intelli- gence

Competitive intelligence describes the active collection of information on a competitor. In the process, all activities remain in the legal sphere.

Forensic Examination

A forensic investigation seeks to secure traceable evidence and build a conclusive chain of evidence.

Summary

In this unit, you have been introduced to speciﬁc examples of computer crime

offenses.

Data theft was explained at the beginning. This is facilitated by some current technological developments, such as IoT, mobile devices, and cloud storage.

Data theft can occur in different ways and is usually the precursor to other crimes.

Digital extortion describes attacks on computer systems that end only after a ransom is paid. The type of attack can vary. The use of ransomware is widespread. In this case, data is encrypted in such a way that the victim can no longer use the data.

Computer sabotage is an offense that describes the disruption of data processing procedures and became part of the StGB in order to cover, among other things, DoS attacks. This type of attack uses a large number of service requests to overload the system.

Industrial espionage tends to be committed inconspicuously and over a longer period of time. In this case, enterprises are spied on by their competitors.

Computer crime is a fundamental challenge for legislators. A well-known topic in Germany is the debate about "Freifunk" (free networks) and the herewith associated "Störerhaftung" (Breach of Duty of Care). A 2017 law was intended to enable the operation of a free WLAN hotspot without the threat of warnings. However, in a recent court case, a 70-year-old woman was convicted of infringing Warner Bros. Entertainment's copyright through activities on a file-sharing site. The defendant does not have a computer or any knowledge of file-sharing sites. The action was presumably carried out by a resident of the house who also uses the connection (Case No. 148 C 400/19). Computer crime offenses are thus part of the current development of legislation and political debate.



# Unit 4

## Attack vectors

#### LEARNING OBJECTIVES

Upon completion of this unit, you will know….

... which attacks can be launched on processors.

... which basic protective measures are implemented by operating systems.

... which attacks are carried out in a network.

... which attacks threaten applications, especially web applications.

... how an attacker can attack at the organisational level.

DL-D-DLMIMWCK01-L04

1. Attack vectors

### Introduction

Once a company has commissioned penetration testing, the contracted service provider starts collecting information and probing for any potential methods of attack on that company. The penetration tester could, for example, steal employee passwords with forged emails or use prepared USB sticks to infect internal computers. They could also examine applications released to the internet for vulnerabilities in order to ﬁnd a way into the internal network. After penetrating the internal network, the next goal may be to gain elevated privileges. For this purpose, attacks are launched at the network level, or operating systems that have not been updated are exploited. In the case of Internet-of-Things devices or industrial equipment, attacks are also carried out using vulnerabilities in the firmware. The penetration tester looks for possible attack vectors through which a system, network, or a last-mentioned device might be attacked. Attack vectors always combine an attack path and an attack technique (cf. BSI 2019a).

The following are examples of possible attacks that you can try out yourself.

For example, Kali Linux can be used as a virtual machine for this attack simulation.

### Chip and firmware level attacks

Hyperthreading Hyperthreading executes multiple processes on one physical processor core. The implementation is closer to the hardware than multithreading.

Attacks at the chip level form the beginning of the attack vectors. Chips are processors in modern computer systems. An example of an attack at the chip level is the ZombieLoad attack. The attack exploits the feature of current processors where several virtual processors are emulated on one physical processor core (hyperthreading). This means that one physical processor processes several threads simultaneously. Hyperthreading brings speed advantages because the physical processor can be utilized more.

The ZombieLoad attack involves an attacker executing its own process on one of the virtual processors. This process can then read out data from another virtual processor. This is possible because modern processors perform so-called out-of-order execution and speculative execution. These features are also used to increase the speed of processors. In the process, out-of-order execution and speculative execution deviate from the specified order of instructions without changing the end result. As a result, these instructions can be distributed in parallel on the processors and processed in advance, thus speeding up the entire instruction chain. These (pre)calculations can therefore be useless under certain circumstances. The results of these two variants are stored in a special buffer. If an error occurs, this cache is emptied (cf. Schwarz et al. 2019).

Attack vectors

The ZombieLoad attack reads this buffer and can thus access data from other processes running on the same physical processor. Accordingly, the attacker cannot directly identify the read data. Theoretically, it is possible to read the passwords of an administrator account or secret keys for other applications. This puts ZombieLoad in the category of side channel attacks (cf. Schwarz et al. 2019).

A side channel attack extracts data via side effects. These are observable effects that occur during the processing of data. The different types of side channel attacks are illustrated in the following table:

|  |  |
| --- | --- |
| Types of side channel attacks | |
| functional | physical |
| micro-architectural | Power consumption |
| cryptograﬁsch | electromagnetic |
| Memory usage | Timing |
| Packet tracing | User interaction |
| Keylogging (software-based) | acoustic |
|  | optical |
|  | thermal |
|  | Network interference |

During decryption, for example, an attempt is made to keep the calculation time identical in order to avoid a side channel attack. This is because this time required for decryption can provide information on the key used or the procedure. With the possibility to measure the power consumption of a processor, a conclusion can be drawn about the procedure or the key even if the time needed for the calculation is the same.

The ZombieLoad attack presented is based on a microarchitectural side channel attack and the way buffers are used in processors. Examples of side channel attacks date back to the 1960s. This was when typewriter strokes caused out-of-order execution and speculative execution via the electrical noise they created.

Out-of-Order Execu- tion and Speculative Execution

These two techniques speed up the execution of processes by increasing the workload of the processors.

Side Channel Attack A side channel attack uses side effect observations of data processing operations to extract information.

Other possibilities include breaking cryptograﬁc processes by measuring the power consumption in various encryption and decryption processes.

Firmware Firmware forms an interface between hardware and further software. This software can be an operating system or an application software.

EFI

The Extensible Firm- ware Interface (EFI) is an interface for computer ﬁrmware and the successor of the BIOS.

In addition to attacks at the chip level, attacks also exist at the firmware level. Firmware comes in many varieties and the borders are fluid. Generally speaking, firmware is software that provides functions of various hardware elements at a level close to the hardware. Further software then builds on the firmware and uses the corresponding functions of the hardware. Software systems in this context are operating systems or other application software. Firmware is found in a wide range of hardware, e.g.:

* Consumer products:
  + Home appliances,
  + Multimedia devices,
  + Automobiles, and
  + Smartphones.
* Computer components:
  + Hard disks,
  + Graﬁk cards, and
  + Mainboard.
* Network components:
  + Router and
  + Firewall.
* IoT devices:
  + Cameras and
  + Wearables.

In many systems running their own operating system, the firmware loads the operating system after its launch. An attacker controlling the firmware also controls the operating system. For this reason, for example, "EFI" was introduced for Windows computers from Windows 8 onwards. "EFI" supports the Secure Boot feature, which ensures that Windows only boots from previously signed boot loaders in the firmware. This means that any changes to the boot loaders are detected, preventing Windows from booting. The firmware thus forms the beginning of a chain of trust that extends to the application software (cf. Morel/Courousse 2019).

A study on implantable medical devices offers an example of inadequately secured firmware. These devices do not store the corresponding firmware in protected memory areas, nor is the authenticity of the firmware verified. Additionally, update functionality and servers are not secured, allowing an attacker to modify the firmware of a corresponding device for its own purpose and roll out the update to all affected devices (cf. Rios/Butts 2017). Other examples are vulnerable "smart" coffee machines, which an attacker can use to mine cryptocurrencies (cf. Goodin 2020).

Attack vectors

Chip and firmware level attacks exist and are steadily increasing due to the Internet-of-Things trend. As firmware updates are less frequent than application or operating system updates, outdated firmware is thus used. This gives attackers an advantage.

### Operating system level attacks

The borderss between the operating system level and the firmware level are fluid. An operating system is an interface between application software and the firmware. In some cases, the firmware is integrated into the operating system, allowing the operating system to access the hardware directly. In this context, an operating system performs the following tasks:

- Display of the graphical user interface,

- Resource management,

- Process management,

- File management, and

- other tools.

Operating systems are designed to run many applications simultaneously. Under the assumption that "applications are vulnerable in principle", operating systems must protect resources and the processor. Two basic defense mechanisms are used for this: rights separation and virtual memory management. These two mechanisms represent a major target for attacks at the operating system level and are briefly explained below.

Modern operating systems assign part of the application memory as virtual memory. The application accesses deﬁned memory areas. However, the individual memory areas can be distributed over several hard disks and main memory. The operating system "translates" the application's accesses into the effective memory locations and returns the stored values. Each time an application accesses memory, verifications are performed to determine whether this application is accessing its own memory area (cf. Gens 2019).

In addition, modern operating systems feature a strict rights separation. Operating system processes operate at elevated rights compared to user processes. Users cannot read or modify certain areas of memory, use certain network interfaces, or execute some commands. However, it is possible for a process to alternate between different levels of privilege as it runs. If a user program crashes, the error response is partially executed with the most elevated rights to allow the operating system to terminate the user's process. This, together with virtual memory management, results in a strict separation between applications on the same operating system and also between the operating system and the applications.

Operating System

An operating system makes the resources of a system (such as memory, hard disk, and main board) available to the application software.

Rights Separation

Rights separation implies the use of different functions and memory areas for different processes.

Virtual Memory Management

This feature allocates a virtual memory to each application, which can be arbitrarily distributed on the physical memory.

Privilege Escalation During a privilege escalation, an attacker gains elevated rights compared to those previously held. This allows the attacker to use more and higher-value functions of the system.

Race Condition A race condition occurs when a program depends on the timing of individual instructions for correct operation.

The attacker's goal may be to break out of the initially infected application.

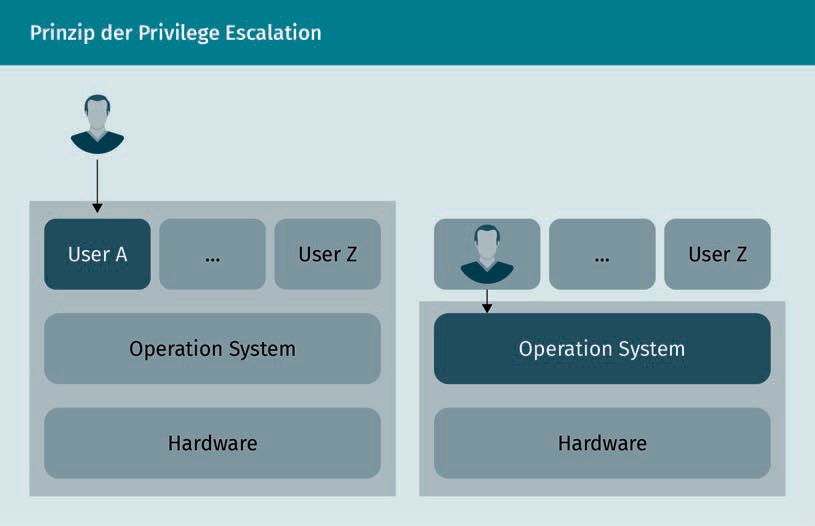
Such attack type is referred to as privilege escalation. In this case, an attacker can

control or start processes with elevated rights. The result is the use of "higher-level"

functions of the operating system, for example, to use the network interfaces for its

own purposes (cf. Gens 2019).

The introductory example already implied that, in the first step, the attacker obtains the rights of a user in order to then perform a privilege escalation. This means that the attacker will want to elevate its rights to a higher level. For example, an attacker will first launch an attack on an externally accessible application, such as a web server or a file share. As soon as the attacker has gained the rights of a user, attacks on the operating system are usually used for privilege escalation. The procedure is illustrated in the following figure (cf. Gens 2019 ):



An example of an attack at the operating system level is Dirty COW. The Linux operating system kernel contains a vulnerability in the copy-on-write (COW) function. The attack on this vulnerability is called Dirty COW in reference to this function. This vulnerability is susceptible to a race condition at its core. Commands can be executed in the "wrong" order during execution. In the case of Dirty COW, this allows for the creation of a new user with elevated rights, including the associated password. If an attacker can successfully execute this attack, it has gained root privileges. By default, the user root on Linux systems is equipped with the most elevated rights (cf. Farah et al. 2017).

To test this type of attack, the "Kioptrix4" virtual machine by Vulnhub can be used together with a Kali Linux system. Access with "normal" rights can be obtained from "Kioptrix4" via an SQL injection.

Attack vectors

Dirty COW can be used to increase rights. After downloading the code for Dirty COW it can be compiled with *gcc -pthread dirty.c -o dirty -lcrypt*. After that, the compiled file is transferred to the "Kioptrix4-VM". There, this file must still be given the execute right via *chmod +x dirty* and the attack must be executed via.*/dirty*. The following output shows the back-up of the file */etc/passwd* and the creation of a new */etc/passwd* with a new root user and the displayed password. The attacker has thus gained elevated rights (cf. Bond 2020).

The vulnerability used in the Dirty COW attack has been present in the Linux kernel since 2007 and was not completely removed until November 2017. Thus, the Linux versions were vulnerable during this period. Given that Linux is used, among other things, for web servers due to its low cost and that these systems are rarely patched, this attack is still successfully carried out today to achieve privilege escalation. Successful attack methods on the operating system level affect all systems with identical operating system status. These attacks work even after a long time if the systems are not continuously updated in a timely manner.

### Network and server level attacks

A network generally connects several systems with each other. These networks can take on different sizes and be closed or open. The internet is one of the largest networks. In most organisations, individual, separate networks are created, which then have specific transfer points and are partially connected to the internet. Attacks on networks can be launched externally or internally.

External attacks are launched from a system outside the network. The most common type of an external attack is the one launched from the internet against a system in the internal network. Internal attacks are launched from a system on a network to a system on the same network. An example of this would be an inside attacker or an attacker who wants to extend their attack inside a network. In addition to the division into external and internal attacks, attacks can be divided into a further seven types (cf. Sharma/Kavita/Agarwal 2019):

Eavesdropping attacks are the first type of attack. In a network, data is exchanged between the different systems. This data can be eavesdropped on in various ways. For example, an internal attacker could eavesdrop on part of the network communication. But this type of attack can also be carried out from the outside. Suppose a system on the network stores a log file about the communication on the network, and this file is accessible through a false conﬁguration via the internet on a web server. An attacker that ﬁnds this file can then launch an eavesdropping attack even from the outside. One measure against eavesdropping attacks is encryption. Even if an attacker eavesdrops on encrypted communication, the only way to obtain usable information is to possess the key.

Eavesdropping Eavesdropping attempts to steal data unnoticed.

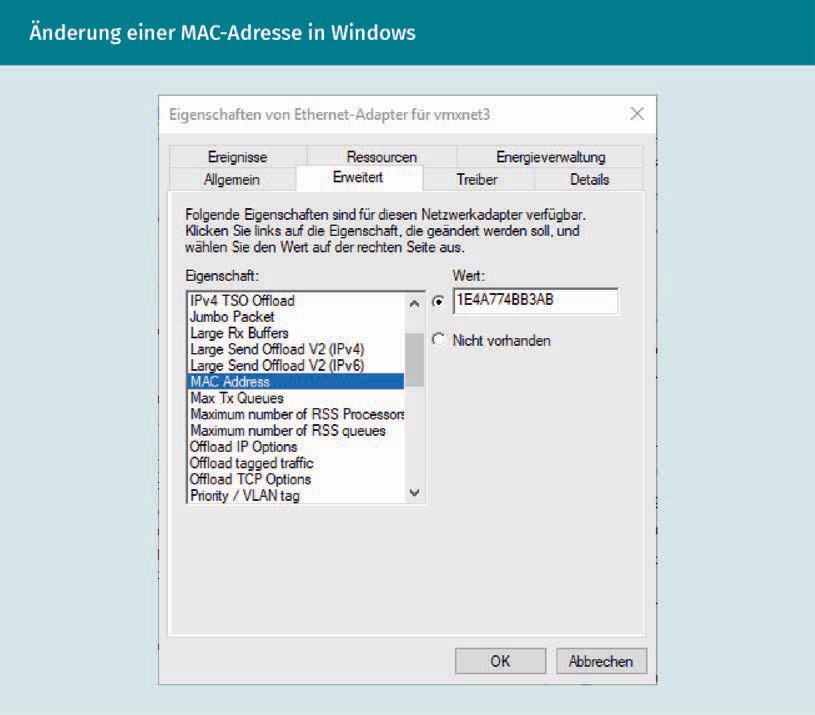
In addition to passive eavesdropping, the modiﬁcation of data turns into an active attack. Provided an attacker has access to data, it can change it at will for its own purposes. The attacker can modify data in transit or while stored in databases or files. For example, an attacker can change the address of an online order to its own address or change the ID of a wallet in a Bitcoin transaction. A virus can modify system files on an infected system in such a way that an attacker can gain access to the system at any time. Modiﬁcation of data can be abused by an attacker in several ways. Usually, this type of attack is relatively conspicuous since data modiﬁcation leaves traces.

Spooﬁng Attack In a spooﬁng attack, an attacker pretends to be another user or system.

Spooﬁng describes a type of attack in which the attacker pretends to be another user or system. The most common form in networks is based on the TCP (Transmission Control Protocol) and IP (Internet Protocol) protocols. Each system has an IP address for identiﬁcation. If an attacker assumes the IP address of another system in the network, the attacker can impersonate that system. Two same IP addresses are not allowed in a network range. However, if a system is shut down and the attacker impersonates this system immediately afterward, spooﬁng can work in this example. Another feature used to identify systems is the media access control (MAC) address. It is assigned to the network adapters produced and is unique throughout the world. The MAC address is used, for example, to restrict access to networks (MAC authentication). Because the MAC address can be changed in the operating system, it is relatively easy to spoof. If an attacker knows the MAC address of a device that has access to the network, the attacker can spoof this MAC address and gain access to the network.

The spoofing of the MAC address can be performed on a Windows system by starting the device manager, searching for a network adapter, and opening the properties via right-click (see the following figure). At this point, any MAC address can be entered. Under Linux, command-line programs such as macchanger enable this conﬁguration.

Attack vectors



In networks, authentication is required for functionalities that are only available to a limited group of users. One form of authentication is, for example, the combination of user name and password. The next type of network attack is based on this form of authentication: password attacks. There are several ways to obtain a user's password. The attacker can elicit the password from the user via a phishing email or use a dictionary attack to guess the password. Dictionary attacks make an attempt to guess a user's password by collecting passwords in a dictionary and then trying them out.

Following a successful password attack, the attacker has access to the victim's user account. This can lead to a situation where the attacker can carry out a spooﬁng attack, posing as the victim within the network. For example, emails can be composed or actions can be launched in the victim's name. If the account has elevated rights within the network, the attacker will also have elevated rights after the successful password attack. In the worst case, this allows the attacker to reset all passwords across the network, view all information on systems, users, and applications, and perform any action. For example, if an attacker gains access to the administrator account of a domain controller in an organisational network through a password attack, it enables the attacker to view, modify, and control the entire structure of the network with computer accounts, services, and user accounts.

Password Attacks

A password attack takes advantage of the fact that passwords are guessable using dictionaries, substitutions, or by way of mindless trial and error.

Dictionary Attack In a dictionary attack, values (e.g. usernames to use or passwords) are taken from a dictionary to guess the correct values.

Key-Recovery Attack   
In a key-revovery attack, a cryptograﬁc key is used to view encrypted information in plain text or to mimic a digital identity.

Man-in-the-middle In a man-in-the-middle attack, the attacker is logically in a position between two communication participants and listens in or manipulates their communication.

In this case, the attacker has control over the organisational network

One type of attack that does not require access data is the denial-of-service attack (DoS attack). In this attack, a service such as a website is disrupted (denial) rendering this service unavailable to users. This type of attack aims to overload services within a network and make them inaccessible to users. It can stand alone and be used for digital blackmailing. Attackers also use DoS attacks to divert attention from other attacks or to make their tracks harder to trace. While a service is overloaded and the attention of the organisation's administrators is on that service, the attacker can gather information and attack other systems. A denial-of-service attack can be carried out at high data rates causing network connections to become overloaded. However, it is also possible to block a service account by performing multiple false authentications with the account. If, for example, an organisation uses its own service account to access an SQL database and an attacker makes several attempts to log in to this account with an incorrect password, the account will be locked after a certain number of incorrect logins and access to the SQL database will be blocked for other applications using this service account as well.

Key-recovery attacks are another type of attack. A key is a string of characters that is known only to a limited group of users and is used to encrypt and/or decrypt data. Keys are sometimes generated by humans, but can also be automated by applications. Once an attacker obtains a key, that person can decrypt encrypted communications and thus read the messages sent in plain text. Depending on the application, it is even possible to imitate the owner of the key. This makes then a combination with a spooﬁng attack.

In the man-in-the-middle (MitM) type of attack, the attacker has gained the ability to intercept, modify, and resend communications between two network participants such that neither of the two original participants notices this attack. This type of attack requires that the attacker is able to reroute messages sent by the sender to themself and then forward them to the receiver. MitM can come with key-recovery attacks if, at the same time, the attacker is able to make both participants think that the identity of the other is credible, provided that there is authentication between the participants (cf. Sharma/Kavita/Agarwal 2019).

An example of a MitM attack operating on many Active Directory networks is Link-Local Multicast Name Resolution protocol (LLMNR) poisoning. After successfully infecting a system within that network, the attacker's goal may be to infect additional systems or gain more elevated rights. One way to do this is by exploiting the LLMNR protocol. This is a Microsoft alternative to name resolution in networks, which usually works via DNS (Domain Name System).

Attack vectors

If a system in a network does not find a resource it is searching for via DNS, this system can query other systems in the immediate vicinity to obtain the resource. Thus, the system infected by the attacker would also be asked for the resource. This system responds with knowledge of that resource. To access this resource, authentication with the NTLM hash of the user password of the requesting system is necessary. The attacker thus obtains this hash and can use it to attempt an impersonation of the requesting user across other services or servers in the system. The attacker intercepts a communication from one system A and forwards it to another system B in order to pretend to be system A there. This can then lead to the compromising of system B.

The attack types presented in this section outline the options available to an attacker in networks. The types of attack overlap to some extent. For example, a MitM attack can also be a spooﬁng attack and requires a prior eavesdropping attack.

### Application level attacks

An application is software designed to perform a specific task, such as word processing, surfing the Internet, or playing solitaire. The large number of applications also means that there is a large number of possible attacks. In the next section, we will distinguish between applications and protocols using ports. This is intended to help structure these applications and protocols. For this, use is made of the so-called "well-known port numbers". A distinction is made between individual protocols within the TCP and UDP (User Datagram Protocol) network protocols using ports. In this context, the Internet Assigned Numbers Authority (IANA) defined the first 1,024 ports (cf. Reynolds/Postel 1992). The relevant applications within these "well-known port numbers" and the associated attacks are described below. Ports TCP/80 and TCP/443 are considered in more detail since these ports are aimed at web applications that represent major targets for attacks.

Among the 1,024 "well-known port numbers", the following are considered in more detail (cf. Reynolds/Postel 1992):

|  |  |  |  |
| --- | --- | --- | --- |
| Auswahl von Ports der TCP- und UDP-Protokolle | | | |
| TCP/UDP-Port | Abkürzung | Protokoll | Beschreibung |
| 20/21/22 | FTP/SFTP | (Secure) File Transfer Protocol | Dateiaustausch mit FTP-Servern |

Poisoning

A poisoning attack means that "poisoned" responses are sent back to the attacker in response to requests from a system, which represent an advantage for the attacker.

Well-known Port Numbers

This list of standardised ports represents the first 1,024 TCP/UDP ports with their associated protocols.

|  |  |  |  |
| --- | --- | --- | --- |
| TCP/UDP-Port | Abkürzung | Protokoll | Beschreibung |
| 22 | SSH | Secure Shell | erlaubt direkten Zugriff auf die Betriebssystem- Shell |
| 25 | SMTP | Simple Mail Transfer Protocol | Versand von E- Mails |
| 53 | DNS | Domain Name System | löst Hostnamen in IP-Adressen auf |
| 80/443 | HTTP/HTTPS | Hypertext Trans- fer Protocol (over TLS/SSL) | lädt Dokumente von Webseiten (CSS, HTML, Bilder usw.) herunter. |
| 110/143 (995/993) | POP3/IMAP  (over TLS/SSL) | Post Ofﬁce Proto- col/Internet Mes- sage Access Pro- tocol | Abholung bzw. Zugriff auf E- Mails |
| 137–139/445 | SMB | Server Message Block | ein Netzprotokoll für Datei-, Druck- und Server- dienste in Netz- werken |
| 1433/1434 | MSSQL | Microsoft-SQL- Server | Abfrage und Management von Microsoft-SQL- Servern |
| 1521 | OracleNet | Oracle Net | Abfrage und Management von Oracle-Daten- bankservern |
| 3306 | MySQL | MySQL Protocol | Abfrage und Management von MySQL-Daten- bankservern |

Attack vectors

The File Transfer Protocol (FTP) is used to transfer data. The basic version is unencrypted. The extension, the Secure File Transfer Protocol, uses the Secure Shell Protocol (SSH) to transfer encrypted data. Among other things, applications use FTP to exchange data. Attackers also use this protocol to spread malware. For example, the Didrex malware opens port 21 on infected systems and starts an FTP server which allows files to be transferred unnoticed. Some firewall conﬁgurations do not restrict connections on FTP ports. FTP has other vulnerabilities, especially when the conﬁguration is incorrect. An incorrectly conﬁgured FTP server allows anonymous connections, i.e., connections without a password or with the default password. In this way, the contents of the FTP server can be accessed and possibly modified without authentication. In the worst case, this can affect the entire content of the system.

The Secure Shell Protocol (SSH) is designed to use an operating system shell of a remote system. A shell makes the operating system's functions available via a command line. For an attacker, this means that accessing a system via SSH may provide full access to almost all of the system's functions. SSH can be secured with a username and password or with SSH keys. An attacker can search for SSH keys after gaining access to a system. Managing a large number of SSH keys creates a problem for organisations. In some cases, these SSH keys are distributed across many locations. Having an SSH key to a privileged account directly gives the attacker elevated rights within the affected system.

The Simple Mail Transfer Protocol (SMTP) is used to send emails. SMTP applications are mostly released to the internet and thus represent a target of external attacks. SMTP features the "VRFY" command to check the existence of a speciﬁc email address. The "EXPN" command is used to list the email addresses in a mail distribution list. This is exploited by attackers for the analysis of existing email addresses in an organisation. Since the email address is used as a log-in user name often, attackers can use this information in a profitable way.

Related to SMTP are the protocols for receiving emails: the Post Ofﬁce Protocol 3 (POP3) and the Internet Message Access Protocol (IMAP). Both are used to access the emails. POP3 downloads the emails completely from the server and then deletes them from it. Thus, these emails are only available in the respective email program. IMAP, on the other hand, leaves the emails on the server. There are always vulnerabilities in email applications that attackers can exploit to gain access to a system. Important information for attackers can be stored in emails. Examples include sensitive information such as passwords or keys. These allow an attacker to extend its rights or even access additional systems.

The Domain Name System (DNS) is an essential protocol for the functioning of the internet and many applications that communicate across multiple systems. Every time an internet user enters "www.google.de" in a browser,

FTP

The File Transfer Protocol is used to transfer data.

POP3/IMAP

POP3 and IMAP protocols are responsible for retrieving and accessing emails, respectively.

DNS

The Domain Name System is one of the foundations of modern networks and the internet. This protocol assigns IP addresses to hostnames.

HTTP

The Hypertext Transfer Protocol transfers HTML documents from a web server to the client. At the client, a browser usually displays the transferred documents.

Session Identiﬁcators

If an indentification feature for a website session (usually integrated into cookies) is predictable, an attacker can appropriate user identity.

the DNS protocol transforms this address into an IP address. Only with this IP address can web pages be downloaded and displayed in the browser. A vulnerability with a CVSS of 10.0 was discovered in the DNS implementation of Windows servers in July 2020. Apparently, this vulnerability had existed for 17 years and a correspondingly large number of systems are vulnerable to attack. In an attack, a crafted DNS request can be used to infect the server. Microsoft classified this vulnerability as "worm-capable" in that an infected server can send the same DNS queries to additional servers. An entire organisational network built on Windows servers can be infected.

Another basis of today's internet is the Hypertext Transfer Protocol (HTTP). It is used to download HTML documents that can then be displayed in the browser. HTML documents form the basis of web pages. The HTTPS protocol represents the encrypted variant of HTTP using Transport Layer Security (TLS) or, in the previous version, Secure Socket Layer (SSL). Servers that provide services via port 80 or 443 are called web servers. Web servers are often exposed to the internet and provide functionality for web applications. Users of these web applications send input to the webserver. This input data can be unstructured and potentially dangerous. Thus, web servers offer a preferred target for attackers and various attack options exist for this purpose (cf. Burato/Ferrara/Spoto 2017). The Open Web Application Security Project (OWASP) regularly publishes a list of the most critical risks for web applications. The first seven risks listed in the OWASP Top 10 are named and briefly explained below (cf. OWASP 2017):

1. Injection: Injection attacks attempt to execute program codes on the server via user input. This category includes, for example, SQL, OS, and LDAP injections. In extreme cases, this can lead to the execution of commands with elevated rights.
2. Broken Authentication: This includes a faulty implementation of authentication and session management. Attackers exploit vulnerabilities or use compromised user credentials (passwords and session IDs). For example, session identiﬁcators can be predictably generated or phished. This allows an attacker to assume the user's identity.
3. Sensitive Data Exposure: Sensitive data on web servers should always be secured. Attackers can otherwise view and modify this information. One type of attack is possible via path traversal, for example. In this case, data that cannot be accessed via legitimate functions of a web server may be accessible to an attacker. With path traversal, a path is composed of backward steps "(../)". Unintentional directory listing on web servers can also reveal sensitive data.
4. XML EXternal Entities (XXE): The XML External Entities feature within XML files can lead to the disclosure of internal files and information and execution of attacks via port scanning, remote code execution, and DoS.

Attack vectors

For example, interfaces used to upload files in XML format, e.g. ".docx" and ".xlsx", can be used to transfer arbitrary data from the webserver to the attacker.

1. Broken access control: Access rights for authenticated users are implemented incorrectly in some cases. This provides an attacker with access to functions and data, for example. This includes access to accounts and sensitive data as well as manipulation of user data and access rights. Many web applications also include functionalities for administrators, which must never be accessible to attackers.
2. Security Misconﬁguration: A web server consists of many frameworks, packages, and plugins. These must all be securely conﬁgured and patched. Outdated software versions mean that a wide variety of attacks can be carried out.
3. XSS: Cross-site scripting is a type of attack that involves inadequate implementation of validation or recoding of untrusted data. An example is the persistence of malicious JavaScript code by an attacker on a sales portal (analogous to Ebay). When a user visits this website, the code is automatically executed and, for example, the user's cookie (including the session ID) is transmitted to the attacker. Sensitive user data can thus be disclosed or functions can be executed on behalf of the user.

Web applications, therefore, offer opportunities for attacks. Thus, appropriate protective measures should be taken to secure web applications. The "Kioptrix2" virtual machine by VulnHub exhibits an SQL injection vulnerability in the login function. Upon accessing the web interface of this VM via the browser and *entering admin' or 1=1 #* in the username field, one has full rights on the web application as a logged-in administrator. This works because the expression *1=1* is always true and the hash symbol marks all other commands as commands. This is a form of SQL injection and will hopefully rarely work in real-world scenarios. More complex SQL expressions can also lead to successful attacks in modern web applications.

The Server Message Block (SMB) protocol is used to share various services in networks and is used by applications to address printers or use file shares. SMB gained a lot of notoriety due to the EternalBlue vulnerability. This vulnerability was discovered by the NSA and only used for internal operations for a few years. After the vulnerability was disclosed by a hacker group, the NSA publicized the vulnerability. The WannaCry extortion Trojan exploited the EternalBlue vulnerability to enable a global attack on 12 May 2017. At times, up to 300,000 systems were infected in this attack. This shows the serious consequences that a programming error in a widely used application can have.

Applications sometimes use a dedicated database to store data. Examples of databases are MySQL, Oracle Net, and Microsoft SQL. Even if attacks on an application are not possible or are unsuccessful, an attacker can view or modify data from an application if it gains direct access to the database. In some cases, an attack on a database is enough to gain full control of the operating system. For example, the "Forbot" worm exploited weak stan-

MySQL

The Structured Query Language is a language used for the modiﬁcation and querying of data in relational databases.

Organisational Measures

Organisational measures include policies such as standards, guidelines, directives, work instructions, role descriptions, specifications for the dissemination of information, and the organisational and procedural structure.

dard passwords and other functionalities of MySQL databases to gain access to the operating system. MySQL provides a feature called User Deﬁned Functions. Executing this option to deﬁne custom functions with the MySQL root user allowed files to be written locally into the system. In the case of the Forbot worm, a ".dll" file was written into Windows systems, which was then executed to identiﬁy the system with the worm. This approach is possible due to weak passwords of the MySQL root user, because the attacker "guesses" these passwords and thus possesses the user's credentials. This attack is a privilege escalation because non-existing privileges of the user deriving from the MySQL application turn into privileges in the operating system. Forbot achieved this initial access by using a list of common passwords for the root user. This dictionary attack was effective in many cases.

Besides the " well-known port numbers" applications and protocols outlined herein, others exist. However, the attack types remain partly identical. A dictionary attack on weak standard passwords or exploitation of implementation vulnerabilities also works for other applications.

### Attacks at the organisational level

Attacks at the organisational level refer to all attacks that exploit vulnerabilities in policies. Policies target information flows, role assignments, processes, and organisational structures and workflows. These organisational measures, together with the technical measures, are intended to increase protection against attacks. For example, an antivirus program reporting an attack on a system would be of less use. If the affected employee does not know whether and to which employee this information must be sent for prompt incident handling, the incident could have a negative impact (cf. BSI 2019a).

This example illustrates how attacks from the previous sections can increase the extent of damage due to a lack of organisational measures. However, there are also forms of attack that directly target the organisational level. The IT-Grundschutz Compendium of the German Federal Office for Information Security lists several forms of attack, briefly described below:

* Unauthorised entry,
* Exposure to outsiders,
* Destruction, vandalism, and sabotage,
* Theft and loss, and
* Social Engineering.

Within every organisation, vulnerable spaces exist. These contain information that needs to be protected in some way. An attacker with access to these spaces can view or manipulate information. Spaces that require protection include, for example, server rooms, data centers, and distribution rooms.

Attack vectors

Access to these rooms should be strictly regulated and additionally equipped with technical measures such as key systems and doors with appropriate resistance classes. If servers or other network devices such as firewalls, routers, WLAN access points, or switches are set up in rooms without access control, an attacker can gain unhindered access. As soon as an attacker gains physical access to a server, the attacker can, in the simplest case, switch off the server or disconnect the power supply, thus limiting the availability of services on the server. However, physical attacks on servers can also be carried out via prepared USB sticks or eavesdropping devices. In addition to server rooms, home office workspaces or archives can also be spaces in need of protection. Of course, any area with access to information, e.g., via the network, is worth protecting; this includes any office workstation with a PC or customer information systems in public areas.

Another potential attack factor is the danger of external persons from outside the institution. These include, for example, visitors and cleaning or maintenance staff. It cannot be assumed that these outsiders will handle information in accordance with the institution's policies. An organised attack group (sometimes also referred to as an advanced persistent threat (APT)) could place its members in service ﬁrms and thus gain access to information by means of information outsider status. Since offices need to be cleaned, a lot of information can be collected by plugging hardware keyloggers into USB ports, for example.

Destruction, vandalism, or sabotage can be perpetrated by both internal and external attackers. Vandalism tends to be characterized by spontaneous activities, while sabotage is targeted and planned. In addition to vulnerable spaces, the target of these attacks can also be technical infrastructures that are set up outside a building, such as cooling systems, network connections, or power supplies. In such cases, attackers can specifically destroy individual devices in order to restrict other systems.

Theft and loss can refer both to physical devices and to data and information. A loss occurs without outside interference, although it can also turn out to be a theft at a later date. In the absence of appropriate protective measures, an attacker who steals the laptop of a field staff member can extract the stored data and possibly even obtain access data to the organisational network, such as an encrypted hard disk.

Social engineering describes attacks that exploit human vulnerabilities via social interaction in order to circumvent security measures in IT systems. In the process, the attacker exploits the fear, helpfulness, or respect for authority exhibited by employees. In phishing, for example, fake emails are used to obtain user names and passwords on a manipulated website. Another form of social engineering attack is CEO fraud. This is where the attacker pretends to be the boss and puts pressure on employees to transfer a large sum of money to an alleged supplier as quickly as possible, for example.

APT

An advanced persistent threat is a complex, persistent, and targeted attack, usually on critical information or IT infrastructure.

There are many more attacks at the organisational level. These play a particularly important role when information requiring very high protection is available and the attacker groups are state-organised. Accordingly, the types of attack mentioned here provide a mere overview.

Summary

In this unit, you have learned about attacks related to computer crime at different levels. First, attacks on the chip and firmware level were presented. These can be carried out via so-called side-channel attacks. At the firmware level, the diversity of firmware, in particular, offers a wide range of attack possibilities. Successful attacks at this level can compromise the chain of trust that extends from the operating system to the applications.

Attacks at the operating system level may attempt to bypass the two basic defenses available at this level: virtual memory management and strict rights separation. The goal of an attack on the operating system can be to achieve elevated rights in order to use the operating system's functions. This type of attack is called privilege escalation.

As soon as several IT systems communicate with each other, a network is required.

This also offers an opportunity to attack. Typical forms of attack include

eavesdropping, modiﬁcation of data, spooﬁng attacks, password attacks,

denial-of-service attacks, key attacks, and man-in-the-middle attacks.

At the application level, it is mainly applications and protocols assigned to well-known port numbers that get attacked. These include FTP, SSH, DNS, and HTTP(S). These applications and protocols carry their own attack scenarios. Web applications represent targets because they are mostly exposed to the internet.

Attacks at the organisational level revolve around the exploitation of organisational policies, such as role assignments, processes, and organisational and operational structures. Perpetrators can come from the internal and external environment of an organisation.

The attack vectors presented herein constitute a fraction of what attackers are currently using and will be using in the future. Every day, known forms of attack are recombined or new attacks are invented. The increased networking of devices and the public flow of information on social networks are just two examples that make new forms of attack possible.



# Unit 5

## IT forensics and electronic evidence

#### LEARNING OBJECTIVES

Upon completion of this unit, you will know….

... how malicious codes are localized and malware is identiﬁed.

... what a polymorphism is.

... how malware can be detected.

... how an IT forensic investigation works and how electronic evidence is detected.

... how files can be recovered depending on the type of deletion.

... which legal limits must be observed.

DL-D-DLMIMWCK01-L05

1. IT forensics and electronic evidence gathering

### Introduction

IT Forensics   
IT forensics discipline transfers the methods of classic forensics, such as securing evidence, chains of evidence, and traceability, to the IT sphere in order to prove computer crime in a way that can be used in court.

Machine Learning Machine learning methods belong to the field of artificial intelligence. Algorithms are supposed to recognize patterns independently on the basis of data sets, among other things.

In 2020, the Brown-Forman Group became the victim of an internet attack. The attackers had spied out the company's network using infected systems. This enabled them to steal 1 TB of data. It was only when they tried to encrypt the data on Brown-Forman's systems to make it unusable for the corporation that the attack was discovered. The attackers then auctioned off the stolen data to the highest bidder. In such a case, the victim must take IT forensic measures. First, to track the attack so that such an attack cannot occur again, and by taking corrective measures. To do this, the malware used must be identiﬁed and appropriate detection mechanisms introduced. Second, it must be determined which data the attacker had access to. This allows the extent of the attack to be assessed. For this reason, traces and evidence must be secured.

### Identiﬁcation, localisation, and the handling of polymorphisms

IT forensics aims at performing data analyzes on data carriers and in networks in order to clarify incidents of computer crime. A strictly methodical approach is essential in order to avoid the covering of traces and to secure evidence (cf. BSI 2011). Since attackers usually use malware for attacks, the analysis of these programs is a focus of IT forensics. The first step is the identification and localisation of malicious code or malicious software (cf. Pitolli et al. 2020).

Malware volumes have increased to such a degree in recent years that most malware is now classified into families. For example, many variants of the "Emotet" malware exist, which are grouped into the "Emotet" family. The task is to classify malware and to identify new "families". Artificial intelligence methods, such as machine learning, are sometimes used for this purpose. These methods use features such as signatures, generated HTTP traffic, function graphs, or the behavior of the malware in a controlled environment, for example, to cluster malware and group it into "families" (cf. Pitolli et al. 2020). The features for detecting malware are discussed in more detail in the next section.

Polymorphic malware is a major problem. This can always generate new polymorphisms of itself. The term polymorphism is derived from genetics and describes the occurrence of several gene variants within a given population. In the case of computer crime, the malware creates copies of itself, which have the same functionality but a different appearance in terms of the characteristics used for detection. Polymorphic malware is capable of performing the following actions:

IT forensics and electronic evidence

* + - Apply different encryptions,
    - Change the file name,
    - Insert unused code, and
    - Substitute functions.

The aforementioned changes mean that previous detection mechanisms do not recognize malware as such because features such as the signature or the function graph have changed. However, the functionality of the malware has remained unchanged. This creates the possibility of defeating defense mechanisms identifying new malware as such. For correct detection, comparison with malware that has already appeared is necessary. Examples of how polymorphic malware can be successfully identiﬁed include fractal analysis algorithms applied to the process trees of a Windows system (cf. Khan/Siddi- qui/Ferens 2017).

The classification of malware into existing families is needed. The identiﬁcation of new malware and thus new families of malware is much more difficult for machines to learn. For new malware, the task is to unlock the functionality of the malware via code analysis. In doing so, the malicious code must be localised. Since the malware on infected systems exists as an executable program and not as a source code file, code analyzes can usually only be performed on the basis of assembler code or simple function graphs. Special programs exist for this purpose, such as "IDA Pro", "binary ninja" or "OllyDbg", but these must be operated by humans.

Such an analysis shows, for example, how Windows functions are called. Windows offers some integrated functions that can be used by applications, but also by malware. These functions can be used to reproduce some of the functionality of malware. For example, the accept function reacts to incoming connections on a port. This can indicate communication with a command & control server or be a legitimate function of an application. The "GetAsyncKeyState" function is used to register keystrokes of a system. Permanent use of this function may indicate a keylogger. Windows functions have a legitimate use and can also be misused for malware.

Meanwhile, algorithms that detect a defective code also exist. This is based on existing information on software, such as function calls or function graphs. As shown earlier, function calls can be used for both legitimate and malicious purposes. Machine learning algorithms can detect patterns and malicious code in an automated way in this context (cf. Narayanan et al. 2017).

Attackers use polymorphisms and other techniques to hamper the identiﬁcation of malware and localisation of malicious code. Artificial intelligence helps to detect malware based on patterns and classify it accordingly.

Polymorphisms   
A polymorphism is a copy of malware that the malware itself has created. The polymorphism may be slightly different from the original, but the functionality remains the same.

Signature

A signature is a recognition feature by which malware can be uniquely identiﬁed, such as a checksum.

Command & Control Server

A C&C server is used by an attacker to send commands to infected systems.

### Detection mechanisms

The previous section primarily dealt with malware attacks and their identiﬁcation. This section will focus on the detection of attacks on computers, although malware is not always used here. A successful password attack on the administrator account can give an attacker access to the systems, yet does not require malware on the victim's systems. The detection for this type of attack is highlighted at the end of this section.

As mentioned in the last study unit, malware can be detected based on a number of characteristics. Based on these characteristics, the following methods for detecting malware are distinguished (cf. Amro/Alkhalifah 2019): detection based on ...

* ... Signatures,
* Heuristics, and
* Behavior.

A fundamental distinction must also be made between on-demand and real time detection. Most applications for detecting malware (including antivirus programs) support both variants. On-demand is actively triggered by the user of the system and attempts the ﬁnding malware on the file system. Real-time detection is activated quasi-permanently and attempts to detect malware in memory and on the file system.

One of the first malware detection methods was based on signature detection. When new malware is found, the string of bytes representing the executable file is recorded in a database. In this case, this is the signature. If an executable file with the same string is found in the future, this is recognized as malware and appropriate countermeasures are initiated. With increasing numbers of malware, the corresponding databases became very large leading to a switch to the executable file hash as the signature. This reduces the size of the database and speeds up the matching process between the database and the files being scanned. But even with the hash as a signature, this type of detection has some disadvantages.

Completely unknown malware would therefore not be detected because the signature is not present in the database. It is not until a new malware has been detected, added to the database of antivirus program operators, and distributed to the systems that this new malware can be detected. This can take up to seven hours or longer in some cases. Due to the modiﬁcation of the malware (polymorphism), this malware is considered new to signature-based detection methods. Thus, the process must be performed for each deviation. These problems are targeted by the upcoming detection methods (cf. Amro/Alkhalifah 2019).

Signature-based

Detection

This type of detection

identiﬁes malware by using

certain characteristics,

such as strings in the byte

code or checksums / hash

values.

IT forensics and electronic evidence gathering

Heuristic analysis provides a means of detection prior to the distribution of signatures for the new malware. Heuristics are used to identify a malicious program based on suspicious properties. This method uses the decompilation of programs and compares the source code with the malware in the database. If the source code is found to have more than a certain percentage of similarity to the source code in the database, it is classified as malware. Another possibility is the isolated execution of the potentially malicious program in a so-called sandbox. In this case, the malware is executed and observed by the antivirus program with regard to malicious behavior (including self-replication, modification of files). The disadvantage of this detection method lies in a large number of false-positive messages, i.e. the user of the system is alerted to a malicious program that is actually a legitimate program. However, false-negative messages are much more dangerous than false-positive messages in this context. This detection method is usually used in conjunction with signature-based detection.

Detection based on malware behavior is similar to the previous variant. However, the system on which the antivirus program is running is not considered here; rather, the behavior of the malware is examined directly. As soon as malicious behavior is detected, the execution is halted. This method also produces false positives, since behavior can be both legitimate and malicious. However, it does provide the ability to stop new malware. Worms provide an example of this detection method. The core functionality of a worm is its ability to spread within a network. This functionality is reflected by behavior involving the following components: similar network traffic is created between computer systems. Gradually, a tree-like structure develops through this network traffic and further reachable systems within the network structure become infected.

Based on this behavior, software can be classified as a worm and the execution of the malware can be stopped. It is difficult for the attacker to change this behavior, as this is the core function of a worm. This is the major advantage of behavior-based detection techniques: Bypassing the detection requires a change in the functionality of the malware or special network traffic, which is hidden from this detection. This is more difficult to accomplish than a signature modification. In most cases, multiple methods of detection are combined, as each method has strengths and weaknesses. Behavioral and heuristic analysis is used for new malware, while signature-based detection is used for known malware (cf. Amro/Alkhalifah 2019).

In addition, attacks are possible without the use of malware, for example by stealing or guessing passwords for user accounts or launching DoS attacks. Neither of these attacks can be detected by malware, but only by network activity. In this case, network traffic can also be analyzed using behavioral analysis. As soon as unusual behavior occurs, this can be an indication of an attack. For example, if an attacker obtains access data for an administrator account, the number of simultaneous logins or the number of logins on a particular system can indicate whether the administrator account is only being used by the effective administrators or by an attacker. If, for instance, the traffic from an internal server to the internet is significantly larger than in the previous month's period, this may indicate that an attacker is stealing data (cf. Marchetti et al. 2016).

Heuristic Analysis

This type of detection identifies malware by checking the code for suspicious properties.

Behavior-based Detection

This type of detec- tion attempts to identify and stop malware by detecting the core functionalities.

Thus, several methods exist for detecting attacks and malware in particular, and these approaches are usually combined.

### Finding electronic evidence

Electronic

Evidence

Electronic evidence refers to information and data that is machine-readable and valid in court.

The main objective of a forensic investigation is to secure forensic evidence. Classic forensic evidence includes DNA, blood traces, or fingerprints. Electronic evidence in relation to computer crime exists in the form of data on hard disks or other storage media. Over time, the number of computer crime cases has increased and digital or electronic evidence on computers or mobile devices has become more crucial. Digital or electronic evidence is information that is stored or transmitted in a machine-readable format and has a sufficient level of integrity and authenticity to be valid in court. This can be a video file, a document, or a log file. Even a password on a sticky note on the monitor is information in a machine-readable format, as this password represents access to an application.

The question is when a machine-readable information possesses sufficient integrity and authenticity. IT forensic investigations always consist of several steps, and there are several similar models. One variant is illustrated below (cf. Lin 2018):

* Preparation,
* Collecting data,
* Saving data,
* Appraisal and analysis of data,
* Reconstruction of incidents, and
* Presentation of results.

The preparation phase of a forensic investigation is used to get the necessary tools ready, both on the software and hardware side. In addition, implications regarding the forensic investigation should be considered. Areas such as IT emergency and IT security management can collide with the investigations. The goal of IT emergency management is to restore the normal state as quickly as possible after an attack. Affected servers, for example, should return to normal operation as quickly as possible in order to make the services provided by the server accessible again. One goal of forensic investigation is to preserve evidence. These two objectives may collide. In addition to these aspects, legal concerns should also be taken into account.

IT forensics and electronic evidence gathering

The collection and back-up of data are performed at the scene of the crime or in   
the compromised system. Particular attention must be paid to the integrity of the data at this point. As with classic forensic investigations, the rule here is that as little evidence as possible must be destroyed. However, this cannot be ruled out. In the example mentioned at the beginning, an IT forensic analysis would be carried out on systems belonging to the group concerned. When an investigation is carried out on a running system using forensic applications, the system's process list is modified. This means that evidence can already be destroyed or altered. The decisive factor here is whether the forensic investigation takes place online or ofﬂine.

When collecting and backing up data, the original data and the copy of the data must never be modified. For this reason, copies of affected systems are created using forensic tools such as write blockers. These tools are used to ensure that when data is copied from a disk, it cannot be written onto the same disk. If the copy is damaged, a new one can be created with a correspondingly modified procedure. This is because complete proof of authenticity must be ensured by delivering unaltered data from the scene of the crime to the court.

Upon completion of these two phases, data can be examined and analyzed. For example, the available data is searched for keywords or hash values of certain files. In addition, services such as log files or browser histories are searched. The recovery of deleted data also falls into this phase. In data analysis, a distinction is made between (cf. Lin 2018):

* File system analysis,
* Log file analysis,
* Mobile device analysis,
* Malware analysis, and
* Multimedia analysis.

File system analysis depends on the speciﬁc file system (e.g., FAT, NTFS, or APFS), the keywords used to search, and the way in which deleted data can be recovered. Attackers sometimes also use techniques to obfuscate data. Log files are files that protocol and record events or actions on a system. These events can be used to reconstruct the processes on a system. In most cases, system logs, web server logs, and Windows event logs are analyzed. The forensic analysis of mobile devices represents a discipline of its own. Smartphones store a lot of data nowadays, as more and more applications work on the smartphone, meaning that a lot of data important for forensics can be found here. Multimedia analysis is also a discipline of its own, as more and more multimedia content is being produced, yet it can also be forged. This means that not only must evidence be found in multimedia content, such as photos or videos, but it must also be proven that it is not fake.

Write Blocker

A write blocker is a hardware or software feature that prevents writing on a data carrier.

Log Files

Log files contain information on actions that have been performed on an IT system.

The analysis of the relevant data is followed by the attempt to reconstruct the events of the crime and the finding of evidence. The data obtained, such as network connections in log files or app activities on a smartphone, represent isolated events that are to be linked to form a chain of events. In most cases, there is a switch between this phase and the previous ones, and event sequences are gradually excluded. Being supported by electronic evidence, the most plausible event chains remain.

The last phase is the presentation of the data. At this stage, it is important that the conclusion and the chain of evidence be presented in a clear and understandable way. This is because the presentation of the results may have far-reaching consequences, such as accusations or legal measures. For this reason, urgent care must be taken to prepare the presentation in a way that is appropriate for the target group, ensuring that the audience understands the results beyond doubt.

Post-mortem Analysis

A post-mortem analysis is a forensic examination that is usually performed on data carriers.

Live Forensics

In contrast to post-mortem analysis, live forensics is performed on running IT systems, usually when the attack on the system is still in progress.

As indicate, it makes a big difference whether a forensic analysis takes place ofﬂine or online. An ofﬂine or post-mortem analysis is initiated after a crime has been committed and is mainly performed on data carrier images. Post-mortem analysis in this context describes the forensic examination of non-volatile data, data carrier images, deleted, or encrypted data on mass storage devices. The advantage is that unintentional data manipulation cannot occur as easily. Online or live forensics, on the other hand, is performed on the running system. In the example presented at the beginning, the enterprise could immediately start a forensic investigation upon discovery of the encryption process. Data and evidence could then be collected on the infected system. This has the advantage of analysis of non-volatile data, such as the contents of RAM or the currently active network connections. This information can be very valuable and may have been lost already in ofﬂine analysis (cf. BSI 2011).

To perform an analysis of one's own file system, the commands *mmls* or *fdisk-lu* can be used in Kali Linux. The hard disks of a Linux system are always located under */dev* and the primary hard disk under */sda.*

### Data and evidence recovery

Recovery of deleted data is a common process in an IT forensic investigation. Malware attempts to cover traces by deleting executable files and emails or other documents. However, it must be noted that the delete function is not implemented in modern operating systems in the sense of permanent destruction of the data (cf. Lin 2018).

Every modern operating system has a special directory that contains deleted files, at least for a certain period of time. This directory, usually called recycle bin, can be emptied by the user via another function. Within the recycle bin, data can also be deleted by the user itself without any problems.

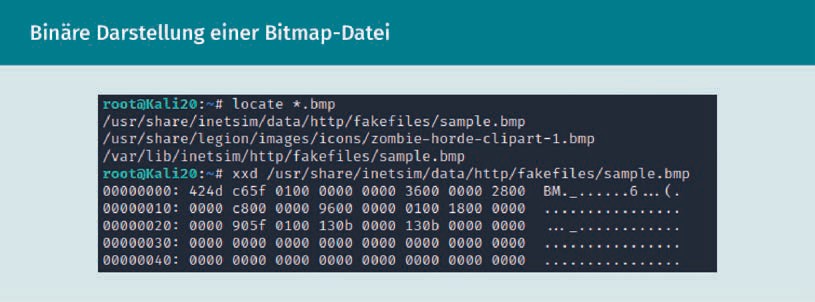
IT forensics and electronic evidence gathering

Sometimes the recycle bin on operating systems is hidden or assigned certain permissions, but the files it contains are still fully available.

If a file is deleted and the recycle bin is then emptied, this file is no longer accessible to the user. However, in this case, the information on the deleted file on the hard disk is not removed. Only data in the file system structure is changed or removed so that this file is no longer visible and usable for the user. However, in addition to the information on the file on the hard disk, metadata about the file in the file system structure remains. This means that the file can be found via the metadata and restored with the data on the hard disk. This type of recovery is therefore based on the remaining metadata of the file system.

However, there are some scenarios where the file system structure is no longer present. The structure may be incomplete, damaged, or no longer present. This can happen due to deliberate or accidental actions. An internal attacker can delete a file system structure with freely available tools, such as the format function. Without this structure, it is much more difficult to recover files. The technique for producing the data, in this case, is called file carving (cf. Lin 2018).

If the file system structure no longer exists, the contents of a file system are just a structureless sequence of bits and bytes. Without knowledge of the beginning and end of a file in the file system, files are difficult to recover. However, many file formats feature deﬁned sequences at the beginning (header) as well as at the end (footer) of the memory area. Files can be recovered via these two indications. To test this for yourself, use locate *\*.bmp* to locate a BMP image file on your Linux system. Then enter the command *xxd [file path]*.



The *xxd* command outputs the binary content of a file. This is represented by the blocks of four consecutive numbers in the output's center. Hence, the binary data of the BMP file starts with the bytes "0x424D".

Recycle Bin  
On Modern

operating systems, the Recycle bin is used to store deleted objects.

File Carving

File carving describes the iden- tiﬁcation and recovery of files without the support of the file system.

This is a special marker used for all BMP files. These markers are also called "Magic Numbers". In this way, a wide range of file types can be identiﬁed during file carving.

Bifragment Gap Car-

ving Bifragment gap carving identiﬁes the start and end of fragmented files on the disk. The fragments are joined if the composite represents valid files.

Wipeout In a wipeout, data is not only deleted but also destroyed. This means that the data on the data carrier is overwritten with meaningless or synthetic data (e.g. zeros).

Fragmented files are another hurdle in file carving. Unless there is enough contiguous memory space, a file is broken into multiple pieces and stored in different locations in the file system. As long as the file system structure is intact, the file is assembled each time it is read or written. In the case of file carving of fragmented files without file system structure, such files must be reassembled. Since 97% of files are either non-fragmented or bi-fragmented (in two sequential fragments), bifragment gap carving is used to find the gap between the header-marked part and the footer-marked part of a file. With these means, files can be recovered based on the binary structure alone.

The above methods are not helpful if files have been completely wiped out by overwriting the binary data. On Linux systems, for example, there is the *dcfldd* commandwhich can completely overwrite a hard disk with "zeros". In this case, the information on the files on the hard disk is completely removed and recovery is impossible (cf. Lin 2018).

After deletion or wipe out of data, only back-ups provide help for recovery. Back-ups are important not only for forensic investigations but also for accidentally or deliberately deleted data and IT emergencies. For these reasons, many organisations use back-ups in a systematic way already. Most back-up mechanisms store changes to data or file structures over a period of a few weeks to several months, depending on available storage space. Thus, deleting a file also results in a time-delayed deletion of the file in the back-up. However, several months can pass before this happens. During this period, it is possible to restore files from the back-up at any time, provided the data in the back-up is accessible for forensic examination.

Another incident, such as ransomware, makes data recovery necessary. Malware that encrypts data also makes that data inaccessible. This case should be considered in a manner similar to that of a wipeout. In such a case, all hopes lie in decrypting the data either with the correct key or with a so-called decryptor. Decryptors exploit vulnerabilities in the cryptograﬁc algorithms of the malware in order to find out the key or to decrypt files even without the key. In this case, back-ups can also be used to restore data, provided they are not encrypted as well.

Thus, deleting data does not directly imply that the contents of the file have also been removed from the file system, making the methods for recovering data very diverse and tailored to each case.

IT forensics and electronic evidence gathering

### Legal limits and predictive policing

In the case of IT forensic analyzes, the legal limitations regarding data protection, such as the GDPR, must also be taken into account. This is an aspect to be observed as early as the preparatory phase of the forensic process. The principles of data avoidance, data economy, anonymization, and others also apply to forensic investigations. Often, forensic investigations analyze data that do not belong to the perpetrator or the crime scene. Public cloud environments offer another example. Here, care must be taken to ensure that only the infrastructure, systems, or services of the organisation that commissioned the investigation are being accessed (cf. BSI 2011).

Predictive policing is an attempt to detect crimes before they occur. It started with classic crimes such as burglaries and theft. Based on statistical characteristics of the crimes and characteristics of the objects, such as the location or value of a house, can be used to determine the probability of a certain houses becoming the target of a burglary in a certain period of time (cf. Meijer/Wessels 2019).

This approach can also be applied to computer crime. Characteristics such as the value that the data provides to the attacker, the security level of the victim, or the classification of the last known victims are decisive here. The FBI has confirmed that it applies predictive policing methods to computer crime investigations within the FBI Cyber Division. Artificial intelligence is used for this task (cf. Collins 2017).

In the banking sector, for example, algorithms using artificial intelligence are already applied to predict criminal acts such as credit card fraud or phishing. Among other things, clustering algorithms such as "k-means" are used. These algorithms work on the collected data and try to calculate clusters in order to draw conclusions about a fraud case. Fraud can thus be prevented earlier or even before it occurs if new data collections exhibit a high similarity to this cluster (cf. Lekha/Praksam 2017).

Summary

Predictive Policing Predictive Policing attempts to use statistical models to predict the likelihood of criminal acts in the future.

In this unit, you learned about IT forensic processes and methods. The first learning cycle dealt with methods for locating malicious codes in malware, e.g., via calls to Windows functions. The identiﬁcation of malware, on the other hand, works via families and algorithms that assign them to these families based on certain characteristics, such as signature or function tree. This process is made more difficult by malware that has polymorphisms. These are copies of malware with identical functionality but different characteristics.

The mechanisms for detecting malware were then explained. The methods first presented rely on signatures, although this comes with a large time lag for new malware. In combination with methods based on heuristics and behavior, both new and known malware can be detected.

The next learning cycle covered the process of an IT forensic investigation and the phases that are passed through until electronic evidence can be determined. In this process, data must be secured and collected, and then, after review and analysis, events must be reconstructed. During this process, it is important to recover deleted data and evidence. Depending on the type of deletion, information on files may still be present and recovery proceeds by searching for the file within the file system structure. Back-ups also help in the recovery of data.

In the last learning cycle, the legal limits of IT forensics are presented using the example of data protection and predictive policing for computer crime. Predictive policing in this context aims to detect computer crime before attacks are launched.



# Unit 6

## Preventive measures

#### LEARNING OBJECTIVES

Upon completion of this unit, you will know….

... what characterizes preventive measures.

... how measures are implemented at the hardware level.

... how access control, authorisation, and authentication are interrelated.

... what the goals of training and raising awareness are.

... which processes need to be considered in the context of incident response planning.

DL-D-DLMIMWCK01-L06

1. Preventive measures

### Introduction

One of the waves of malware attacks that infected Deutsche Bahn display boards, among others, was launched by “WannaCry” in 2017. "WannaCry" exploited several vulnerabilities to spread the malware in networks. Many of the network attack methods worked based on outdated software stands. There are preventive measures against this type of attack, such as patch management, increasing awareness, and training. Strict authorisation and authentication also limit the spread of "WannaCry" within a network.

### Measures at hardware level

Preventive Measures

Preventive measures are taken in advance of an incident in order to reduce or eliminate the damage caused by the incident.

Trusted Platform Modules (TPM)

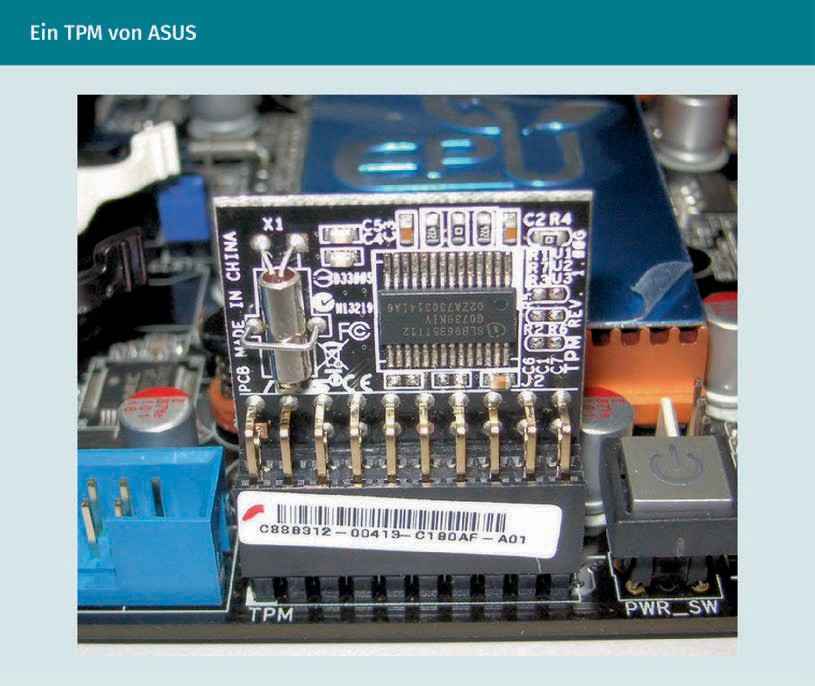
A Trusted Platform Module (TPM) provides a secure storage location for cryptographic keys.

Preventive measures are measures taken prior to the occurrence of a security incident. The aim is to prevent the security incident, reduce the likelihood of an occurrence, and/or mitigate the extent of the damage caused by the incident. A systematic way of planning, implementing, and controlling preventive measures is an information security management system (ISMS). This aims to manage information security activities and thus fulfills the requirements of an organisation, especially with regard to preventive measures (cf. BSI 2017).

Preventive measures for hardware include infrastructural measures. Hardware systems such as servers, switches, and routers should always be kept in a locked room and protected from theft. However, not only servers and active network components are at risk of theft, but also workstations or WLAN access points. These cannot always be stored in a locked room. For this reason, other protective measures, such as locks, must be installed here.

Another way to provide preventive protection at the hardware level is the use of so-called Trusted Platform Modules (TPM). These are special chips for the secure storage and processing of cryptographic keys, among other things. The design of a TPM provides protection against unintentional alteration of the keys. The keys in the TPM can be used to encrypt or generate further keys for other applications, making the TPM an important trust component (cf. Pritchard 2020).

Preventive measures



The standard for an ISMS in accordance with requirements of IT protection calls for the use of such TPMs on both the servers and the clients and embedded systems. The main focus here is on securing the key for full hard disk encryption. Following the theft of a mobile terminal with a fully encrypted hard disk coupled with the absence of access by the attacker to the corresponding key, the attacker will not be able to view the information on the hard disk. A theoretical exception would be the successful guessing of this key. A brute force attack, i.e. trying out the possible keys, would with current key lengths for hard disk encryption (AES-256) with all computers on this earth take an infinite number of times longer than the existence of the universe.

In research, protection measures are fathomed at the hardware level. Some of the most serious hardware-level attacks in recent years are "Meltdown" and "Spectre." These two side-channel attacks exploit the out-of-order execution of modern processors. Thus, information on processes running on the same physical processor as the malware can be harvested. The manufacturer took measures against these vulnerabilities and the corresponding attack at the software level. These prevented the attack but did not eliminate the actual vulnerability, as it resides in the hardware (cf. Lipp et al. 2018).

One possibility in terms of hardware-based protective measures is to program mechanisms for detection directly on an integrated circuit. This monitors the work steps on a processor. Specifically, the use of algorithms that can be implemented on a "Field Programmable Gate Array" (FPGA) and that can check the control mechanisms on another processor for patterns of attacks, such as "Meltdown", "Spectre" or "Rowhammer", are proposed. These algorithms run in parallel with the actual work processes and stop the work processes as soon as a suspicious pattern is detected. This protective measure is independent of software, but has some weaknesses in terms of malware modification, as patterns can change (cf. Congmiao 2020).

### Access rights, authorisation, and authentication

Access Rights

Access permission allows a user to use an IT system.

Authorisation Authorisation is the right of a user or an IT system to access a resource.

Authentication Authentication deals with the proof of identities, among other things.

Authentication processes are based on either knowledge, identity, or

possession.

In light of preventive measures, the terms access rights, authorisation, and authentication are introduced. In this context, access refers to the use of network components, IT systems, or other systems. Access rights allow a person to use one of these components. This applies not only to workstation computers or servers but also to mobile devices and printers, for instance. To implement access control, authorisation and authentication are required (cf. BSI 2019a).

Authorisation describes the verification of whether a person, hardware component, or application is authorized to perform a specific action. This therefore explicitly relates not only to persons but also to communication between applications or IT components.

Authentication or authentification describes the verification of authenticity. One example is checking whether a communication partner is who they claim to be. Authentication of identities is usually ensured by password entries, smart cards, or biometric features. IT systems or applications can also authentiﬁcate one another (cf. BSI 2019a).

Authorisation and authentication are usually sequential processes. This is because authorisation of a user or IT system can only function correctly if the user or IT system has undergone authentication first.

In general, the regulation of access rights comes first in the sequence of preventive measures. There must be a concept for the holding of rights to determine which teams, departments, or function holders have access to which applications or IT systems. In addition, the allocation, modification, and withdrawal of access rights must be regulated. This process must then be run through every time an employee joins, is transferred, or leaves. This is particularly important when an employee leaves, as otherwise, employees who are no longer part of the organisation retain access to IT systems

Preventive measures

(cf. BSI 2019a). If access means (such as smart cards) are used in order to grant access rights, these must of course also be distributed, changed, or withdrawn within the process.

Once access rights have been defined, checking these rights must be possible in the course of authorisation of applications and IT systems. Applications and IT systems may only allow access if the authorisation was successful. Due to the exposure of web applications, this area is given greater weight. For this reason, the IT-Grundschutz Compendium includes several measures for authorisation and access control in web applications (see BSI 2019a). Web applications usually have an area accessible to every user and one reserved for administrators. This area contains functionalities that should only be accessible to administrators. If the protection for this only consists of a URL that is not included in the navigation, such as "www.beispielanwendung.de/admin", then this is not sufficient. Tools such as "Dir-buster" use word lists to find URLs. Authorisation must be established here in order to gain access to "/admin".

Provided that access rights have been assigned and authorisation has been established, the users and IT systems must be correctly authentiﬁed beforehand. It has already been mentioned that a user can be authentiﬁed as such by means of a password (knowledge factor). Provided a user enters the correct password, the identity is proven. This process of authentication depends on the strength of the authentication. To this end, every organisation should create a password policy and take technical and organisational steps toward its implementation (cf. BSI 2019a). However, there are other ways to authenticate a user besides password usage. Especially for mobile devices, biometric authentication methods (factor being), such as fingerprint scanning or facial recognition, are more and more common. Even these measures are not free of vulnerabilities, however, this is a feature that a person always has with them and, unlike a password, cannot forget. However, the use of biometric authentication methods also always poses a problem in terms of data protection law, since these features uniquely identify people.

Two measures for authorisation and authentication are single sign-on (SSO) and multi-factor authentication (MFA). With SSO, authentication processes for different systems are reduced to one authentication process. Thus, a user must be authentiﬁed once, for example, when logging into the organisational network. After that, this proof can be made available to access and authorise further applications by means of an authentication token. One advantage is that the user only has to maintain one authentication feature, which means that the password strength can be set higher, for example. A disadvantage of SSO is its dependence on the availability of the SSO system. Among other things, the authentication service Kerberos is used in the Windows environment to implement SSO for users. Other examples are the authentication via digital service providers such as Google, Facebook, or Amazon to log into other web applications. Protocols such as OpenID or OAuth are most commonly used in this case (cf. Evans 2019).

IT-Grundschutz Com- pendium

The IT-Grundschutz Compendium

contains building blocks of basic IT protection along with the threats and requirements regarding IT systems.

Single Sign-on (SSO) Single sign-on is based on a one-time authentication of a user or IT system. This can be used for other resources or services.

Multi-factor Authenti- cation (MFA)

Multi-factor authentication requires multiple authentication factors (knowledge, being, and possession) for successful authentication.

FIDO

The FIDO standard enables secure password free authentication. A separate key pair is stored in the FIDO authenticator for each service or web application.

Multi-factor authentication refers to authentication in name. Using MFA, authentication is performed with multiple factors, i.e., instead of using only a password, additional factors are required. For example, possession of an object, such as the user's own smartphone or a security token, can be added as another factor. In two-factor authentication, for example, both the password (knowledge) and a generated string produced by an authenticator on a smartphone or the security token (possession) must be correct. This significantly increases security because the generated string remains valid on personal devices for only a short time. Thus, for a successful attack, the password would have to be present (e.g., through phishing) and the attacker would have to be in possession of the unlocked smartphone. The BSI requires this type of authentication to be used to access critical services or administrator accounts for instance (cf. BSI 2019a).

Another standard for authentication in web applications is Fast-IDentity- Online (FIDO). This tool attempts to resolve the problem using password-based authentication for web applications. This problem is based on low password quality, using the same password when accessing different services, and high success rates when it comes to phishing. Application examples of authentication by FIDO can be the password free authentication (e.g., via cryptograﬁc keys) and using as a "second" factor (possession of a FIDO key). This can be done via "smart devices" or hardware tokens (cf. FIDO key). From a technical standpoint, this procedure is based on asymmetric encryption. A request is made to the user for authentication. The user uses the private key stored in the FIDO key, for example, as proof of his identity. After transmitting the response encrypted with the private key, the requester can verify the identity with the corresponding public key (cf. Laborde et al. 2020).

Some of the actions and effects listed here can be tested using the OWASP Juice Shop, a vulnerable web application that is available on "Github". The OWASP Juice Shop can be set up on a dedicated computer and should never be made available to the internet. This web application contains several vulnerabilities that occur when authentication or authorisation measures are implemented incorrectly or not at all. The "Access the Administration Section of the Store" challenge targets hidden URLs and shows the danger of allowing weak passwords. The challenge "Log in with Bjoern's Gmail Account" illustrates the implementation of SSO with Open Authorisation and the associated vulnerabilities.

### Awareness & training

Measures such as training and raising awareness play a significant role in preventing attacks. Malware, spread by forged and manipulated emails, has a lower potential to cause damage if awareness is increased and employees are trained for this type of attack.

Preventive measures

Simply making employees aware of this attack vector used to spread malware can lead to a conspicuous email being questioned.

Basically, a distinction must be made between at least two target groups for training and raising awareness. The target group of administrators requires training on the IT systems used in the organisation. These include directory services (such as Active Directory or OpenLDAP), groupware (e.g., Exchange or Lotus Notes), databases, memory systems, network management, and the types of servers in use ( e.g., Linux and Windows). This is a prerequisite for the appropriate competencies of administrators in the context of conﬁguration, administration, and operation of IT systems. Information and guidelines for this are specified in the information security management. This technical training must be repeated regularly.

Users of certain IT systems must be trained with a modified focus and different training content. This helps to prevent incorrect use. Examples include the use of cell phones, industrial systems, WLAN clients, or VPN access. Such training includes correct use, the necessary security settings, and an explanation of why these settings are important to organisational security. If users cannot be blocked from changing conﬁgurations, they must be made aware of the need to maintain the conﬁguration in place. The requirement is for employees to handle the systems that process information safely. Factors such as technical afﬁnity and rights that an employee needs to perform their tasks also count. For example, developers can and often must be granted local administrator rights on their computers. This is required for the task and the employees are mostly of sufficient technical afﬁnity (cf. BSI 2019a).

In addition to this more technical training on specific systems, employees of an institution must also undergo an awareness and training program on general information security. The primary goal is to create security awareness among employees. Other objectives in this context are (cf. BSI 2019a):

* Provide knowledge on information security regulations (e.g., password and communication policy),
* Create awareness of information security measures (e.g., explain the necessity and effect of protective measures by demonstrating real attacks),
* Provide training on security features and their limitations (e.g., use a password manager or VPN access),
* Recognize and report security incidents,
* Observe protective measures and handle information carefully (e.g., do not leave a piece of paper with a password on the monitor),
* Raise awareness of social engineering (e.g., recognize fake emails or phone calls), and,
* Change in security culture.

Active Directory

Active Directory is a directory service with a database including information on elements in a domain. It manages users and groups, their passwords and permissions.

Awareness

Security awareness describes the sensitivity of employees to information security measures, the current threat situation and security incidents.

Security culture

Security culture

refers to unwritten values according to which the organisation works with regard to security aspects.

IT-Grundschutz and

ISO 27001

Both principles describe the structure of an ISMS and its elements. They are based on a risk-based approach and standardised requirements.

Especially the last point requires some explanation. Peter Drucker coined the phrase "culture eats strategy for breakfast." This phrase suggests that a strategy cannot be enforced in opposition to the culture of an organisation. The phrase "culture eats compliance for breakfast" is similar, where "compliance" stands for adherence to the totality of rules in an organisation, including the rules for information security. If the majority of employees do not believe in these values in line with their day-to-day work, they will not implement security measures. The introduction of new preventive measures, for example, that should be part of everyday business in the future will find little acceptance and thus generate little benefit if the inner values of the employees tend to follow the motto "We've always done it this way" (cf. Bryant-Smith 2018).

However, organisational culture is not necessarily the antithesis of information security. It is possible to develop a positive information security culture with the help of training and measures to raise awareness. A model with targeted training and awareness measures was developed for this purpose. It is tailored to demographic groups, hierarchical levels, departments, and regions. Using the model, it is possible to change the organisational culture in a positive way for information security as well as to measure the state of change in a cyclical manner. This approach must be followed over several years to show success (cf. Da Veiga 2015).

Training and awareness-raising as preventive measures have far-reaching consequences for aspects of information security and are therefore required by most frameworks and standards for information security management, such as IT-Grundschutz or ISO 27001. Since the effectiveness of most protective measures depends on their acceptance by employees, there are procedures for an ISMS. These point out awareness-raising as the most important preventive measure (cf. ISIS12 2018).

The effectiveness of awareness-raising measures must be assessed. Key figures are available to quantify the success of awareness measures. These key figures can be generated, for example, by testing employees with phishing emails sent internally. In this case, phishing emails are sent by the company's own security department or a service provider that lures the user to a fake website. In this case, the website is not malicious. The aim here is to record the number of employees who have clicked on links in these emails. This enables the current maturity level of the employees to be determined and, if necessary, further awareness-raising and training measures to be planned. However, this procedure should only be carried out in consultation with the data protection officer and the staff or works council representative.

### Incident response planning

The reactive measures of incident response planning include four components (cf. BSI 2019a):

Preventive measures

* Security incident detection,
* Security incident handling planning,
* IT forensic precaution, and
* Emergency management planning.

Detecting an incident is a prerequisite for responding to it. This detection is achieved by evaluating log files from various applications and systems. The applications and systems generate these log files, which contain information on processes within the application or system. Examples are the authentication or authorisation of users, changes to files, or network access. The issue here is the number of logs. These cannot be analyzed without technical assistance. This can be understood by looking at the log files of one's own computer. On Windows, the event viewer function is available for this purpose, and on Linux, the command *ls -la /var/log* and then, *cat /var/log/auth.log* can be entered to view the log file for authentication. Use *cat /var/log/\* | wc -l* to display the number of lines of all log files in the */var/log* directory. The number of lines on a Kali Linux VM that is not connected to an organisational network, for example, is over 40,000.

Intrusion detection systems (IDS) evaluate this volume of data in a (partially) automated and efﬁcient manner. These can be divided into host-based IDS (HIDS) and network-based IDS (NIDS). The first variant analyzes events on a system and the second one on a network. Both can be signature-based and behavior-based. Thus, either feature (signature) or conduct is classiﬁed. As soon as an anomaly occurs, it is evaluated as an incident. In particular, current literature is using artificial intelligence to improve detection with anomaly-based NIDS. This is where normal behavior is clustered with algorithms, such as "k-means", in order to better differentiate anomalies from normal behavior (cf. Coulibaly 2020).

The detection of a security incident is followed by the handling of this incident. This process is referred to as security incident management. Obviously, the procedure for resolving a security incident depends on the specific case. However, some steps can be generalized. Once an incident is discovered, there must be a reporting path and an escalation plan for it. Whether a server has crashed due to an automated attack or a back-up of all customer data is freely available on the internet, just to name one example, makes a difference. Subsequently, the cause of the incident must be found, the effects contained, and normal operations restored. Afterward, the security incident must be documented and followed up with in order to take preventive measures against its recurrence (cf. BSI 2019a).

In addition to detecting and handling the security incident, measures relating to IT forensics and business continuity management must be planned. For example, IT forensic service providers should be contracted prior to the occurrence of an incident, or dedicated staff should be established for this purpose. Emergency management is a discipline in its own right. The (critical) (business) processes

Log files Applications and IT systems create log files. They time-stamp and store information on activities and processes

Intrusion Detection System (IDS)

An intrusion detection system detects attacks on a network or computer.

Security Incident Management

Security incident management takes care of the process for security incidents.

This ranges from the identiﬁcation to the elimination of the causal problem.

Emergency management Emergency management focuses on the availability of IT systems and attempts to restore them after an emergency.

within an organisation and the availability of the necessary resources (including IT systems) are the focus here. The activities of IT forensics, emergency management, and incident detection and response must be coordinated (cf. BSI 2019a).

Summary

This unit focused on preventive measures against computer crime. Preventive measures are taken prior to an incident to reduce the damage of the incident or to prevent it.

At first, measures at the hardware level were presented. In addition to infrastructural measures designed to prevent hardware theft, there are special chips that implement protective measures at the hardware level, such as Trusted Platform Modules (TPM). Current research proposes programmable chips that prevent vulnerabilities at the hardware level, such as "Meltdown" and "Spectre".

Another category of preventive measures are access rights and measures for authentication and authorisation. This involves proving the identiﬁcation of users and IT systems and assigning rights to certain resources. For stronger authentication, multi-factor authentication and single sign-on are used.

Training and measures to raise awareness were also addressed. In principle, a distinction must be made here between training courses to build up the specialist knowledge of administrators and users with regard to the correct use of IT systems on the one hand, and training and raising awareness on information security on the other. The second category must additionally take into account the culture of an organisation, as the latter needs to have a positive attitude toward information security.

Incident response prepares the organisation for a security incident. In this process, incident detection must first be established. This is usually achieved with intrusion detection systems. Furthermore, the handling of the incident must be planned in conjunction with IT forensics and emergency management.



# Unit 7

## Reactive measures

#### LEARNING OBJECTIVES

Upon completion of this unit, you will know….

... what types of consequences need to be considered after a security incident.

... how to prevent persistent damage.

... how information is exchanged and what hurdles exist in the process.

... when to collaborate with security authorities.

... what recommended actions companies should take.

DL-D-DLMIMWCK01-L07

1. Reactive measures

### Introduction

Organisations that have fallen victim to computer crime are usually reluctant to publish information on it. The attack on the Heise publishing house using "Emotet", on the other hand, was made public in a very transparent manner. The gateway was an email with a malicious attachment ("Emotet"), which was opened and thus caused the malware to run. Following the initial infection with the "Emotet" Trojan and the automatically downloaded "Trickbot" Trojan, the attackers manually rolled out the "Ryuk" ransomware. Thus, important data was encrypted. After the incident was discovered, the network connections of the affected systems were disconnected as a reactive measure and a complete network area was isolated. Subsequently, IT forensic services were commissioned to reconstruct the events of the infection. At the same time, external communication was carried out, as certain processes and websites were no longer available at the time and organisational procedures had to be changed at short notice. Reactive measures are manifold and will be examined in more detail below.

### Initial assessment and extent of damage

Reactive Measures

Reactive measures are measures taken after an incident.

Primary Consequences

The primary consequences result directly from a

Incident.

Secondary Consequences

The secondary consequences result from the primary consequences and are thus triggered by the incident in an indirect manner.

This learning cycle is about reactive measures. These are measures which aim to reduce the consequences of threats (cf. Humpert 2004). The first step in the initial assessment of the extent of damage caused by a cyberattack is to analyze the consequences of the attack. Generally, a distinction is made between primary and secondary consequences. Primary consequences are direct results of an incident and secondary consequences result from the primary consequences (cf. Stelzer 1993).

Examples of combinations of primary and secondary consequences include:

* Primary: Infection of a server with a virus;
  + Secondary: Failure of an application;
  + Secondary: Derival of mission-critical data;
* Primary: A DoS attack makes a website inaccessible;
  + Secondary: The company's reputation is severely damaged;
  + Secondary: Customer orders cannot be accepted;
* Primary: A disgruntled administrator deletes the entire production databases, including the back-ups;
  + Secondary: Production is at a standstill for several days;
  + Secondary: A sales loss of several million euros is recorded.

The examples show far-reaching consequences and go beyond technical consequences. In addition to physical and digital damage caused by computer crime, four further categories are distinguished:

Reactive measures

|  |  |
| --- | --- |
| Schäden durch Computerkriminalität in Organisationen | |
| Kategorie | Beispiele |
| physisch/digital | * Beschädigung * Zerstörung physischer Dinge * Abﬂuss von Daten * Identitätsdiebstahl |
| ökonomisch | * Unterbrechung der Produktion * Verlust von Kunden * Strafzahlungen |
| psychologisch | * Frustration * Verwirrung * Angst |
| reputationsbezogen | * schlechtere Außenwahrnehmung * geschädigte Kunden- und Lieferantenbeziehun- gen * Verlust von Akkreditierungen oder Zertiﬁzierun- gen |
| sozial | * schlechtere interne Moral |

Estimating the extent of the damage caused by an attack that is currently in progress requires a damage assessment carried out prior to the attack. For this purpose, attack possibilities are created in the form of a graph based on the network structure, for example, and a simulation model is applied to this structure. This graph represents the possibilities for intrusion, propagation, and complete access to this network by an attacker. Thus, the simulation of the initial infection of the system could be based on the graph. Examples include the opening of a malicious email by an employee or the exploitation of a vulnerability on a web page of the organisation. Subsequently, there are several opportunities for the attacker to spread across the network. Examples include reusing user authentication via LLMNR (Link-Local Multicast Name Resolution) poisoning, or exploiting vulnerabilities of only internally accessible applications. Exhibiting all these possibilities and the dependencies between them results in the creation of a graph showing the attack possibilities. In this way,

the simulation can, for example, provide information on the effects of an infection of server X on client group A and network section B. In addition to simulation, such systems can also be fed with (near) real-time data enabling the extent of damage to be calculated directly in the event of an attack (cf. Kotenko/ Chechulin 2013).

Calculating the extent of damage is difficult due to the high number of different secondary consequences. Only forensic analysis reveals which primary consequences result from an attack, e.g., which IT systems are infected. Estimating the secondary consequences then raises further questions: To what extent is the external perception worsened as a result of the attack? What contractual penalties will we have to pay in the event of a data leak? How many systems in a network must be replaced?

### Suppression of persistent damage

Stopping persistent damage, like assessing damage, is highly dependent on the nature of the attack. As previously discussed, damage can be caused by primary or secondary consequences. There are actions available to stop the primary consequences, which are effective for many types of attacks.

Network Access   
A system has network access if it can reach other systems in the same physical or virtual network via protocols.

Virtual Desktop

A virtual desktop is a workstation that is virtualized on a server. This means that the employee's working environment does not run on the local computer.

Insofar as an attack is discovered while the first system is being infected and before propagation throughout the organisational network takes place, one possible reactive measure is always to shut down the affected system. Doing so restricts availability as, in the case of a workstation, the employee can no longer work or, in the case of a server, the service is no longer available. Optionally, network access can be blocked or disabled as well. Prior to the development of virtual environments, it was sufficient to pull the network cable of a workstation computer or disconnect the power supply when an infected workstation computer was reported. This prevented the infection from spreading further. If an organisation uses virtual desktops, disconnecting the network connection or turning off the local computer at the employee's workstation will have no effect. The local machine is only used to access the virtual machine and the latter continues to run on the host system, even if the employee's machine is turned off. This demonstrates the importance of verification with respect to the effectiveness of reactive measures, such as switching off individual systems.

In addition to the individual systems, the entire network or parts of it can also be deactivated. In the Heise publishing house example, a network segment was already largely infected when the security incident was discovered. Isolation, i.e., disconnecting a network segment from adjacent segments and the internet prevented ongoing damage. It should be noted here that modern networks work with virtual networks and there is usually no longer any physical separation. Thus, vulnerabilities in routers or switches can bypass a software-based barrier.

Reactive measures

Malware often requires commands issued by a command-and-control server (C&C server) to spread. This communication can be prevented by blocking the corresponding IP addresses of the C&C server via a firewall. However, there are usually several command-and-control servers, so this does not permanently prevent damage. A more secure solution, in this case, is to disconnect the public internet connection. Again, the question is whether this is implemented physically via disconnecting a connection or disabling a router, or on the software side via firewall rules or application settings. Disconnecting the public internet prevents the malware from communicating with the C&C servers, but it severely restricts the organisation's ability to operate and the availability of services. In addition, modern systems of an organisation are not located in a single location or may not be accessible by the organisation. When servers are operated in the cloud, an organisation often does not have the option of disconnecting them from the power supply or from the public internet, as they are located in remote data centers.

Shutting down systems and disconnecting network segments is usually the only solution to prevent lasting damage in the case of malware such as "Emotet". Other approaches might also help in the case of malware that only exploits specific vulnerabilities, to name one example. In 2019, the CVE-2019-19781 vulnerability (also known as "Shitrix") was published. This vulnerability was located on Citrix systems. It was detected and exploited by attackers with mass scans on the internet after publication. In such cases, information on the vulnerability must first be researched.

A patch for this vulnerability is found in the case of "Shitrix". It must be applied very promptly. However, the vulnerability also means that once infected, servers are not secure after this update. The infection is not removed by the update and the server thus remains vulnerable. In this case, scripts are used to debug an infection. A search engine or special tools are suitable to find this information. One example is "searchsploit" which comes pre-installed on a Kali VM. With *searchsploit citrix*, the "Shitrix" vulnerability described above can be found under the keyword "Citrix Application Delivery Controller and Citrix Gateway". The exploit can be displayed with *searchsploit -x multiple/webapps/ 47902.py*. The command shows the Python program listed here. In contrast to this is the defender side, i.e. how a vulnerability can be closed. Disconnecting from the public internet stops the malware from communicating to the C&C servers, but severely limits the organisation's ability to work and the availability of services. In addition, an organisation's modern systems do not reside in only one location or are not within the organisation's access. When servers operate in the cloud, an organisation often does not even have the ability to disconnect them from power or the public internet because they are located in remote data centers. This is countered by the defender side, i.e., how a vulnerability can be closed. Information on this can be found, for example, on the website of the MITRE Cooperation (cf. The MITRE Cooperation 2020).

Command-and-con- trol Server

A command-and-control server is used to transmit commands to infected systems.

Buffer Overflow   
A buffer overﬂow is a software vulnerability. In this case, the size of a value that is written into the buffer (memory area) is not checked. This means that almost any malicious code can be executed.

Computer Emergency Response Teams

(CERT)

A CERT is a dedicated team tasked with detecting attacks and implementing reactive measures.

Threat Intelligence Sharing Platforms

(TISP)

The term threat intelligence means usable information on threats.

Thus, the selection of reactive measures to stop persistent damage is not trivial and cannot be reduced to a few measures. For this reason, research suggests so-called frameworks for response processes to control reactive measures. Much like damage assessment, this involves putting one's own systems, possible attack scenarios, possible reactive measures, and other framework conditions into a framework. In the event of an attack, reactive measures can thus be taken manually, semi-automatically, or automatically (cf. Nespoli et al. 2018). For example, an attack scenario can be to exploit a buffer overflow on an FTP server. Immediately after detection, this server is automatically disconnected from the network, since the FTP functionality in the example is not deemed critical for the organisation. However, as soon as another server is attacked through this vulnerability, the automatic reaction could be to block the FTP ports on the firewall.

The selection of reactive measures to stop persistent damage is the subject of research. Measures that were effective a few years ago no longer work when dealing with virtual or outsourced IT infrastructures. Automated systems with insights on the network structure, the possible attacks, and the reactive measures can provide a remedy.

### Collection, exchange, and distribution of information

Information on attacks and threats has historically been collected by organisations' IT security departments or Computer Emergency Response Teams (CERTs), for internal use. In recent years, applications have been established to formalize the collection, sharing, and distribution of information related to computer crime. Along the same lines, research has taken up this topic. The aforementioned systems are collectively known as Threat Intelligence Sharing Platforms (TISP).

Information on threats or attackers related to computer crime is called threat intelligence. Several definitions of this term exist. Threat intelligence must be based on relevant information, on the basis of which appropriate actions (reactive and preventive measures) can be carried out. There are different types of threat intelligence (cf. Tounsi/ Rais 2017):

* Strategic Threat Intelligence: Information on the general threat situation caused by computer crime to make strategic decisions about future risks.
* Operational Threat Intelligence: Information on the specific threat situation faced by the individual organisation.

Reactive measures

* Tactical Threat Intelligence: Information on general procedures used by computer criminals. Also referred to as Tactics, Techniques, and Procedures (TTP).
* Technical Threat Intelligence: Information generated by technical components such as servers, clients, firewalls, or switches.

Types of threat intelligence range in descending order according to the long-term nature of the information and the measures resulting therefrom. Technical threat intelligence enables short-term reactions and is thus the basis for reactive measures. The TISPs mentioned above also work mainly with technical threat intelligence (cf. Tounsi/Rais 2017).

During an attack, an organisation's monitoring systems, such as “Splunk” or “Snort”, which are responsible for the identiﬁcation of the attack (intrusion detection), collect a great deal of data. A TISP ﬁlters and correlates this data into so-called Indicators of Compromise (IOC). An IOC is an indication of a successful attack on a system or network. Adding a user to a server's local administrators’ group is not necessarily an IOC. Mass creation of local administrators on different servers can cause a correlation to an IOC. Thus, an IOC is a direct indication of a successful attack.

The distribution and exchange of such information is possible via TISPs. The point of the exchange is that an attack on one organisation can presumably affect other organisations in a timely manner. In the past, such information was exchanged manually between IT security officers (e.g., by telephone). With the help of TISPs, organisations can exchange IOCs and information such as Indicators of Attack (IOA) automatically and without significant delay. In contrast to IOCs, IOAs indicate an immediate attack currently in progress. Some information may be irrelevant to organisation A and critical to organisation B. If malware in organisation A is currently attacking IoT devices with default credentials, this is an IOA. This is not critical to organisation A because the credentials have been changed. After distributing this IOA to organisation B, and since this organisation has not changed the default credentials, a successful attack can be prevented before it hits organisation B.

The benefits of sharing and distributing information are obvious, but there are challenges that come with using TISPs. Data quality must be ensured. A standard for the exchange must be established and a relationship of trust must exist between all parties involved. This is necessary because, for example, IOCs should not be made public or available to malicious parties.

Indicators of Com- promise (IOC)

An Indicator of Com- promise is information indicating that a system or network has been compromised.

### Cooperation with security authorities and cooperation partners

The primary relevant security authority for computer crime in Germany is the Federal Office for Information Security (BSI). Other relevant authorities include the criminal investigation authorities (e.g., state and federal criminal investigation offices, police) and the Federal Office of Civil Protection and Disaster Assistance (BBK). In addition, the competent data protection supervisory authority (federal or state data protection commissioner) may be of relevance, depending on the type of data stolen. In the previous leaning cycle, it has been demonstrated that sharing information on attacks or attempted attacks with authorities and cooperation partners is always beneficial to the community. However, this also poses risks to one' s own organisation, as information on attacks usually contains sensitive data concerning company infrastructure and may also lead to diminished value of the company. Because of this hurdle, cooperation exists on a voluntary and on a compulsory basis.

Critical Infrastructure Operators

Critical infrastructure operators (CIOs) provide important services for a large part of the population and must therefore be particularly well equipped to withstand attacks.

The German Act on Increasing the Security of Information Technology Systems (IT Security Act) requires operators with so-called critical infrastructure to implement minimum standards with regard to IT security. The associated organisations must also submit reports on IT security incidents to the BSI and BBK (cf. Adelmeyer/Petrick/Teute- berg 2017). Critical infrastructure operators include organisations from one of the following sectors (cf. BBK 2020):

* Nutrition,
* Government and administration,
* Energy,
* Health,
* IT and ICT,
* Transportation and traffic,
* Media and Culture,
* Water, and
* Finance and insurance.

There are threshold values for each sector as to when a company belongs to the critical infrastructure. For hospitals, for example, a threshold is defined by the maximum number of available beds. In the case of water utilities, the threshold is defined by the number of citizens to be supplied. All companies within these sectors that exceed the threshold are obliged to cooperate with the security authorities in the event of an IT security incident. One important reason for this is the targeted prevention of further attacks on operators belonging to the same sector.

There is also a duty to cooperate with security authorities when a cyber attack has resulted in the loss of a certain amount of personal data. In order to protect data, article 33 of the GDPR obliges organisations to inform authorities in case

Reactive measures

of a risk to the freedom and rights of natural persons. Typically, these notifications are delivered to state or federal data protection authorities.

Collaboration with cooperation partners is based on voluntary participation and is mainly coordinated via networks such as the Cybersecurity Alliance (ACS). This alliance was founded in 2012 by the BSI and BITKOM. Its purpose is to inform its members regarding cybersecurity and to improve cybersecurity in the Federal Republic of Germany (cf. Eckert 2018). The ACS provides information on the topic of computer crime and cyber attacks. Furthermore, in addition to citizens, companies that are not CIOs can also voluntarily report IT security incidents.

Other countries also have standardised ways of reporting cyberattacks. In the USA, for example, there are several agencies that have been set up as contact points for such reports. In addition to the Federal Bureau of Investigation (FBI), these include the National Cyber Investigative Joint Task Force, Homeland Security Investigations (HSI), and the National Cybersecurity and Communications Integration Center (NCCIC) (cf. Homeland Security 2020).

### Recommended actions for companies

In principle, it is difficult to issue blanket recommended actions to companies in the context of preventive measures, as these recommendations should always be tailored to the circumstances. Depending on the IT infrastructure, the industry, the target area, and the preventive measures already implemented, there are differentiated recommended courses of action. However, the security authorities named in the previous leaning cycle have already drawn up some generic recommended actions.

The ACS has divided general recommended actions following an IT security incident into organisational and technical measures. It also explicitly refers to precautionary measures for IT security incidents and the adaptation of generally applicable recommendations for action to specific circumstances. The organisational recommendations for action after an IT security incident include the following points (cf. Cybersecurity Alliance 2020):

* + - Establishment of a crisis management team: Responsible to take decisions and distribute responsibilities.
    - Internal communication: Internal decision-makers (management, IT security officer, data protection officer, etc.) must be informed about the incident.
    - Information gathering: It is necessary to find out what took place, how this came to light, and what the potential impact is.

*Allianz für Cybersi- cherheit* (ACS or Cybersecurity Alliance)

The ACS is a voluntary association of various organisations with the aim of increasing cybersecurity.

Crisis Management Team A crisis management team must be able to meet at short notice and be

well-equipped with decision-makers to be able to make timely decisions.

Privileged

User Accounts

A privileged user account holds elevated rights within a system. Mostly these accounts reflect administrators or " root " in Linux systems.

Monitoring Monitoring in the IT environment means the supervision of IT systems and networks. This is used to control the status of the systems or to detect attacks.

* External communication: Based on the information gathered, a decision must be made as to how external communication is to be designed. Who may need to be informed?
* External support: Obtain external support to deal with the incident. The yellow pages of the German Electrical and Electronic Manufacturers' Association (VDE) or the BSI's lists of IT security service providers can be of assistance in that regard (cf. BSI 2020; Müller/ Hauschke 2019).

To facilitate initial information gathering, the Cybersecurity Alliance has developed an IT Emergency Card. It provides employees with questions to answer when an IT security incident is discovered. In this way, the information flow gains efficiency, and unnecessary inquiries are prevented (cf. Cybersecurity Alliance 2020).

The checklist of recommended technical actions by the Cybersecurity Alliance should ideally be processed in parallel with organisational measures. The technical recommendations for action include (cf. Cybersecurity Alliance 2019):

* Privileged user accounts: No logins with privileged user accounts should be made using potentially infected systems. In general, a check if new privileged accounts have been created and are used for the attack should be performed.
* Information on the network: Identification of the affected systems. These systems should be disconnected from the network and the internet.
* Compromise: If a service on a system is infected, the entire system should be considered infected. All credentials on an infected system should be considered infected, and if the controller of an Active Directory is infected, the entire network should be considered infected.
* Monitoring: If no monitoring has yet been activated on the network and for logging, such monitoring should be activated in cooperation with the data protection officer and the works council/staff council representative. This should allow the scope of the incident to be assessed, data derival to be detected, and IT forensic measures to be permitted.
* Back-ups: If complete, up-to-date ofﬂine back-ups exist, they should be stored securely and not be connected to the network or any infected system.

In this context, the focus lies on avoiding errors that exacerbate the incident after the fact - such as privileged logins into infected systems. Other subjects of focus include gathering information on monitoring and limiting the incident. In addition to these recommendations, there are also specific instructions addressing attacks involving ransomware or a DDoS.

In principle, planning reactive actions after a security incident does not replace preventive measures. Systematic information security management, including implemented preventive measures, helps to stop computer crime as soon as an attack attempt is made.

Reactive measures

Summary

This unit covered reactive measures, which are measures taken after a security incident. The first learning cycle covers the subject of damage extent and initial assessment. First, it was explained what primary and secondary consequences are and what the general consequences of a cyber attack may be. It was also explained that the extent of damage in modern IT infrastructures is only possible with the help of automated systems and knowledge about the infrastructure and the attack.

The second learning cycle addresses the interruption of persistent damage. General advice was provided, such as disconnecting the power or network connection of infected systems. However, these measures no longer work reliably in modern IT infrastructures with virtual and cloud-based environments, meaning that automated systems have also found their way in here. These systems have the capability to automatically or semi-automatically take action to stop persistent damage.

Another topic was the collection and exchange of information. Indicators of Compromise and Indicators of Attack were presented. These are aggregated pieces of information that allow the drawing of specific conclusions about attacks. These IOCs and IOAs can then be exchanged and distributed via Threat Intelligence Sharing Platforms to provide protection to other organisations against the same attack.

The fourth learning cycle outlines the cooperation with security authorities and cooperation partners. A distinction must be made between voluntary and compulsory cooperation. Under the IT Security Act and the GDPR, operators of critical infrastructure are obliged to pass on information on security incidents to security authorities such as the BSI or the BBK. It is also possible to share information with cooperation partners via voluntary associations, such as the Alliance for Cybersecurity.

The final learning cycle presents recommended actions for companies after a security incident. It uses suggestions from the Cybersecurity Alliance, which are divided into organisational and technical recommended actions.



# Unit 8

## The current security situation

#### LEARNING OBJECTIVES

Upon completion of this unit, you will know….

... which security authority reports are relevant.

... which long-term and short-term conclusions to draw from the reports.

... which current topics are covered by the Europol Awareness Campaign.

DL-D-DLMIMWCK01-L08

1. The current security situation

### Introduction

Netscaler A Netscaler controls access from external IT systems to internal systems or applications. A Netscaler combines the functions of a firewall, a VPN, and Load Balancers.

*Polizeiliche Kriminal-*

*statistik* (Police Crime   
Statistics or PKS)

The police crime statistics are aggregated statistics on the criminal statistics data in Germany's federal states.

The current security situation is sometimes difficult to assess but provides important information on strategic and also operational measures against cybercrime. The latest situation reports published by the national security authorities, for example, state that ransomware is a favorite tool used by cybercrime operators. This makes encryption Trojans the most likely attack scenario for organisations. Knowing this, the focus can be placed on high-quality ofﬂine back-ups. The current security situation also includes ad-hoc reports, such as the January 2020 vulnerability in Citrix Netscaler. Netscaler is intended for internet access to internal resources, and for this reason, is exposed to the internet. This vulnerability was present on a large number of Netscaler. This change in the security posture must be responded to immediately with operational protections to prevent infection.

### Current reports by security authorities

In the German environment, several security authorities issue reports on IT security, cybersecurity, or computer crime. For example, the BSI annually publishes a report on the state of IT security in Germany. The 2019 report outlines ransomware as the main focus of cyberattacks, in particular in connection with the malware "Emotet". In addition to this area of focus, identity theft and botnets with spam and DDoS attacks are also presented (cf. BSI 2019b).

In addition to the BSI, the BKA also publishes a report on cyber and computer crime. The 2018 Federal Situation Report presents some key figures on cybercrime:

* 87,106 cases of cybercrime in the narrower sense,
* 271,864 cases involving the internet (this corresponds to 4.9% of all recorded crimes), and
* 60.7 million euros in damage caused by computer fraud.

In addition to these figures, which have their basis in Police Crime Statistics (PKS) and concrete criminal law paragraphs, a steady increase in the number of cybercrimes in the narrower sense is pointed out. In addition to identity theft, DDoS attacks, and ransomware, cybercrime-as-a-service and customized, multilayer malware packages are also listed as "phenomena in the field of cybercrime" (cf. BKA 2018).

In its capacity as the U.S. security authority, the FBI also publishes an Internet Crime Report. The data in this report is based on the crime statistics of the Internet Crime Complaint Center and thus on public data supplied by the security authorities.

The current security situation

Ransomware is, once again, named as the "hot topic" for 2019. In addition, however, criminal approaches that specifically target older people are also mentioned, as are approaches based on posing as technical support staff in order to convince victims to release control of their computers (cf. IC3 2019).

One report by a multinational institution is the Threat Landscape of the European Union Agency for Cybersecurity (ENISA). In addition to an overview of the top 15 threats, in which malware takes the first place, an assessment of the COVID 19 pandemic in terms of cybersecurity is also provided there. In this context, ENISA presents the cybersecurity difficulties of the large proportion of home-based workplaces in the wake of the pandemic. As a result, much of organisations' data leaves the supposedly secure internal network. Thus, new protections must be established for this form of work. In general, the pandemic is a catalyst for the digitization of processes and thus also calls for innovative forms of protective measures (cf. ENISA 2020).

Another source of reports on the security situation is the Cybersecurity Cluster Bonn e. V. and the associated *Weisenrat für Cyber-Sicherheit* (Council of Eminent Persons for Cybersecurity). The Cybersecurity Cluster Bonn e. V. was founded together with the BSI, the German Armed Forces Cyber and Information Space, and Fraunhofer SIT, among others, and regularly produces reports on cybersecurity. In the annual report of the Council of Eminent Persons for Cybersecurity 2020, recommendations are made on how (cf. Council of Eminent Persons for Cybersecurity 2020):

* Technology must adapt to people in order to relieve and protect them.
* Manufacturers must commit to regular vulnerability testing and security updates.
* Digital processes and infrastructures must become more attack-resistant.
* Sustainable products must be designed to be cryptoagile.

Although these recommendations are at a high level of abstraction, such strategic recommendations are also part of the long-term security situation. Other sources for reports of this kind are research institutions specifically dealing with this topic (e.g., the Fraunhofer Institute), security authorities of other nations (e.g., the National Crime Agency - UK), or special associations or clusters focusing on computer crime or cybersecurity (e.g., the Information Security Forum).

### Evaluation of the security authorities' recommendations

The BSI's 2019 situation report includes the following current attack types and associated recommendations (cf. BSI 2019b):

Cryptoagility

Cryptoagility is the capability of a crypto system to replace cryptograﬁcal algo- rithms that have become insecure, thus ensuring a continuously secure state.

|  |  |
| --- | --- |
| Lagebericht des BSI aus dem Jahr 2019 | |
| Angriffsart | Empfehlung |
| Identitätsdiebstahl | * Verwendung von HTTPS statt HTTP * Multi-Faktor-Authentiﬁzierung * Anti-Spooﬁng-Maßnahmen (bspw. DMARC oder SPF) |
| Schadprogramme | * Verwendung ständig aktueller Sicherheitsupdates * Ofﬂine-Back-ups * Monitoring |
| Ransomware | * entsprechende Backupstrategie * restriktive Nutzung von RDP- und anderen Freiga- ben nach außen |
| DDoS | * spezialisierte Dienstleister |
| Botnetze | * Patchmanagement |
| Spam | * Awareness |

These recommendations represent basic preventive measures, which are also recommended as part of IT-Grundschutz. These measures are classified according to the corresponding current attack strategies. They do not represent new findings to organisations that are already dealing with information or IT security. For small and medium-sized enterprises that want to prepare themselves for current threats, this represents a list of the most urgent measures in short form. It should by no means be regarded as exhaustive (cf. BSI 2019b).

The FBI and BKA reports focus on similar topics and recommendations, with a greater degree of emphasis on private individuals. The recommendations of the Council of Eminent Persons for Cybersecurity are interesting, but the high level of abstraction means that they cannot be translated into concrete measures. The first recommendation aims to stop considering people as the weakest link in cybersecurity and to prevent people's mistakes through technology if possible.

The current security situation

Organisations are making attempts to teach security awareness to their employees, but the success rates are rather low. Thus, technology is more likely to catch the risks of cybercrime and prevent human errors. This necessitates the consideration of security aspects as early as when technologies are being designed (Security by Design).

Another recommendation is to perform vulnerability tests and security updates on a regular basis. Vulnerability testing is sometimes performed when technologies are designed, but usually not on an ongoing basis as the technology is developed. This process must be made more permanent, for example by obliging organisations to introduce Vulnerability Disclosure Programs (VDP) as part of their own technology development. This means that vulnerabilities can be safely reported by security researchers and even rewarded.

In addition to technology, digital processes and infrastructures should also be strengthened to counter attacks. On the one hand, attacks must be made more difficult through measures such as security by design or patch management. On the other hand, parts of a process or infrastructure should continue to function even during an attack. The report of the Council of Eminent Persons calls for a political framework in that respect, such as minimum standards for IT security in companies (cf. the Council of Eminent Persons for Cybersecurity 2020).

The last recommendation made also carries great importance: cryptoagile products. Cryptoagility in this context describes the property of products to be capable of keeping cryptographic procedures up to date in the long term. Cryptographic procedures and secure key lengths have been repeatedly discarded as insecure in recent years. Products with non-interchangeable procedures thus became insecure. Assume that a software product released in 1980 exclusively supports the DES encryption method with a key length of 56 bits that was current at that time. This implementation has been obsolete since 1997. Unless the software is cryptoagile and the encryption method can be replaced with, for example, its successor AES, the software can no longer be used securely. Cryptoagile products should be capable of using new cryptograﬁc methods over their lifetime to prevent any vulnerabilities. This recommendation also refers specifically to future quantum computing, since this technology of the future requires new cryptographic processes (post-quantum cryptography) and makes some current processes (especially asymmetric processes) obsolete.

### Current topics of the Europol Awareness Campaign

The Europol Awareness Campaign is a prevention campaign run by the European Cybercrime Centre (EC3) in cooperation with many European countries. Mostly one-page information sheets on specific focal points are produced to draw attention to this topic and to raise awareness among organisations and private individuals. In 2016, the focus was on mobile awareness. In addition to the threat posed by malware from the web or app stores, information on mobile ransomware is also provided. Advice to organisations and on the use of mobile end devices is provided also. Below is a list of recommendations on how to deal with mobile devices in the corporate environment (cf. EC3 2020):

Security by Design The principle of security by design implies that importance is attached to IT security as early as when technologies are being designed. For example, measures to enhance security are implemented directly and user errors are also prevented.

Vulnerability Disclo- sure Programs (VDP) A VDP allows security researchers to report security vulnerabilities in software or websites to operators without the threat of penalties, allowing them to be resolved.

Patch Management Patch management is concerned with regular checks on the availability of updates or patches for any software in use as well as their installation.

Quantum Computing Quantum computing refers to the use of quantum computers. Quantum computers possess the potential to exceed the computing power of computers based on semiconductors.

Bring Your Own

Device "Bring your own device" is a company policy that allows the use of personal devices by employees.

Jailbreak and Roo-

ting "Jailbreak" or "Rooting" refers to the process of unlocking a mobile device from the manufacturer's restrictions, i.e. obtaining root rights.

Cyberscam Cyberscam refers to the types of fraud perpetrated with the help of the internet.

* Employee information: Employees must be trained to understand the risks of using mobile devices.
* Guidelines for BYOD (Bring your own device): If employees are allowed to use their own devices, rules must be defined accordingly.
* Guidelines for mobile devices: Guidelines must be defined and reviewed. If a device does not meet these guidelines, it must not be connected to the network.
* Caution with public networks: Public networks represent a major risk factor when it comes to corporate data.
* Software updates: Software updates must always be applied promptly.
* Apps from trusted sources only: Apps and software for mobile devices must only be obtained from trusted sources.
* Prevent Jailbreak/Rooting: Jailbreak and Rooting must be prevented or prohibited.
* Consideration of cloud storage: The use of cloud storage should be weighed against storing data on the mobile device.
* Mobile security app: Mobile security apps can be installed for additional monitoring of the mobile device software.

These recommendations provide a solid basis for the use of mobile devices in organisations. The theme of the Europol Awareness Campaign in 2017 was “Say No”, The aim was to show young people the threat of IT skills for malicious purposes.

In 2018, the European Cybercrime Centre focused on the topic of cyberscam. Different types of cyber scams were the subject of discussion, such as CEO Fraud, phishing, investment fraud, and online shopping fraud. For organisations, CEO Fraud is particularly relevant, as it can be used to obtain payment requests from business accounts. In addition to employee awareness and the dual control principle, patch management, as well as internal logging, were presented as recommended countermeasures. It was also pointed out that publicly available information, as the one contained in organisational charts, telephone lists, or descriptions of internal processes, should be kept to a minimum, as it can be used to launch attacks that appear authentic.

Recommendations of this kind have a short lifespan, especially with regard to computer crime, and must be updated regularly. In this area, new combinations of attacks and completely new types of attacks emerge within a short period of time. Thus, up-to-date recommendations are necessary here at all times in order to react to current threats.

The current security situation

Summary

In this unit, the current security situation and sources were analyzed for evaluation. First, the reports of the security authorities were presented. These include ofﬁcial German institutions such as the BSI and the BKA. However, reports from foreign security organizations such as the FBI are also of interest. In addition to these sources, non-governmental organizations and their reports were also presented, such as the Cybersecurity Cluster Bonn e. V.

These reports and the recommendations they contain were evaluated. A clear distinction must be made between security authority reports, such as those of the BSI or FBI, which present the current security situation and make recommendations in the form of preventive measures, on the one hand, and strategic recommendations, such as those of the Cybersecurity Cluster Bonn, on the other hand. Both should be considered at different time scales. For example, recommendations from the BSI, such as patch management, can and should be implemented immediately. By contrast, recommendations, such as security by design or designing cryptoagile products, can be implemented over a longer-term planning horizon.

At the end of this unit, the Europol Awareness Campaign was highlighted. It provides preventive explanations on certain key cybersecurity risk topics. The focus of the last years was placed on mobile awareness and cyberscam.



# Appendix 1

## Bibliography

Bibliography

Adelmeyer, M./Petrick, C./Teuteberg, F. (2017): *IT risk management of cloud services in the context of the IT security law.* In: HMD Praxis der Wirtschaftsinformatik, 54. Jg., Heft 1, S. 111–123.

Adloff, N. (2020): *Emotet – Erfolgsgeschichte einer Malware. [Emotet - success story of a malware.]* In: Revisionspraxis PRev., Heft 1, S. 16–20.

Agraﬁotis, I. et al. (2018): *A taxonomy of cyber-harms: Deﬁning the impacts of cyber- attacks and understanding how they propagate*. In: Journal of Cybersecurity, 4. Jg., Heft 1, S. 1–15.

Allianz für Cybersicherheit (2019): *Ich habe einen Vorfall – Checklisten. [I have a situation - checklists.] (URL:* https:// [www.allianz-fuer-cybersicherheit.de/ACS/DE/IT-Sicherheitsvorfall/Unternehmen/unter-](http://www.allianz-fuer-cybersicherheit.de/ACS/DE/IT-Sicherheitsvorfall/Unternehmen/unter-) nehmen\_node.html?nn=13221194&cms\_pos=3 [letzter Zugriff: 09.12.2020]).

Allianz für Cybersicherheit (2020): *Verhalten bei IT-Notfällen. [Required conduct in the event of IT emergencies.]* (URL: https://www.allianz- fuer-cybersicherheit.de/SharedDocs/Downloads/ACS/Notfallkarte/IT-Notfall- karte\_DINA4.pdf? blob=publicationFile&v=10 [letzter Zugriff: 09.12.2020]).

Amro, S./Alkhalifah, A. (2019): *A Comparative Study if Virus Detection Techniques.* In: International Journal of Computer and Information Engineering, 9. Jg., Heft 6, S. 1566– 1573.

Barrientes, C. et al. (2018): *Source Code Analysis for Secure Programming Practices.* In: International Conference on Computational Science and Computational Intelligence (CSCI), S. 819–824.

BBK – Bundeamt für Bevölkerungsschutz und Katastrophenhilfe (2020): *Deﬁnition "Kri- tische Infrastruktur". [Definition “Critical infrastructure”.]*

(URL: https://[www.kritis.bund.de/SharedDocs/](http://www.kritis.bund.de/SharedDocs/) Downloads/BBK/DE/Downloads/Kritis/KRITIS\_Sektoreneinteilung.pdf? blob=publica- tionFile [letzter Zugriff: 09.12.2020]).

BKA – Bundeskriminalamt (2018): *Cybercrime – Bundeslagebild. [Federal Report on cybercrime]* (URL: https:// [www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/](http://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/) Cybercrime/cybercrimeBundeslagebild2018.html?nn=28110 [letzter Zugriff: 09.12.2020]).

BKA – Bundeskriminalamt (2020): *Cybercrime – Deﬁnition und Erscheinungsformen. . [Cybercrime definitiond and occurences]* (URL: https://[www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cyberc-](http://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cyberc-) rime\_node.html [letzter Zugriff: 09.12.2020]).

Bond, M. (2020): *VulnHub — Kioptrix: Level 4*. (URL: https://bond-o.medium.com/vuln- hub-kioptrix-level-4-bc4184a79eeb [letzter Zugriff: 09.12.2020]).

Bonik, M./Schaale, A. (2016): *Internetpiraterie. [Internet piracy]* In: Informatik Spektrum, 39. Jg., Heft 5, S. 393–396.

Brodowski, D./Freiling, F. (2011): *Cyberkriminalität. Computerstrafrecht und die digitale Schattenwirtschaft.* *Cybercrime. [Computational Criminal Law and the Digital Shadow Economy.]* Freie Universität Berlin, Berlin.

Bryant-Smith, R. (2018): *Culture eats compliance for breakfast: Why team culture is the key to risk management.* In: Governance Directions, 70. Jg., Heft 7, S. 414–418.

BSI – Bundesamt für Sicherheit in der Informationstechnik (2011): *BSI Leitfaden IT- Forensik. [BSI Guide IT Forensics.]* BSI, Bonn.

BSI – Bundesamt für Sicherheit in der Informationstechnik (2017): *BSI Standard 200*–*1.*

Bundesanzeiger, Köln.

BSI – Bundesamt für Sicherheit in der Informationstechnik (2019a): *IT-Grundschutz- Kompendium [IT-Grundschutz Compendium.] , 2. Edition 2019.* Bundesanzeiger, Köln.

BSI – Bundesamt für Sicherheit in der Informationstechnologie (2019b): *Die Lage der IT-Sicherheit in Deutschland.* [*The state of IT security in Germany.]* BSI, Bonn.

BSI – Bundesamt für Sicherheit in der Informationstechnologie (2020): *Liste zertiﬁzierter IT-Sicherheitsdienstleister in den Geltungsbereichen IS-Revision und IS-Penetrationstests. [List of certiﬁed IT security service providers in IS auditing and IS penetration testing.]* (URL: https://[www.bsi.bund.de/DE/Themen/ZertiﬁzierungundAnerkennung/](http://www.bsi.bund.de/DE/Themen/ZertiﬁzierungundAnerkennung/) Stellen/IS\_REV\_PEN/IS\_REV\_Dienstleister/IS\_REV\_Dienstleister\_node.html [letzter Zugriff: 09.12.2020]).

Burato, E./Ferrara, P./Spoto, F. (2017): *Security Analysis of the OWASP Benchmark with Julia*. First Italian Conference on Cybersecurity, Venedig (ITA).

Collins, F. (2017): *Watson for Cyber Security – sort of like 'Minority Report', but for cybercrime.* (URL: https://[www.linkedin.com/pulse/watson-cyber-security-sort-like-minority-](http://www.linkedin.com/pulse/watson-cyber-security-sort-like-minority-) report-fred-collins [letzter Zugriff: 09.12.2020]).

Congmiao, L. (2020): *Securing Computer Systems Through Cyber Attack Detection at the Hardware Level.* University of California, Irvine (USA).

Coulibaly, K. (2020): *An overview of Intrusion Detection and Prevention Systems*. Cornell University, Ithaca (USA).

Crelin, J. (2020): *Denial-of-Service attack*. Grey House Publishing, Amenia (USA).

Da Veiga, A. (2015): *An Information Security Training and Awareness Approach (ISTAAP) to Instil an Information Security-Positive Culture.* Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance, Lesvos (GRC).

Deutscher Bundestag/WD – Wissenschaftlicher Dienst (2014): *"Identitätsdiebstahl" im Internet. Überblick und rechtliche Implikationen. ["Identity Theft" on the Internet. Overview and legal implications.]* (URL: https://[www.bundestag.de/](http://www.bundestag.de/) resource/blob/480340/aad11f36eec56c3cbad0b94973dff9b7/WD-7-183-14-pdf-data.pdf [letzter Zugriff: 09.12.2020]).

Eckert, C. (2018): *IT-Sicherheit. Konzepte – Verfahren – Protokolle. [IT Security. Concepts - Procedures - Protocols.]* De Gruyter Studium, Berlin.

EC3 – European Cybercrime Centre (2020): *Europol Awareness Campaign*. (URL: https:// [www.bka.de/DE/IhreSicherheit/RichtigesVerhalten/StraftatenImInternet/EuropolAware-](http://www.bka.de/DE/IhreSicherheit/RichtigesVerhalten/StraftatenImInternet/EuropolAware-) nessCampaign/europolAwarenessCampaign\_node.html [letzter Zugriff: 09.12.2020]).

ENISA – European Union Agency for Cybersecurity (2020): *ENISA Threat Landscape.*

ENISA, Iraklio (GRC).

Evans, R. (2019): *The Future of Security, Yesterday: All About Authentication, Authoriza- tion and More*… University of Georgia, Athen (USA).

Farah, T. et al. (2017): *Study of the Dirty Copy on Write, a Linux Kernel memory Allocation Vulnerability*. International Conference on Consumer Electronics and Devices, London (GBR).

Fireeye Mandiant (2020): *M-Trends 2020.* Fireeye, Milpitas (USA).

FIRST (2017): *Common Vulnerability Scoring System v 3.0.* First, Cary (USA).

Gens, D. (2019): *OS-Level Attacks and Defenses: From Software to hardware-based exploits.* Technische Universität Darmstadt, Darmstadt.

Goodin, D. (2020): *When coffee makers are demanding a ransom, you know IoT is scre- wed.* (URL: https://arstechnica.com/information-technology/2020/09/how-a-hacker- turned-a-250-coffee-maker-into-ransom-machine/ [letzter Zugriff: 09.12.2020]).

Hasso-Plattner-Institut (2020): *HPI Identity Leak Checker*. (URL: https://sec.hpi.de/ilc/ search?lang=de [letzter Zugriff: 09.12.2020]).

Heidrich, J. et al. (2020): *Daten-Leak bei Autovermietung Buchbinder: 3 Millionen Kun- dendaten offen im Netz. [Data leak at Buchbinder car rental company: 3 million customer data exposed on the web.]* (URL: https://[www.heise.de/ct/artikel/Daten-Leak-bei-Autover-](http://www.heise.de/ct/artikel/Daten-Leak-bei-Autover-) mietung-Buchbinder-3-Millionen-Kundendaten-offen-im-Netz-4643015.html [letzter Zugriff: 09.12.2020]).

Hofer, A./Weiß, M. (2016): *Wirtschafts- und Industriespionage. [Economic and industrial espionage.]* Springer Fachmedien, Wiesbaden.

Homeland Security (2020): *Cyber Incident Reporting. A Uniﬁed Massage for Reporting to the Federal Government.* (URL: https://[www.dhs.gov/sites/default/ﬁles/publications/](http://www.dhs.gov/sites/default/ﬁles/publications/) Cyber%20Incident%20Reporting%20United%20Message.pdf [letzter Zugriff: 09.12.2020]).

Horten, B./Gräber, M. (2020): *Cyberkriminalität*. [*Cybercrime*.] In: Forensische Psychiatrie, Psychologie, Kriminologie, 14. Jg., S. 233–241.

Huber, E. (2019): *Cybercrime: Eine Einführung.* [*Cybercrime introduction*.] Springer VS, Wiesbaden.

Literaturverzeichnis

Humpert, F. (2004): *IT-Sicherheit.* [*IT-security*.] In: HMD – Praxis der Wirtschaftsinformatik, 10. Jg., Bd. 236.

Hunt, T. (2020): *haveibeenpwned.* (URL: https://haveibeenpwned.com/ [letzter Zugriff: 09.12.2020]).

IC3 (2019): *Internet Crime Report.* FBI National Press, Washington, D. C. (USA).

ISIS12 (2018): *Handbuch zur efﬁziente Gestaltung von Informationssicherheit für kleine und mittlere Organisationen.* *[Handbook on efﬁcient design of information security for small and medium-sized organizations.]* ISIS12, Bayreuth.

Johnson, A./Ward, R. (2020): *Introduing The 'Uniﬁed Side Channel Attachl Model' (USCA- M).* 8th International Symposium on Digital Forensics and Security (ISDFS), Beirut (LBN).

Khan, M./Siddiqui, S./Ferens, K. (2017): *Cognitive Modeling of Polymorphic Malware Using Fractal Based Semantic Characterization.* IEEE International Symposium in Tech- nologies for Homeland Security (HST), Boston (USA).

Kleijssen, J./Perri, P. (2017): *Cybercrime, evidence and Territoriality: Issues and Options.*

In: Netherlands Yearbook of International Law, 47. Jg., S. 147–172.

Koch, A. (2008): *Denial-of-Service-Angriffe, Computersabotage § 303b StGB.* Studien zum Strafrecht *[Denial-of-service attacks, computer sabotage Section 303b StGB. Criminal law studies]*, Bd. 16, S. 126–127.

Kotenko, I./Chechulin, A. (2013): *A Cyber Attack Modeling and Impact Assessment Fra- mework.* 5th International Conference on Cyber Conﬂict, Tallinn (EST).

Kraatz, E. (2016): *Aktuelle examensrelevante Fälle des Computerbetrugs (§ 263a StGB).*

*[Current exam-relevant cases of computer fraud (Section 263a StGB)]*

In: Juristische Ausbildung, Heft 8, S. 875–883.

Laborde, R. et al. (2020): *A User-Centric Identity Management Framework based on the W3C Veriﬁable Crdentials and the FIDO Universal Authentication Framework.* IEEE 17th Annual Consumer Communications & Networking Conference, Las Vegas (USA).

Lekha, K./Praksam, D. (2017): *Data mining techniques in detecting and predicting Cyber crimes in Banking sector.* Conference: IEEE sponsored International Conference on Energy, Communication, Data Analytics and Soft Computing Vol. III. IEEE, Chennai (IND).

Lin, X. (2018): *Introductory Computer Forensics.* Springer Nature Switzerland, Cham.

Lipp, M. et al. (2018): *Meltdown*. Graz University of Technology, Graz (AUT).

Mahjabin, T./Yiao, Y. (2019): *Mitigation Process for DNS Flood Attacks.* 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas (USA).

Marchetti, M. et al. (2016): *Analysis of high volumes of network trafﬁc for Advanced Per- sistent Threat detection.* In: Computer Networks, 109. Jg., S. 127–141.

Marge, R./Iovan, S. (2018): *The Impact of Economic Company Data Theft.* In: Fiabilitate si Durabilitate, Heft 1, S. 273–278.

Meijer, A./Wessels, M. (2019): *Predictive Policing: Review of Beneﬁts and Drawbacks.* In: International Journal of Public Administration, 42. Jg., Heft 12, S. 1031–1039.

Morel, L./Courousse, D. (2019): *Idols with Fett of Clay: On the Security of Bootloaders and Firmware Updaters for the IoT.* 17th IEEE International New Circuits and Systems Conference, München.

Müller, S./Hauschke, S. (2019): *VDE/DKE Yellow Pages zum IT-Security NAVIGATOR.* VDE, Frankfurt a. M.

Namanya, A. et al. (2018): *The World of Malware: An Overview*. IEEE 6th International Conference on Future Internet of Things and Cloud, Barcelona (ESP).

Narayanan, A. et al. (2017): *A multi-view context-aware approach to Android malware detection and malicious code localization.* In: Empirical Software Engineering, 23. Jg., Heft 3, S. 1222–1274.

Nespoli, P. et al. (2018): *Optimal Countermeasures Selection Against Cyber Attacks: A Comprehensive Survey on Reactions Frameworks.* In: IEEE Communications Surveys & Tutorials, 20. Jg., Heft 2, S. 1361–1396.

Nicola, S. (2019): *Hackers Dump Data on Merkel, Politicians in Giant German Leak.*

Bloomberg, NYC.

Oberly, D. (2019): *Best Practices for Effectively Defending Against Ransomware Cyber Attacks*. In: Intellectual Property & Technology Law Journal, 31. Jg., Heft 7, S. 17–20.

OWASP – Open Web Application Security Project (2017): *OWASP Top 10.* (URL: https:// wiki.owasp.org/images/9/90/OWASP\_Top\_10-2017\_de\_V1.0.pdf [letzter Zugriff: 09.12.2020]).

Pierson, M./Ahrens, T./Fischer, K. (2018): *Recht des geistigen Eigentums. [Intellectual property right.]* A. Franke, Tübingen.

Pitolli, G. et al. (2020): *MalFamAware: Automatic Family Identiﬁcation and Malware Classiﬁcation Through Online Clustering*. International Journal of Information Security, University of Southampton (GBR).

Pritchard, J. (2020): *Trusted Platform Module (TPM).* Grey House Publishing, Amenia (USA).

Reynolds, J. K./Postel, J. (1992): *Request for Comments 1340, Assigned Numbers.* USC/ Information Sciences Institute, Marina del Rey (USA).

Literaturverzeichnis

Rios, B./Butts, J. (2017): *Security Evaluation of the Implantable Cardiac Device Ecosys- tem Architecture and Implementation Interdependencies.* (URL: https://www.ledeco- deur.ch/wp-content/uploads/2017/05/Pacemaker-Ecosystem-Evaluation.pdf [letzter Zugriff: 09.12.2020]).

Schwarz, M. et al. (2019): *ZombieLand: Cross-Priviledge-Boundary Data Sampling*. Cor- nell University, Ithaca (USA).

Sharma, N. V./Kavita/Agarwal, G. (2019): *Network Attacks and Intrusion Detection Sys- tem: A Brief.* 2nd International Conference on Intlligent Communcation and Computatio- nal Techniques (ICCT), Jaipur (IND).

Singelnstein, T. (2011): *Erfüllt die Angabe falscher Personalien bei Auktionensgeschäf- ten im Internet den Tatbestand des § 269 StGB?* [*Does the provision of fake personal data in online auction transactions constitute an offense under Section 269 of the German Criminal Code?]* In: Juristische Rundschau, 86. Jg., Heft 9, S. 375–381.

Sokolov, D. (2020): *Massive Bitcoin-Betrugswelle überrollt Twitter. [Massive Bitcoin scam wave sweeps Twitter.]* (URL: https:// [www.heise.de/news/Massive-Bitcoin-Betrugswelle-ueberrollt-Twitter-4844911.html](http://www.heise.de/news/Massive-Bitcoin-Betrugswelle-ueberrollt-Twitter-4844911.html) [letz- ter Zugriff: 09.12.2020]).

Stelzer, D. (1993): *Sicherheitsstrategien in der Informationsverarbeitung – Ein wissens- basiertes, objektorientiertes Beratungssystem für die Risikoanalyse. [Security strategies in information processing - A knowledge-based, object-oriented advisory system toward risk analysis.]* Deutscher Universi- tätsverlag, Wiesbaden.

Stirnimann, S. (2018). *Der Mensch als Risikofaktor bei Wirtschaftskriminalität. [Humans as a risk factor in white-collar crime.]* Springer Gabler, Wiesbaden.

Tanriverdi, H./Streule, J. (2020): *BMW von Hackern ausgespäht*. *[BMW targeted by hackers.]* (URL: https:// [www.tagesschau.de/investigativ/br-recherche/bmw-hacker-101.html](http://www.tagesschau.de/investigativ/br-recherche/bmw-hacker-101.html) [letzter Zugriff: 09.12.2020]).

The MITRE Cooperation (2020): *CVE-2019-19781.* (URL: https://cve.mitre.org/cgi-bin/ cvename.cgi?name=CVE-2019-19781 [letzter Zugriff: 09.12.2020]).

The No More Ransom Project (2020): *No More Ransom*. (URL: https://www.nomoreran- som.org/ [letzter Zugriff: 09.12.2020]).

Tounsi, W./Rais, H. (2017): *A survey on technical threat intelligence in the age of sophis- ticated cyber attacks*. In: Computers & Security, 72. Jg., S. 212–233.

Wang, Z./Sun, L./Zhu, H. (2020): *Deﬁning Social Eingineering in Cybersecuriy*. In: IEEE Access, 8. Jg., S. 85.094–85.115.

Weisenrat für Cyber-Sicherheit (2020): *Jahresbericht des Weisenrats für Cyber-Sicher- heit.[ Annual Report of the Council of Eminent Persons on cybersecurity].* Weisenrat für Cyber-Sicherheit, Bonn.

Wikimedia Commons (2009): *TPM Asus.* (URL: https://commons.wikimedia.org/wiki/ File:TPM\_Asus.jpg [letzter Zugriff: 11.12.2020]).