**QUESTION 1OF 319**

**DLMIMWCK01\_Open\_light/Lesson 01**

What are the characteristics of a root kit and what functionalities does it provide? Explain briefly.

A rootkit can take complete control of a computer. The name comes from the user of administrative rights on Linux systems (“root”) and thus describes the basic functionality of rootkits: gaining elevated rights on a computer, thereby taking complete control. [3 points]

In addition to gaining elevated rights, rootkits can hide themselves by migrating into legitimate processes or providing their functionality without a file. Moreover, they can secure permanent access by building backdoors into systems. In most cases, rootkits also provide the ability to install additional modules. [3 points]

**QUESTION 3 OF 319**

**DLMIMWCK01\_Open\_light/lesson 01**

What is the main characteristic of ransomware? Name and briefly describe two ways ransomware works.

Ransomware attempts to extort a ransom by launching attacks on computers and systems. These attacks are only stopped once the ransom has been paid. [2 points]

[2 points per method]

DoS attack: Here, systems are blocked through the generation of mass access attempts. This blockade only ends once the ransom has been paid.

Encryption trojan: A trojan encrypts all of an organization’s data, making it inaccessible to the organization. The key to unlock the data is, supposedly, released once the ransom has been paid.

**QUESTION 4 OF 319**

**DLMIMWCK01\_Open\_medium/Lesson 01**

Briefly describe the differences between the terms “computer crime” and “internet crime”. Which umbrella English term are both phenomena combined under? Briefly discuss to what extent the distinction between the two individual terms is meaningful in the current context.

There is no uniform definition of the terms “computer crime” and “internet crime”. In general, computer crime is understood to be all acts that are directed against computers or that use a computer as a tool. [2 points]

Internet crime, in turn, covers all acts that involve the use of the internet. [2 points] Cybercrime combines both phenomena. [1 point]

Since a computer or modern information and communication technology is always used for cybercrime, these two terms merge and are referred to collectively in English as “cybercrime”. [1 point]

**QUESTION 5 OF 319**

**DLMIMWCK01\_Open\_medium/Lesson 01**

Name and briefly describe the five levels used to classify vulnerabilities and then categorize the following example under one of the levels. Give reasons for your choice. Example:

When a certain set of laptops is booted, a possibly connected device is analyzed during the initialization of the USB interfaces, and program code may under certain circumstances be executed on the USB device in the process. This allows an attacker to gain elevated rights.

5 levels [15 points; 3 per level + description]:

Vulnerabilities at the chip or firmware level relate to vulnerabilities on processors or the firmware. Firmware is the software that provides low-level functions of the hardware.

Operating system level vulnerabilities. Operating system level vulnerabilities affect the software that make all the hardware resources available to the application software.

Vulnerabilities at the network and server level

These are vulnerabilities that are based on communication between systems in a network or that exploit server functionalities of a system.

Application level vulnerabilities

These are vulnerabilities that exploit applications. Applications are any programs that run on an operating system and are provided with access to resources on it.

Vulnerabilities at the organizational level

Vulnerabilities at the organizational level relate to guidelines, processes, and organizational structures.

The example can, for instance, be classified as a firmware or operating system vulnerability. The justification is important. Obviously, the software that aims to make the USB device available to the rest of the system executes program code contained on the device. Normally, this software is only supposed to detect and analyze the device, but in this case, code is executed through a vulnerability.

This software is called firmware because it provides low-level hardware functionality, so this is a firmware level vulnerability. [3 points]

The president of an organization reports increased attempts to contact them on social media from people they do not know.

What type of attack may be in progress here and what is the attacker’s goal? Name three typical goals that the attacker may be trying to achieve through these attempts to contact.

**QUESTION 6 OF 319**

**DLMIMWCK01\_Open\_medium/Lesson 01**

The attacker is attempting to gather information about an individual and extract that information from them. The targeted person is a high-value target as access to an organization’s president can yield valuable information or possibly large sums of money. As such, this attack qualifies as whaling. Whaling describes attacking “whales” i.e., high-value targets. [3 points]

Possible uses for the information of a high-value target include [1 point per example; max. 3 points]

CEO fraud, theft of sensitive data, and obtaining access data .

Name the five levels into which weaknesses can be classified and then categorize the following example into one of the levels. Give reasons for your choice.

Example:

During an update, a payroll application opens a TCP port to check for update dependencies. If an attacker sends certain requests to this port, the application sends back sensitive information in response.

**QUESTION 7 OF 319**

**DLMIMWCK01\_Open\_medium/Lesson 01**

5 levels [15 points; 3 per levels + description]:

Vulnerabilities at the chip or firmware level
Relate to vulnerabilities on processors or the firmware. Firmware is the software that provides low-level functions of the hardware.

Operating system level vulnerabilities

Operating system level vulnerabilities affect the software that makes all hardware resources available to the application software.

Vulnerabilities at the network and server level

These are vulnerabilities that are based on communication between systems in a network or that exploit server functionalities of a system.

Application level vulnerabilities

These are vulnerabilities that exploit applications. Applications are any programs that run on an operating system and are provided with access to resources on it.

Vulnerabilities at the organizational level

Vulnerabilities at the organizational level relate to guidelines, processes, and organizational structures.

The example can, for instance be classified as a network or application level vulnerability. The justification is important. Obviously, the application is not processing the data sent on the port correctly or neither the data sent nor its sender are checked for authenticity.

This would mean the vulnerability is in the payroll software and therefore at the application level. [3 points]

**QUESTION 14 OF 319**

**DLMIMWCK01\_Open\_light/lesson 02**

Section 269 of the StGB was introduced in response to the inapplicability of which sections?

State why this was necessary.

Inapplicability of Section 267 of the StGB to the falsification of digital data of probative value. [3 points]

Section 267 of the StGB covers the forgery of physical documents, but not digital ones. Section 269 of the StGB was created to deal with this. [3 points]

**QUESTION 15 OF 319**

**DLMIMWCK01\_Open\_light/lesson 02**

How is identity defined in the context of misuse of identity? Provide four examples of identifying characteristics.

Fundamentally, a person’s “identity” clarifies who they are. As such, an identity includes distinguishing characteristics that allow for a person or organization to be uniquely recognized. [2 points]

Tax ID, ID card, username/password, name + date of birth, name + address, cryptographic key. [max. 4 points; 1 point per example]

**QUESTION 17 OF 319**

**DLMIMWCK01\_Open\_medium/Lesson 02**

Why is the crime of theft **not** applicable to identity theft?

Is there a criminal liability gap here? Give reasons for your answer.

Section 242 of the StGB, Theft, is only applicable to movable objects. Identity in relation to computer crime is a digital asset, usually in the form of a username/password or cryptographic keys. For this reason, this section is not applicable to identities. [3 points]

No gap in criminal liability exists, as several other sections cover identity theft, such as Sections 202a, b, and c of the StGB, Section 42 of the BDSG, and Section 238 of the StGB [3 points, 2 example sections required].

**QUESTION 16 OF 319**

**DLMIMWCK01\_Open\_Heavy\_F1/Lesson 02**

You work in an organization as an information security officer and discover that some of the organization’s Office365 accounts are being misused for malicious purposes by an attacker. You identify that some email addresses including password have been stolen by data theft. Under which law section does this act fall? Give reasons for your choice. How can you find out which user accounts are affected? What measures would you take afterwards? Name four measures and justify your choices.

Sections 202a, 202b, and 202c may apply.

Section 202a of the StGB is applicable here, for example, because data theft has occurred and Section 202a penalizes data espionage. However, other sections are also applicable. [3 points]

There are services, such as haveibeenpwned or the Hasso Plattner Institute, which make the data included in data thefts searchable. Domains or individual usernames can be searched. These services can be used to find out whether an email address or password has been stolen. [3 points]

Training: Employees must be trained in the proper use of services, such as O365, in order to eliminate operator errors and teach them how the software normally behaves, such as when to allow macros.

Awareness: Employees must be made aware of risks, such as the theft of their access data.

Awareness must also be created in that credentials should not be used more than once, especially if the credentials are used for administrative or other critical services.

MFA: The use of multi-factor authentication helps to protect access to services, as the second factor is always required.

Regular checking of haveibeenpwned: haveibeenpwned can also be checked regularly so that data theft is noticed immediately, before an attacker actively exploits the data. [3 points per measure + justification]

**QUESTION 20 OF 319**

**DLMIMWCK01\_Open\_medium/Lesson 02**

What law section other than the StGB applies to identity theft and what does that section say?

Section 42 of the BDSG also governs identity theft. [2 points]

Section 42 of the BDSG focuses on the mass/commercial disclosure and unauthorized publication of data. Thus, this section is designed to apply mainly to personal data. [2 points]

Section 42 of the BDSG also focuses on publication with malicious intent. [2 points]

**QUESTION 25 OF 319**

**DLMIMWCK01\_Open\_Heavy\_F1/Lesson 02**

You work in an organization as an information security officer and discover that the access data to GitHub repositories has been stolen by a competitor. This crime happened some time ago and the source code is already being used in the competitor’s software. What legal provisions can you use to take action against the competitor’s use of the source code? Name two law sections and give reasons for your choice. What is the basic challenge of protecting source code? Name three measures you would take to protect the source code.

Again, justify your choice.

Section 142 of the PatG or Sections 106-108 of the UrhG. [1 point]

The organization may attempt to protect the software under patent law. In this case, Section 142 of the PatG can be used to take action against the competitor’s use.

In addition, software is always protected by copyright law and thus action can be taken under Sections 106-108 of the UrhG. [2 points]

Computer programs are not protectable under patent law. This is laid down in Section 1 (4) of the PatG Art. 52 of the EPC. “Computer-implemented inventions”, on the other hand, are patentable. These are computer programs that solve concrete technical problems. The distinction between these two constructs under patent law is blurred. Thus, in the case of theft of source code or software, it must always be determined whether a patent for a computer-implemented invention exists or whether copyright to the source code should be considered to exist. [3 points]

[1 point per example and 3 points per justification; max. 12 points] Developer security review:

Developers have access to the source code on a daily basis and thus the possibility to steal it. A developer should always be screened before being hired, including their criminal record, so that previous criminal offenses are uncovered, and no developers are hired who may have already betrayed confidence in the past.

MFA:

If the source code was leaked via stolen passwords, multi-factor authentication should be introduced. This ensures that even if a password is stolen, there is no access to the source code by external parties.

Review for publicly available services:

In modern development environments, source code is organized in source code management systems, such as GitHub. The organization must check whether these are configured correctly. In cloud services, it is quite possible that source codes have been made publicly available if default settings are used.

**QUESTION 26 OF 319**

**DLMIMWCK01\_Open\_light/lesson 03**

You work in a company that manufactures highly complex medical products. One of the biggest risks for you is data theft.

What aspects should be considered before IoT devices are deployed in the enterprise? Name three aspects.

IoT devices increase the amount and type of data generated. IoT devices increase the scope of attack openings.

IoT devices are mostly poorly secured.

... [6 points; 2 points per aspect]

**QUESTION 27OF 319**

**DLMIMWCK01\_Open\_light/lesson 03**

What is a decryptor and what is it used for?

A decryptor is a piece of software used to decrypt files without the key. Malware also has flaws and there are security researchers who analyze and exploit these loopholes, allowing decryptors to be created. They decrypt files encrypted by encryption trojans without requiring the key to be known. [3 points]

The advantage of decryptors is that if a decryptor is available for an encryption trojan, a victim of that encryption trojan does not have to pay a ransom and does not have to have any other measures, such as backups, in place, since the original data can be decrypted. [3 points]

**QUESTION 29 OF 319**

**DLMIMWCK01\_Open\_medium/Lesson 03**

You read in the newspaper this morning that a vulnerability in current home routers can be used to spin up a botnet.

Explain the characteristics of computer sabotage.

Using the example, describe how botnets can be used for computer sabotage.

According to this, computer sabotage includes all acts that interfere with data processing operations which are of substantial importance to another party. [2 points]

Botnets can be used for DDoS attacks. [1 point]

Botnets consist of millions of individual bots that can easily launch a DDoS attack because they work in coordination through a C&C server. If an attacker takes over the routers via the vulnerability, a botnet is built within seconds and can be exploited. [3 points]

**QUESTION 31OF 319**

**DLMIMWCK01\_Open\_medium/Lesson 03**

How is industrial espionage defined and how is it different from economic espionage?

Industrial espionage describes the act of a competitor or individual spying on a company.

Industrial espionage has several synonyms, such as competitor spying, company espionage, or factory espionage. In criminal law, industrial espionage is criminalized under Section 17 of the UWG on Betrayal of Business or Company Secrecy or Section 202a of the StGB on Data Espionage. [3 points]

Economic espionage has the same goal as industrial espionage but is state-directed. [3 points]

**QUESTION 27OF 319**

**DLMIMWCK01\_Open\_Heavy\_F1/Lesson 03**

Systems in a company are infected by malware via several manipulated emails. When the incident is followed up on, it is discovered that the email was written in poor English and came from a contact person who had **nothing** to do with the company.

Under which structural subtype of cyberattacks in the proper meaning of the word would you classify the attack? Give and explain two reasons for your answer.

What measures can be taken to **prevent** this fromhappening again? Name and describe two measures.

What other structural subtypes of cyberattack exist? Describe them.

This was an undirected attack, as the company was clearly hit by mass emails. This means the attack was launched against many potential victims in an untargeted manner, in the hope that a small percentage would fall victim to the attack. [3 points]

Indications that suggest an undirected attack include, for example, the fact that the email was written in poor English. This indicates that there was no direct intended target.

This is particularly true if these emails are sent to non-anglophone organizations. Other indications may include lack of correspondence with the sender. [3 points]

Spam filter:

A spam filter can filter out mass emails using various mechanisms or mark them as [suspicious]. This draws the employees’ to this email or prevents it from reaching them at all.

Training:

Employees can be trained on what fake emails look like, focusing on, for example, errors in grammar or the fact that little information is available about the subject or contact person.

[3 points per example + justification]

An attack is described as targeted when the perpetrator has chosen a specific victim. The victim may be known or unknown to the perpetrator. A classic example of this attack is: Mr. Meier wants to harm his former employer because it fired him, so he sends a virus to his former colleague. They open the virus, which attacks the company’s entire IT network. Scalpel-like attacks are being used more and more frequently. This type of attack requires intensive preparation and mostly aims to destroy infrastructure. Targeted information about the infrastructure, organization, and people is collected. [3 points per different subtype]

**QUESTION 35 OF 319**

**DLMIMWCK01\_Open\_Heavy\_F1/Lesson 03**

As the CEO of an engineering company, you learn of a ransomware attack on a company in a similar position. You wonder whether you are sufficiently protected. After checking with the IT administrator, they list your backup intervals as follows:

Design data – weekly – locked in safe

Stock database – daily – on server hard disk

Customer data – weekly – on server hard disk

Accounting – weekly – locked in safe

How do current ransomware attacks work? Name three measures that can be taken against such attacks.

What criteria must a backup meet as a measure against a ransomware attack?

Discuss whether the features of the backups provide effective protection against ransomware attacks and describe three points of criticism.

Currently, ransomware attacks mostly take the form of encryption trojans. The attackers encrypt all accessible data and only release keys in return for a ransom. [3 points]

Measures against ransomware attacks include backups, always keeping patches up-to-date, and employee awareness regarding how ransomware enters the system: emails with malicious attachments. [3 points]

Offline, complete, and up-to-date. [3 points]

Choice of criticism is left to the student, what matters is the justification. For example:

Construction – is weekly sufficient? (Daily is necessary here!)

Stock data – daily is sufficient, but online backup does nothing to prevent ransomware!

Accounting – is weekly sufficient? (This is tax-relevant data and involves high recovery costs!)

[3 points per point of criticism + description]

**QUESTION 38 OF 319**

**DLMIMWCK01\_Open\_light/lesson 04**

What component does an open port for MySQL suggest? Describe the two possible attacks on this component.

MySQL is a database and makes it available to other applications. This database then contains all this application’s data. [2 points]

One attack option that malware often uses to build botnets is to exploit standard database passwords. The attacker can then read out all the data in the database. [2 points]

Another possibility is SQL injection. Here, code is injected into the database via user input on a web page in order to read usernames and passwords or other data. [2 points]

**QUESTION 40 OF 319**

**DLMIMWCK01\_Open\_light/Lesson 04**

The manufacturer of a smartphone reports that the firmware of a large number of devices has a vulnerability that allows the attacker to control all the functions of the firmware.

Briefly describe what firmware is and give two examples of components that are equipped with firmware.

What type of attack can an attacker launch using this vulnerability in the example given? Describe an attack.

Firmware comes in many varieties and the boundaries are fluid. In general, firmware is software that provides functions of various hardware elements at a very low level. More complex software like operating systems or other application software then builds upon firmware and uses the corresponding functions of the hardware. [2 points]

Consumer products

* Household appliances
* Multimedia devices
* Automobiles
* Smartphones Computer components
* Hard disks
* Graphics cards
* Mainboard

[1 point per example; max. 2 points]

An typical attack would involve infiltrating malicious code into the operating system since the firmware usually loads the operating system first, which the attacker then controls. This can then be used to eavesdrop on data or cause irreparable damage to the devices. [2 points]

Many other examples are possible!

**QUESTION 41 OF 319**

**DLMIMWCK01\_Open\_medium/Lesson 04**

Your organization operates an email server that is exposed to the public internet. During a penetration test, the TCP ports 22,110 and 25 are shown to be open.

First, explain what attack possibilities need to be considered for an email server that uses the ports described.

Which port is **not** needed for email functionality and what risk does it represent?

Since ports 110 and 25 are open, SMTP and POP3 are in use. In this case, an attacker can query email addresses through faulty configurations. This information can then be used for spear phishing or normal phishing attacks. In addition, email servers can obviously have vulnerabilities such as buffer overflows that allow malicious code to be executed. [3 points]

Port 22 belongs to the SSH protocol and is not required for the functionality of an email server. This protocol should be disabled because it gives an attacker another way to gain access. If an attacker has access to a system, SSH passwords or SSH keys can be stolen or manipulated. [3 points]

**QUESTION 44 OF 319**

**DLMIMWCK01\_Open\_medium/Lesson 04**

Your organization operates its own server room. A service provider regularly cleans it at night. The spouse of one of the service provider’s employees was fired by your organization last week and the employee takes revenge by loosening a cable of the core switch while cleaning. A day passes before the cause is found. Your information security officer classifies this as an attack at the organizational level.

Briefly describe when an attack is assigned to this level and what category that attack is placed in.

Describe one action that would have prevented this incident.

Attacks at the organizational level refer to all attacks that exploit an organization’s regulations or that are only possible through vulnerabilities in these regulations. These regulations include information flows, role distributions, processes, and organizational structures and workflows.

This attack should be classified under exposure to outsider attacks. [3 points]

One measure against this attack would be to only deploy the institution’s own personnel in the server rooms or to constantly monitor outsiders while in server rooms. [3 points]

**QUESTION 45 OF 319**

**DLMIMWCK01\_Open\_Heavy\_F1/Lesson 04**

An attacker has managed to infect the internal communication server via a vulnerability in a programming interface of a CRM application. This is used for the internal employee chat application. The attacker does **not have** elevated rights and thus can only influence some of the system’s functions. For example, the attacker can read messages between employees and also edit them.

Which two types of attack can the attacker perform with just these abilities? Describe them briefly along with an example attack scenario.

The attacker’s goal is to take the position of a man-in-the-middle within the chat application. First, explain what a man-in-the-middle attack is.

What further malicious function on the infected system does the attacker require in order to perform a man-in-the-middle attack?

How can the attacker deploy this type of attack in the above example?

Describe two examples.

Eavesdropping attacks are the first type of attack. In a network, data is constantly being exchanged between the systems in the network. This data can be eavesdropped on in many different ways. Eavesdropping in this case means that an attacker can read it. In the case of a CRM application, an attacker could read data about customers and suppliers. A more critical example would be bidding documents. [3 points]

Modification of data goes one step further. If an attacker has access to data, they can change it at will for their own purposes. Data can be changed during transmission or while stored in databases or files. The attacker thus has full control over the data. In a CRM system, for example, it could be critical if an attacker changed contract terms or conditions. [3 points]

In a MitM attack, the attacker has gained the ability to intercept, modify, and resend communications between two network participants so that neither of the original participants is aware of the attack. This type of attack requires the attacker to be able to redirect messages sent by one participant, modify them, and then forward them to the other participant.

At the same time, where there is an authentication process in place between the participants, the attacker must be able to make both participants believe in the identity of the other. [3 points]

Before the attacker can perform a MitM attack, they must gain the ability to adopt the identity of the original sender when sending their modified message, i.e. a spoofing attack. Without this feature, the recipient will notice the tampering. [3 points]

The attacker can manipulate messages that contain bank details, for example, so that transactions are transferred to their account. This gives them a direct financial advantage. [3 points]

However, the attacker can also ask the User Help Desk for a password reset link on behalf of an administrative user and thus gain access to an account with elevated rights. This would allow the attacker to access additional systems. [3 points]

**QUESTION 47 OF 319**

**DLMIMWCK01\_Open\_Heavy\_F1/Lesson 04**

In your role as information security officer, the project manager for your organization’s website informs you that a vulnerability exists on the website that allows an attacker to create a reverse shell in order to execute their desired commands. However, they immediately reassure you that this shell only has the low privileges that a website user has (www-data) and therefore there is no danger at all.

Explain what rights separation and privilege escalation is in terms of modern operating systems in this context.

Describe the relationship between these two terms as they relate to computer crime.

Using the example given, give two reasons why the statement of the project manager is **not** correct with regard to the hazardous situation and outline the procedure by which an attacker could exploit this gap.

Modern operating systems also feature strict separation of rights. This means that the processes of the operating system run with higher rights than the processes of the users. It follows that users cannot read or modify certain areas of memory, use certain network interfaces, or execute some commands.

It is quite possible for a process to jump between different rights levels during execution. [3 points]

However, an attacker’s goal is usually to break out of the initially infected application. This is referred to as privilege escalation. This means that an attacker has the ability to control or start processes with elevated rights so that they can use all the functions of the operating system, in order for example, to use all the network interfaces for their own purposes. [3 points]

If an attacker gains control of a normal user account without elevated rights, the goal is usually to perform privilege escalation. This is necessary because of the rights separation applied in operating systems, as the attacker cannot access all the files and use all the functions of the system with restricted rights. [3 points]

The project manager is wrong for several reasons. They are correct that the user www-data has only been granted limited rights, but even a reverse shell with limited rights can cause great damage. For example, an attacker could read the source code of the web page or possibly read databases. [3 points]

Furthermore, the reverse shell as www-data also serves as a means of performing privilege escalation. If there is a vulnerability or misconfiguration on the webserver that allows the attacker to gain elevated rights, they can exploit this via the shell as www-data. Thus, the vulnerability on the web page is only the first link in the chain and therefore much more dangerous than presented. [3 points]

An attacker would exploit the vulnerability and be able to execute commands as www-data. After finding a way to escalate their rights on the system, they could modify the website’s code, causing significant financial and reputational damage to the organization. [3 points]

**QUESTION 49 OF 319**

**DLMIMWCK01\_Open\_light/Lesson 05**

After a serious security incident in an organization, an IT forensic service provider is commissioned and sets up a meeting. The service provider says during the meeting that live forensics will not be used. Describe the term “live forensics” in relation to IT forensics and explain two advantages of this approach.

Online or live forensics is performed on the system whilst it is running. The system may therefore still be under the influence of an attack. This also means that volatile data, such as process lists or the main memory, can be read out. [3 points]

This allows data and evidence to be collected from the infected system. The advantage of this is that volatile data, such as the contents of the main memory or the currently active network connections, can be analyzed. This information can be very valuable and might be lost during offline analysis. [3 points]

**QUESTION 52 OF 319**

**DLMIMWCK01\_Open\_light/lesson 05**

Describe what bifragmented file carving is and how it differs from normal file carving.

Is there any data that **cannot be restored** using bifragmented file carving?

Since 97% of all files are either non-fragmented or bi-fragmented, i.e. split into two parts, bifragment file carving looks for the gap between the part of a file that has the marker for the header and the part that has the marker for the footer. Using these means, files can be recovered based purely on their binary structure. [3 points]

Normal file carving only finds data that is stored contiguously on the disk. [2 points]

Yes, data that is distributed over three or more parts. [1 point]

**QUESTION 45 OF 319**

**DLMIMWCK01\_Open\_medium/Lesson 05**

You are analysing a medium-sized IT landscape after an attack, including the organization’s cloud connections. There are also strict requirements issued by the works council regarding the processing of employee data.

What requirements regarding legal limits do you have to consider during this IT forensic investigation?

When analyzing cloud infrastructures, care must be taken to ensure that work is only being carried out on systems belonging to the commissioning organization. No data belonging to other organizations may be collected or analyzed. [3 points]

In addition, data protection considerations must be complied with for internal data. For example, the collected data must be anonymized if internal employees’ data is included. In general, the principles of data economy and data minimization apply. [3 points]

**QUESTION 46 OF 319**

**DLMIMWCK01\_Open\_medium/Lesson 05**

You work for a malware analysis specialist and have just received a new type of root kit for analysis. The signature in the form of a checksum is so far not recognized in the databases, but the process calls strongly resemble another malware.

What is a signature related to malware? Describe this and explain the problems with using signatures for malware detection.

Based on the example, describe in what other ways the malware can be categorized.

When a new malware is found, the string of bytes representing the executable data is added to a database. This is then its signature. Signatures can also be generated using checksums. [2 points]
Malicious programs may have the ability to change their signature. This is called polymorphism. This makes using the signature to match with known malware samples very difficult. [2 points]

The malware can be grouped into families using other characteristics, such as the process calls it generates. Since malware can change these characteristics only by making substantial changes to its code, this cannot be accomplished by polymorphism. This makes these features less susceptible to polymorphism than a signature. [2 points]

**QUESTION 57 OF 319**

**DLMIMWCK01\_Open\_Heavy\_F2/Lesson 05**

You are the sole IT administrator of an organizational network that mainly provides production data to employees and machines, and the use of a new virus protection concept is currently being discussed. No personal data or confidential information is processed.

First, explain the three types of malware detection. Then, using the example, explain one advantage and disadvantage for each of the different types.

Describe an attack that would not be captured by **any of** these three methods.

One of the first methods of detecting malware was signature-based detection. When new malware is found, the string of bytes representing the executable file is added to a database. This is then its signature. If an executable with the same string is found in the future, this is detected as malware and appropriate countermeasures are initiated. [3 points]

Heuristics-based detection provides an option for detecting new malware before their signatures are distributed. Heuristics are applied to attempt to identify a malicious program based on system behavior. This does not require knowledge of the malware itself but does require knowledge of vulnerabilities and attack opportunities. [3 points]

Behavior-based detection of malware is similar to the previous method, but instead of looking at the system on which the anti-virus program is running, the behavior of the malware is examined directly. As soon as a malicious behavior is detected, the execution is stopped. [3 points]

The signature-based method reliably detects known malware. Since it is mostly known malware that is used in mass campaigns, it offers good protection as long as your own organization is not the first victim. Since the data being processed is not critical, most attacks will be mass campaigns. [3 points]

The heuristics- and behavior-based detection methods also detect unknown malware based on its behavior or other characteristics. Thus, these are suitable for new and more complex threats. The disadvantage is the high percentage of false positives, which cause a lot of work. In a small IT department with not very critical data, this type of detection is less useful. Ideally, all methods should be combined in a practicable way. [3 points]

An attack that would not be detected by these three methods would be a social engineering attack on an administrator account, allowing an attacker to gain control. No malware is used here, so signature-based detections cannot work. For this reason, only the behavior that the attacker displays while using the administrator account can be detected. Unless the attacker generates any noticeable activity, the attack will not be detected by behavior- or heuristics-based detections. [3 points]

You are a specialist in data recovery and receive daily orders from a wide variety of companies and individuals.

For the examples below, explain where the data is on the disk including any metadata and describe and justify how you would proceed to recover the data.

1. A distraught elderly person calls and says they pressed the wrong buttons and their collection of photos of their grandson is no longer where it was.
2. A student contacts you because they accidentally deleted the latest version of their master’s thesis instead of an outdated one and also accidentally emptied the Recycle Bin.
3. An organization contacts you after a cyberattack in which the attacker tried to cover their tracks by deleting the entire NTFS file structure of a server. The organization wants to locate clues about the criminal on the server’s hard drive.
4. An organization contacts you because a batch script run by the storage area network administrator has inadvertently completely overwritten two server disks with 0s.
5. The data is probably still in the Recycle Bin since modern operating systems always put files in the Recycle Bin when they are deleted to allow the user to restore them. [3 points]

The data is still present on the disk and in the file system structure. Only the reference to the data has been moved from the original directory to the Recycle Bin. The data can be restored using the Recycle Bin function. [3 points]

1. The data is deleted and removed from the Recycle Bin, so some data in the file structure is deleted, but some other data is still present. [2 points]

Here the file can be recovered via the file system structure because there are still traces of the file. This allows the file to be restored. Special tools exist for this. [2 points]

1. The file system structure is therefore completely destroyed, i.e. there is no more data contained in the structure. But the data is still present somewhere on the disk. [2 points] File carving techniques must be used to find this data. This involves looking for specific headers and footers to find the files in the byte code on the disk. [2 points]
2. Since the entire hard disk was overwritten with 0s, the data you are looking for cannot be found anywhere in the file system structure, nor on the disk. [2 points]

Here only trying to find a backup can help because the data is irrevocably lost (wiped-out). [2 points]

[The distribution of 3 points and 2 points may vary depending on where the student places general explanations of the file system structure. These are required in order to complete the task but only needed to be stated in one part.]

**QUESTION 61OF 319**

**DLMIMWCK01\_Open\_light/Lesson 06**

Your organization equips its server cabinets with fire- and burglar-proof doors according to requirements issued by the ISMS.

Using the example above, explain what a preventive measure is. Also give three examples of other preventive measures.

Preventive measures are measures that are taken before a security incident occurs. The aim is to prevent the security incident, reduce the probability of occurrence or reduce the consequences of the incident. In this case, the server room is secured preventively before a break-in or fire. [3 points]

Examples [1 point per example; max. 3 points]

Password protection

Security guard

Perimeter protection (fence) around the building

**QUESTION 63 OF 319**

**DLMIMWCK01\_Open\_light/lesson 06**

Your organization uses a large number of different applications and employees have complained several times that remembering such a large number of passwords is impossible. Your solution in order to reduce the number of passwords is SSO.

What does SSO mean and what benefit does it offer in terms of password diversity? Describe an example where SSO can help reduce password diversity.

SSO stands for “single sign-on” and describes the possibility of logging into additional services once a user has been authenticated. This means that authentication does not have to be performed individually for each service. [2 points]

The advantage is that a user logs in once and does not need to log into other services again because the authentication is reused, meaning the password does not have to be entered again. This means a user does not have to remember multiple credentials. Thus, more complex password rules can be enforced, or biometric authentication can be used. It also makes it easier to change passwords. [2 points] For example, the login to the Windows operating system can be used for other services, so that a user only has to enter their Windows password in the morning and then all other services, such as web applications or merchandise management systems, rely on this authentication. [2 points]

**QUESTION 65 OF 319**

**DLMIMWCK01\_Open\_medium/Lesson 06**

Your organization is in the process of implementing Microsoft 365 and corporate data will be made accessible from outside the organizational network for the first time. Currently, applications are mainly accessed using a username and password. Your information security officer suggests MFA365 for accessing Microsoft.

First, explain what MFA means.

Then describe whether MFA should be applied in the example above. Give reasons for your answer.

MFA: Multi-factor authentication, as the name suggests, relates to authentication only. With MFA, authentication is performed using multiple factors, i.e., instead of using only a password to authenticate a user, additional characteristics are required. For example, possession of a personal item such as a smartphone or a security token can be added as another characteristic. [3 points]

In this example, MFA365 should be used to access Microsoft, but only if the access is initiated outside the organization’s network, as an attacker can easily initiate authentication outside the network, and a lack of MFA – i.e., using only username/password – gives them a much greater chance of tapping into the organization’s data. [3 points]

**QUESTION 59 OF 319**

**DLMIMWCK01\_Open\_medium/Lesson 06**

Your organization is in the process of implementing a collaboration tool for working together and, for the first time, it will be possible to access corporate data from outside the organizational network.

Currently, applications are mainly accessed using a username and password. Your information security officer suggests MFA for access to the collaboration tool.

First, explain what MFA means.

Then describe whether MFA should be applied in the example above. Justify your answer.

MFA: Multi-factor authentication, as the name suggests, refers to authentication only. With MFA, authentication is performed using multiple factors, i.e., instead of using only a password to authenticate a user, additional characteristics are required. For example, possession of a personal item such as a smartphone or a security token can be added as another characteristic. [3 points]

In this example, MFA should be used to access the collaboration tool, but only if the access is initiated from outside the organization’s network, since an attacker can easily initiate authentication outside the network, and a lack of MFA – i.e., using only username/password – gives them a much greater chance of tapping into the organization’s data. [3 points]

**QUESTION 70 OF 319**

**DLMIMWCK01\_Open\_Heavy\_F2/Lesson 06**

Your organization is spread across several locations and employees have the option of working from home. These connections are implemented via VPN. This VPN is activated via a smart card that is inserted into the employees’ laptops. Following an incident in which an attacker – pretending to be a support employee – tricked an employee into handing over the smartcard, large-scale training and awareness measures are now being implemented for all employees.

Using the example, describe the eight objectives of such a training and awareness program.

Which other user groups should be trained in particular?

[2 points per objective + application of the example] Generate security awareness.

Create awareness that the smart card is extremely important.

Impart knowledge of information security regulations.

The rule that operational items (smart card) must never be given out must be observed.

Generate awareness of information security measures.

Justify need for VPN to make it clear to employees that this is necessary.

Provide training on security functionalities.

Provide training on the general functioning of the VPN and the smartcard. What happens if an attacker gains access? Detect and report security incidents.

How could the employee have reported the incident correctly? Observe security measures and careful handling of information.

Smartcards contain critical information and must be handled with care.

Raise awareness of social engineering.

Raise awareness that support staff will never ask for passwords or smart cards.

Change in safety culture.

In general, the safety culture must be changed. Safety measures should not be perceived as a nuisance but should instead actively involve employees.

In addition to employees, administrators must also receive special training to ensure that they configure applications correctly and securely, such as a VPN. [2 points]



**QUESTION 72 OF 319**

**DLMIMWCK01\_Open\_Heavy\_F2/Lesson 06**

You are the information security officer of a medium-sized mechanical engineering company and are asked to create an authorization concept. The following user groups and accesses to clearances in the network are relevant:

All users – includes all employees – clearance: business trip planning
Designers – including all employees in the Design department – clearance: construction plans

Accounting – includes all payroll and financial accounting staff

– clearance: employee remuneration

First, explain the terms “authentication”, “authorization”, and “access authorization”.

Then describe the methods you would use to implement authentication, authorization, and access authorization for the above user groups and clearances. When doing so, address the protection requirements of the respective clearances and explain two measures to implemented in order for each to meet these protection requirements.

Authentication describes verifying authenticity, i.e., whether the communication partner is who they claim to be. Authentic information must have been created or sent by the specified source. Authentication is usually ensured using passwords, smart cards or biometric features. [3 points] Authorization describes verifying whether a person, hardware component, or application is authorized to perform a certain action. This therefore explicitly applies not only to persons but also to communication between applications or IT components. [3 points]

Access authorization allows a person, a component, or a service to use a specific resource. Thus, the access authorization combines operational authentication and authorization. [3 points]

All users – includes all employees – clearance: business trip planning

Since this user group includes all users and business trip planning is public for all users, a normal level of protection is required here. Authentication can therefore be achieved using a username and password, which are assigned to each employee at the start of their job. Authorization is then achieved using the authorized user ID, and SSO should be used in combination with the operating system login. A password flow should be defined. [3 points]
Designers – includes all design staff – clearance:

Construction plans:

The construction plans are critical data for the company, as industrial espionage in this area would be devastating. For this reason, a second factor should be used here.

Either the IP address of the employee’s PC, one-time passwords via SMS, or other tokens can be used as a second factor. Only on this basis should clearance be authorized. [3 points]

Accounting – includes all payroll and financial accounting staff – clearance:

Employee compensation:

This clearance also requires a high level of protection. An MFA procedure could be used here, or the clearance could be encrypted so that the content covered by the clearance can only be decrypted with a previously distributed key or user certificate. [3 points]

The measures to secure the accesses are up to the student. The justification is important!

**QUESTION 74 OF 319**

**DLMIMWCK01\_Open\_light/lesson 07**

You work as an IT admin in a construction business with 20 employees and a small IT infrastructure. You discover that one of the workstations is infected with a ransomware and immediately start collecting information in the network.

Following the Alliance for Cybersecurity’s organizational recommendations, what steps did you omit and what are the consequences? Briefly describe these two steps.

Name and explain a step which follows after the mentioned collection of information.

Omitted:

Establishment of a crisis team: Currently, the IT admin is making all the relevant decisions. This competence should be transferred to the crisis team. [2 points]

Internal communication: Internal decision-makers are unaware of the infection and far-reaching consequences may be overlooked [2 points].

Another step:

External support:

External IT consultants or IT forensic experts may be recruited to clean up the incident and repair the damage. [2 points]

**QUESTION 76 OF 319**

**DLMIMWCK01\_Open\_light/Lesson 07**

How is an attack graph constructed in relation to network attacks and computer crime? Describe the usefulness of such an attack graph.

To construct an attack graph, possible attacks are represented in the form of a tree-like graph based on the organization’s own network structure, and a simulation model is applied to this structure. This graph represents all the ways in which an attacker could break into the network, spread, and gain complete access. [3 points]

This can then be used, for example, to simulate what effects an infection of server X would have for client group A and network section B. In addition to simulation, such systems can also be fed with (near) real-time data, allowing for the extent of damage to be calculated immediately in the event of an attack also. [3 points]

**QUESTION 7OF 319**

**DLMIMWCK01\_Open\_medium/Lesson 07**

What is CRITIS and what organizations are included under this term?

Give an example of a CRITIS organization from one of the following areas and explain why it belongs to this category:

* Media and culture,
* Water
* Finance and insurance.

By passing the Act to Increase the Security of Information Technology Systems (also known as the IT Security Act or IT-SiG), the legislator obliged operators of “critical infrastructure” to implement minimum standards with regard to IT security. Certain sectors, such as food, water or finance, belong to CRITIS. For each sector, there are thresholds that define when a company belongs to the critical infrastructure. [3 points]

A bank, such as Commerzbank, belongs to CRITIS because large amounts of money are processed electronically on a daily basis, and the supply of current accounts and the money of a large number of citizens must be guaranteed. [Other examples would be public broadcasting (media) or local water suppliers (water).]

**QUESTION 80 OF 319**

**DLMIMWCK01\_Open\_medium/Lesson 07**

What is CRITIS and which organizations are covered by this term?

Give an example of a CRITIS organization from one of the following areas and explain why it falls into this category:

Health

IT and ICT

Transport and traffic

By passing the Act to Increase the Security of Information Technology Systems (also known as the IT Security Act or IT-SiG), the legislator obliged operators of “critical infrastructure” to implement minimum standards with regard to IT security. Certain sectors, such as food, water or finance, belong to CRITIS. For each sector, there are thresholds that define when a company belongs to the critical infrastructure. [3 points] Hospitals that have a certain number of beds belong to CRITIS because if the infrastructure of this hospital were to be successfully attacked and the medical care of thousands of people were compromised, the consequences would be catastrophic. [3 points] Other examples would be the Bundesnetz, the Bundestag’s network (IT), or Schenker (transport).

**QUESTION 82 OF 319**

**DLMIMWCK01\_Open\_Heavy\_F2/Lesson 07**

Explain what “threat intelligence” means in the context of computer crime.

What are the types of threat intelligence?

Name four types of threat intelligence and explain in one sentence what information belongs to that type.

Classify the following examples into the types of threat intelligence:

1. Organized cybercriminals are planning further attacks on Linux in the future.
2. Beginning yesterday, Emotet has been using encrypted attachments to bypass virus scanners.
3. The IP address of the C&C server of a new malware is 10.127.541.99.
4. The NotCredya malware uses the URL badguy675.evil.com to retrieve up‑to‑date commands.
5. An anonymous source gives you information that there is an internal perpetrator in your organization.
6. Attackers have been exploiting the CVE-2021-1234 vulnerability since yesterday.
7. Information in social networks is increasingly being used against organizations.

Information about threats or attackers related to computer crime is called “threat intelligence”. There are several definitions of this term. The important thing is that threat intelligence must be relevant information that can enable appropriate actions (reactive and preventive measures) to be carried out. [3 points]

[1 point per item listed; 1 point per explanation].

Strategic threat intelligence: information on the general threat situation caused by computer crime for strategic decisions on future risks.

Operational threat intelligence: information about the specific threat situation for one’s own organization.

Tactical threat intelligence: information about the general approach of 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.

[1 point per correct assignment]

* 1. Strategic
	2. Tactical
	3. Technical
	4. Technical
	5. Operational
	6. Tactical
	7. Strategic

**QUESTION 83 OF 319**

**DLMIMWCK01\_Open\_Heavy\_F2/Lesson 07**

You are the IT manager of a medium-sized service provider specializing in software development. You are also responsible for screening all of the security messages from the IT infrastructures and you try to detect attacks at an early stage. After you were barely able to avoid severe consequences from a malware attack last week, you learn from another expert in your field on a customer’s site that the same malware also struck their company eight weeks ago. If you had known the characteristics of the malware, you would have been able to detect the threat directly and intervene.

You remember from your studies that a tool exists for sharing threat information called “TISPs”.

What is a TISP and how does it work?

After inquiring with senior colleagues, you find that there have been efforts to introduce a TISP before. However, this was unanimously rejected.

List and briefly explain five reasons that discourage organizations from using a TISP.

A TISP is a threat intelligence sharing platform. Threat intelligence is knowledge about threats, i.e., characteristics that uniquely identify threats such as malware or malicious behavior. This knowledge can be shared via TISPs, so that once an attack has occurred, the knowledge is shared with many organizations, in order to prevent from occurring the attack there. [3 points]

[1 point per reason given and 2 points per explanation; max. 15 points; 9 reasons exist in the required reading].

Negative publicity:

Many organizations try to keep any sign of weakness under wraps, and an indication of an attack, even if unsuccessful, is seen as bad publicity. For this reason, this information is not allowed to leave the company and is not shared. This affects software developers particularly strongly, as once infected, it will be difficult for that developer to continue selling software.

Laws and privacy:

Every piece of information that is shared with other organizations would have to be evaluated as to whether it may be shared or not under legal and data protection considerations. Many organizations are reluctant to do this because of the complexity of the issue.

Quality concerns:

Since the quality of the TISP’s supplying systems in other organizations is unclear, the quality of the data supplied is also unclear. An IOC should be such that a direct recommendation for action can be derived from it, but for this to be possible, the monitoring systems that supply the TISP must also work as required. Trustworthy software is also a quality feature here.

Cost factor:

TISPs are expensive and can be unaffordable, especially for smaller companies.

Low estimation of the risk of an attack:

Many business leaders are not yet aware of the consequences of a cyberattack, so implementing a TISP is not a priority.

**QUESTION 86 OF 319**

**DLMIMWCK01\_Open\_light/lesson 08**

What does it mean for software to be crypto-agile?

Describe one reason why crypto-agility is necessary.

Crypto-agile:

Crypto-agility is the ability of a system to swap the cryptographic algorithms being used. In the case of software, cryptographic methods could be incorporated via external libraries that can be exchanged, or configuration interfaces could define the cryptographic algorithms. [3 points]

Imagine a software product, published in 1980, that only supports the encryption procedure DES, which was current at this time. Due to its small key length of 56 bits, this method has been obsolete since 1997. Unless the software is crypto-agile and the encryption method can be replaced with its successor, AES, the software can no longer be used securely. [3 points]

**QUESTION 88 OF 319**

**DLMIMWCK01\_Open\_light/lesson 08**

What is the recommended source of preventive cybersecurity measures for a small or medium-sized business?

List five of these recommended preventive measures.

BSI [1 point]

[1 point per measure]

Use of HTTPS instead of HTTP

Multi-factor authentication

Anti-spoofing measures (e.g., DMARC or SPF)

Always applying current security updates

Offline backups Monitoring

Appropriate backup strategy

Restrictive use of RDP and other clearances to external specialized service providers

Patch management awareness

**QUESTION 90 OF 319**

**DLMIMWCK01\_Open\_medium/Lesson 08**

Your organization programs a collaboration tool for video-based learning. Security has **not** played a major role in the release process so far. However, vulnerabilities have repeatedly come to light. For this reason, a Vulnerability Disclosure Program (VDP) is currently being discussed.

Explain what a VDP is. Name and describe two advantages of a VDP.

A VDP allows security researchers to report security gaps in software or on websites to operators, without the threat of penalties, so that they can be closed. The reported vulnerabilities can then be fixed by the software’s manufacturer. [3 points]

The advantage is that vulnerabilities are continuously searched for, i.e. including after every minor release or patch. In addition, these vulnerabilities are searched for by professionals who know the attackers’ techniques. This knowledge usually goes beyond that of the developers. [3 points]

**QUESTION 92 OF 319**

**DLMIMWCK01\_Open\_medium/Lesson 08**

Describe what the term “cyberscamming” means. Illustrate using an example.

Cyberscamming: Cyberscamming refers to any type of fraud that is perpetrated with the help of the internet. There are different types of cyberscam, such as CEO fraud, phishing, romance scam, investment fraud, or online shopping fraud. [3 points] CEO fraud: CEO fraud is particularly relevant for organizations, as it is used to make requests for payment from business accounts. The attacker pretends to be the boss and uses aggression and time pressure to push employees to perform actions that benefit the attacker. [3 points]

**QUESTION 93 OF 319**

**DLMIMWCK01\_Open\_Heavy\_F2/Lesson 08**

You are the administrator of a small facade manufacturer, and you are asked to present a list of effective security measures to your boss. Your IT infrastructure generally consists of a web server for the company homepage, an email server, and a hard disk cluster for central data storage.

After some Google research, you find the 2019 BSI report on the state of IT security in Germany and note some of the measures.

Name and describe six measures included in the 2019 BSI state report.

[1 point per item listed, 2 points per example application]

HTTPS instead of HTTP:

The web server should run with HTTPS to prevent MitM attacks. This protects the customers and confidentiality.

Multi-factor authentication:

Employees or exposed employees (such as admins or management) should log in using multiple factors, i.e., with an additional factor such as a OTP on their cell phone or a hardware token.

Offline backups:

The backups of the hard disk cluster must be created regularly. In addition, the current backup must be kept offline, i.e., separate from the company network. The central data store must be backed up urgently in this case, as this is the only data store.

Monitoring:

The network, homepage activities, user authentication, and email activities should be scanned with a monitoring system so that conspicuous behavior can be detected immediately, and actions can be taken.

Patch management:

All systems must be patched regularly. First and foremost, this includes the web server, as this is open to the internet and is therefore subject to constant automated scans and attacks. Next, the email server and the rest of the internal servers should be patched.

Awareness:

Employees should be provided with training and awareness-raising measures. Administrators should be trained in security-critical applications (e.g., monitoring) and all employees should be made aware of the topic of spam, for example.

**QUESTION 95 OF 319**

**DLMIMWCK01\_Open\_Heavy\_F2/Lesson 08**

You are the managing director of a mechanical engineering company with a focus on digital sales models. Now that several sales employees are allowed to use their own phones for professional purposes, many other employees also want to use this option. In order to minimize the risks to the company of using private devices, you have been tasked with managing the handling of “bring your own device”.

According to the “European Cybercrime Centre”, what advice should be followed when applying BYOD?

Name and describe the nine suggestions in one sentence each.

[1 point for each item named; 1 point for description]

Employee understanding: Employees must be trained on 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.

Mobile device policies: Policies must be set and verified. If a device does not meet these policies, no connection to the network may be established.

Beware of public networks: Public networks pose a great risk to corporate data.

Software updates: Software updates must always be installed promptly.

Apps only from trusted sources: Apps and software for mobile devices may only be obtained from trusted sources.

Prevent jailbreak/rooting: Jailbreaking and rooting must be prevented or prohibited.

Consider 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 to further monitor the software on the mobile device.

Which of the following acts counts as cybercrime in the broader sense?

**Choose an answer:**

Forging a website

Man-in-the-middle attack *Sale of illegal goods*

Theft of login data (phishing)

**QUESTION 121 OF 319**

**DLMIMWCK01\_MC\_heavy/lesson 01**

**QUESTION 122 OF 319**

**DLMIMWCK01\_MC\_light/lesson 01**

Which level does **not** represent abasic categorization of vulnerabilities?

**Choose an answer:**

Organizational level vulnerabilities

Network and server level vulnerabilities Application level vulnerabilities

*Client level vulnerabilities*

**QUESTION 123 OF 319**

**DLMIMWCK01\_MC\_heavy/lesson 01**

Suppose a vulnerability allows the cryptographic security of an encryption to be leveraged by measuring the vibrations of the processor.

What level would you place this vulnerability at?

**Choose an answer:**

*Firmware and chip level vulnerability*

Network and server level vulnerability Organizational level vulnerability

Application level vulnerability

**QUESTION 124 OF 319**

**DLMIMWCK01\_MC\_medium/lesson 01**

What evolution is attributed to fifth-generation malware?

**Choose an answer:**

Commercialization of malware

Self-replication

*Malware-as-a-Service*

Use of the internet

**QUESTION 125 OF 319**

**DLMIMWCK01\_MC\_light/lesson 01**

What are the two basic types of malware analysis?

**Choose an answer:**

Immersive and continuous Reversive and progressive Post and pre-analysis

*Static and dynamic*

**QUESTION 126 OF 319**

**DLMIMWCK01\_MC\_light/lesson 01**

What is the basic characteristic of a trojan horse?

**Choose an answer:**

It uses update functions of other applications.

It spreads itself independently.

It does not cause any damage.

*It is hidden in legitimate software.*

**QUESTION 128 OF 319**

**DLMIMWCK01\_MC\_medium/lesson 01**

Which of the following is **not a** basic component of a botnet?

**Choose an answer:**

Botmaster Bots

*Botware*

Command and control server

What act is does Section 42 of the BDSG focus on?

**Choose an answer:**

Commercial storage and unauthorized retention of personal data

*Commercial disclosure and unauthorized publication of personal data*

Commercial disclosure and unauthorized publication of any data

Commercial disclosure and unauthorized publication of identifiers

**QUESTION 137 OF 319**

**DLMIMWCK01\_MC\_medium/lesson 02**

Which of the following law sections applies to an attacker obtaining a publicly attested SSL certificate in order to use it to launch man-in-the-middle attacks in the future?

**Choose an answer:**

Section 42 BDSG: Penal provision

Section 202a StGB: Data espionage

Section 253 StGB: Extortion

*Section 202c StGB: Acts preparatory to data espionage and phishing*

**QUESTION 139 OF 319**

**DLMIMWCK01\_MC\_medium/lesson 02QUESTION 136 OF 319**

**DLMIMWCK01\_MC\_medium/lesson 02**

What act does Section 202 cover?

**Choose an answer:**

*Interception of data* Data espionage

Identity abuse

Fraud

**QUESTION 142 OF 319**

**DLMIMWCK01\_MC\_light/lesson 02**

What are platforms that allow users to upload data that can be downloaded by other users from that platform called?

**Choose an answer:**

*Filehosters*

E-Hosters Hostfilers Filelisters

**QUESTION 143 OF 319**

**DLMIMWCK01\_MC\_light/lesson 02**

What acts does Section 269 of the StGB cover?

**Choose an answer:**

*Forgery of data of probative value* Misuse of identity

Misuse of evidence

Misuse of personal data

**QUESTION 146 OF 319**

**DLMIMWCK01\_MC\_heavy/lesson 02**

When does a phishing email fall under Section 269 of the StGB?

**Choose an answer:**

When counterfeit products are sold

*When a contractual relationship with the recipient is falsified*

When services are advertised that are never provided

When the sender is falsified

**QUESTION 147 OF 319**

**DLMIMWCK01\_MC\_medium/lesson 02**

Which of the following acts is **not** included in the law section on computer fraud?

**Choose an answer:**

*Incorrect use of programs*

Unauthorised influence on processing

Incorrect configuration of the computer program

Use of incorrect or incomplete data

**QUESTION 149 OF 319**

**DLMIMWCK01\_MC\_light/lesson 03**

Which of the following devices is already available for purchase as part of the IoT?

**Choose an answer:**

Disposable bottle

Packet of gum

*Lamp*

Roof beam

**QUESTION 151 OF 319**

**DLMIMWCK01\_MC\_heavy/lesson 03**

What term is used to describe a person who exploits vulnerabilities in a piece of software, contrary to the manufacturer’s licensing guidelines, in order to give users of the software more ways to use it?

**Choose an answer:**

Black hat White hat Red hat *Grey hat*

**QUESTION 154 OF 319**

**DLMIMWCK01\_MC\_medium/lesson 03**

What are the categories of motives for cyberattacks?

**Choose an answer:**

External and internal Exposed and internalized

Externalized and internalized

*Extrinsic and intrinsic*

**QUESTION 156 OF 319**

**DLMIMWCK01\_MC\_medium/lesson 03**

If possible, what means should **not be** used to recover data after an encryption trojan attack?

**Choose an answer:**

*Payment of the ransom* Restoration of backups

Use of a decryptor

Deployment of IT forensic personnel

**QUESTION 157 OF 319**

**DLMIMWCK01\_MC\_medium/lesson 03**

As a security officer for a national corporation, you are alerted that suspicious software has been found on one of your servers. In the course of the forensic investigation, you discover that this software is Emotet and that it has already infected some systems, but no damage has been done. The only consequences so far are that some connections have been established to your network via a remote maintenance port.

What is the attacker’s approach here?

**Choose an answer:**

*Encryption trojan operators are estimating the value of you organization as a target.*

Emotet operators are testing the malware’s functionalities.

The operators of a DoS-as-a-Service portal are preparing an attack.

Intelligence agencies are exploring their network to steal data.

**QUESTION 160 OF 319**

**DLMIMWCK01\_MC\_light/lesson 03**

What distinguishes a DoS from a DDoS attack?

**Choose an answer:**

*The number of targets attacked*

The type of malware used

The number of attacking devices

The type of internet line used by the attacker

**QUESTION 162 OF 319**

**DLMIMWCK01\_MC\_light/lesson 03**

Which of the following is **not a** synonym for industrial espionage?

**Choose an answer:**

Industrial espionage

Company spying

*Economic espionage*

Factory espionage

**QUESTION 163 OF 319**

**DLMIMWCK01\_MC\_light/lesson 04**

Which of the following is a chip level attack?

**Choose an answer:**

DirtyZombie HorrorLoad *ZombieLoad* ZombieLine

**QUESTION 166 OF 319**

**DLMIMWCK01\_MC\_heavy/lesson 04**

A new type of attack allows hard disk data to be read out via an extended temperature sensor in hard disks with a motorized read head.

To which functional and physical type of attack does this new attack belong?

**Choose an answer:**

Power consumption and acoustic Cryptographic and electromagnetic Processor load and interference

*Storage utilization and thermal*

**QUESTION 168 OF 319**

**DLMIMWCK01\_MC\_medium/lesson 04**

A new type of attack allows conclusions to be drawn about the asymmetric key pairs used based on the power supply of a Trusted Platform Module.

To which functional and physical type of attack does this new attack belong?

**Choose an answer:**

Micro-architectural and acoustic Processor load and timing

Thermal and user interaction

*Cryptographic and power Consumption*

**QUESTION 169 OF 319**

**DLMIMWCK01\_MC\_light/lesson 04**

Which of the following terms represents a type of attack on networks?

**Choose an answer:**

Loofing attack Groofing attack Splinter attack *Spoofing attack*

**QUESTION 171 OF 319**

**DLMIMWCK01\_MC\_medium/lesson 04**

What do the letters DNS stand for in the context of network protocols?

**Choose an answer:**

Domain Name Switch Domain Numeration System Data Name System

*Domain Name System*

**QUESTION 173 OF 319**

**DLMIMWCK01\_MC\_light/lesson 04**

On which port is a DNS connection established according to the RFC 1340?

**Choose an answer:**

443

*53*

22

110

**QUESTION 176 OF 319**

**DLMIMWCK01\_MC\_heavy/lesson 04**

Your website administrator dashboard shows the input that visitors enter into the upload function. You notice abnormal input values that look like file path manipulations, such as “/../../../etc/passwd” or “/../../../../var/log/auth.log”.

What form of attack is an attacker trying to execute here?

**Choose an answer:**

XXS

*Path traversal*

XXE

Spoofing

**QUESTION 177 OF 319**

**DLMIMWCK01\_MC\_light/lesson 05**

What is the overall goal of IT forensics?

**Choose an answer:**

*Clarification of computer crime incidents*

Securing the traces of an ATP attack

Analysis of log files and monitoring systems

Presentation of attack vectors at the executive level

**QUESTION 180 OF 319**

**DLMIMWCK01\_MC\_medium/lesson 05**

How can a polymorphism **not** arise?

**Choose an answer:**

Use of another type of encryption

Change of file name

Insertion of unused code

*Actions of the victim*

**QUESTION FROM 182 OF 319**

**DLMIMWCK01\_MC\_heavy/lesson 05**

You work for a large pharmaceutical company and protecting internal information is a top priority. Your company has already been the target of several attacks caused by previously completely unknown malware.

Which detection method needs to be implemented urgently in the company?

**Choose an answer:**

Signature-based detection Fractal-based detection *Behavior-based detection*

Morphism-based detection



**QUESTION 184 OF 319**

**DLMIMWCK01\_MC\_light/lesson 05**

Which two types of detection are distinguished with regard to malware?

**Choose an answer:**

Off-demand and time-windowed VOD and delayed

*On-demand and real-time*

By-order and instant

**QUESTION 186 OF 319**

**DLMIMWCK01\_MC\_light/lesson 05**

What is the main activity to be performed in the preparation phase of a forensic investigation?

**Choose an answer:**

Backup of data

Evaluation of data

*Preparation of all the necessary tools*

Multimedia analysis

**QUESTION 188 OF 319**

**DLMIMWCK01\_MC\_heavy/lesson 05**

You work for an IT forensic service provider and have the data of all the network connections, the process list of a server and the contents of the file system in front of you. Currently, you are trying to find out which process called which network interfaces with which executable files.

What stage of the IT forensic investigation are you in?

**Choose an answer:**

Evaluation of data *Reconstruction of events* Collection of data

Preparation

**QUESTION 189 OF 319**

**DLMIMWCK01\_MC\_medium/lesson 05**

Which of the following techniques should be used after a disk has been wiped out?

**Choose an answer:**

*None of the below*

File carving

Signature-based recovery

Bi-fragmented file carving

**QUESTION 191 OF 319**

**DLMIMWCK01\_MC\_light/lesson 06**

When are preventive measures taken?

**Choose an answer:**

After infection by a virus, but before the IT forensic investigation

After a security incident

During a security incident

*Before a security incident*

**QUESTION 194 OF 319**

**DLMIMWCK01\_MC\_medium/lesson 06**

Which of the following is a preventive measure?

**Choose an answer:**

Shutting down a network segment to contain the spread of a worm

Notifying public agencies of a virus attack

*Creating a policy on the use of cryptographic keys*

Restoration of all servers from backups in the course of disaster recovery

**QUESTION 195 OF 319**

**DLMIMWCK01\_MC\_light/lesson 06**

What does SSO mean?

**Choose an answer:**

Single Signature Over Save Sign-On

Save Signature-On

*Single Sign-On*

**QUESTION 198 OF 319**

**DLMIMWCK01\_MC\_heavy/lesson 06**

During internal application development, a web developer introduces a new administration tool for websites. When presenting it to colleagues, the web developer mentions that the tool is accessed via the URL [“](http://www.beispielfirma.de/app/administration)www.beispielfirma.de/app/administration”.

Is this access secure from unauthorized parties?

**Choose an answer:**

Yes, if the URL is mixed with special characters, for example “/app/adm!n!5trat!0n”.

*Yes, if a login is required to call up “/app/administration”.*

Yes, if very few employees are aware of the existence of the URL.

Yes, if no links to “/app/administration” exist.

**QUESTION 199 OF 319**

**DLMIMWCK01\_MC\_light/lesson 06**

What is Active Directory?

**Choose an answer:**

Operating system

Threat intelligence sharing platform Network management tool

*Directory service*

**QUESTION 202 OF 319**

**DLMIMWCK01\_MC\_heavy/lesson 06**

For which protection standard does the BSI’s IT-Grundschutz stipulate an automatic response to security-relevant events?

**Choose an answer:**

Low

Standard

Normal

*Increased*

**QUESTION 203 OF 319**

**DLMIMWCK01\_MC\_medium/lesson 06**

What does the abbreviation IDS mean?

**Choose an answer:**

Incident Determination System Incident Detection System *Intrusion Detection System* Intrusion Determination system

**QUESTION 205 OF 319**

**DLMIMWCK01\_MC\_light/lesson 07**

Which of the following represents a physical consequence?

**Choose an answer:**

Negative press coverage

Inability to provide a service to a customer

*Defect of a hard disk*

Inability to fulfil an order

**QUESTION 208 OF 319**

**DLMIMWCK01\_MC\_heavy/lesson 07**

To which type of threat intelligence does the following information belong? “Emotet emails are currently being sent with real conversations to appear trustworthy to the recipient!”

**Choose an answer:**

*Tactical* Long-term Strategic Technical

**QUESTION 209 OF 319**

**DLMIMWCK01\_MC\_light/lesson 07**

Who should make all the decisions in the event of a cyberattack?

**Choose an answer:**

The employee who discovers the attack The forensic service provider

*The crisis team*

The system administrator of the infected system

**QUESTION 212 OF 319**

**DLMIMWCK01\_MC\_medium/lesson 07**

On which programming defect is a buffer overflow based?

**Choose an answer:**

“.NET 3.4.1” is used instead of “.NET 4.1”.

No meaningful error message is displayed to the user.

*The length of an input value is not checked.*

Implicit type conversion is allowed.

**QUESTION 214 OF 319**

**DLMIMWCK01\_MC\_medium/lesson 07**

What types of threat intelligence exist?

**Choose an answer:**

Medium, long-term, acoustic, political Short-term, network, delayed, critical Historical, instant, proactive, organizational

*Strategic, operational, tactical, technical*

**QUESTION 215 OF 319**

**DLMIMWCK01\_MC\_medium/lesson 07**

What kind of IOC is left by an attacker who finds out an administrator’s credentials via social engineering on social networks and exploits them to change customers’ data via a poorly programmed administration interface?

**Choose an answer:**

Host-based Email Network

*None of the above*

**QUESTION 218 OF 319**

**DLMIMWCK01\_MC\_light/lesson 07**

Which industry does **not** qualify as a critical infrastructure operator?

**Choose an answer:**

Public broadcasting

*Universities*

Banks Intelligence

**QUESTION 220 OF 319**

**DLMIMWCK01\_MC\_medium/lesson 08**

What source can you use to identify concrete figures on criminal offenses in Germany?

**Choose an answer:**

PSK

*PKS*

Police statistics channel Police crime rate

**QUESTION 221 OF 319**

**DLMIMWCK01\_MC\_heavy/lesson 08**

You are a development team leader in a software development company. One of their products currently only supports the entry of passwords with a length of six characters. Since such short passwords pose a security risk, the company is discussing how authentication should be performed in the future. What should be done according to the 2020 recommendations of the Council of Eminent Persons for Cybersecurity?

**Choose an answer:**

*Introduction of authentication by means of biometric procedures*

Introduction of a minimum length of 14 characters Increase of password length to 20 characters

Remove authentication

**QUESTION 223 OF 319**

**DLMIMWCK01\_MC\_heavy/lesson 08**

What measures against DDoS attacks does the BSI recommend in the 2019 situation report?

**Choose an answer:**

*Specialized service provider* Awareness campaigns Deploying DMARC

New server hardware

**QUESTION 225 OF 319**

**DLMIMWCK01\_MC\_heavy/lesson 08**

You own a business that collects documents from publicly available sources, aggregates them, and makes them searchable.

Which of the following is most important to you?

**Choose an answer:**

Multi-factor authentication Awareness training

Commissioning of a scrubbing center

*Offline backups*

**QUESTION 227 OF 319**

**DLMIMWCK01\_MC\_light/lesson 08**

According to ENISA, cybersecurity is being mostly strongly impacted by what impact of the COVID-19 pandemic?

**Choose an answer:**

Increased need for information

*Significant expansion of remote working*

Increased number of intensive care patients Vaccine development.

**QUESTION 229 OF 319**

**DLMIMWCK01\_MC\_light/lesson 08**

According to ENISA, which trend calls for new forms of protective measures?

**Choose an answer:**

*Digitization of processes*

Skills shortage

Expansion of renewable energies Trend toward on-premises services

**QUESTION 231 OF 319**

**DLMIMWCK01\_MC\_light/lesson 08**

What does the abbreviation VDP stand for in the context of cybersecurity?

**Choose an answer:**

Vulnerability Defacement Program Vulnerability Don’t Patch *Vulnerability Disclosure Program* Vulnerability Disclosure Path