DLMIMWCK01\_lesson01\_question01

Which description applies to all acts of computer crime?

* All acts directed against computers or using computers as a tool (1 pts)
* Only acts directed against computers (0 pts)
* Only acts using computers as a tool (0 pts)
* All acts directed against computers and using the internet as a tool (0 pts)

DLMIMWCK01\_lesson01\_question02

What is the goal of ransomware?

* Ransomware disrupts data processing operations and attempts to extort a ransom. (1 pts)
* Ransomware aims to spread unnoticed. (0 pts)
* Ransomware displays intrusive advertisements to the victim. (0 pts)
* Ransomware aims to use the victim’s computer for further attacks. (0 pts)

DLMIMWCK01\_lesson01\_question03

Which of the following vulnerabilities exists at the organizational level?

* Lack of four-eyes principle (1 pts)
* Lack of software updates (0 pts)
* Network without a firewall (0 pts)
* Master data system without authentication (0 pts)

DLMIMWCK01\_lesson01\_question04

By definition, what kind of vulnerability do social engineering attacks exploit?

* Human vulnerability (1 pts)
* Technical vulnerability (0 pts)
* Infrastructural vulnerability (0 pts)
* Management level vulnerability (0 pts)

DLMIMWCK01\_lesson01\_question05

Which of the following attacks targets the victim’s password?

* Phishing (1 pts)
* Dumpster diving (0 Pts)
* Baiting (0 Pts)
* Whaling (0 pts)

DLMIMWCK01\_lesson02\_question01

Which of the following sections may apply to appropriation of identity?

* Section 202a StGB (1 pts)
* Section 142 PatG (0 pts)
* Section 153 StGB (0 pts)
* Section 146 StGB (0 pts)

DLMIMWCK01\_lesson02\_question02

Which of the following laws forms the core of intellectual property law?

* Utility Model Act (1 pts)
* Law against Unfair Competition (0 pts)
* Telecommunications Act (0 pts)
* General Data Protection Regulation (0 pts)

DLMIMWCK01\_lesson02\_question03

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

* Forgery of legal documents (1 pts)
* Fraud (0 pts)
* Counterfeiting (0 pts)
* Defamation (0 pts)

DLMIMWCK01\_lesson02\_question04

Which of the following acts is not a prerequisite for Section 263a of the StGB (Computer Fraud) to apply?

* Unauthorized execution of a program (1 pts)
* Unauthorized use of data (0 pts)
* Incorrect configuration of a computer program (0 pts)
* Use of incorrect or incomplete data (0 pts)

DLMIMWCK01\_lesson02\_question05

Which of the following sections does not apply to the theft and misuse of online account credentials using a virus?

* Section 185 StGB (1 pts)
* Section 269 StGB (0 pts)
* Section 202a StGB (0 pts)
* Section 263a StGB (0 pts)

DLMIMWCK01\_lesson03\_question01

Which of the following technological developments is not conducive to data theft?

* Multi-factor authentication (1 pts)
* Mobile devices (0 pts)
* Internet-of-Things (0 pts)
* Social networks (0 pts)

DLMIMWCK01\_lesson03\_question02

Which of the following characteristics of a backup exacerbates the consequences of a ransomware attack?

* Online (1 pts)
* Complete (0 pts)
* Current (0 pts)
* Offline (0 pts)

DLMIMWCK01\_lesson03\_question03

Which of the following statements about DDoS attacks is not true?

* DDoS attacks require credentials that allow access to the target system. (1 pts)
* DDoS attacks create an overload on the target system. (0 pts)
* DDoS attacks are launched from a large number of computers. (0 pts)
* DDoS attacks often use botnets. (0 pts)

DLMIMWCK01\_lesson03\_question04

Which of the following is a synonym for industrial espionage?

* Company espionage (1 pts)
* Economic espionage (0 pts)
* Competitive intelligence (0 pts)
* Aggressive market research (0 pts)

DLMIMWCK01\_lesson03\_question05

What kind of malware does a decryptor help against?

* Ransomware (1 pts)
* Adware (0 pts)
* AES-256 (0 pts)
* SMB (0 pts)

DLMIMWCK01\_lesson04\_question01

Which of the following is not a side effect that can be used for a side-channel attack?

* Process list (1 pts)
* Timing (0 pts)
* Electromagnetic waves (0 pts)
* Power consumption (0 pts)

DLMIMWCK01\_lesson04\_question02

Which of the following is an operating system’s basic defense mechanism against attacks?

* Rights separation (1 pts)
* Out-of-order execution (0 pts)
* Multithreading (0 pts)
* SMB (0 pts)

DLMIMWCK01\_lesson04\_question03

Which property of a service restricts a DoS attack?

* Availability (1 pts)
* Confidentiality (0 pts)
* Integrity (0 pts)
* Authenticity (0 pts)

DLMIMWCK01\_lesson04\_question04

Which protocol is usually used on TCP port 443?

* HTTPS (1 pts)
* DNS (0 pts)
* VoIP (0 pts)
* POP3 (0 pts)

DLMIMWCK01\_lesson04\_question05

Which of the following is not an organizational regulation?

* Log entry (1 pts)
* Role distribution (0 pts)
* Organizational structure (0 pts)
* Process descriptions (0 pts)

DLMIMWCK01\_lesson05\_question01

How is a polymorphism created?

* Rearrangement of functions (1 pts)
* Infection of a new system (0 pts)
* Callback to the command and control server (0 pts)
* Password interception (0 pts)

DLMIMWCK01\_lesson05\_question02

Which of the following is not a type of malware detection method?

* File system structure-based detection (1 pts)
* Signature-based detection (0 pts)
* Behavior-based detection (0 pts)
* Heuristics-based detection (0 pts)

DLMIMWCK01\_lesson05\_question03

What data can be used during a post-mortem analysis?

* File system structure (1 pts)
* Memory (0 pts)
* Process list (0 pts)
* List of active network connections (0 pts)

DLMIMWCK01\_lesson05\_question04

What technique is used when the file system structure of a disk is destroyed?

* File carving (1 pts)
* Tcpdump (0 pts)
* NTFS reload (0 pts)
* Fragmented binary (0 pts)

DLMIMWCK01\_lesson05\_question05

What procedure or application can help in the event of a wipeout?

* Restoring from a backup (1 pts)
* Use of a decryptor (0 pts)
* File carving (0 pts)
* Restoring the Recycle Bin (0 pts)

DLMIMWCK01\_lesson06\_question01

What does the abbreviation ISMS mean?

* Information security management system (1 pts)
* Information protection management system (0 pts)
* IT security monitoring system (0 pts)
* Information and safety management service (0 pts)

DLMIMWCK01\_lesson06\_question02

What kind of benefit does a TPM not provide?

* Protection against theft (1 pts)
* Cryptographic key storage (0 pts)
* Beginning of a chain of trust (0 pts)
* Cryptographic key management (0 pts)

DLMIMWCK01\_lesson06\_question03

What process does MFA safeguard?

* Authentication (1 pts)
* Authorization (0 pts)
* Allocation of access rights (0 pts)
* Access control (0 pts)

DLMIMWCK01\_lesson06\_question04

What is the main goal of awareness-raising activities?

* Creation of awareness (1 pts)
* Establishment of SSO (0 pts)
* Intrusion detection (0 pts)
* Introduction of security incident handling (0 pts)

DLMIMWCK01\_lesson06\_question05

Which of the following processes is not directly related to incident response planning?

* Change management (1 pts)
* Business continuity management (0 pts)
* IT forensics (0 pts)
* Security incident handling planning (0 pts)

DLMIMWCK01\_lesson07\_question01

Which of the following is a reactive measure?

* Disabling all administrator accounts after a malware attack (1 pts)
* Updating anti-virus patterns (0 pts)
* Hiring a consultant to set up an ISMS (0 pts)
* Enabling logging on a domain controller (0 pts)

DLMIMWCK01\_lesson07\_question02

What are the categories of damage that are related to computer crime?

* Physical, digital, economic, reputational (1 pts)
* Physical, economic, transistor, psychological (0 pts)
* Reputational, motor, psychological, monetary (0 pts)
* Economic, social, digital, axiomatic (0 pts)

DLMIMWCK01\_lesson07\_question03

What type of threat intelligence is also referred to as TTP?

* Tactical (1 pts)
* Strategic (0 pts)
* Technical (0 pts)
* Taxonomic (0 pts)

DLMIMWCK01\_lesson07\_question04

Are private sector organizations in Germany obligated to join the Cybersecurity Alliance?

* No, it is not mandatory. (1 pts)
* Yes, it is mandatory. (0 pts)
* Yes, if they are critical infrastructure operators. (0 pts)
* Yes, if they are covered by the Official Secrets Act. (0 pts)

DLMIMWCK01\_lesson07\_question05

Which of the following are included in the Cybersecurity Alliance’s organizational recommendations for action?

* Establishment of a crisis team, internal and external communication, and external support (1 pts)
* Internal and external communication, monitoring of the network, and external support (0 pts)
* Internal communication, monitoring of the network, and convening of the internal crisis team (0 pts)
* External communication, convening of the crisis team, and external support (0 pts)

DLMIMWCK01\_lesson08\_question01

Which of the following organizations is a source for reports on the current security situation related to computer crime?

* Information Security Forum (1 pts)
* Institute of Electrical and Electronics Engineers (0 pts)
* Federal Office for Information Security (0 pts)
* Cybersecurity e.V. (0 pts)

DLMIMWCK01\_lesson08\_question02

Which of the following attacks within one’s own organization can patch management not help to prevent?

* DDoS (1 pts)
* Botnets (0 pts)
* Malicious programs (0 pts)
* Ransomware (0 pts)

DLMIMWCK01\_lesson08\_question03

At what point does Security by Design take the security aspect into consideration?

* Systems design (1 pts)
* User acceptance testing (0 pts)
* Rollout (0 pts)
* Development phase (0 pts)

DLMIMWCK01\_lesson08\_question04

Who launches the Europol Awareness Campaign?

* EC3 (1 pts)
* CIA (0 pts)
* BSI (0 pts)
* ECC (0 pts)

DLMIMWCK01\_lesson08\_question05

What topics has Europol Awareness previously covered?

* Mobile awareness and cyberscams (1 pts)
* Mobile awareness and crypto-agility (0 pts)
* Cyberscams and mobile agility (0 pts)
* Cyberscams and security by design (0 Pts)