**QUESTION 1 OF 78**

**DLMCSECRAM01\_E\_Offen\_leicht/Unit 01**

**Define and explain the properties of a cyber catastrophe.**

Blast radius (1p): A large group of users is affected by the event. (1p)

Outage (1p): A service provided to the end user is degenerated. The end user is not able to use this service which impacts his work or life. (1p)

Uncontrollability (1p): The organization is no longer able to control an event that affects it. (1p)

**QUESTION 2 OF 78**

**DLMCSECRAM01\_E\_Offen\_leicht/Unit 01**

**Describe the different kinds of cyber catastrophes. Give an example for each one.**

Global Cyber Catastrophe (1p): The blast radius for this catastrophe has a global radius. The event has a global impact. (1p)

Local Cyber Catastrophe (1p): The blast radius is restricted to a group of users. The event impact is restricted to a group of people or an organization (1p)

Examples:

Global Cyber Catastrophe: (1p)

* **Code Red**
* **Conficker**
* **Dyn DDoS attack**
* **WannaCry / Not Petya Ransomware Local Cyber Catastrophe: (1p)**
* **AWS Cloud disruption**
* **Garmin ransomware attack**
* **Azure AAD outage**

**QUESTION 3 OF 78**

**DLMCSECRAM01\_E\_Offen\_mittel/Unit 01**

**An organization has identified a design flaw in their web application which would cost 10.000€ to fix. The application processes intellectual property from customers and the design flaw might expose this data. Explain when and why the organization needs to mitigate the risk.**

The organization needs to mitigate the risk when the potential loss is higher than the cost fixing the design flaw (3p). This is due to the fact that risk management should prevent the organization from loosing money as fixing is cheaper than leaving the design flaw in the system (3p).

**QUESTION 4 OF 78**

**DLMCSECRAM01\_E\_Offen\_mittel/Unit 01**

**Explain why risk abstraction is needed in an organization. Give two examples how risks can be abstracted.**

Risk abstraction is needed to summarize risks for different management level (2p).

Examples:

Crypto malware attack can be abstracted to a financial risk (2p) A data breach can be abstracted to a reputation risk (2p).

**Explain the difference between a risk and a threat and how they link together.**

**Give an example for a threat with a resulting risk for the organization and one example of a threat without a risk to an organization.**

A risk is the level of impact (1p) a threat can have on an organization in combination with the likelihood (1p) of that threat occurring.

A threat is the source of a risk. Generally speaking, a threat is an event (1p) with the potential to harm the organization (1p). This resulting harm can affect the organization itself or an asset of the organization (1p).

Not all threats to an organization are also risks of this organization (1p) but all risks contain a threat (1p). A threat that stands on its own independent (1p) from an organization would not cause an issue (1p).

For example, an exploit for a specific system is a severe threat (1.5p). But if the organization is not using this particular system, it does not constitute a risk (1p) as it is impossible that this threat would cause an issue (1.5p).

On the other side a vulnerability in a web application has a threat of exploiting this vulnerability (1.5p). If assets from the organization is stored on that application there is a risk for this organization that these assets get stolen or harmed (1.5p).

To sum up, a threat becomes a risk for the organization if there is a likelihood (1.5p) that this threat will cause an impact. (1.5p)

**Define and explain the different threat sources and give two examples for each one.**

Malicious (1p): An intentional action from a human. This action is intended to harm the asset (2p).

* **An unauthorized users gains access to internal data due to an exploit (1.5p)**
* **Someone steals an authorization token to gain access to the administrative interface (1.5p) Human non-malicious (1p): A non intentional action from a human which harms the asset. This action is not intended to harm the system and was most of the time a mistake from an involved party. (2p)**
* **A bug in the software exposes internal data to external users (1.5p).**
* **The deployment of a new patch goes wrong because some systems were missed (1.5p)**

Non-human (non-malicious) (1p): An action or event which is not started by a human actor. This action is an act of nature beyond control (2p).

* **Flooding destroys a data center (1.5p)**
* **A storm prevents the start of a plane with critical replacement components on it (1.5p).**

**QUESTION 7 OF 78**

**DLMCSECRAM01\_E\_Offen\_leicht/Unit 02**

**List the different components of likelihood and impact in the OWASP risk rating methodology.**

Likelihood:

* **Threat agent (1p)**
* **Attack vector (1p)**
* **Vulnerability (1p)**
* **Security Controls (1p) Impact:**
* **Technical impact (1p)**
* **Business impact (1p)**

**QUESTION 8 OF 78**

**DLMCSECRAM01\_E\_Offen\_leicht/Unit 02**

**Explain the definition of the likelihood and the impact in the OWASP risk rating methodology. List also the sub categories.**

The impact describes how high the potential damage is a threat can cause to an organization (1p). OWASP defines the impact in two categories. The technical impact and the business impact (2p). The likelihood describes how likely it is that a threat can occur in an organization (1p). The likelihood is split in wasp in following categories:

* **Threat agent (0.5p)**
* **Attack vector (0.5p)**
* **Vulnerability (0.5p)**
* **Security Controls (0.5p)**

**QUESTION 9 OF 78**

**DLMCSECRAM01\_E\_Offen\_mittel/Unit 02**

**List three risk management strategies and name an example for each.**

Avoid the risk (1p): The data center is in a thunderstorm area. Move the data center to a different area where are no thunderstorms (1p).

Reduce or mitigate risk (1p): The data center is in a thunderstorm area. Build the data center thunderstorm proof (1p).

Transfer the risk (1p): The data center is in a thunderstorm area. Get an insurance for elemental damage (1p).

Accept the risk (1p): The data center is in a thunderstorm area. Accept the risk that a thunderstorm might impact the data center (1p).

**QUESTION 10 OF 78**

**DLMCSECRAM01\_E\_Offen\_mittel/Unit 02**

**Define the risk management category for following examples.**

1. **The data center is in a thunderstorm area. Move the data center to a different area where are no thunderstorms**
2. **The data center is in a thunderstorm area. Build the data center thunderstorm proof**
3. **The data center is in a thunderstorm area. Get an insurance for elemental damage.**
	1. **The data center is in a thunderstorm area. Move the data center to a different area where are no thunderstorms -> Avoid the risk (2p).**
	2. **The data center is in a thunderstorm area. Build the data center thunderstorm proof -> Reduce or mitigate risk (2p).**
	3. **The data center is in a thunderstorm area. Get an insurance for elemental damage -> Transfer the risk (2p).**

**An identified risk has following values. Calculate the overall risk level (Include the calculation for each step).**

* **The threat actor has network and programming skills (6).**
* **The motivation is a high reward (9).**
* **Special access or resources are required (4).**
* **Only partners have access to the system (5).**
* **The vulnerability was difficult to discover (3).**
* **The exploitation is difficult (5).**
* **The vulnerability is quite obvious (6).**
* **There is active logging and reviews in place (3).**
* **There might be minimal critical data disclosed (6).**
* **The integrity is slightly corrupted (1).**
* **There is only a minimal service disruption possible for secondary services (1).**
* **The threat is fully traceable (1).**
* **There is a significant effect on the annual profit (7).**
* **Loss of goodwill is possible (5).**
* **There might be minimal compliance violations (2).**
* **The privacy is at most affected for a single individual (1)**



Calculate the overall risk level (2p): Both likelihood and impact are medium therefore the risk is medium

**Rate and explain the likelihood of the threat agent and the vulnerability for following scenario:**

**A data breach occurred. The attacker was one employed network/system administrator at the organization and gained a lot of money out of selling the data. Special access to the production database was used to extract the data via a misconfigured permission management system. The vulnerability was easy to find and exploit for the attacker as he had all necessary information available. The attacker got knowledge about this vulnerability through a ticket which was assigned to his team. So it was obvious for him. Fortunately, the system had active logging and the log files were reviewed to find the attacker quickly.**

Threat agent:

* **Skill level: network/system administrator (1p) -> (6) network and programming skills (1p)**
* **Motive: gained a lot of money out of selling the data (1p) -> (9) high reward (1p)**
* **Opportunity: Special access to the production database was used (1p) -> (4) special access or resources required (1p)**
* **Size: attacker was one employed network/system administrator (1p) -> (2) system administrators (1p)**

(1p)



Vulnerability:

* **Ease of discovery: easy to find and exploit for the attacker as he had all necessary information available (1p) -> (7) easy (1p)**
* **Ease of exploit: easy to find and exploit for the attacker as he had all necessary information available (1p) -> (7) easy (1p)**
* **Awareness: got knowledge about this vulnerability through a ticket which was assigned to his team (1p) -> (6) obvious (1p)**
* **Intrusion detection: system had active logging and the log files were reviewed (1p) -> (3) logged and reviewed (1p)**

(1p)



**List the STRIDE threats and the desired properties for each threat.**

* **Spoofing (0.5p) <-> Authentication (0.5p)**
* **Tampering (0.5p) <-> Integrity (0.5p)**
* **Repudiation (0.5p) <-> Non-Repudiation (0.5p)**
* **Information (0.5p) Disclosure<-> Confidentiality (0.5p)**
* **Denial of Service (0.5p) <-> Availability (0.5p)**
* **Elevation of Privileges (0.5p) <-> Authorization (0.5p)**

**QUESTION 14 OF 78**

**DLMCSECRAM01\_E\_Offen\_leicht/Unit 03**

**List and explain six LINDDUN threats.**

* **Linkability (0.5p): An adversary is able to link two items of interest without knowing the identity of the data subject(s) involved. (0.5p)**
* **Identifiability (0.5p): An adversary is able to identify a data subject from a set of data subjects through an item of interest. (0.5p)**
* **Non-repudiation (0.5p): The data subject is unable to deny a claim (e.g., having performed an action, or sent a request). (0.5p)**
* **Detectability (0.5p): An adversary is able to distinguish whether an item of interest about a data subject exists or not, regardless of being able to read the contents itself. (0.5p)**
* **Disclosure of information (0.5p): An adversary is able to learn the content of an item of interest about a data subject. (0.5p)**
* **Unawareness (0.5p): The data subject is unaware of the collection, processing, storage, or sharing activities (and corresponding purposes) of the data subject’s personal data. (0.5p)**
* **Non-compliance (0.5p): The processing, storage, or handling of personal data is not compliant with legislation, regulation, and/or policy. (0.5p)**

**Describe the three similarities and three differences between STRIDE and LINDDUN.**

Similarities:

* **LINDDUN and STRIDE are both threat model methodologies. (1p)**
* **Both are mnemonics for the threat categories. (1p)**
* **Both rely on system modeling and drawing DFDs. (1p)**

Differences:

* **STRIDE focuses on the systems assets and LINDDUN focuses on the data subjects' items of interest. (1p)**
* **STRIDE focuses on system threats and LINDDUN on privacy threats. (1p)**
* **STRIDE focuses mostly on external attacks and LINDDUN also considers how to protect the users data from the system itself. (1p)**

**QUESTION 16 OF 78**

**DLMCSECRAM01\_E\_Offen\_mittel/Unit 03**

**List and explain three Data Flow Diagram symbols.**

Process (1p): Any executed code controlled by the system. (1p)

Data flow (1p): Any data flow between processes, data stores, or external entities. (1p) Data store (1p): Any sub-system that stores data controlled by the system. (1p)

External entity (1p): Any external entity (user or system) that interacts with the system but is not controlled by the system itself. (1p)

Trust boundary (1p): A boundary between two entities which marks a change of trust (e.g., corporate network to the internet) (1p)

**QUESTION 17 OF 78**

**DLMCSECRAM01\_E\_Offen\_schwer\_F1/Unit 03**

**Draw an attack tree in list style for following scenario.**

**The main goal is to exfiltrate data. This can be done through two ways. The first one is to get the data through an employee. The employee can either be bribed or threaten. The other way is to break into their system. For that it is needed to find a vulnerability and to exploit the vulnerability.**

1. **Exfiltrate data (2p)**
	1. **Get data through employee (3p)**
		1. **Bribe employee (2p)**
		2. **Threaten employee (2p)**
	2. **Break into the system (&) (3p the & is important)**
		1. **Find vulnerability (2p)**
		2. **Exploit vulnerability (2p) (2p) for the proper representation**

**QUESTION 18 OF 78**

**DLMCSECRAM01\_E\_Offen\_schwer\_F1/Unit 03**

**List the STRIDE threats and an example for each threat.**

* **Spoofing (1p): A user can change his user-ID in the front-end to impersonate another user (2p)**
* **Tampering (1p): A user is able to manipulate a DB query to overwrite data from other users (2p)**
* **Repudiation (1p): If no system logging in place user actions cannot be reconstructed. (2p)**
* **Information Disclosure (1p): An open API endpoint disclosed internal documents (2p)**
* **Denial of Service (1p): A malicious user input let the application crash (2p)**
* **Elevation of Privileges (1p): With a malicious input a user is able to gain elevated privileges (2p)**

**List and explain the three risk management level according to NIST.**

* + - 1. **Organization (1p): The organization level constitutes the highest level. Risks faced by the entire organization and the organization-wide risk management processes are managed at this level. (1p)**
			2. **Mission/business process (1p): The mission/business process level is the second level. Activities conducted at this level do not address technical risks but instead focus on the management of product or project risks. (1p)**
			3. **Information system (1p): The third level addresses risk from the perspective of the information system with an emphasis on the technical and organization risks faced by an information system. (1p)**

**QUESTION 20 OF 78**

**DLMCSECRAM01\_E\_Offen\_leicht/Unit 04**

**List and explain the three goals for mitigation measures according to BSI.**

* **Completeness (1p): Do the standard security measures provide protection for all aspects of each threat? (1p)**
* **Mechanism strength (1p): Do the protection mechanisms recommended in the standard security measures counteract each threat adequately? (1p)**
* **Reliability (1p): How difficult is it to circumvent the planned security mechanisms? (1p)**

**Map the six statements to the six tasks in risk management according to the ISO/IEC 27005:**

* **Defining the scope**
* **Identifying the risk**
* **Avoid the risk**
* **Accepting the leftover risks**
* **Present the risks to the management**
* **Write down the risks in a ticket system for tracking**
* **Defining the scope -> Context establishment (1p)**
* **Identifying the risk -> Risk assessment (1p)**
* **Avoid the risk -> Risk treatment (1p)**
* **Accepting the leftover risks -> Risk acceptance (1p)**
* **Present the risks to the management -> Risk communication (1p)**
* **Write down the risks in a ticket system for tracking -> Risk monitoring and review (1p)**

**QUESTION 22 OF 78**

**DLMCSECRAM01\_E\_Offen\_mittel/Unit 04**

**List and give examples to the steps in the risk management process part of the ISO/IEC 27005.**

Risk identification (1p): Do a threat model to identify the threats (1p).

Risk estimation (1p): Use the threats from the threat model and rate the risk of those (1p).

Risk evaluation (1p): Compare the identified risks and see which one needs immediate attention (1p).

**Describe the risk assessment process defined by the BSI Standard 100-3.**

The BSI Standard 100-3 describes how to conduct a risk analysis based on the IT-Grundschutz and is divided into seven parts: (1p)

Preliminary work (1p):

* **The first part section describes the work that needs to be completed prior to a risk assessment. (1p)**

Preparing the threat summary (1p):

* **The threat summary is the first thing viewed by a decision-maker (1p). Accordingly, it is important that it is informative and provides an overview of the security status of the analyzed system. (1p) Determination of additional threats (1p):**
* **The IT-Grundschutz model features a defined set of threats to systems (1p). However, in certain circumstances, additional isolated threats faced by a system may go beyond the scope of those specified in the IT-Grundschutz model. (1p)**

Threat assessment (1p):

BSI Standard 100-3 describes checking whether measures already implemented or planned in the security concept, generally standard security measures taken from the IT-Grundschutz Catalogues, offer adequate protection for each threat, or whether gaps exist. (2p)

Handling risks (1p):

As a general rule, the threat assessment generally identifies a number of risks that are not adequately mitigated by the security measures taken from the IT-Grundschutz Catalogues. (1p) Consolidation of the security concept (1p):

The security concept will need to be consolidated if additional security measures are added to handle the remaining risks (1p). In addition, all risks need to be documented in the security concept along with their risk handling strategy (1p).

Feedback to the security process (1p):

Following successful risk analysis, the outcome of the analysis and the security concept can be used to modify the security process. (1p)

**List six steps of the risk management process according to NIST SP 800-37 and give and explain one example tasks for each one.**

Prepare (1p):

* **Define a risk management strategy (1p): Establish a risk management strategy for the organization that includes a determination of the risk tolerance. (1p)**

Categorize (1p):

* **Categorize and document the systems (1p): The systems are characterized and documented. This includes the purpose of the system, the responsible persons and general system descriptions. (1p)**

Select (1p):

* **Select a baseline protection to reduce the risk of those systems (1p): The baseline control are pre-defined sets of controls specifically assembled to address the protection needs of a system. Control baselines serves as a starting point for the protection of a systems. (1p)**

Implement (1p):

* **Implement the developed controls (1p): The organization is implementing the previously defined security controls. (1p)**

Assess(1p):

\*Assess the security controls (1p): The security controls are assessed to check if the defined controls reduce the risk (1p)

Authorize(1p):

* **Risk authorization (1p): Determine if the risk from the operation or use of the information system or the provision or use of common controls is acceptable. (1p)**

Monitor (1p):

* **Monitor system changes(1p): Monitor the information system and its environment of operation for changes that impact the security and privacy posture of the system. (1p)**

**Describe the two ways of assessing a black swan event.**

The first assessment strategy for black swan events is to assess events and analyze what would happen to the scope (2p). These events can be previous black swan and disaster events. These events are then played out and the resulting risks for the assets analyzed. (1p)

The second assessment strategy is basically the first one in reverse. In this strategy threats for the assets are assessed and then events which might lead to risks are found (2p). These risks can be results from well-known threats from threat model strategies. Now with this threat in mind scenarios for that might be found. Natural events might be a possibility. (1p)

**QUESTION 26 OF 78**

**DLMCSECRAM01\_E\_Offen\_leicht/Unit 05**

**Explain "identify", "analyze" and "plan" from the SEI risk management paradigm.**

Identify:

In the first step the risks will be discovered and identified. This is typically done in the risk assessment. (2p)

Analyze:

After the risks are identified they need to be analyzed. This is also done in the risk assessment. Analyzing the risks contains rating it. I.e., defining the likelihood and the impact of the risks to the organization. This is important to help the decision makers focus on the proper risks. (2p)

Plan: Following the risk analysis, the identified and rated risk can be tackled. For that a mitigation plan needs to be established for each risk. This plan contains the measure and a timeframe for implementing that measure. (2p)

**List six items which should be included to proper track risks according to SEI.**

* **Date (1p)**
* **Risk ID (1p)**
* **Risk Name (1p)**
* **Mitigation plan (1p)**
* **Deadline (1p)**
* **Implementation control (1p)**

**QUESTION 28 OF 78**

**DLMCSECRAM01\_E\_Offen\_mittel/Unit 05**

**List six assumptions which can be used for threat modeling.**

* **The employees of the organization are trusted. (1p)**
* **The cloud provider does not act in a malicious way. (1p)**
* **The used hardware has no known vulnerabilities. (1p)**
* **The physical security is assured. (1p)**
* **The cloud infrastructure acts as described. (1p)**
* **The network infrastructure of the data center is well designed and secure. (1p)**

**A vulnerability in a web application was found. This vulnerability might be used to access internal data on the server. The vulnerability can only be exploited when a user is logged in. List nine possible mitigation measures and classify the mitigation strategy of those measures. Name one mitigation measure for each mitigation strategy.**

* **Develop a fix for the vulnerability (1p) (Risk reduction/mitigation) (1p)**
* **Only allow trusted users to log-in (1p) (Risk avoidance) (1p)**
* **Deploy a web application firewall to block the malicious requests (1p) (Risk reduction/mitigation) (1p)**
* **Move the sensitive data away from the vulnerable web application (1p) (Risk avoidance) (1p)**
* **Change the web application so that it can only be accessed from the internal network (1p) (Risk avoidance) (1p)**
* **Get an insurance which covers the data loss of the internal documents (1p) (Risk transfer) (1p)**
* **Get a contractor for hosting and managing the server and the web application (1p) (Risk transfer) (1p)**
* **Accept the risk as it would cost more to fix the vulnerability (1p) (Risk acceptance (1p)**
* **Implement measures that the data can't be directly accessed from the web application (1p) (Risk reduction/mitigation) (1p)**

**An organization is processing personal data from customer. They are stored together with the project data for these customers. All data are stored in databases and networks stores. Processed are the data by a cluster of workers and then displayed on the frontend server. The secrets are stored with processes in place for access.**

**List the assets in the correct category and explain each category. Give an example for each technology used in the supporting assets.**

Primary assets: Primary assets are the assets which are the focus of the business and the attacker. These assets “make the money”. Business activities and information are the primary assets. (2p)

* **Personal customer data (1p)**
* **Customer project data (1p)**

Supporting assets: The secondary or supporting assets are things which support the primary assets and are only relevant when a primary asset is affected by a supporting asset. (2p)

* **Database (1p): MySQL Database (1p)**
* **Network store (1p): SMB Network share (1p)**
* **Worker cluster (1p): Virtual Machines (1p)**
* **Frontend server (1p): Apache web server (1p)**
* **Secrets (1p): Access token for the database (1p)**
* **Processes (1p): Key rotation process (1p)**

**QUESTION 31 OF 78**

**DLMCSECRAM01\_E\_Offen\_leicht/Unit 06**

**List four duties a security champion can have.**

* **Threat modeling (1.5p)**
* **Risk assessment (1.5p)**
* **Risk tracking (1.5p)**
* **Motivate the team to follow security controls (1.5p)**
* **Checking or writing security best practices (1.5p)**
* **Defining secure coding guidelines for the project team (1.5p)**
* **Do security reviews (1.5p)**
* **Implement automated security scanners (1.5p)**

**List and describe three steps in the organizational incident response preparation.**

* **Asset management (1p): The asset management stores all information about all possible asset at the organization. This can be primary or supportive assets. (1p)**
* **Roles and responsibilities (1p): The roles and responsibilities define who has what to do in the incident response process. Some roles are e.g., the on-call team, the incident investigator, the incident manager or IT operations. (1p)**
* **Access concept (1p)t: The access concept describes how the incident response team can access systems or asset. This includes normal read-only access for e.g., monitoring and logging or full administrative access in the incident event. (1p)**
* **Communication (1p): A definition of the communication is needed as in an incident case communication needs to be established quickly. This includes internal communication, communication to customers and communication to law enforcements. (1p)**
* **Process documentation (1p): All the tasks of the incident response management need to be defined in processes. This helps teams to have a guideline on how to prepare for an incident and how to handle such. (1p)**
* **Governance and Policies (1p): The incident response management needs to be unified for the organization. Therefore, governance and policies should be used to define this process. These policies can contain e.g., the definition of cyber incidents, the general reporting of such events, the escalation process or how to rate and prioritize incidents. (1p)**
* **Training (1p): Response to incidents need to be trained. This should be done to keep the incident response teams on track with new technologies and the environment and processes of the organization. (1p)**

**QUESTION 33 OF 78**

**DLMCSECRAM01\_E\_Offen\_mittel/Unit 06**

**List the three steps in crisis management and give an example for each.**

* **Readiness (1p): Setting up communication channels. (1p)**
* **Response (1p): Analyze and resolve the crisis. (1p)**
* **Recovery (1p): Do a root-cause analysis. (1p)**

**List the three steps of the post-processing phase in the incident response process and give an example for each.**

Lessons learned (1p): Gather the incident response handlers and conduct a meeting to discuss the incident response process and what could have been better (1p).

Documentation (1p): Use a documented management system to write down the conducted steps to mitigate the incident (1p).

Enhancement of the organization (1p): Send an email to the organization with the root-cause of the incident and a hardening proposal (1p).

**QUESTION 35 OF 78**

**DLMCSECRAM01\_E\_Offen\_schwer\_F2/Lektion 06**

**Explain the four resilience engineering control sets and add two examples to each control set.**

* **Resistive controls (1p): These controls are used for slowing down and frustrating the attacker as a first hurdle. (1.5p)**

\*\* Rate-limit failed logins (1p)

\*\* Implement a captcha for the web formular (1p)

* **Protective controls (1p): Protective controls are designed for the attack prevention. (1.5p)**

\*\* Set up proper input validation in the software (1p)

\*\* Separate the backend from the internet (1p)

* **Detective controls (1p): This control set should contain measures to detect an attack or a malicious event. (1.5p)**

\*\* Implement proper logging and monitoring (1p)

\*\* Set up a SIEM for log correlation (1p)

* **Compensation controls (1p): Compensating controls are second line defenses if a first line defense is not possible (1.5p)**

\*\* Deploy a web application firewall to block malicious input (1p)

\*\* Set up multi factor authentication for all internet facing applications (1p)

**QUESTION 36 OF 78**

**DLMCSECRAM01\_E\_Offen\_schwer\_F2/Lektion 06**

**An incident was detected in a web application via the logging system. The attackers were able to access the production database server. List in the correct order and explain the steps in the handling part of the incident response process. Also, give an example for each step for the scenario.**

Classification (1p): In the classification the input event which led to the incident will be analyzed and decided if this is a real incident or a false-positive. (1.5p)

* **Analyze the log and see if it is a true-positive (1p)**

Triage (1p): : In the triage the impact of the incident is analyzed. Here the affected assets need to be found. With new information the triage can be done again in the handling process. (1.5p)

* **Analyze the server and determine the blast radius (1p)**

Containment (1p): After the affected assets are found the impact of the incident needs to be contained. (1.5p)

* **Try to manage the impact of the incident by disconnecting the server from the internet (1p) Eradication / Recovery (1p): After the incident is contained the environment needs to be cleaned up and all traces from the incident removed or fixes. Also, short term mitigations can be applied in this step. (1.5p)**
* **Clean up the database server and remove the traces of the attacker (1)**

Reconstruction / Root-cause analysis (1p): When the incident is contained and under control the root-cause analysis can start. In this analysis evidence is analyzed how the incident could happen. (1.5p)

* **Analyze all gathered data and find the root cause of the incident (1p) (0.5p for the correct order)**

**What is the goal of risk management?**

**Select one:**

**Remove all possible risks for a business**

**Plan the mitigation measures for identified risks**

**Help the decision-makers understand the risk for the organization and bring it to an acceptable level**

**Propose proper business plans according to the average risk**

**The correct answer is: Help the decision-makers understand the risk for the organization and bring it to an acceptable level**

**QUESTION 38 OF 78**

**DLMCSECRAM01\_E\_MC\_leicht/Unit 01**

**What was the root cause of the Capital One Data Breach in 2019?**

**Select one:**

**A misconfigured service**

**A long running attack with multiple stages A misused public functionality**

**A nation state attack**

**The correct answer is: A misconfigured service**

**Which statement is correct about a cyber catastrophe?**

**Select one:**

**Cyber catastrophes have no impact on the real world.**

**Cyber catastrophes impact a large group of users.**

**Cyber catastrophes have always a high impact on the real world. Cyber catastrophes normally don't impact any user.**

**The correct answer is: Cyber catastrophes impact a large group of users.**

**QUESTION 40 OF 78**

**DLMCSECRAM01\_E\_MC\_mittel/Unit 01**

**Which of the following risks can be abstracted as a denial of service risk for**

**an organization?**

**Select one:**

**An attacker gains access to the internal systems and leaks internal documents.**

**An internal employee disclosed internal meeting minutes about hiring processes.**

**The service provider for payment processing refuses to disburse funds as a guarantee.**

**A crypto malware encrypts customer data and the service can't be provided to the user anymore.**

**The correct answer is: A crypto malware encrypts customer data and the service can't be provided to the user anymore.**

**What is the threat source of a misconfigured server which exposes customer**

**data?**

**Select one:**

**Non-human non-malicious**

**Human malicious Human non-malicious Non-human malicious**

**The correct answer is: Human non-malicious**

**QUESTION 42 OF 78**

**DLMCSECRAM01\_E\_MC\_schwer/Unit 01**

**Which of the events can be classified as a global cyber catastrophe?**

**Select one:**

**A crypto malware encrypts all data in an organization.**

**A bug in a service disrupts it and the users can't access it anymore.**

**A storm brings down the electricity in an office and hinders the employees from working. A global DNS outage makes the internet unusable.**

**The correct answer is: A global DNS outage makes the internet unusable.**

**QUESTION 43 OF 78**

**DLMCSECRAM01\_E\_MC\_schwer/Unit 01**

**A decision maker found out that a risk in the organization with 50M € annual**

**profit might cost them annually 450.000 €. What would be the logical decision?**

**Select one:**

**The risk needs to be mitigated if the mitigation costs are < 1% of the profit.**

**The risk can be accepted as the cost of the risk is < 1% of the profit.**

**The risk can be accepted if the mitigation cost of the risk is annually < 450.000 €. The risk needs to be mitigated as the cost of the risk is > 0.1% of the profit.**

**The correct answer is: The risk can be accepted if the mitigation cost of the risk is annually <**

**450.000 €.**

**What is the correct formula for describing a risk?**

**Select one:**

**The correct answer is:**

**QUESTION 45 OF 78**

**DLMCSECRAM01\_E\_MC\_leicht/Unit 02**

**What of the following statements describes the threat actor defined by**

**OWASP?**

**Select one:**

**Skill level**

**Awareness**

**Ease of Discovery Maturity**

**The correct answer is: Skill level**

**What is the highest reputation damage defined by OWASP?**

**Select one:**

**Bankruptcy**

**Brand damage**

**Loss of major accounts Loss of goodwill**

**The correct answer is: Brand damage**

**QUESTION 47 OF 78**

**DLMCSECRAM01\_E\_MC\_mittel/Unit 02**

**A risk has the overall impact of 2.6 and the likelihood of 7.3. What is the risk**

**level in the OWASP risk matrix?**

**Select one:**

**Critical**

**Low High Medium**

**The correct answer is: Medium**

**Which of the following events can be rated as a black swan event?**

**Select one:**

**An attacker finds a vulnerability in a system and deletes all data. The organization is now**

**bankrupt.**

**An attacker finds a vulnerability in the organizations server. He defaces the website and the organization loses reputation.**

**Two storms bring down both data centers located on different continents. The service of the organization can't be offered while the storm lasts.**

**Cosmic rays flip a bit in the communication. A single set of data needs to be retransmitted.**

**The correct answer is: Two storms bring down both data centers located on different continents. The service of the organization can't be offered while the storm lasts.**

**QUESTION 49 OF 78**

**DLMCSECRAM01\_E\_MC\_schwer/Unit 02**

**A frontend system has a vulnerability were in a very specific edge case**

**privileged access can be gained. The software is closed source. Rate the ease of exploit.**

**Select one:**

**Automated**

**Difficult Easy Theoretical**

**The correct answer is: Theoretical**

**QUESTION 50 OF 78**

**DLMCSECRAM01\_E\_MC\_schwer/Unit 02**

**An organization offers a service to users. A bug allows authenticated users**

**to crash parts of the service. The service will recover transparently for the users. Mark the proper risk management strategy?**

**Select one:**

**Mitigate the risk by deploying a bug fix at all costs**

**Avoid the risk by disabling user authentication**

**Transfer the risk by getting an insurance for cyber attacks which costs 1% of the current annual profit**

**Accept the risk as there is no real impact for the organization**

**The correct answer is: Accept the risk as there is no real impact for the organization**

**QUESTION 51 OF 78**

**DLMCSECRAM01\_E\_MC\_leicht/Unit 03**

**Which of the following elements is a valid element in an attack tree?**

**Select one:**

**Source**

**Node Data flow Actor**

**The correct answer is: Node**

**What is a security property a system should have according to STRIDE?**

**Select one:**

**Cleanliness**

**Integrity Simplicity Spoofing**

**The correct answer is: Integrity**

**QUESTION 53 OF 78**

**DLMCSECRAM01\_E\_MC\_leicht/Unit 03**

**What threat is the same in LINDDUN and in STRIDE?**

**Select one:**

**Spoofing**

**Unawareness Disclosure of information Linkability**

**The correct answer is: Disclosure of information**

**A user is able to change his user ID to impersonate another user. Which**

**STRIDE threat is describing this?**

**Select one:**

**Information Disclosure**

**Linkability Spoofing**

**Elevation of Privileges**

**The correct answer is: Spoofing**

**QUESTION 55 OF 78**

**DLMCSECRAM01\_E\_MC\_mittel/Unit 03**

**With a bug in a software a user is able to manipulate the data of other users.**

**Which STRIDE threat is describing this?**

**Select one:**

**Denial of Service**

**Spoofing**

**Elevation of Privileges Tampering**

**The correct answer is: Tampering**

**QUESTION 56 OF 78**

**DLMCSECRAM01\_E\_MC\_schwer/Unit 03**

**A node in an attack tree contains the threat "impersonating an employee".**

**What is a valid sub node for this threat?**

**Select one:**

**Flooding the server with requests**

**Stealing an employee card**

**Hindering an employee going to work Cold calling the company as an supplier**

**The correct answer is: Stealing an employee card**

**QUESTION 57 OF 78**

**DLMCSECRAM01\_E\_MC\_schwer/Unit 03**

**What is a correct data flow diagram?**

**Select one:**

**The correct answer is:**

**What NIST Publication provides a risk management framework?**

**Select one:**

**Special Publication 300-80**

**Special Publication 100-03**

**Special Publication 420-69**

**Special Publication 800-37**

**The correct answer is: Special Publication 800-37**

**QUESTION 59 OF 78**

**DLMCSECRAM01\_E\_MC\_leicht/Unit 04**

**What is the third level of the NIST organization-wide risk management?**

**Select one:**

**Project**

**Information system Mission/business process Organization**

**The correct answer is: Information system**

**What is described in the BSI 100-3?**

**Select one:**

**How to do threat management based on IT-Grundschutz**

**How to do risk assessment based on IT-Grundschutz How to do risk management based on IT-Grundschutz How to do threat modeling based on IT-Grundschutz**

**The correct answer is: How to do risk assessment based on IT-Grundschutz**

**QUESTION 61 OF 78**

**DLMCSECRAM01\_E\_MC\_mittel/Unit 04**

**The following mitigation measure is defined. To which strategy can this be**

**assigned to according to BSI?**

**The IT infrastructure will be duplicated to a different data center in a different country.**

**Select one:**

**Risk transfer**

**Risk acceptance**

**Risk reduction through additional security measures Risk avoidance through restructuring**

**The correct answer is: Risk reduction through additional security measures**

**An organization is planning their risk management according to the ISO/IEC**

**27005. Currently they are identifying the scope of the process. Which step in ISO/IEC 27005 is this?**

**Select one:**

**Context establishment**

**Risk assessment Risk communication Risk treatment**

**The correct answer is: Context establishment**

**QUESTION 63 OF 78**

**DLMCSECRAM01\_E\_MC\_schwer/Unit 04**

**In what NIST risk management category can the following policy be**

**classified:**

**Establish organization-wide forums to consider all types and sources of risk.**

**Select one:**

**Project**

**Organization Mission/business process Information system**

**The correct answer is: Organization**

**QUESTION 64 OF 78**

**DLMCSECRAM01\_E\_MC\_schwer/Unit 04**

**In what NIST risk management category can the following policy be**

**classified:**

**Allocating management, operational, and technical security controls to information systems and environments of operation as defined by the information security architecture.**

**Select one:**

**Information system**

**Mission/business process Organization**

**Project**

**The correct answer is: Mission/business process**

**QUESTION 65 OF 78**

**DLMCSECRAM01\_E\_MC\_leicht/Unit 05**

**What is a primary asset?**

**Select one:**

**Employees**

**Processes Cryptographic material Intellectual property**

**The correct answer is: Intellectual property**

**What diagram type shows the logical flow of an application?**

**Select one:**

**Sequence Diagram**

**Class Diagram Data Flow Diagram**

**Deployment Diagram**

**The correct answer is: Data Flow Diagram**

**QUESTION 67 OF 78**

**DLMCSECRAM01\_E\_MC\_leicht/Unit 05**

**How can black swan events be mitigated?**

**Select one:**

**It is not possible.**

**Get an insurance. Reduce the likelihood. Reduce the impact.**

**The correct answer is: Reduce the impact.**

**What should always be done in a risk assessment?**

**Select one:**

**Find at least one critical risk**

**Focus on human malicious events Define at least 5 assets Document the assessment**

**The correct answer is: Document the assessment**

**QUESTION 69 OF 78**

**DLMCSECRAM01\_E\_MC\_mittel/Unit 05**

**A requirement catalogue can be helpful in the risk management process. In**

**which part of the process is such a catalogue most useful?**

**Select one:**

**Assessment preparation**

**Threat modeling Mitigation proposal**

**Documentation and Reporting**

**The correct answer is: Threat modeling**

**QUESTION 70 OF 78**

**DLMCSECRAM01\_E\_MC\_schwer/Unit 05**

**A self-developed web application is running in a public cloud. What item**

**should be in scope for?**

**Select one:**

**The data center**

**The user's browser**

**The self developed parts**

**The system where the cloud runs on**

**The correct answer is: The self developed parts**

**QUESTION 71 OF 78**

**DLMCSECRAM01\_E\_MC\_schwer/Unit 05**

**In what asset category is the system administrator?**

**Select one:**

**Business asset**

**Human asset Primary asset Supporting assets**

**The correct answer is: Supporting assets**

**What is resilience engineering?**

**Select one:**

**Resilience engineering is planning the incident response process.**

**Resilience engineering is implementing security solutions to existing systems. Resilience engineering is threat modeling each application.**

**Resilience engineering is designing and implementing systems with a security focus.**

**The correct answer is: Resilience engineering is designing and implementing systems with a security focus.**

**QUESTION 73 OF 78**

**DLMCSECRAM01\_E\_MC\_leicht/Unit 06**

**What is the goal of an IDS?**

**Select one:**

**To correlate and log all security events**

**To detect employee misbehavior To block incoming network traffic**

**To detect intrusions into the network**

**The correct answer is: To detect intrusions into the network**

**What should be defined for a proper risk management policy?**

**Select one:**

**Risk hunger**

**Risk clearance Risk integrity Risk appetite**

**The correct answer is: Risk appetite**

**QUESTION 75 OF 78**

**DLMCSECRAM01\_E\_MC\_mittel/Unit 06**

**What training should be part of the risk management training?**

**Select one:**

**How to present risks**

**How to do security reviews How to write secure code How to manage developers**

**The correct answer is: How to do security reviews**

**A proper logging infrastructure is implemented into the new systems. What**

**control is this in the resilience engineering process?**

**Select one:**

**Protective controls**

**Detective controls Resistive controls Compensation controls**

**The correct answer is: Detective controls**

**QUESTION 77 OF 78**

**DLMCSECRAM01\_E\_MC\_schwer/Unit 06**

**What is the reason to get a cyber insurance?**

**Select one:**

**To get a tick on the HIPAA checklist**

**To complete the existing cyber security strategy To shift the need of implementing security controls To get a go-out-of-jail card**

**The correct answer is: To complete the existing cyber security strategy**

**QUESTION 78 OF 78**

**DLMCSECRAM01\_E\_MC\_schwer/Unit 06**

**A presentation is held to inform the organization about changes in the**

**software to mitigate a vulnerability. In what step of the incident process is this normally done?**

**Select one:**

**Technical preparation**

**Organizational preparation Handling**

**Post-processing**

**The correct answer is: Post-processing**