**Cyber Security Assessment 2- Ben Smerd (22072922)**

*Risk Assessment Scenario Description for Learning Management System (LMS)*

1. **Scope and Focus of the Risk Assessment**

In the evolving digital education world, Universities have taken up the new method of providing learning for students through Learning Management Systems (LMS). These management systems provide Universities with better methods for delivering, managing, monitoring and providing students with their studies. Due to an increased reliance on these systems, Universities can face increased risk to cyber threats. Using the CORAS method, we will systematically identify, evaluate, and treat security risks affecting the LMS. The CORAS process is a model-based risk analysis method which is used throughout cybersecurity to visualise assets, threats and treatments clearly though diagrams.

The scope of this risk assessment includes:

* The student portal, where students submit assignments, view grades and can access course materials.
* The instructor portal which is responsible for assignment grading, student performance analysis and course creation.
* Administrator backend which handles user management, provides data analytics and allows for course approval.
* Third party tool integrations including cloud storage services, external educational resources and video conferencing.
* Authentication server which manages user access, interfacing with both student and instructor portals for ensuring secure logins.
* The local database that supports the LMS, storing courses, user information and system data for retrieval and analysis.

The focus of this risk assessment includes:

* Confidentiality- ensuring that sensitive data such as student personal information, student grades and examination records are only accessible to the correctly authorised parties.
* Integrity- ensuring that data is safeguarded and processed against unauthorised modification including grade tampering or malicious content being injected.
* Availability- Uninterrupted and reliable access to the system is maintained, especially during critical periods such as examination periods and releasing of grade periods.
* Authentication and Non-repudiation- Verifying user identities and ensuring actions taken within the system can be reliably traced back to the source of it.
* Privacy Compliance- Meeting data obligations under cyber law, especially when dealing with student records and third party data processes.

1. **Target of the Risk Assessment**

The main target of this risk assessment for the party is the operations of the Learning Management System (LMS) and how it plays a central role for the university in delivering educational services, management of academic operations and the achievement of institutional outcomes. Why the LMS is the main target for this risk assessment is because it is the primary channel which the university delivers teaching and manages the engagement with students and staff members, so security is extremely important from the perspective of the university.

1. **Asset Diagram**

**A diagram of a diagram of money

AI-generated content may be incorrect.**

Within this CORAS diagram, we identify the key party being the University Analysis Client as shown within the Asset diagram. We further categorise direct and indirect assets based on their proximity and control within the LMS.

The direct assets represent the components and subsystems owned and operated by the university and include the student and instructor portals, authentication server, administration backend local database and the web server. These assets are the most central to the LMS system operations and the main focus of internal security controls

The indirect assets are cloud storage, video conferencing, student/teacher devices, internet infrastructure and the external learning API. These are services which are expanded from the LMS functionality but also introduce additional threat surfaces and reliability risks. These external systems are critical to the specified services that the university delivers through their LMS, which includes them in the focus of the risk assessment.

The asset diagram also shows interactions between assets, such as: the student portal uploads/downloads to the cloud storage, the auth server verifies login for the student portal and instructor portal, the admin backend validates roles through the auth server and the web server passes read/writes on data to the local database. Showing the interconnection and communication between assets allows us to identify the risk exposure landscape.

1. **Analysis of Unwanted Risks**

The LMS must uphold strong security to protect both the educational outcomes and institutional integrity. Based on the systems architecture and the universities stated security requirements, this risk assessment will focus on the confidentiality, integrity, availability mainly but also we will focus on the privacy, authentication and non-repudiation. These requirements are focused on especially in the context of high-stakes academic activities like online exams and grading.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Threat** | **Unwanted Incident** | **Damaged Asset** |
| A | External Attacker | SQL injection attack modifies grade records | Local Database |
| B | External Attacker | DoS attack causes login failure during peak usage | Authentication Server |
| C | Insider | Privileged admin accesses and exports student data | Administrative Backend |
| D | External Attacker | Phishing email leads to stolen student credentials | Student Portal and Auth Server |
| E | Third-Party Failure | Unauthenticated user hijacks online exam session | Video Conferencing Service |

1. A malicious external actor can insert a specific value into an input field on the LMS which launches an SQL injection. They can do this by manipulating the query structure and this can give them access or modify the grade records of multiple students. This unwanted incident highlights the critical need for input validation, parameterised queries and strict database access controls to maintain strong backend security.
   1. **Confidentiality-** At very high risk as the academic data and potential personal information can be uncovered.
   2. **Integrity**- Severely impacted as grades can be altered which undermines the trust in academic records.
   3. **Availability**- Possibly impacted if database data corruption causes system errors or outages.
2. An attacker floods the LMS login system with traffic in a denial of service (DoS) attack during an exam period, which causes legitimate users not able to authenticate and access the platform. Mitigation for this are requirements such as: rate limiting, firewall configuration and traffic anomaly detection systems to ensure uptime and resilience for the system.
   1. **Availability-** Critically impacted with students and instructors being locked out during essential operations.
   2. **Confidentiality/Integrity-** Not directly impacted but service disruptions could delay academic processes and generate institutional risk.
3. A privileged LMS administrator uses elevated access rights to retrieve student data for unauthorised purposes. Controls such as: role based access control (RBAC), activity logging and privileged access monitoring are necessary to mitigate insider threats.
   1. **Confidentiality-** Violated when student records, including personal data may be exposed.
   2. **Integrity-** At risk when admin level edits go unrecorded if proper auditing is not enforced.
   3. **Non-repudiation-** Weakened without proper logs because actions may be difficult to trace.
4. A student receives an email impersonating the LMS login portal and upon entering their credentials they accidentally share their login information with an attacker who later uses it to access the students account. Preventative measures include: two-factor authentication, email filtering and user education on phishing recognition.
   1. **Confidentiality-** Exposed as the attacker gains access to person student data.
   2. **Integrity-** Compromised when the assignments or submissions potentially can be tampered with.
   3. **Authentication-** This has failed when attackers can bypass legitimate access processes.
5. An instructor shares a Zoom meeting link for an online exam without authentication or access restrictions. An external user obtains the link and joins the session which disrupts the exam. Controls to mitigate this involve: waiting rooms, authentication for meeting access and log reviews from third parties.
6. **Prioritise Assets based on Importance**

|  |  |  |  |
| --- | --- | --- | --- |
| **Asset** | **Operational Importance** | **Consequence Value** | **Priority Level** |
| Local Database | Stores critical data: grades, student records, assignments, system logs | Severe- data loss, breaches, integrity compromise, legal implications | 1 |
| Authentication Server | Controls access to the LMS system for all users | Severe- denial of access, unauthorised logins, broken accountability | 2 |
| Student Portal | Primary interface for assignment submission, grade viewing and course access | Major- interrupts core learning workflows, lowers user trust | 3 |
| Administrative Backend | Manages accounts, roles, course approvals and analytics | Moderate- risk of privilege misuse or data leakage | 4 |
| Video Conferencing Tool | Supports live classes and exams, third party management | Moderate- impacts availability and exam integrity | 5 |

Helping the next step of risk analysis the LMS assets have been evaluated on their functional role, criticality to learning operations and potential impact if compromised. The local database is ranked highest due to its central role in storing academic records, user credentials and system logs. A breach here would severely affect confidentiality, integrity and institutional compliance. Authentication server follows as its compromise would prevent access across all user roles or enable unauthorised access. The student portal and administrative backend are vital to usability and operational control but carry lower risk if compromised. Video conferencing tool is still a vital asset however its easier to isolate if compromised.

1. **Risk Estimation Table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat Scenario** | **Asset Affected** | **Likelihood** | **Consequence** | **Justification** |
| 1. SQL injection alters grade records | Local Database | Likely | Severe | SQL injection is a common exploit, damaging grades impacts academic integrity and legal |
| 1. DoS blocks login during peak | Authentication Server | Possible | Major | Attacks may be timed during important periods like exams, temporary outage causes disruptions temporarily (not permanent) |
| 1. Insider admin leaks student data | Administrative Backend | Possible | Major | Insider threats are harder to detect and can result in privacy violations and legal breaches |
| 1. Phishing leads to stolen student credentials | Authentication server + Student Portal | Likely | Moderate | Users regularly fall for phishing where limited access usually prevents more extreme consequences |
| 1. Unsecured video links allows exam disruption | Video conferencing tool | Unlikely | Moderate | Rare but impactful, can affect exam integrity for the university reputation |

Each scenario was assessed based on the likelihood of occurrence and the severity of the impact. The likelihood was determined using known threat prevalence and levels of exposure. Consequence was considered based on data sensitivity, legal exposure and operational impact.

1. **Threat Diagrams**
   1. **SQL Injection- Local Database**

A diagram of a triangle and a black line

AI-generated content may be incorrect.

* 1. **Denial of Service (DoS)- Authentication Server**

A black and white text on a white background

AI-generated content may be incorrect.

* 1. **Insider Misuse- Administrative Backend**

A diagram of a process

AI-generated content may be incorrect.

* 1. **Phishing Attack- Authentication Server + Student Portal**

A diagram of a system

AI-generated content may be incorrect.

e. **Unauthorised Access to Online Exam- Video Conferencing Tool**

**A diagram of a system

AI-generated content may be incorrect.**

1. **Risk Matrix**
   1. **Risk Evaluation Matrix**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Minor (0.1-0.2)** | **Moderate (0.3-0.4)** | **Major (0.5-0.6)** | **Severe (0.7-0.8)** | **Catastrophic (0.9-1.0)** |
| **Rare (0.1-0.2)** | **Low** | **Low** | **Medium** | **Medium** | **High** |
| **Unlikely (03-04)** | **Low** | **Medium** | **Medium** | **High** | **High** |
| **Possible (0.5-0.6)** | **Medium** | **Medium** | **High** | **High** | **Extreme** |
| **Likely (0.7-0.8)** | **Medium** | **High** | **High** | **Extreme** | **Extreme** |
| **Almost Certain (0.9-1.0)** | **High** | **High** | **Extreme** | **Extreme** | **Extreme** |

* 1. **Risk Evalation Summary**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Threat Scenario** | **Likelihood** | **Impact** | **Score** | **Matrix Cell** | **Risk Level** | **Acceptable** |
| SQL Injection | 0.9 | 0.9 | 0.81 | Top-right | Extreme | No |
| DoS | 0.6 | 0.8 | 0.48 | Middle-right | High | No |
| Insider | 0.6 | 0.7 | 0.42 | Mid-high | High | No |
| Phishing | 0.8 | 0.5 | 0.40 | Mid-right | High | No |
| Zoom Link | 0.3 | 0.4 | 0.12 | Low-middle | Medium | Yes |

The risk evaluation process for the LMS involved assessing each threat scenario listed above using a weighted factor model with likelihood and impact values normalised between 0.1 and 1.0 with the risk score being evaluated as risk = likelihood x impact. The risk scores were plottd against the risk evaluation matrix which identified acceptable and unacceptable risk levels. Because of the core security goals of confidentiality, integrity, availability and privacy, we must identify any threats rated as high or extreme are unacceptable.

1. SQL injection poses the highest risk to academic and data integrity.
2. DoS on authentication server discrupts availability during critical times.
3. Insider access to student data violates privacy and legal obligations.
4. Phishing for credential theft compromises user accounts.
5. Zoom disruption considered acceptable due to lower risk.
6. **Treatment Diagrams**
   1. **SQL Injection- Local Database**

Treatment includes adding in input sanitisation to block any injection attempts by the external attacker.

A diagram of a computer system

AI-generated content may be incorrect.

* 1. **Denial of Service (DoS)- Authentication Server**

Adding a rate limit will stop any network flooding.

A diagram of a diagram

AI-generated content may be incorrect.

* 1. **Insider Misuse- Administrative Backend**

Role based access control helps restrict specific priveleges. Audit logging allows for tracking of any malicious behaviour.

A diagram of a flowchart

AI-generated content may be incorrect.

* 1. **Phishing Attack- Authentication Server + Student Portal**

User security awareness training will prevent users clicking on dodgy emails. Multi factor authentication will prevent unauthorised access with stolen credentials.

A diagram of a system

AI-generated content may be incorrect.

* 1. **Unauthorised Access to Online Exam- Video Conferencing Tool**

Because the threat related to video conferencing tool was deemed acceptable we don’t need to create a treatment diagram.

1. **Summary**

This risk assessment report has applied the CORAS methodology to evaluate the security of the Learning Management System (LMS) for the University. By analysing critical assets, threat scenarios and risk levels, we were able to identify key vulnerabilities which are impacting the core cyber security principles such as: confidentiality, integrity, avaialbility and privacy. Being able to target the specific threats for a scenario, we were able to target treatments to be developed for each risk, this included: SQL injection, DoS attack, insider misuse and phishing. Each treatment aligns with the organisational security policies, such as: enforcing RBAC, implementing MFA and securing application code.

Prioritising assets using the risk estimation process ensures that the resources of the univeristy are directed towards the areas of highest impact risk. By identifying unacceptable risk thresholds and applying appropriate controls, we can ensure resilience against both the external and internal threats. This safeguards academic data and service reliability but it also ensures alignment with the legal and compliance obligations surrounding student information and exam integrity. The CORAS strategy strengthens the LMS’s overall security framework and supports the univeristy in delivering a secure and reliable digital educational service and platform.