

Security Considerations

After completing the LMS Security Awareness Web-based Training integration, security testing will guarantee that the data has not been damaged. Cybercrime is a lucrative business opportunity for successful enterprises. As online learning grows in popularity, so does its attractiveness to hackers and cybercriminals; this should come as no surprise, given that learning management systems contain a wealth of sensitive student information and sensitive instructional data, both of which can be exploited by cybercriminals. (Idaho State University, 2007)

In the learning management system (LMS), a security breach may harm the reputation of the institution and the level of trust that customers have in the system. The IT testing teams oversee ensuring that the system's information is protected against cyber threats, online criminals, and fraudsters, as well as from other sources. It may be necessary to automate the testing of the content management system to guarantee that it is secure. (Idaho State University, 2007)

F-SECURE must decide on the design of test cases for the e-learning website to avoid security risks before, during, and after implementation, such as those presented by hackers. (Idaho State University, 2007):

- ✓ Vulnerability scanning - A network vulnerability is a security flaw that an attacker may use to damage network assets, create a denial of service, or steal potentially sensitive data. Threat actors are always on the hunt for new vulnerabilities to exploit, as well as finding previously exploited vulnerabilities that may have gone unpatched for an extended period. In a cyberattack, a threat actor might be a single individual who breaks security policies, a group of people, an organization, or a complicit nation in the assault. It is vital to reduce a

threat actor's window of opportunity since cyberattacks result in financial losses and system downtime. (Dosal, 2020)

- ✓ Security scanning - To enhance cybersecurity business protection, it is essential to keep updated on its security technology, security upgrades, and the tactics, strategies, and procedures employed by different threat actors. (Infosec Resources, 2021)
- ✓ Phishing testing - Allow users to submit suspicious emails and generate in-depth reports to identify struggling users, show compliance, and identify and track down troublesome individuals. (Infosec Resources, 2021)
- ✓ Posture assessment - An organization's security posture refers to the overall state of the organization's cybersecurity preparedness. The first step is to compile a detailed inventory of every device, application, service, and cloud instance that has access to the company network or information. (Balbix, 2022)

Having an accurate asset inventory is essential for maintaining a solid security posture. In most security requirements, including the 1996 Health Insurance Portability and Accountability Act (HIPAA), the ability to manage and audit the company inventory is considered a minimum need. Having an accurate and up-to-date asset inventory guarantees that the organization can keep track of the types and ages of the hardware that it is currently using. The ability to discover technological gaps and refresh cycles becomes more manageable with the help of this data collection process. (Balbix, 2022)

- ✓ Audits - Security audits are thorough assessments of the organization's information system; this examination often compares the security of the organization's information system to a

checklist of industry best practices, externally defined standards, or government legislation. (AuditBoard, 2022)

- ✓ Risk assessment – Risk identification/assessment/mitigation is the process of detecting potential security hazards and determining the level of harm they represent to an organization. Information technology risk assessment aims to manage risks to avoid security incidents and compliance failures. Nonetheless, since no business has the resources necessary to identify and eradicate all cybersecurity threats, information technology professionals must utilize the security risk assessment to help them narrow their focus. (NetWrix, 2020)
- ✓ Ethical hacking is a legal effort to obtain unauthorized access to a computer system, application, or data allowed by the user. Performing an ethical hack entail reproducing malicious attackers' techniques and behaviors in a safe environment. This approach aids in the identification of security vulnerabilities, which may subsequently be addressed before a hostile attacker has the chance to make use of the vulnerability. (Synopsys, 2021)
- ✓ Countermeasures for password attacks (University of Houston Clear Lake, 2022):

Users/Passwords/Systems requirements:

- Multiple character kinds, including the capital, lowercase, numerals, and symbols, are included inside the document
- Have a minimum of eight characters in their length (longer is even better)
 - Do not include any portion of a username or email address
 - Do not include any terms that can be found in a dictionary

- If possible, user passwords should be updated regularly (such as every 30 days);
This is referred to as password aging
- The requirements of excessively complicated passwords or changing them too often might lead to security risks
- Users must be prohibited from writing down their passwords
- Keep a record of passwords history to avoid re-use
- Multifactor authentication should be implemented
- Examine computer systems to see whether there are an excessive number of unsuccessful login attempts
- Account lockout should be implemented to prevent accessing accounts after several incorrect passwords have been entered
- Keep an eye out for sniffer and password-stealing tools on the network or computer
- Local Security Policy or the Default Domain adjustments
- Password policies for all machines in an Active Directory domain

Information Security Risk Mitigation:

Protections and procedures for specifying the sequence of activities to be undertaken to attain a given objective are made possible by automated protections and processes. However, even firms with high-security measures are prone to mistakes made by their employees. In many cases, the "people" component of the equation is disregarded. Technology and procedures must be integrated with staff education to reduce social engineering mistakes and enhance awareness of

the possible consequences of negligence. Employees must understand the hazards they are exposed to and their role in protecting themselves from them. Staff members must be taught to recognize suspicious communications and new threats to keep their companies safe. (King, 2018)

It is vital to have a vulnerability management plan that searches for new vulnerabilities frequently to avoid cybersecurity assaults. Without a vulnerability testing and patch management system in place, historical security problems on the network may remain unpatched for an extended period, giving attackers more substantial possibilities to exploit holes and launch attacks against the network. (Infosec Resources, 2021)

The Vulnerability Assessment policy aims to establish controls and processes to identify vulnerabilities in the firm's technology infrastructure and information system components that attackers could exploit to cause business disruptions, steal, or leak sensitive data. Vulnerabilities in the firm's technology infrastructure and information system components are defined as those that an attacker could exploit to exploit weaknesses, steal, or leak sensitive data. (Infosec Resources, 2021)

One of the Patch Management policy objectives is to establish rules and processes that will provide adequate protection against risks that might threaten the data security of the information system. Because of the practical implementation, a familiar setup environment safe against known operating systems and application software vulnerabilities must be created. (Infosec Resources, 2021)

References

- AuditBoard. (2022, March 12). AuditBoard. Retrieved March 12, 2022, from <https://www.auditboard.com/blog/what-is-security-audit/>
- Balbix. (2022, February 18). What is Security Posture? Retrieved March 12, 2022, from <https://www.balbix.com/insights/what-is-cyber-security-posture/>
- Dosal, E. (2020, January 16). Understanding the Importance of Vulnerability Management. CompuQuip Cybersecurity. Retrieved November 12, 2021, from <https://www.compuquip.com/blog/importance-of-vulnerability-management>
- Idaho State University. (2007, May). LMS Final Report. Instructional Technology Resource Center Idaho State University. <https://www.isu.edu/media/libraries/itrc/itrc-annual-reports/documents/Moodle-Fall-Pilot-Report.pdf>
- Infosec Resources. (2021, June 12). Vulnerability and patch management. Retrieved November 11, 2021, from <https://resources.infosecinstitute.com/certification/vulnerability-and-patch-management/>
- Karasavvas, T. (2021, June 9). AT&T Cybersecurity. Retrieved from AT&T Business: <https://cybersecurity.att.com/blogs/security-essentials/vulnerability-management-explained>
- King, Z. M. (2018). Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment. Frontiers. Retrieved November 12, 2021, from <https://www.frontiersin.org/articles/10.3389/fpsyg.2018.00039/full>

NetWrix. (2020, May 8). The Purpose of IT Risk Assessment. Why Bother? Retrieved March 12, 2022, from <https://blog.netwrix.com/2020/05/08/purpose-it-risk-assessment/>

University of Houston Clear Lake. (2022). Password Attacks and Countermeasures | University of Houston-Clear Lake. Retrieved March 12, 2022, from <https://www.uhcl.edu/information-security/tips-best-practices/pwattacks>

Synopsys. (2021). What Is Ethical Hacking and How Does It Work? | Synopsys. Retrieved March 12, 2022, from <https://www.synopsys.com/glossary/what-is-ethical-hacking.html>