LAKE SUPERIOR STATE UNIVERSITY PROCEDURES MANUAL

Administrative Policy

Section: Information Technology | Section Number: 3.3.4

Subject: Internet-Facing On-Premise Servers Risk Management | Date of Present Issue: 10/18/2024

Date of Previous Issues: None

Policy Statement:

To protect Lake Superior State University (LSSU) from potential security threats posed by internet-facing on-premise servers, strict guidelines and procedures must be followed. This policy ensures that all on-premise servers exposed to the internet are secure, monitored, and managed according to best practices, thereby minimizing the risk of unauthorized access, data breaches, and other cyber threats.

Scope:

This policy applies to all LSSU departments, faculty, staff, and third-party vendors responsible for the deployment, management, or maintenance of on-premise servers that are accessible from the internet.

Definitions:

- **Internet-Facing Server:** Any server hosted on LSSU premises that is directly accessible from the public internet.
- **On-Premise Server:** A server physically located within LSSU’s facilities.

Procedures:

1. **Server Registration and Approval:**
   - All internet-facing on-premise servers must be registered with the IT department prior to deployment.
   - A risk assessment must be conducted by IT to evaluate the server's exposure to potential threats. Approval from IT is required before the server is connected to the internet.
2. **Security Configuration:**
   - Internet-facing servers must be configured following LSSU's security standards, including the implementation of firewalls, intrusion detection/prevention systems (IDPS), and regular patch management.
   - Servers must enforce secure authentication methods, such as multi-factor authentication (MFA), and ensure that only authorized users have access.
   - Data transmitted to and from the server must be encrypted using industry-standard protocols (e.g., TLS).
   - No configuration protocols may be accessible from the internet (SSH or administrative webpages). All configuration protocols must be only accessible using VPN connections.

3. **Vulnerability Management:**
    - IT will conduct regular vulnerability scans and penetration tests on internet-facing servers to identify and address potential security weaknesses.
    - Any identified vulnerabilities must be remediated within 24 hours, following IT's established patch management process. Servers with critical vulnerabilities that cannot be immediately patched must be isolated or taken offline immediately until the issues are resolved.
    - IT will maintain an inventory of all internet-facing servers and track the status of vulnerabilities and their remediation efforts.
4. **Monitoring and Incident Response:**
    - Continuous monitoring of internet-facing servers will be conducted using security information and event management (SIEM) tools to detect suspicious activity or potential security incidents.
    - In the event of a detected security incident, IT will initiate an incident response protocol, including isolating the affected server, conducting a forensic investigation, and reporting the incident to university leadership.
    - The affected server will remain offline until IT confirms that all security issues have been addressed and the server is safe to reconnect to the internet.
5. **Decommissioning and Data Sanitization:**
    - When decommissioning an internet-facing server, all data must be securely wiped, and any sensitive information must be removed.
    - The server's removal from the network must be documented, and IT must be notified to update the server inventory.
6. **Enforcement and Compliance:**
    - Non-compliance may result in the server being disconnected from the network until it meets the required security standards.

Responsibilities:

- **LSSU IT:** Responsible for implementing, enforcing, and reviewing this policy, including conducting risk assessments, vulnerability management, and incident response.
- **Departments and Individuals:** Responsible for ensuring that internet-facing servers under their control comply with this policy and promptly address any identified security risks.

Review Cycle:

This policy will be reviewed annually by the IT Department to ensure its effectiveness and alignment with evolving security threats and university requirements.