A Comprehensive Cybersecurity Strategy for the Art Gallery Project: Combining Essential Eight, NIST Cybersecurity Framework, and CIS Critical Security Controls

Introduction: To ensure robust cybersecurity for our art gallery project, we have integrated three widely recognized frameworks: the Essential Eight, the NIST Cybersecurity Framework, and the CIS Critical Security Controls. This document outlines our comprehensive approach, which incorporates elements from each framework to address the unique needs and challenges of our art gallery project.

Our Integrated Cybersecurity Strategies:

1. Asset Management and Inventory (CIS Control 1 & 2):

- Maintain an up-to-date inventory of hardware and software assets.
- Regularly review and update the inventory to track authorized and unauthorized assets.

2. Secure Configurations (CIS Control 5):

- Establish and maintain secure configurations for all systems, applications, and network devices.
- Implement the least functionality principle and disable unnecessary services and features.

3. Vulnerability Management (CIS Control 3):

- Implement a vulnerability management program to identify, assess, and remediate security vulnerabilities in a timely manner.
- Monitor for emerging threats and update security measures accordingly.

4. Controlled Use of Administrative Privileges (Essential Eight & CIS Control 4):

- Limit the number of users with administrative access and review user privileges regularly.
- Implement multi-factor authentication (MFA) for users with elevated privileges.

5. Secure Network Architecture (NIST Framework - Protect):

- Design and maintain a secure network architecture, including segmentation and appropriate access controls.
- Regularly review and update network configurations to enhance security and minimize risks.

6. Continuous Monitoring (NIST Framework - Detect & CIS Control 6):

- Implement continuous monitoring and logging solutions to detect and analyze potential security threats.
- Establish a process for reviewing logs and addressing identified security incidents.

7. Incident Response and Recovery (NIST Framework - Respond & Recover & CIS Control 19):

- Develop a comprehensive incident response plan to manage and mitigate potential security breaches.
- Train relevant personnel on their roles and responsibilities during a security incident and regularly review and update the plan.

8. Security Awareness and Training (CIS Control 17):

- Conduct regular security awareness and training programs for all employees to emphasize their role in maintaining a secure environment.
- Provide specific training on identifying and reporting potential security threats, such as phishing attempts and social engineering.

9. Data Protection and Backups (Essential Eight):

- Regularly back up critical data, systems, and configurations to ensure quick recovery in the event of a security incident.
- Test the backup process and store backups securely, either offsite or using a cloud-based storage solution.

10. Application and System Updates (Essential Eight):

- Keep software applications and operating systems up to date with the latest security patches.
- Establish a regular maintenance schedule and prioritize updates based on potential risks and impacts.

Conclusion: By integrating elements from the Essential Eight, NIST Cybersecurity Framework, and CIS Critical Security Controls, our art gallery project will benefit from a comprehensive and robust cybersecurity strategy. Continuous monitoring, assessment, and improvement of our cybersecurity measures will help maintain a resilient and secure environment, ensuring the success of our art gallery project.

Himanshu
217662806
Deakin university