Corporate IT Security strategy

Goals

Establish Security Assessment Program

- Identify and assess all existing security vulnerabilities.
- Perform penetration testing on critical systems and networks.
- Evaluate current security policies and procedures.

Inventory of Systems and Assets

- Create and maintain a detailed inventory of all systems, assets, and data.
- Identify the unknown systems to ensure a complete understanding of the technology landscape.

Define Security Policies

- Develop and document comprehensive security policies that cover data handling, access controls, and incident response.
- Establish secure remote access policies, including the use of MDMs, VPNs.
- Ensure policies align with industry best practices and compliance standards.

User Education and Awareness

- Implement ongoing security awareness training for all employees, focusing on phishing prevention and safe online practices.

Endpoint Protection

- Implement endpoint protection solutions for Windows, MacOS, and Linux devices.
- Establish a vulnerability management program.

Identity and Access Management (IAM)

- Establish Single Sign-On (SSO) to streamline user access.
- Strengthen Google Identity provider configurations.
- Enforce multi-factor authentication (MFA) for all user accounts.
- Establish automated audit and review of user access and permissions.

Incident Response Plan

- Develop a detailed incident response plan with clear roles and responsibilities.
- Conduct regular tabletop exercises to ensure readiness.
- Establish clear channels for reporting security incidents and communicate effectively with employees in case of a breach.

Monitoring and Logging

- Implement a robust monitoring and logging system to detect and respond to security incidents.
- Set up an alerting system for reporting suspicious activities.

Vendor Security Assessment

- Assess the security posture of all third-party vendors, especially those providing critical services.
- Implement continuous monitoring policies.

Required resources

Security Infrastructure: Invest in tools and services to securely operate the existing environment and establish a baseline security. Various Open source (OSS) and enterprise offerings can be utilized.

IT Security Team: Establish a dedicated IT security team to run and manage the program.

Employee Training Programs: Allocate resources for regular cybersecurity training sessions to educate employees on the latest threats and best practices.

Incident Response Team: Establish a dedicated incident response team equipped with the necessary tools and resources to address security incidents promptly.

Priorities

1. **Inventory and Asset:** Create an inventory of all systems, assets, and data. This does not have to be perfect but is critical to the next step.
2. **Risk Assessment:** Conduct a thorough risk assessment to identify vulnerabilities and prioritize mitigation efforts based on potential impact and likelihood.
3. **Incident Response:** Develop and regularly test incident response plans to ensure a swift and effective response to security incidents.
4. **Employee Training Programs:** Allocate resources for regular cybersecurity training sessions to educate employees on the latest threats and best practices.
5. **Policies and Procedures:** Develop and document comprehensive security policies that cover data handling, access controls, and incident response.

Implementation plan

Phase 1 (0-3 months):

- Implement a basic inventory/asset management system.
- Conduct a comprehensive security assessment.

Phase 2 (3-6 months):

- Establish a dedicated incident response team and conduct tabletop exercises to test incident response plans.

- Conduct phishing simulation exercises.

Phase 3 (6-12 months):

- Invest in endpoint protection and detection solutions.

Phase 4 Continuous:

- Implement continuous monitoring and threat intelligence integration.
- Regularly update and enhance security policies and procedures based on emerging threats.
- Conduct periodic security drills and simulations.
- Establish a comprehensive vulnerability management program.

Monitoring and Evaluation:

1. **Key Performance Indicators (KPIs):**
    - Number of successful phishing simulations.
    - Time to detect and respond to security incidents.
    - Percentage reduction in vulnerabilities identified during audits.
    - Mean Time to Detect (MTTD)
2. **Regular Reviews:**
    - Conduct quarterly security reviews to assess the effectiveness of implemented measures.
    - Adjust the strategy based on emerging threats and changing business requirements.