4GEEKS ISMS

ISMS Scope

Purpose: The purpose of this Information Security Management System (ISMS) is to protect the sensitive information and critical assets of 4Geeks. This includes safeguarding data, maintaining system integrity, ensuring confidentiality, protecting against unauthorized access or breaches.

Scope: This ISMS applies to all operations conducted by 4Geeks worldwide, including but not limited to:

- Headquarters in Florida
- Remote offices and partnerships in Spain, Germany, LATAM

Assets: The following information assets are within the scope of this ISMS:

- **Hardware:**
  - Servers, workstations, routers, switches, and security devices.
- **Software:**
  - Linux Debian 12 (Bookworm), Wordpress, Apache, MySQL, Node.js, PHP, etc.
- **Data:** Students' personal information, financial records, research data, program reports, donor information.
  - Financial records, personnel files, research data, program reports, donor information.
- **Physical Locations:**
  - 4Geeks headquarters facilities, remote offices

Compliance Requirements: This ISMS is designed to comply with applicable legal requirements, including:

- General Data Protection Regulation (GDPR)
- Health Insurance Portability and Accountability Act (HIPAA) for healthcare data
- International Data Privacy Principles (IDPP)

Exclusions: The following areas are excluded from this ISMS scope:

- Third-party vendors unless they provide services that directly affect 4Geeks' information assets.
- Financial transactions handled by external financial institutions.

Responsibilities: Key stakeholders have defined responsibilities for implementing and maintaining the ISMS. These include:

- 4Geeks Headquarters: Madrid, Berlin, Miami, LATAM, Oversees global implementation, updates policies as needed.
- Regional Directors: Manage local compliance with 4Geeks' information security standards.
- Office Managers: Ensure adherence to regional and corporate guidelines.

Risk Assessment Results

Identified Assets

- The organization owns one Server and several workstations, routers, switches, and other hardware devices.
    - Applications include various software systems such as HRIS (Human Resources Information System), CRM (Customer Relationship Management), and ERP (Enterprise Resource Planning) systems.

Incident Report: WordPress Website Attack

Date: October 8, 2024

Time: 07:35 AM

Victim: 4Geeks Server

- **Server Configuration**
    - **Operating System:**
        - Debian Bookworm (Debian 12)
    - **Services:**
        - Web server (Apache/NGINX)
        - Database server (MySQL/MariaDB)
        - File storage server (Samba/SFTP)
        - Application servers (Node.js, PHP)

Attacker IP: 192.168.0.134

Description: A malicious actor exploited a WordPress vulnerability to gain unauthorized access to the 4Geeks server. The attacker targeted the WordPress installation and exfiltrated sensitive files, including `wp-config.php`, which contained database credentials.

Attack Details:

1. **System Enumeration:**
    - The attacker identified the WordPress version through directory traversal or file content analysis using nmap and wpscan.
2. **Sensitive Information Gathering:**
    - The attacker extracted `wp-config.php`, which contains database credentials, indicating an attempt to gain access to the backend and manipulate data.
3. **Data Exfiltration:**
    - Sensitive files were exfiltrated from `/var/www/html` directory, including WordPress core files, plugins, themes, and media assets.

Impact:

- Sensitive data exposure: The attacker gained access to database credentials, which could have led to unauthorized access and manipulation of sensitive data.

- Data loss: The attacker exfiltrated media assets, which could have been used for further attacks or to compromise reputation.

Mitigation:

- Patch the WordPress installation to the latest version.
- Implement strong password policies and multi-factor authentication for user accounts.
- Keep all system and application logs for monitoring and alerting.
- Regularly review and update the security policies and procedures.

Recommendations:

- Implement a firewall to protect the server from external attacks.
- Limit access to the WordPress installation to only necessary IP addresses and ports.
- Regularly backup the database and test the restoration process.
- Encrypt sensitive data at rest and in transit.
- Conduct security awareness training for all employees to recognize and report suspicious activities.

Timeline:

- **08/Oct/2024:16:49:46**: Attacker identified and modified WordPress directories.
- **08/Oct/2024:08:01**: Attacker identified and modified WordPress directories.
- **08/Oct/2024:08:01**: Attacker extracted `wp-config.php`.
- **08/Oct/2024:09:27 - 09:56**: Attacker exfiltrated files and directories.

Security Policies and Procedures

Security Policy

1. **Purpose:**
   - This policy outlines the commitment of 4Geeks to information security practices, ensuring the protection of sensitive data and systems against unauthorized access or disruption.
2. **Scope:**
   - Applies to all operations conducted by 4Geeks worldwide, including personnel and partners.
3. **Policy Statement:**
   - 4Geeks is committed to maintaining the confidentiality, integrity, and availability of all physical and electronic information assets.
4. **Responsibilities:**
   - All employees, contractors, and third-party users are responsible for adhering to this policy and reporting any security incidents.

Server Access Control

1. **Password Policies:**
   - Implement strict password policies with complex passwords rotating every 90 days for server administrators.
   - Passwords must be at least 12 characters long and include a mix of uppercase, lowercase, numbers, and special characters.
2. **SSH Access:**
   - Limit SSH access to specific IP addresses and use key-based authentication.

- Disable root login and use sudo for administrative tasks.

3. **Account Management:**
   - Regularly review and update user accounts, removing access for former employees and contractors.
   - Implement multi-factor authentication (MFA) for all administrative access.

Firewall Configuration

1. **Purpose:**
   - To secure internal systems by controlling traffic between different network segments.
2. **Configuration:**
   - Allow HTTP/S, SSH, DNS, ICMP (for ping) within the DMZ.
   - Allow only necessary services between the internal and external server groups.
   - Implement stateful inspection and intrusion detection/prevention systems (IDS/IPS).
3. **Monitoring and Maintenance:**
   - Regularly review firewall rules and logs to ensure compliance with security policies.
   - Update firewall firmware and software to protect against vulnerabilities.

Incident Response Plan

Objective

To ensure the security of the 4Geeks server and recover from any potential attacks or breaches.

Scope

The recovery plan covers the following aspects:

1. Network Segmentation
2. Firewall Implementation
3. DMZ Implementation

Procedure

1. **Network Segmentation:**

   - Deploy a separate server for the web server and database management system.
   - Use a firewall to control traffic between the web server and database server.

2. **Firewall Implementation:**

   - Configure firewalls to allow only necessary traffic (e.g., HTTP/S, SSH) between the web server and database server.

3. **DMZ Implementation:**

   - Implement a DMZ to isolate the web server from internal networks.
   - Configure firewalls to allow only HTTP/S traffic between the web server (in the DMZ) and client machines.

Testing and Validation

- Conduct regular security audits to verify the effectiveness of the implemented controls.
- Test the recovery plan by simulating attacks and verifying the response.
- Update and patch the server and applications regularly.

Communication and Reporting

- Establish communication channels with stakeholders to notify them of any security incidents or breaches.
- Maintain a secure communication channel for incident reporting and response.

Continuous Monitoring and Improvement

- Implement continuous monitoring and logging mechanisms to detect and respond to security incidents promptly.
- Regularly review and update the recovery plan based on the latest security threats and best practices.

Risk Assessment and Mitigation

- Conduct a comprehensive risk assessment to identify and prioritize risks.
- Develop and implement mitigation strategies to address the identified risks.

Incident Response Plan

- Establish an incident response plan that outlines the procedures to be followed in case of a security incident.
- Include procedures for data backup, system restoration, and communication with external parties.

By following this recovery plan, 4Geeks can significantly improve its security posture and better protect against potential attacks. The plan can be adapted and expanded based on the specific needs and requirements of the organization.

Remember to regularly test and validate the implemented controls to ensure their effectiveness. Additionally, it is crucial to keep the server and applications up to date with the latest security patches and updates.

Proposed Typology Solutions

Typology Solution #1: Divide External Access from Internal Use

Implementation Plan:

1. **Network Segmentation:**
    - Deploy two separate servers for external and internal use.
    - Use a firewall to control traffic between the segments.
2. **Firewall Implementation:**
    - Configure firewalls to allow only necessary traffic (e.g., HTTP/S, SSH) between the segments.

Typology Solution #2: Divide Access with DMZ

Implementation Plan:

1. **Network Segmentation:**

    - Deploy two servers for external access and internal use.
    - Implement a DMZ to isolate web services from internal networks.
2. **DMZ Implementation:**
    - Configure firewalls to allow only HTTP/S traffic between the web server (in the DMZ) and client machines.
    - Internal file storage and database management systems operate on separate servers within the internal network.

Data Backup and Recovery

- Implement automated backup solutions daily for critical data.
    - Use cloud-based backup services to ensure data is stored offsite.
    - Encrypt backups to protect data integrity and confidentiality.
    - Maintain multiple backup copies, including at least one offline copy to protect against ransomware.
- Test the disaster recovery procedures regularly.
    - Conduct quarterly recovery drills to ensure all team members are familiar with the process.
    - Verify the integrity of backups by performing regular restore tests.
    - Document any issues encountered during tests and update procedures accordingly.

Employee Awareness Training

- Conduct annual security awareness training sessions.
    - Cover topics such as phishing, password management, and data protection.
    - Include interactive elements like quizzes and simulated phishing exercises to reinforce learning.
- Encourage employees to report suspicious activities or potential breaches.
    - Provide clear guidelines on how to report incidents and ensure anonymity if desired.
    - Foster a culture of security awareness by recognizing and rewarding proactive behavior.
    - Regularly update training materials to reflect the latest threats and best practices.

ISMS Manual for 4Geeks

Introduction

The purpose of this Information Security Management System (ISMS) is to establish formalized security policies, standards, and controls designed to protect the sensitive information and critical assets owned or controlled by 4Geeks. The manual outlines procedures for the implementation of these policies.

In today's digital age, where cyber threats are constantly evolving, it is crucial for 4Geeks to stay ahead of potential security challenges. The ISMS provides a structured approach to managing and securing information assets, ensuring that the organization can effectively identify, assess, and mitigate information security risks. This system not only helps to prevent data breaches and cyberattacks but also ensures compliance with international regulations and standards, such as ISO/IEC 27001:2013, which is globally recognized for setting the criteria for an effective information security management system.

The ISMS Manual emphasizes the importance of a systematic approach to protecting sensitive data and ensuring that all stakeholders across 4Geeks’ diverse operational and geographical locations are equipped with the necessary knowledge and resources to contribute to the protection of information. It defines specific roles and responsibilities for personnel involved in the management and protection of information, ensuring clear accountability and engagement from all team members in safeguarding information assets. This document is not just a set of technical procedures; it also integrates security practices into the organizational culture, helping to foster a security-conscious mindset among employees at all levels.

Applicable Laws and Regulations

To ensure comprehensive compliance, 4Geeks adheres to various international, European, and American laws and regulations, including but not limited to:

International Standards

- **ISO/IEC 27001:2013**: Information Security Management Systems (ISMS) standard.
- **ISO/IEC 27002:2013**: Code of practice for information security controls.

European Regulations

- **General Data Protection Regulation (GDPR)**: Regulation (EU) 2016/679 on data protection and privacy in the European Union.
- **NIS Directive**: Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.
- **ePrivacy Directive**: Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.

Spanish Laws

- **Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD)**: Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights.
- **Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE)**: Law 34/2002 on Information Society Services and Electronic Commerce.

American Regulations

- **Health Insurance Portability and Accountability Act (HIPAA)**: U.S. law designed to provide privacy standards to protect patients' medical records and other health information.
- **Federal Information Security Management Act (FISMA)**: U.S. law aimed at improving the security of federal information systems.
- **California Consumer Privacy Act (CCPA)**: State statute intended to enhance privacy rights and consumer protection for residents of California, USA.

Risk Assessment Methodology

- Risk assessment involves identifying potential threats, vulnerabilities, and their likelihood and impact.
- Risks are prioritized based on a weighted scoring system (likelihood x impact).
- Regular reviews and updates to the risk assessment process ensure it remains effective and up-to-date with evolving threats and organizational changes.
- The risk assessment process includes identifying assets, evaluating threats and vulnerabilities, assessing risks, and determining appropriate risk treatment strategies.
- Risk treatment options include risk avoidance, risk mitigation, risk sharing, and risk acceptance, depending on the organization's risk appetite and the potential impact on its operations.

- Detailed documentation of identified risks, assessment results, and treatment plans is maintained to ensure transparency and accountability.

Monitoring and Measurement

Regular internal audits and external security assessments will be conducted to ensure compliance with this ISMS. Key performance indicators include:

- **Employee awareness rates**
  - Measured through regular training sessions and awareness programs.
  - Surveys and quizzes to assess employee understanding of security policies and procedures.
- **Incident response times**
  - Time taken to detect, report, and respond to security incidents.
  - Effectiveness of incident response plans and procedures.
- **Data breach prevention metrics**
  - Number of attempted and successful data breaches.
  - Effectiveness of implemented security controls in preventing breaches.
- **Compliance with security policies and procedures**
  - Regular audits to ensure adherence to established security policies and procedures.
  - Identification and rectification of non-compliance issues.
- **Effectiveness of security controls and measures**
  - Regular testing and evaluation of security controls.
  - Continuous improvement based on audit findings and security assessments.
- **Frequency and severity of security incidents**
  - Tracking and analysis of security incidents to identify trends and areas for improvement.
  - Implementation of corrective actions to prevent recurrence.
- **Time taken to detect and respond to security incidents**
  - Monitoring and improving detection and response capabilities.
  - Use of security information and event management (SIEM) systems for real-time monitoring.
- **Number of security training sessions conducted and employee participation rates**
  - Regular training sessions to keep employees informed about the latest security threats and best practices.
  - Tracking participation rates to ensure comprehensive coverage.

By continuously monitoring and measuring these indicators, 4Geeks can ensure that its ISMS remains effective and aligned with its security objectives, enabling the organization to proactively address potential security challenges and maintain a strong security posture. Regular management reviews and continuous improvement initiatives will help 4Geeks adapt to new threats and changes in the regulatory landscape, ensuring the ongoing protection of its information assets.

Server Maintenance

Maintaining the 4Geeks server and its services is crucial for ensuring the security, stability, and performance of the organization's IT infrastructure. The following guidelines outline the maintenance procedures for the server's operating system and key services:

- **Debian Bookworm**

    - Regular Updates: Ensure the operating system is up-to-date with the latest security patches and updates.
    - System Monitoring: Use tools like `top`, `htop`, and `systemd` to monitor system performance and resource usage.
    - Log Management: Regularly review system logs located in `/var/log` to identify and address potential issues.
    - Backup: Implement regular backup procedures for critical system files and configurations.

- **Apache**

    - Configuration Management: Regularly review and update Apache configuration files located in `/etc/apache2`.
    - Security Updates: Ensure Apache is updated with the latest security patches.
    - Performance Tuning: Optimize Apache settings for performance, such as adjusting `MaxRequestWorkers` and `KeepAlive` settings.
    - Log Analysis: Monitor Apache logs located in `/var/log/apache2` for errors and unusual activity.

- **SSH**

    - Configuration Hardening: Secure SSH by updating the configuration file `/etc/ssh/sshd_config` to disable root login and use key-based authentication.
        - Set `PermitRootLogin no`
        - Set `PasswordAuthentication no`
    - Regular Updates: Ensure the SSH service is up-to-date.
    - Monitoring: Use tools like `fail2ban` to monitor and block suspicious login attempts.

- **MySQL**

    - Regular Backups: Implement regular backup procedures for databases using tools like `mysqldump`.
    - Security Updates: Ensure MySQL is updated with the latest security patches.
    - Performance Tuning: Optimize MySQL settings for performance, such as adjusting `innodb_buffer_pool_size` and `query_cache_size`.
    - User Management: Regularly review and update MySQL user permissions to ensure least privilege access.

- **WordPress**

    - Regular Updates: Ensure WordPress core, themes, and plugins are up-to-date.
        - Use the WordPress dashboard or WP-CLI for updates.
    - Security Plugins: Install and configure security plugins like Wordfence or Sucuri to enhance WordPress security.
    - Backup: Implement regular backup procedures for WordPress files and databases.

- **WP-Plugins**

    - Regular Updates: Ensure all WordPress plugins are regularly updated to the latest versions.
    - Security Review: Regularly review and remove any unused or vulnerable plugins.

    - Compatibility Check: Ensure plugins are compatible with the current version of WordPress and other installed plugins.

- **General Maintenance**

    - Automated Tasks: Use cron jobs to automate regular maintenance tasks such as updates, backups, and log rotation.
    - Security Audits: Conduct regular security audits to identify and address potential vulnerabilities.
    - Documentation: Maintain detailed documentation of all maintenance procedures, configurations, and changes.

By following these maintenance guidelines, 4Geeks can ensure the security, stability, and performance of its server and services, thereby supporting the organization's overall information security objectives.

Conclusion

This document outlines the Information Security Management System (ISMS) for 4Geeks, detailing policies, procedures, controls, and risk assessment findings. The implementation of these measures will enhance the protection of sensitive information and critical assets against unauthorized access or disruption. By adhering to international standards and regulations, 4Geeks demonstrates its commitment to maintaining high standards of information security and compliance.

In conclusion, the ISMS is a vital component of 4Geeks' overall strategy to protect its information assets. By implementing a robust and dynamic ISMS, 4Geeks can ensure the confidentiality, integrity, and availability of its information, thereby safeguarding its operations and reputation. The active involvement of all employees, along with regular reviews and continuous improvement, will ensure the long-term success and effectiveness of the ISMS.