Recovery 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.