Rick Abraham

My Company  Dallas, TX

Risk Assessment - Network Security Risks

Contents

[Introduction 2](#_Toc182497743)

[Purpose 2](#_Toc182497744)

[Scope 2](#_Toc182497745)

[Risk Identification 2](#_Toc182497746)

[Assets: 2](#_Toc182497747)

[Threats 2](#_Toc182497748)

[Vulnerability: 2](#_Toc182497749)

[Impact: 2](#_Toc182497750)

[Risk Rating: 2](#_Toc182497751)

[Risk Analysis 3](#_Toc182497752)

[Likelihood: 3](#_Toc182497753)

[Impact Severity: 3](#_Toc182497754)

[Overall Risk Level: 3](#_Toc182497755)

[Mitigation Recommendations 3](#_Toc182497756)

[Mitigation Strategy: 3](#_Toc182497757)

[Implementation Timeline: 3](#_Toc182497758)

[Monitoring and Review 3](#_Toc182497759)

[Frequency: 3](#_Toc182497760)

Risk Assessment - Network Security Risks

# Introduction

Purpose: To assess, identify, and manage network security risks that may impact the organization, with a focus on minimizing exposure to unauthorized access, data breaches, and loss of network integrity.

Scope: This assessment encompasses all network-related assets and configurations, including but not limited to firewalls, VPNs, routers, switches, intrusion detection/prevention systems (IDS/IPS), and any other network security devices. This policy applies to on-premises and cloud environments, as well as remote access configurations.

# Risk Identification

Assets: Firewalls, VPNs, routers, switches, IDS/IPS.

Threats:

* **Unauthorized Access:** Exploitation of network entry points through vulnerabilities, weak or outdated configurations, and lack of robust authentication.
* **Configuration Weaknesses:** Insecure firewall rules, misconfigured VPN settings, and outdated or unpatched firmware/software.
* **Insufficient Network Segmentation**: Inadequate separation between critical and non-critical network zones, increasing the likelihood of lateral movement by attackers.

Vulnerabilities:

* Weak firewall rules and a lack of deny-by-default configurations.
* Absence of multi-factor authentication (MFA) on VPN access.
* Inadequate or irregular patch management.
* Absence of IDS/IPS monitoring or insufficient logging and alerting.

Impact: Data breaches, compromise of network integrity, unauthorized data access, potential ransomware deployment, and potential for lateral movement within the network.

Risk Rating: **High**

# Risk Analysis

Likelihood: **High.** The organization faces a constant threat of unauthorized access attempts due to common attack vectors, especially on external network entry points.

Impact Severity: **High.** A breach of network security could result in significant financial loss, data compromise, regulatory fines, and damage to reputation.

Overall Risk Level: **Critical**

# Mitigation Recommendations

Mitigation Strategy:

* **Firewall Hardening**:
  + Implement a **deny-all, allow-specific policy** by default, allowing only essential and well-defined ports/protocols.
  + Apply strict rules for outbound traffic, as well as for inbound, to reduce the risk of data exfiltration.
  + Regularly review and update firewall rules to account for newly identified threats or changes in network requirements.
* **VPN Security Enhancements**:
  + Enforce **multi-factor authentication (MFA)** for all VPN users to prevent unauthorized access.
  + Employ **strong encryption protocols** and disable outdated or insecure protocols (e.g., PPTP).
  + Establish VPN access limitations based on user role and enforce stringent access controls for high-privilege users.
* **Regular Audits and Updates**:
  + Conduct **quarterly network audits** to assess configurations, firewall rules, and device firmware updates.
  + Implement **automated patch management** for network devices and ensure rapid response for critical updates.
  + Include firmware updates as part of regular maintenance for routers, switches, and other network devices.
* **Intrusion Detection and Logging**:
  + Deploy an **intrusion detection/prevention system (IDS/IPS)** to monitor for unusual or suspicious activity across the network.
  + Enable comprehensive logging for all network devices, including firewalls, VPNs, routers, and switches.
  + Set up **real-time alerts** for unauthorized access attempts or anomalous activities, with incident response protocols in place for critical alerts.
* **Network Segmentation**:
  + Implement **network segmentation** to isolate sensitive data and critical systems from less secure zones.
  + Apply **micro-segmentation** within sensitive areas for granular access control.
  + Utilize VLANs to minimize the spread of unauthorized access if one segment is compromised.
* **Threat Intelligence and Training**:
  + Regularly update the security team with **threat intelligence feeds** on emerging network security threats.
  + Conduct **bi-annual security training** for all users, emphasizing secure VPN practices and recognizing phishing or social engineering attempts that may impact network security.

Implementation Timeline:

* **Immediate:** Firewall rule update to deny-all policy, VPN MFA enforcement.
* **Within 30 days:** IDS/IPS deployment, logging adjustments, and VPN configuration updates.
* **Ongoing:** Monthly access log reviews, quarterly audits, and real-time alert monitoring.

# Monitoring and Review

Frequency:

* **Monthly**: Review VPN and firewall access logs to detect and respond to unauthorized access attempts. Ensure alert systems are fully operational and regularly tested.
* **Quarterly**: Conduct network security audits, including firewall rules, VPN configurations, device firmware checks, and IDS/IPS efficacy.
* **Bi-Annually**: Perform a comprehensive review of network security controls against industry standards and update policies accordingly.
* **Annually**: Reassess risk factors, threats, and vulnerabilities, incorporating any changes in technology, compliance requirements, or threat landscape.

Incident Response:

* Establish an incident response team (IRT) trained specifically for network incidents.
* Conduct **drills for network intrusion scenarios** every six months to evaluate the organization’s readiness and response.
* Maintain and periodically update an incident response playbook that addresses critical network security incidents.

Documentation and Compliance:

* Document all network configurations, firewall rules, VPN settings, and access control policies.
* Maintain records of quarterly audits, monthly log reviews, and incident response outcomes.
* Ensure compliance with applicable regulations and standards (e.g., NIST 800-53, ISO 27001) to align with best practices and legal requirements.