4.3.1 Vulnerability Management policy

Contents

Version	Adjustment Date	Approved By	Approval Date
2.0	4/7/2024	Saud Alsulami	7/7/2024

1. Definitions

For purposes of this “Vulnerability Management policy” the following definitions apply:

- **Risk assessment:** the process of identifying, analyzing, and evaluating potential risks and vulnerabilities in a system, organization, or process.
- **Vulnerabilities:** weaknesses or flaws in a system's design, implementation, or configuration that could be exploited by attackers to compromise the integrity, confidentiality, or availability of the system.
- **Remediation:** the process of addressing and resolving identified vulnerabilities or risks.
- **Likelihood:** the probability or chance that a specific risk will materialize.

2. Purpose

The policy serves multiple purposes, including reducing risks, ensuring compliance with regulations, protecting valuable assets, preventing incidents, optimizing resource allocation, fostering continuous improvement, enhancing incident response readiness, promoting security awareness, documenting processes and responsibilities, and providing assurance to third parties.

3. Scope

This policy applies to all information assets within the organization, encompassing systems, applications, networks, and databases.

4. Policy

4.1. Specialized tools must be used to discover and analyze vulnerabilities, for example, Nessus.

4.2. The tools used to identify vulnerabilities must be approved by the Cybersecurity officer and technical advisor.

4.3. Conduct vulnerability scans must be according to the following frequency:

4.3.1. Quarterly for the rest of the internal/ external servers, network, database applications, and systems.

4.3.2. When there is a need to repeat the vulnerability scan, for example, to ensure that there are no critical vulnerabilities from a previous scan.

4.3.3. After any significant change to the network (internal or external).

4.4. Analyzing the impact of vulnerabilities discovered on critical information assets must be done by the cybersecurity officer, technical advisor, and NOC team.

4.5. The cyber security officer is responsible for:
- 4.5.1. Assigning a criticality level (Critical - High - medium - low) to each vulnerability.
- 4.5.2. Define and assign timeframes for remediation based on criticality as follow:
  - Critical: 10 days
  - High: 15 days
  - medium: 30 days
  - Low: 60 days
- 4.5.3. Generating a comprehensive Vulnerabilities Report

4.6. The vulnerabilities reports must be included the following:
- 4.6.1. Executive Summary:
  - Brief overview of the report.
  - High-level summary of critical vulnerabilities.
  - Recommendations for mitigation.
- 4.6.2. Introduction:
  - Purpose of the vulnerability assessment.
  - Scope and limitations of the assessment.
- 4.6.3. Methodology:
  - Description of the tools and techniques used.
  - Explanation of the testing environment.
- 4.6.4. Detailed Findings:
  - Comprehensive list of identified vulnerabilities.
  - Each vulnerability should be categorized by severity (e.g., high, medium, low).
  - Include details such as vulnerability type, description, and affected assets.
- 4.6.5. Risk Assessment:
  - Impact analysis of each vulnerability on the system.
  - Likelihood of exploitation.
  - Risk rating for each vulnerability.
- 4.6.6. Recommendations:
  - Proposed remediation or mitigation measures for each vulnerability.
  - Prioritization of recommendations based on severity and impact.
- 4.6.7. Timeline:
  - Include the timeline of the vulnerability assessment.
  - Dates of testing, reporting, and any follow-up actions.

4.7. The report must be delivered to the technical advisor, relev
NOC.

4.8. Any reported vulnerability that is not resolved within its timeframe must be escalated to CEO.

5. Non-compliance

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

6. References

- ISO 27002
- National Cybersecurity Authority's (NCA) ECC standards
- SANS