NETWORK
EDGE

SECURITY AUDIT AND ASSESSMENT SERVICES

OVERVIEW

Network Edge Security Audit and Assessment Services provides customers with a High-Level overview of their overall ICT Information Security Framework. The output of the Audit and Assessment process is a report that provides detailed visibility into the security state of scoped ICT infrastructure and a detailed benchmark assessment of Confidentiality, Integrity and Availability (also known as the CIA triad).

The scope of Audit and Assessment Services include:

- NETWORK PENETRATION TESTING AND ASSESSMENT
- WEB APPLICATION PENETRATION TESTING AND ASSESSMENT
- WIRELESS NETWORK PENETRATION TESTING AND ASSESSMENT
- VOIP INFRASTRUCTURE PENETRATION TESTING AND ASSESSMENT
- NETWORK CONFIGURATION SECURITY AUDIT AND REVIEW
- SECURITY CONTROL AND FRAMEWORK AUDIT AND REVIEW
- REGULATORY COMPLIANCE AND STANDARD AUDIT

At the completion of every Pentest, Audit, or Assessment, a detailed report provides customers with an overview of existing Security Controls and Framework for the scoped environment. The report lists vulnerabilities and missing controls and provides recommendations to remediate security issues, mitigate vulnerabilities, and pass industry or regulatory security compliance requirements.

Network Edge Security Audit and Assessment Services enables businesses to validate and enhance the security posture of their overall ICT environment by mitigating risks associated with protecting critical data from possible threat or attack vectors, both externally and internal to the organisation.

Security Audit and Assessment Services focus on the discovery and identification of weaknesses and vulnerabilities, but do not extend to attempts at exploiting and testing any weaknesses or vulnerabilities that are discovered.

"We'll work with you to provide the best solution for your business"

SERVICES DESCRIPTION

Network Penetration Testing and Assessment

Network Edge use Centre for Internet Security (CIS) and National Institute of Standards and Technology (NIST) controls as the base security framework to assess the output from network scans. The assessment determines the network security attacks that potentially could occur within the scanned network. Network Pentest is divided into two different assessment phases.

- EXTERNAL – Assesses the network from a hacker's point of view to find out what exploits and vulnerabilities are accessible to the outside world
- INTERNAL – Scans the internal network infrastructure to discover exploits and vulnerabilities

Web Application Penetration Testing and Assessment

Network Edge leverages the Open Web Application Security Project (OWASP) security framework as a basis to assess web infrastructure for any misconfiguration and known vulnerabilities. An external scan is performed on customer provided and confirmed public IP addresses that host external facing services.

Wireless Network Penetration Testing and Assessment

Network Edge leverages current 802.x standards and Penetration Testing Execution Standard (PTES) as the foundation for our wireless assessment methodology. This simulates 'real world attacks' to determine the vulnerabilities within an organisation's wireless infrastructure.

VoIP Infrastructure Penetration Testing and Assessment

NENZ leverages the CIS and NIST industrial VoIP standard as the foundation for assessment of IP telephony infrastructure. This simulates real world attacks to determine the vulnerabilities within an organisations VOIP Security design and associated network.

SECURITY AUDIT AND ASSESSMENT SERVICES

Network Configuration Security Audit and Review

Network Edge uses NIST and CIS standards as a base to perform a configuration and access control audit on all customer workstations, servers, and network devices (routers, firewalls, switches, voice). Actions available as a result of the audit will strengthen an organisation against the possibility of an external exploit.

Security Control and Framework Audit and Review

Network Edge uses the CIS AAA Standard and NIS best practise to perform an audit of access management, authorisation processes, and accounting standards (AAA) for security compliance and password hardening. Actions available as a result of the audit are targeted at preventing dictionary or brute force attacks due to the use of weak passwords and non-secured controls.

Regulatory Compliance and Standards Audit

The Network Edge Security Audit and Assessment Service also includes industrial security compliance audits such as: PCI Compliance, HIPAA Compliance, ISO Compliance, NIST and CIS compliance, so that customers can meet their regulatory compliance requirements.

REPORTING

The output from all Network Edge Security Audit and Assessment Services is generation of a comprehensive report that describes all of the discovered Security Vulnerabilities with recommendations to remediate risks, enhance infrastructure security, meet Security Framework standards, and/or meet Industrial Regulatory Compliance requirements.

ESTIMATE OF EFFORT

The following table indicates how Network Edge determines if a Security Audit and Assessment customer is a Small Business, Medium Business, or Large Business.

	Small Business	Medium Business	Large Business
Number of Users	1 - 10	11 to 200	201 and more
Number of Devices	1 - 50	51 to 300	301 and more
Number Servers	1- 5	6 to 20	21 and more

The following table indicates the typical effort involved in completing the Security Audit and Assessment Services based on customer type.

	Small Business		Medium Business		Large Business	
	Security Reporting	Pentest Assess	Security Reporting	Pentest Assess	Security Reporting	Pentest Assess
Security Service	Hours	Hours	Hours	Hours	Hours	Hours
Network Penetration Testing	2	8	4	30	10	100+
Web Application Penetration Testing	2	4	4	20	6	40
Wireless Network Penetration Testing	2	4	4	30	6	60
VoIP Infrastructure Penetration Testing	2	4	4	40	7	100+
Network configuration Security Audit and Review	2	10	5	50	10	120+
Security Control and Framework Audit and Review	2	4	4	30	7	60
Regulatory Compliance and Standard Audit	3	6	6	20	12	35