Network Security Assessment

TPx is a leader in cybersecurity for small and medium businesses and public-sector organizations. Our depth of expertise enables us to offer standards-based security consulting services developed from our experiences in solving strategic and operational challenges for customers.

TPx consultants are subject matter experts in their field and thought leaders in security. All of our offerings are based on best practices derived from Information Security Standards (CISSP Domains, NIST, ISO 27000 series, etc.) and our extensive experience deploying, architecting, operating, and securing environments nationwide.

Traditional network management has evolved in recent years to the point where it cannot be approached without considering the associated security ramifications. Any attempt to treat security as an “add-on” to network design and operations in today’s hyperconnected world is destined to create more problems than it solves.

To avoid this, TPx incorporates security considerations throughout its network assessment service, yielding a comprehensive Network Security Assessment that results in actionable recommendations for a robust, high-performing, and secure networking environment.

Assessment Benefits

- Fully document your network assets & architecture
- Understand your traffic flows and uncover asset misconfigurations
- Validate policies for data retention, network monitoring, and configuration and change management
- Identify gaps in your monitoring and reporting capabilities
- Target high-impact areas for reducing risk

Overview

TPx's Network Security Assessment methodology is founded on industry standards such as ISO 27001, ISO 27033, CIS "Top Twenty" and current best practices. It is designed to evaluate the security posture and functional capabilities of your organization's environment, and its ability to transmit and safeguard your organization's critical data. The assessment will be divided into three phases, covering the following:

- **Documentation & Visualization** of the existing network environment. TPx will inventory and catalog your existing network assets and architecture.
- **Security Strategy** TPx will assess the network policies, standards and procedures as well as all the security management processes, and roles and responsibilities related to the network.
- **Operational Function & Hygiene** TPx will assess the technical measures implemented in your network infrastructure.

Network Assessment Activities

The approach for the network security assessment is to evaluate your organization's network security posture and profile. Posture refers to your organization's current ability to transfer, maintain and protect data within the corporate network. Profile refers to the minimum target of capability required to protect information and manage associated risks, which an organization should aim to achieve.

Your information security posture will be assessed based on a set of categorizations (e.g., access controls and network protections). The categorizations covered for the assessment focus on areas of cybersecurity that have the highest likelihood of incidents and breaches for your organization.

The objective of this effort is to assess your infrastructure's adherence to industry standards of ISO 27033. TPx will review the organization through interviews, policy review, validation and investigation of process to provide a numerical rating that reflects that maturity/resiliency of your security infrastructure. The assessment will focus on the following areas:

Phase 1: Documentation & Visualization

Physical Inventory

- Hardware Inventory Spreadsheet
- Layer 1-2 Diagrams/Documentation (will create during the engagement if doesn't exist)
- Layer 3 Diagrams/Documentation (review for accuracy)
- Rack Elevation Diagrams/Documentation (review for accuracy)
- Environmental Capabilities (review for accuracy)

Design & Architecture Review

- Network Overview Architecture
- Traffic Flow
- Services and OLA's
- MPLS/VPN Service
- QOS Standards
- Layer 3 Routing
- Layer 2 Optimization

Phase 2: Documentation & Visualization

Network Infrastructure Security

- Misconfiguration or Design flaws
- Weak authentication or encryption protocols
- Centralized Authentication, Authorization, and Accounting
- Attack Awareness (IPS/IDS)
- Control Plane Policing/Security
- Rogue DHCP/Client Detection
- Infrastructure Physical Security

Performance Monitoring & Analysis

- Netflow Capabilities
- Client Experience Capabilities
- Packet Capture Capabilities

Phase 3: Operational Function & Hygiene

Infrastructure Monitoring & Management

- Central Monitoring/Alerting Capabilities
- Syslog Capabilities
- Host End Monitoring/Management
- Software Management (networking)
- Configuration validation capabilities
- EoL/EoS hardware and licensing

Configuration Management

- Centralized Configuration Backup
- Centralized Configuration Automation
- Configuration Change Management Workflow

Reporting

Upon completion of the assessment, TPx will provide two reports: an Executive Summary and a detailed Best Practices report. The reports will speak to two different levels of resources: the leadership and the security practitioner. A detailed recommendations report will be provided and validated with your personnel. The objective of this report is to present the results and observations related to your network security posture. In addition, you will receive recommendations for your top three priorities based on your business, your sensitive data, your exposure landscape, and the network state.

TPx will also provide an updated network diagram, wireless saturation for the primary location, and recommendations on how to best create or update your security documentation.

43% Small businesses are the target of 43% of all cyberattacks

Verizon 2020 Data Breach Report