

Security Vulnerability Assessment for SMB, U.S. and Canada

HP Care Pack Services

Reporting Data

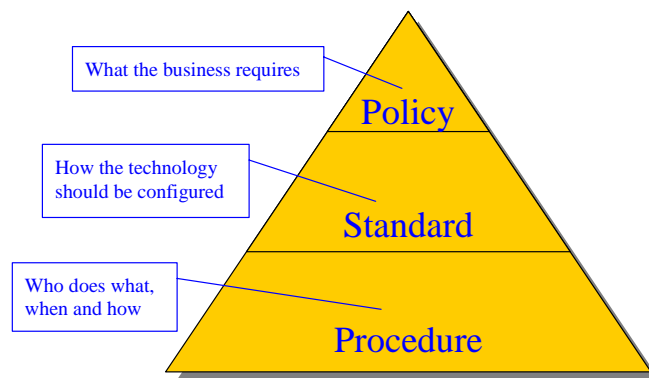
Small and medium businesses (SMBs) face the same security vulnerabilities as larger enterprise customers in business today. However, SMBs frequently do not have the same resources to prevent hackers and protect intellectual property. HP Security Vulnerability Assessment for SMB can help by providing accurate, actionable information to start building an effective security plan, with results, reports and analysis designed specifically for SMBs. Security Vulnerability Assessment for SMB service adheres to ISO 17799 International Standards, and utilizes industry recognized “Best Practices”, applicable Government Regulations and HP’s extensive experience in the security industry.

Assessment Service Reporting Objectives

Security Infrastructure and Policy Review. Analyzes the Customer’s security policy, standards and procedures for “best practices”, completeness (including accessibility and audit procedures) and includes a summary of findings in the Discovery and Recommendations Report

Wireless Security Review. If applicable, analyzes the Customer’s wireless security design and policies, and produces a summary of findings in the Discovery and Recommendations Report.

Penetration Testing of Perimeter Systems. Tests devices that protect the Customer’s network from the Internet, including firewalls, intrusion detection devices, routers and traffic analyzers and produces a Results Report on a per IP address basis.



Policy, Standards and Procedure Hierarchy

Consulting. Provides a review of the Results Report within the Discovery and Recommendations Report, including documentation of areas requiring specific attention resulting from the assessment. The HP Security Consultant will also address any additional security concerns the Customer may have about their overall IT infrastructure.

The Assessment Process

Pre-Assessment Work. An interview between an HP Security Consultant and the Customer, with the Customer providing Security Infrastructure and Policy documents, Wireless Design diagrams, and IP addresses to be tested, with identification of any specific concerns that the customer may have about their network.

The Test. HP conducts a vulnerability scan of the Customer's perimeter devices, and "fingerprints" each device for a variety of security characteristics.

The Results. A results report is generated by IP address with relevant "fingerprint" information about that address.

Sample Test Results Report

1.2.3.1	Undeterminable. No Ping response. No accessible ports. Likely a Firewall.
1.2.3.2	Undeterminable. No Ping response. No accessible ports. Likely a Firewall.
1.2.3.3	Undeterminable. No Ping response. No accessible ports. Likely a Firewall.
1.2.3.4	Undeterminable. No Ping response. No accessible ports. Likely a Firewall.
1.2.3.5	Undeterminable. No Ping response. No accessible ports. Likely a Firewall.
1.2.3.6	Microsoft Windows Millennium Edition (Me), Windows 2000 Professional or Advanced Server, or Windows XP – ISA Firewall
1.2.3.7	Microsoft Windows Millennium Edition (Me), Windows 2000 Professional or Advanced Server, or Windows XP – ISA Firewall
1.2.3.8	Microsoft Windows Millennium Edition (Me), Windows 2000 Professional or Advanced Server, or Windows XP – ISA Firewall
1.2.3.9	Microsoft Windows Millennium Edition (Me), Windows 2000 Professional or Advanced Server, or Windows XP – ISA Firewall
1.2.3.10	Cisco Router. V 61. running ACLS being used as a firewall device.
1.2.3.11	Cisco Router. V 61. running ACLS being used as a firewall device.
1.2.3.12	Cisco Router. V 61. running ACLS being used as a firewall device.
1.2.3.13	Microsoft Windows Millennium Edition (Me), Windows 2000 Professional or Advanced Server, or Windows XP- Web Server
1.2.3.14	Microsoft Windows Millennium Edition (Me), Windows 2000 Professional or Advanced Server, or Windows XP- Web Server
1.2.3.15	Microsoft Windows Millennium Edition (Me), Windows 2000 Professional or Advanced Server, or Windows XP- Web Server

Analysis. The HP Security Consultant uses the results data to check for vulnerabilities specific to that particular device and "fingerprint" profile, as well as other generic vulnerabilities and areas of potential risk. The HP Security Consultant will identify the most critical issues and specific concerns and map this information into a Discovery and Recommendations Report, sorted by level of urgency. Each recommendation will be defined, and a High, Medium and Low estimate of benefit and cost will be provided.

Sample Discovery and Recommendations Report

Description	Urgency	Benefit	Cost
Remove all system welcome banners that identify the system type	High	High	Low
Use HTTPS VS HTTP for added security	High	High	Low
Disable echo reply requests on all perimeter nodes	High	High	Low
Remove all telnet or ftp ports from perimeter nodes	High	High	Low

For More Information

For more information on Security Vulnerability Assessment for SMB service and reporting data, contact either an HP sales office in the US (or Canada), or an HP authorized reseller or visit our Web site at:

www.hp.com/go/securityassessment