IT VULNERABILITY ASSESSMENT

PROPOSAL FOR COMPANIES OF EVERY BRANCH OF INDUSTRY
Your Situation

Without-patch management your business is exposed to numerous risks. The lack of updates is the most common cause of network vulnerabilities. With our network scanner (Vulnerability Scanner) you can identify and fix open vulnerabilities in time, not giving the hackers a chance to attack. We provide both security and function-enhancing patches for Microsoft®, Mac OS X®, Linux® operating systems, and to more than 50 applications from different developers.

Our Proposal

Networks, including virtual environments are reviewed with over 50,000 vulnerability checks and assessments. Operating systems and applications go through security checks, based on the SANS top 20 (SysAdmin, Audit, Network Security), OVAL (Open Vulnerability and Assessment Language) amongst others. We will help you to determine the current security status of your network, identify risks and the level of danger through open vulnerabilities and closing security flaws as soon as possible. We evaluate in detail which applications represent a threat to the security of your network. Moreover, we deliver a comprehensive overview of installed software, hardware and mobile devices in your IT environment. You will also receive information about the status of security programs (antivirus, anti-spam, firewalls), open ports, running services and shared media.

Your Benefits

• Information regarding vulnerabilities and risks of your IT infrastructure.
• Existing hardware assessment and identification.
• Reducing your IT Risks.
• Increasing resilience of your IT infrastructure.
• IT Governance and Compliance to create an automatic inventory of all connected IP devices.
• Plans for patching available systems to the latest fixes and updates.

Process

In an initial consultation we define the scope and the precise sequence of vulnerability scans.

• Scanning agreement (IP address ranges, reference to risks and liability)
• Information on IT support, IT admins, external suppliers, etc.
• Special requirements such as Network monitoring tools like What’s Up Gold, etc.
• Update Vulnerability database on the scanning engine (Notebook)
• Definition proxy for Vul-scan Notebook (if necessary)
• Creating a Black List (esp. Servers, which should not be scanned)
• Scanning method settings (full, with / without applications, USB ports, etc.)
• Targeted networks configuration (IP range, LAN segments)
Process (cont.)

• Date and time of the scan configuration
• Generate of a Vulnerabilities Report (PDF)
• Analysis of Vulnerability Report
• Optional scans:
  • SNMP Scan
  • SQL Server Scan
  • WiFi (WLAN scan)

What we offer

The following products are contained in this service package:

• Identification of active components (hardware and software inventory)
• Detailed investigation and analysis of the existing local area network security risks, vulnerabilities in operating systems and applications like Adobe Reader, Java, etc.
• Optional: Managed IT vulnerabilities minimization recommendations
• Optional: Performing an IT risk analysis

Additional Services

• Information Security Management System (ISMS)
• Information security and data protection audits
• Security for family offices.
• IT Risk Management
• Raising awareness for employees
• IT-Forensics and investigations
• Internet Reputation Management
• Business Continuity Management & Disaster Recovery Programs (BCM)
• Governance, Risk management, and Compliance (GRC)
• Industrial safety equipment (SCADA)