Microsoft® Security Health Check 4.5

Proactive security evaluation of security processes and operating system configuration.

Based on Trustworthy Computing, Microsoft best practices security guidance, and direct customer experience.

Key Benefits

- Clear results identifying top findings including risk, vulnerability, and host configuration issues
- Results include remediation procedures for all discoveries with documented potential impacts based on Microsoft guidance
- Operating system evaluation ranging from Windows XP to Windows 2008 R2 / Windows 7
- Defense in Depth approach

Microsoft | Services

Overview

Security Health Check (SECHC) is a proactive security engagement. The main goal of the SECHC is to help customers avoid security compromises on hosts, and in network environments using supported Microsoft operating systems and services.

No changes or impact on the customer environment are made during the engagement. The Security Health Check is an assessment-only engagement which provides recommendations based on Microsoft published security guidance.

How the Offering Works

The onsite analysis begins when a Microsoft engineer discusses results of the security survey and host configurations directly with your company's technology owners. The Microsoft engineer confirms findings and configurations with you.

Each result and reviewed configuration setting is compared with the relevant Microsoft guidance, and any gaps between current practices and this guidance are reported.

You will receive a final report listing all gaps identified, associated recommendations, references, and evidence collected. The report will also include a scorecard for the environment, which gauges how adherent the environment is compared to Microsoft best practices.

A verification for existing hidden malicious software, can be made prior to the onsite engagement period using additional techniques and tools (Note: This verification is optional)

Delivered by experienced and accredited Microsoft engineers, a Security Health Check helps you:

- Gain an overview of technical and operational security practices within your organization
- Establish operating system baselines which include key security configurations
- Understand security issues and receive consultation and guidance and to help minimize their business impact

Security Guidance

SECHC processes and tools were designed to assess one environment and one chosen host per role. These hosts can serve as models for baseline security analysis that can be replicated to all other hosts in the network with the same role. For example, a typical review of hosts in SECHC might include:

1 Domain Controller
1 File and Print Server
1 SQL Server
1 Exchange Server
1 Web Server
1 Laptop computer

With each serving as a model for other machines of the same type.

Around 40% of the checklist in the Microsoft SECHC is related to host security settings and options, and these checks are repeated for each host. The remaining 60% is related to security processes and architecture: physical security, network infrastructure, patch management, antivirus management, Web applications/ infrastructure, messaging, and databases.

Continuous review of Evaluations

SECHC has a continuously reviewed and updated checklist for host configurations, security processes and network environment to ensure relevance.

IT Requirements/Deliverables

You will receive a deliverable package including all presentations, final reports,consolidation spreadsheets containing all findings, all data collected, relevant Microsoft whitepapers, and relevant tools used during the engagement.

Engagement Logistics

SECHC can be delivered remotely or onsite, according to your needs.

Onsite deliveries will take three days for a scope of up to 5 hosts. One extra day is needed for each additional group of up to 3 hosts, up to a maximum of 10 hosts in 5 days.

Remote deliveries will follow the same course as any remote support case currently handled by our phone support teams.

For more information about consulting and support solutions from Microsoft, contact your Microsoft Services representative or visit www.microsoft.com/services.