Heritage Technology Solutions

13600 S. Kenton Ave
Crestwood, IL 60445
Phone: (708)597-5005 | Fax: (708) 597-5091
www.htspc.net

HTS Approach to Network Managed Services

Heritage Technology Solutions understands the need to review, test, document and analyze an organizations IT infrastructure. Below is a summary of phases for our approach.

Phase 1: Thorough review of the most recent audits of the IT network with a strong focus on recommendations.

Phase 2: Thorough review of all network documentation including but not limited to:

A. Diagrams of: Network topology; Active Directory Structure; Virtual Environments.
B. Guides regarding common services and procedures.
C. Inventory of: Servers; PCs; routers; switches; firewalls; wireless systems.
D. Backup and archive strategy, local and remote.
E. Uninterruptible Power Supply deployment and policy.
F. Antivirus hierarchy and deployment.
G. Current patch strategy and management.
H. Password requirements and logon limitations (location, time of day, remote, etc.).
I. Hosted services such as: email system; WEB hosts.
J. DNS and MX records – internal and external.
K. Warranties and/or contracts in force and expiration dates
L. Licenses/activation keys
M. Applications
N. Monitoring
O. Internet Service Providers and Infrastructure providers
P. Voice networks
Q. Camera networks
R. Vendor contact information

Phase 3: These documents are then compared with the findings from a range of automated and manual scanning tools, and physical inspections of the sites.
The tools typically used, but not limited to are:

A. Network Detective
B. Nessus
C. LabTech
D. Scrutinizer
E. DumpSec
F. WireShark
G. Microsoft Baseline Security Analyzer
H. RepAdmin
I. NetDiag

All scanning and surveys are coordinated with site administrators/IT staff to reduce the possibility of any interruption to normal business flow. ***No "down time" is ever a part of due diligence***.

Phase 4: Business application servers are endpoints are evaluated for:

A. Currently supported Operating System, with current service packs and critical patches
B. Software must be genuine, licensed and Vendor-Supported.
C. Sufficient hardware resources such as: RAM; Processor Cores; Hard Drive Space; Network connectivity.

Phase 5: Backup procedures are evaluated for meeting a variety of recovery scenarios.

A. Recovering a lost/corrupt of file.
B. Restoring an application server from a component failure (hard drive, power supply, etc.)
C. Rapid replacement of a catastrophic hardware failure (fire, flood, extended loss of power, black hole).

Phase 6: Antivirus hierarchy and deployment is evaluated for:

A. Ensuring versions and definitions are deployed as scheduled.
B. Deployment of definitions is distributed in a manor to reduce network congestion.
C. Controls are in place to ensure functionality.

Phase 7: Network infrastructure components are evaluated for:

A. Currently supported architecture and firmware version.
B. Sufficient internal resources such as: RAM; Processor; acceleration modules; interface throughput; port density.
C. Manageability and control.
D. Availability of security controls and restrictions.
E. Bandwidth capacity and burst capability.
F. Redundant paths and fail over capability.
G. Encryption of data passing through public infrastructure.

Phase 8: Baseline security configurations considerations:

A. VLAN topology and structure is evaluated to ensure traffic from: data; voice; infrastructure management; third party devices are kept separate and intercommunications is strictly limited.
B. Infrastructure management communication protocols (i.e. SNMP, EIGRP, SSH) are encrypted and limited to known sources and endpoints.
C. Remote connectivity and management is limited to known source and destination IP addresses, using defined uncommon ports.
D. Switch topology and layout to ensure rapid redundancy, but limit interjection of rogue devices or connections. Block VLAN hopping, and the interjection of foreign DHCP providers.

Phase 9: Compilation and client review

Phase 10: Approvals of any projects