HCP Consulting Services, L.P.
PHONE 1-800-682-0484 FAX 210-579-1366

Cyber Attack Hardening Guide

Multi-Layered approach to Enterprise Security

1. **Outer perimeter** – As the first layer of defense HCP selects a subscription based firewall appliance that combines multiple security features into a single platform to protect against attacks, viruses, Trojans, spyware and other malicious threats.
    - Install and configure firewall appliance
    - Enable/configure Content Filtering System
    - Enable/configure Gateway Anti-virus
    - Enable/configure Intrusion protection
    - Enable/configure to allow all external access via VPN tunnels only

2. **Server/Enterprise security** – Key infrastructure pieces are hardened and configured for secure resource sharing
    - Implementation of Active Directory user security
    - Anti-virus on all servers with daily scans and definition updates
    - Default accounts disabled
    - Unnecessary ports are closed
    - Implement group policy on use of USB drives and external devices

3. **Workstation security** - Allow only necessary resources and access to the
    - Allow only necessary resources and external access to workstations and users
    - Anti-virus on each workstation with daily scans and daily definition updates
    - Group policy enforcement of locked workstations if left idle
    - AD security on workstation access

Network redundancy at multiple layers is also used to ensure uptime and productivity. Here are a few.

- Choose multiple Internet providers
- Implement multiple switches provide protection against switch and network port failure at the switch level
- Multiple NICs on server provide protection against network port failure at the server level
- Use of UPS and power on different circuits