

Cyber Security Overview PSFC

Brandon Savage
MIT-PSFC

5 Year Review May 9th 2008

PSFC Cyber Security Outline



- How do we organize our Cyber Security effort?
 - Authentication
 - Authorization
 - Integrity
 - Availability
- Additional Security Resources
- Future Security Enhancements
- Wrap Up
- With MIT's open data policies Cyber Security is more of a challenge. (ex. MIT's network does not use Firewalls.)

What is Cyber Security at PSFC



- Authentication
 - Who are you?
- Authorization
 - What resources an Authenticated Users can access?
- Integrity
 - Am I connected to the resource advertised?
 - Protection from outside intruders.
- Availability
 - Systems need to be up 24/7.
 - When unauthorized access occurs, system availability can be compromised.
 - When Key systems fail there must be recovery tools and systems in place for recovery in a timely fashion. Including system data and operations.

Authentication / Authorization



-
- Authentication
 - All PSFC domain resources are controlled through Windows Active Directory LDAP servers.
 - Passwords are required to be 8 characters long and contain both letters and numbers.
 - No clear text passwords are used.
 - Monthly scans of security logs and firewall logs.
 - Authorization
 - Controlled using the Windows Active Directory LDAP servers and RedHat Enterprise Linux servers.
 - All User accounts and IP enabled hardware are managed through an in house Network Management system that interfaces with Windows LDAP server and our Linux computers.

Integrity



-
- Am I connected to where I think I am?
 - Only secure protocols (SSH,SFX etc) are allowed to Linux systems which require certificates when connecting.
 - Remote Access to the PSFC network uses certificates as well.
 - Certificates help ensure you are connecting to a known location.
 - Protection from outside intruders.
 - The PSFC network is secured using a border firewall.
 - PSFC Domain computers also have local firewall, enabled by policy, allowing only a hand full of open ports. (most are internal access only)
 - All Linux systems use a local firewall that employs black list technology.
 - Server side email scanning.
 - Client side virus protection and scanning provided by MIT/IS&T.

Availability



- Network Remote Access
 - PSFC uses VPN to gain access to the PSFC network from the internet this requires a certificate.
 - PSFC also uses the Cisco VPN on campus for limited PSFC access from the internet. Kerberos Certificates are required for this access.
- Backup / Recovery
 - All Key systems are backup daily using a combination of backup strategies. (Disk to Tape and Imaging)
 - Windows and Macs are backed up using Retrospect and Tivoli backup software.
 - Domain Controllers (LDAP) and Engineering Data are backed up using Retrospect software. Images are also taken twice daily on all Domain Controllers to facilitate minimal down time.
 - Our SQL server uses Retrospect backup as well as Imaging and SQL transaction log backups.
 - Netvault is used to backup cmod data shots, Linux home directories, web servers as well as email servers.

Availability



- Remote System Management
 - Remote access Cards (RAC's).
 - Remote Access KVM's.
 - Remote Access Power (Used to remotely power cycle systems).
 - In house Account and IP device Management System.
- Network Policies Enforced
 - Automatic update for Windows Systems in domain.
 - Password length and content.
 - Anti Virus Software Updates.
 - Data tape archiving.

Additional Security Resources



-
- PSFC also taps other security resources.
 - MIT/IS&T
 - ESNet
 - Network and Security Consultants

Wrap Up



-
- Future Security Enhancements.
 - All remote system access through VPN.
 - The segmentation of our network.
 - At the PSFC we strive to provide sufficient computer and network security to protect our systems and data while minimizing its detrimental effects on user productivity.