Security Standard: Network

Scope

This standard applies to all Network Devices (except personally-owned devices within the residential network) that connect to the centrally-managed RIT network infrastructure or that process RIT Confidential or RIT Operationally Critical information whether or not they are part of the RIT centrally-managed infrastructure.

Requirements

The following security controls are required to be implemented.

1. **Currently deployed RIT Network Devices**
   - 1.1. If an RIT Network Device currently deployed is not capable of complying with a specific requirement of the Standard then that specific requirement is waived for that device.
   - 1.2. All other RIT Network Devices currently deployed should comply with all requirements of the Standard.

2. **Purchase and deployment of new Network Devices**
   - 2.1. All Network Devices purchased after the effective date of this standard should support all requirements of the standard.
   - 2.2. All Network Devices deployed after the effective date of this standard should be configured to implement all requirements of this standard.

3. **Physical security**
   - 3.1. All Network Devices should be secured in an area with physical access control.
   - 3.2. Core network equipment should be located in an alarmed area.
   - 3.3. Core network equipment should be attached to an appropriately designed UPS and generator system.

4. **Authentication and access lists**
   - 4.1. Access to Network Devices should be controlled by access lists so that the equipment is accessible only from a limited number of locations.
   - 4.2. Access to configuration backups should be restricted to authorized personnel only.
   - 4.3. All networks should be protected from Layer-3 IP address spoofing by an access list or other means.
   - 4.4. All external connections to RIT should be protected by an access list that blocks certain high-risk TCP/UDP ports.
   - 4.5. This list is maintained by ITS and is reviewed by ITS on a yearly basis (or as needed). Changes are subject to the change control process.
   - 4.6. Centralized user-level authentication should be used to authenticate all interactive users making changes to all Network Devices.

4.7. Hard-coded passwords will be allowed as necessary for non-interactive purposes, as well as recovery of Network Devices that have become disconnected from the network.
4.8. Whenever possible, network devices will display a trespassing banner at login.
4.9. This banner text shall not provide the underlying characteristics of the network device. Sample banner text may be found via the Network Standard Web page.

5. Network management

5.1. On any 802.1q trunk, the native VLAN should not be VLAN 1.
5.2. Plain-text protocols should not be used in network management.
5.3. Management traffic should be separated from user traffic.
5.4. Network Device management interfaces should be on a management network.
5.5. Any console ports used for device management should be secured by a username/password or other ISO-approved method.
5.6. Network management services should transition from SNMPv1, v2, v2c to SNMPv3 (or other option that does not use plaintext community strings).
5.7. Default SNMP community strings should be changed.
5.8. Initial prohibited protocols will include LDAP without use of TLSv1.2, FTP, telnet, remote host protocols, SSHv1, SSLv1, SSLv2, SSLv3. The list is maintained at http://www.rit.edu/security/content/network-security-standard.

6. Intrusion Detection System

6.1. An IDS service should be deployed on the links to/from the Institute network and the public Internet or Internet2. Hosts that are detected via the rule set shall be automatically blocked from further network access until the cause of the detection is understood and remediated.
6.2. The IDS configuration will be reviewed by ITS every six months or upon changes to the configuration.

7. Anti ARP-spoofing

7.1. Anti ARP-spoofing technologies should be deployed on user-edge Network Devices.
7.2. Features that support DHCP/ARP snooping should be enabled on Network Devices to better secure layer-2 networks from techniques such as ARP spoofing.

8. Change control

8.1. Any changes involving significant risk to the Institute network should go through a change control process.
8.2. The change control process should include:

- Problem statement
- Supporting data
- Potential solutions
- Impact/Risks
- Management approval of changes

9. Logging and monitoring

9.1. All Network Devices should log to a logging/network management system.

9.2. To ensure the integrity of the network, all Network Devices should be regularly monitored for their ability to be reached by a centralized network management system.

9.3. Any logs, including but not limited to, network, telecom, security, and IDS logs shall be confidentially provided to the AVP Risk Management, AVP Human Resources or Chief Legal Affairs Officer upon written request to the CIO.

10. Passwords

10.1. Passwords on Network Devices should be changed in accordance with the currently stated password standard.

10.2. Network administrators shall disable or change all manufacturers' default passwords.

11. Configuration backups

11.1. The configuration of all pieces of network equipment should be backed up regularly.

11.2. The configurations should be subject to managed revision control. Any changes in configuration should automatically notify the Network Administrator(s) in a timely manner.

11.3. An audit of network configurations may be conducted by either ITS or IACA.. IACA may review the audit results upon request.

12. VPN

12.1. Any VPN service that is deployed for use at RIT should be configured to not allow connection to the Internet except through RIT.

12.2. Any new VPN service should undergo a security review.

13. Vulnerability scanning & quarantine

13.1. The network should be scanned regularly for hosts that are vulnerable to remotely exploitable attacks. Hosts that are vulnerable will be "moved" to a quarantine network where they may be allowed to self-remediate.

13.2. All data gathered from the vulnerability scanning and quarantine processes should be classified as RIT Confidential information.

13.3. The quarantine network will allow hosts to access services necessary to patch and remediate infections. These services may be provided through a proxy server.

13.4. Explicit blacklisting or permanent whitelisting of the ITS vulnerability scanner is prohibited.

13.5. Notification to administrators of registered subnets or individual network addresses in the event of quarantine or blocking:

- The local administrator of the registered subnet or individual addresses is responsible for maintaining accurate registration information.
- Unless the network may be harmed without immediate quarantine or blocking of compromised computers, the Network Administrator should notify administrators of systems found to be vulnerable by the vulnerability scanner before the systems are placed into quarantine or blocked.
- If immediate quarantine or blocking is necessary to avoid harm to the network, the Network Administrator should notify the administrators of affected systems in a timely manner.

14. Wireless Security

14.1. All new wireless Network Devices should support ISO-Approved Encryption Methods.

14.2. Minimum levels of security should be adhered to according to a schedule developed by the ISO in collaboration with the RIT community.

15. Device Registration

15.1. Before being allowed on the network, all network devices or systems with an IP address on the network should be registered in an ISO-approved registration system.

- This device registration should include all MAC addresses and the name of the party responsible for the device.
- Guest access should be registered with appropriate contact information.

Effective Date: August 1, 2009

Standard History:
November 1, 2006
November 11, 2013
October 19, 2015