(http://www.uni.edu/its)

Network Citizenship Guidelines

Technology Guideline

The University of Northern Iowa relies on the integrity of its digital network. The proper management of systems that serve vital business functions or are used to store confidential university data is essential to the network. It is equally important that personal workstations be managed securely to prevent network attacks, system intrusion attacks and packet sniffing. By attaching to the campus network through a wired, dial-up or wireless network connection the system administrator agrees to maintain their system in a fashion that reduces the threat to network vulnerabilities. Threats could include direct attacks on UNI resources or UNI resources being used to launch attacks on remote resources as part of an Internet or Homeland Security threat.

Guideline

This Guideline is intended to identify practices that protect the integrity of the campus network and its resources by identifying best practices for system security, assigning responsibility for assessing vulnerabilities, monitoring for network attacks and probes, and taking action to ensure network health.

System Administration responsibility for university-owned computers and hand held devices that are capable of connecting to the campus network resides with the Technology Support group for that College/Division/Unit. In some cases responsibility for specific machines may be assigned to departmental staff. Faculty, staff, students and affiliates whom have received explicit permission to connect their personally owned computers/devices to the campus network via the Internet, ResNet, UNI modem pool, UNI Wireless access, or UNI Virtual Private Network assume the System Administration responsibility for their machines.

ITS is responsible for identifying and publishing best practices for system security, assessing vulnerabilities for systems connected to UNI-Net, monitoring network attacks and probes, and ensuring the health of the campus wired and wireless networks.

By connecting to the university network, System Administrators agree to:

- Use the network in a fashion that does not noticeably degrade service to others such as inordinate use of network bandwidth (e.g. downloading many large files during busy hours) or use that would be considered invasive (e.g. scanning machines outside of an individual’s administrative control or sniffing of packets).
- Abide by Acceptable Use of Computing Resource policy and other applicable University Policy and State and Federal Law.
- Follow UNI best practices on system configuration and security to ensure that key system vulnerabilities are addressed in order to mitigate the risk and loss associated with threats to the campus network. Key vulnerabilities will change over time as new threats and risks emerge.
- Submit their machines to vulnerability scans by authorized ITS staff designed to identify security vulnerabilities.
- Work with ITS staff to address and resolve security problems identified on any system in an expedited fashion.
    - Respond to vulnerabilities within a defined period of time following receipt of notification of this problem.
    - Remove from the network, machines that are infected, compromised, or modified in such a fashion that they are impacting network health.

- Report compromises and security incidents to ITS staff on a timely basis.

Procedure

- ITS reporting of security problems to System Administrators ITS will report security problems and best practices to address known security problems to College and Divisional Technical staff, ResNet users, and individuals connecting to UNI's Wireless network and Virtual Private Network Server via email and the World Wide Web (E.g. ITS-Announce, ResNet-Announce, UNI-Online, MyUNIverse, ResNet Web space, UNI Security Portal).
- System Administrator reporting of security problems to ITS System Administrators should send mail in a timely manner to abuse@uni.edu [1] if they become aware of a network security problem.
- Handling of security threats ITS will apply system wide blocks at the campus gateway router(s), both permanent and temporary, and will work with System Administrators to close known security vulnerabilities as quickly as possible while maintaining network connectivity.
- Removal of machines from University Network Systems that have been infected or compromised and pose an immediate threat to campus information or network health will be removed from the campus network with minimal or no advance warning. Immediate action is often necessary to isolate the intrusion or attack and minimize the risk to other systems. Connectivity will be restored when the system is repaired, best practices implemented, and the threat eliminated.
- High Risk Vulnerabilities When a known exploit is identified that is capable of damaging systems, data or network reliability, the Associate Vice President for Information Technology will declare this a High Risk Vulnerability. High Risk Vulnerabilities must be patched within a short period of time based on the level of the threat, as short as 24 hours or less. Systems that are not patched within this timeframe may be removed from the network.
- Connecting machines to UNI-Net Systems that are connected to UNI-Net should be scanned by the System Administrator for virus' and worms and have virus protection software installed in real time mode with live update set for retrieval of current definitions file. Systems connecting to UNI-Net must have the all critical patches installed for the Operating System (OS) and critical patches for all sub-systems installed.
- Scanning of systems on UNI-Net ITS Network Services will conduct periodic scans of machines connected to UNI-Net looking for current service level. These scans will be initiated from specific machines by authorized central staff. Periodic scans will focus on OS, system utility vulnerabilities, the status of virus protection, and for vulnerabilities of our standard, supported product suite. In addition, ad hoc scans will be conducted to look for specific vulnerabilities (e.g. Microsoft RPC exploit, Code Red Worm, mail servers configured as an open relay). These scans do not access user data and will be run only after a determination is made by ITS NS staff on the impact of each scan on end user machines. Blocking of ITS Periodic and Ad Hoc Scans could result in removal from the network.

Drafted November 20, 2003

Links:
[1] mailto:abuse@uni.edu