SECURING NETWORK CONNECTED DEVICES

Category: Information Technology
Responsible Office: Information Security Office
Responsible Executive: Chief Information Officer

Date Established:
Date Last Revised: **5/26/11**
Date Posted to Library: 9/2/2011

Summary

One of the major shared resources of the University is its data network. The University's ability to conduct its business is dependent on reliable, stable access to the network and through the network to the Internet. University network and Internet connectivity can be jeopardized by computers/workstations, servers, and other devices that are not adequately protected from attack. Protection is optimized only when principal users maintain the operating systems of their devices, install, continuously run and regularly update antivirus software - when applicable, and apply patches that close known security breaches as soon as they become available.

Compromised or vulnerable devices connected to the University network present potential harm to the network, to other devices on the network, to other networks and the devices attached to them, and to the overall standing of the University's information technology enterprise. Delays in responding to compromised devices could result in losses of data and productivity, other operational problems, legal consequences, and harm to the University's reputation. Consequently, it is imperative that a compromised device be secured in order to eliminate the risk it poses. If a compromised device is being actively used in a way that threatens the integrity of the University network or other devices on the University network, it may be necessary to disconnect it temporarily from the network and secure it before it is reconnected. Because vulnerable devices may at any time be compromised, they must be remediated expeditiously.

Policy

A principal user who connects a device to the University network is responsible for working with appropriate staff to secure the device against compromise. Specifically, any device connected to the University network must (when applicable):

1. have an authorized fixed IP address or be appropriately registered for DHCP;
2. be configured to run a supported version of an operating system for which patches for newly identified security breaches are developed and distributed in a timely manner;
3. be configured in such a way that known vulnerabilities - such as open FTP ports and open relays - are eliminated or minimized;
4. be maintained in such a way that patches which close known security breaches are applied as soon as they become available;
5. have antivirus software installed on it that runs continuously and is updated regularly;
6. be scanned and determined to be free of viruses and other known compromises that may have been introduced to its operating environment; and
7. be used for appropriate purposes related to the educational and research missions of the University or to the conduct of its legitimate business activities.

Further, it is **highly recommended** that **firewalls** be installed and run continuously on devices whenever possible and practicable.

Principal users who fail to fulfill the foregoing responsibilities are subject to the actions described in the following sections.

Definitions

1. A **device** can be a computer/workstation, server, mobile device, cellular telephone, or any other instrument capable of connecting to and interacting with the University network and other devices on the network.
2. A **principal user** is an individual who owns, is the primary user of, or the individual or group responsible for the administration of a device.
3. For the purposes of this policy, a device is considered **compromised** once it has been substantiated:
    i. that its security is breached and that unauthorized processes or user(s) have access to and are able to control its data and/or resources;
    ii. that it has been configured in a way that could threaten, harm, or interfere with the operation, integrity, or network access of other devices; or
    iii. that it is actively being used to threaten, harm, or interfere with the operation, integrity, or network access of other devices.
4. A device is considered **vulnerable** once it has been substantiated that known actions necessary to prevent it from being compromised have not been taken - despite those actions having been recommended by the Office of the CIO or by entities charged by the CIO to secure the University's computing and networking infrastructure.
5. A device is considered **connected** to the University network when it is attached:
    i. to a trusted administrative Ethernet port (not requiring authentication for its use) on the network;
    ii. to a ResNet port in the Residence Halls;
    iii. to an open Ethernet port (requiring authentication to a firewall for its use) on the network;
    iv. to a wireless access point (requiring authentication to a firewall for its use) on the network;
    v. through an ISP via a VPN (virtual private network) session;
    vi. via connections established at institutions affiliated with the University, such as hospitals; or
    vii. by any means that enables its access to the University network.

Procedure

Securing Compromised or Vulnerable Devices Connected to the University Network

A principal user who connects a device to the University network is responsible for working with appropriate staff to secure the device against compromise as soon as actions to address known vulnerabilities are identified. If a device is compromised, the principal user is responsible for working with appropriate staff to ensure that collateral risks or damage to the information

technology infrastructure of the University, other devices on the University network, and other Internet-connected devices and networks around the world are prevented or minimized.

A compromised device, as specified in *definition 3* below, should be immediately secured, shut down, or disconnected from the University network by the principal user. The principal user is responsible for initiating or cooperating with efforts to secure the device. The principal user is also responsible for initiating or cooperating with efforts to identify and notify other principal users whose devices may have been affected. Principal users who reconnect disconnected devices that they know are compromised and have not yet been secured are in violation of University policies and are subject to further actions and, possibly, sanctions.

As a last resort, in the cases of compromised devices connected to the University network as specified in *definitions 5.i.* and *5.ii.* below, when time constraints permit no other course of action or when a principal user is unavailable or uncooperative, it may be necessary to suspend temporarily the network connection of the compromised device. This action should be taken, preferably, by the IT service organization responsible for supporting the principal user in question.

When a campus computer is actively attempting to compromise the integrity and or availability of UB's IT infrastructure, it will be disconnected from the network **immediately** and the owner and/or IT support staff will be notified of the problem and the protective actions taken.

As a last resort in the cases of compromised devices connected to the University network as specified in *5.iii., 5.iv., 5.v.,* and *5.vi.* below, when time constraints permit no other course of action or when a principal user is unavailable or uncooperative, it may be necessary for CIT to suspend temporarily the principal user's UBit account. This action should be taken, preferably, only after the principal user and (when applicable) the IT service organization responsible for supporting the principal user in question have been notified. When a principal user who is a faculty or staff member cannot be notified prior to this action or is unresponsive or uncooperative, every reasonable effort will be made to communicate with (in ascending order): the affected department chair or head, the affected Dean or Vice President, or the CIO. In such an event, the parties who would normally be consulted should be notified of the suspension as soon as possible after the action is taken.

Such temporary disconnections and suspensions should be imposed only until such time as the precipitating problem has been redressed. When a principal user who is a faculty or staff member cannot be notified prior to this action or is unresponsive or uncooperative, every reasonable effort will be made to communicate with (in ascending order): the affected department chair or head, the affected Dean or Vice President, or the CIO. In such an event, the parties who would normally be consulted should be notified of the disconnection or suspension as soon as possible after the action is taken.

Principal users are strongly encouraged to seek the advice of an IT support professional before reconnecting a previously disconnected or suspended device. If such a device is reconnected to the network and has not been secured, further action may be necessary to ensure that the device is properly secured.

Disconnection or suspension is considered a course of action to be avoided whenever possible and to be taken only when deemed necessary in the measured professional opinion of responsible parties in the Office of the CIO, CIT, or the IT service organization responsible for supporting the

principal user in question. Within a reasonable time after the disconnection or suspension is imposed, a post-mortem analysis of the sequence of events leading to the suspension should be conducted. All affected or interested parties should be invited to participate in the post-mortem. The primary purpose of the post-mortem should be to determine - without recrimination - whether the suspension was justified by the facts and whether alternative, equally effective actions could have been taken.

Applicability of Policy

This policy applies to all University data regardless of its medium and/or form, and to all those who handle University information (faculty, staff, students, third party contractors, and any others).

Policy Review and Update

The Chief Information Officer or his designee will periodically review and update this policy as needed. Questions concerning this policy should be directed to the Office of the Associate VP for Information Technology.

Compliance

Violations of this policy will result in appropriate disciplinary measures in accordance with University policies, applicable collective bargaining agreements, and state and federal laws.

Contact Information

Information Security Officer
517 Capen Hall
University at Buffalo
sec-office@buffalo.edu
(716) 645-3582

Related Information

University Documents:

Standards for Securing Regulated Private Data
Social Security Number Policy

Other Documents:

New York State Information Security Policy