Server Security Procedure

Procedure Number: PSU-NK-ITS-008
Date: February 15, 2018
Page Count: 3

Purpose:

The purpose of this procedure is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Penn State New Kensington. Effective implementation of this procedure will minimize the risk of unauthorized access to campus and university proprietary information and technology.

Scope:

This procedure applies to server equipment owned and/or operated by all agents of Penn State New Kensington. This procedure is specifically for equipment on the internal New Kensington Data Network including administrative systems as well as faculty and student research or test systems.

Definitions:

Server - For the purposes of this procedure, this is defined as a computer that resides on the New Kensington Data Network that provides services approved by the NK IT Department. Desktop computer and lab computer systems are not germane to the scope of this procedure.

New Kensington Data Network – The technology infrastructure, hardware, and software installed at the campus which is used to facilitate the flow of digital information between (but not limited to) computers, printers, servers, mobile devices, the Internet, etc. This includes both the wired and wireless networks at Penn State New Kensington.

NK ITS Department – The department that oversees IT resources at Penn State New Kensington to include the System Administrator, IT Specialist and IT Director

Denial of service attack - An attack designed to prevent a system from providing services to its users.

Dictionary attack - The automated use of a 'dictionary' of potential passwords used to attempt to compromise an account or a series of accounts.

TCP Wrappers - is a host-based networking access control system that is used to filter network access to IP based servers

Demilitarized Network Zone (DMZ) - is a physical or logical sub network that enables computers in this zone to reach the Internet but not the IT resources that are part of the New Kensington Data Network.

Procedure:

Ownership and Responsibilities

All internal servers deployed at Penn State New Kensington must be owned by the campus. The system administrator responsible for each server must sign and agree to the "End-User Computing Agreement." The signed procedure must be provided to the Director of Information Technology and kept on file for the lifespan of the server. The installation of a new proposed server must be approved by the individual's department head and the Director of Information Technology. A decision will be made based on business needs and final approval will be granted by the campus Chancellor. Configuration Guidelines must be monitored for compliance.

Server Configuration Requirements

- Operating System configurations should be in accordance with approved campus guidelines to ensure a significant level of security against unauthorized access.
- Services and applications that will not be used must be disabled, where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers or other security mechanisms.
- The most recent security patches must be installed on the system within one-week of release. The only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk; their use should be avoided. Do not use a trust relationship when some other method of communication will suffice.
- Always use standard security principles of least required access to perform a function.
- If a methodology for secure channel connection is available and technically feasible, privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers must be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating in areas accessible to persons other than the intended system administrators.
- Anti-virus software must be installed when applicable and set to update virus definitions automatically.
- Servers hosting services available to an external network (outside of the campus) or the Internet (e.g. www/sftp/ssh/smtp/pop/imap, etc.) must be placed on a Demilitarized Network Zone (DMZ) to assure segregation of network traffic and best security practices.

PennState New Kensington

Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as documented in AD-95.
- Security-related events will be reported to the Director of Information Technology, who may review logs and report incidents to the Office of Information Security (OIS). Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Dictionary attacks
    - Unauthorized network scanning
    - Denial of service attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.

Compliance

- Audits will be performed on a regular and random basis by authorized NK ITS Department personnel.
- Audits will be managed by the Office of Information Security (OIS) or NK ITS Department personnel, in accordance with the Incident and Disaster Tolerance / Response Procedure. The campus will present pertinent findings to the appropriate system administrator for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

Enforcement

Any employee found to have violated this procedure may be subject to disciplinary action by their administrative unit, the campus, or the University. Systems involved with severe security breaches may be confiscated for forensic analysis.

Procedure History:

September 19, 2019 – Removed firewall exceptions because we no longer manage a local firewall
February 15, 2018 - Procedure created based off previous campus policy.