Security Strategy

Contents

Introduction

CaTS recognizes the importance of safe, secure, and reliable computing networking resources to the university. CaTS is dedicated to the protection of these resources from threats, both internal and external, that could disrupt communications, damage information or equipment, or otherwise render these resources unavailable. It is CaTS charge to establish and maintain a secure environment for the university's computer and network resources.

Policy

CaTS shall identify, create and publish a framework of security policies that address the security of data and information technology resources. The policies will apply to key security topics such as system and network management, authentication and authorization, appropriate or responsible use, and data stewardship.

Perimeter

Internet-based attacks cannot be prevented. Therefore, it is important to stop them at the first point of contact. Hardware and software on the perimeter of Wright State's network must be able to identify and limit the effects of an attack while supporting an open academic and research-oriented environment. CaTS acknowledges the challenges of perimeter security and seeks to recognize, control and manage Internet traffic. As new tools, such as those that analyze the behavior of network traffic, become available, they will be studied and added to the perimeter defense as applicable. Currently, firewalls protect main campus, computer lab environments, server segments, and residence halls from hostile inbound traffic from the Internet.

Infrastructure

CaTS shall further define university communities, providing a multi-layered, tiered, zone, or ring approach for network security. Traffic from these zones to other zones on campus will be required to traverse a variety of security technologies such as firewalls, network access control lists, etc. This will provide for flexibility, protection and accommodation of the greatest number of users while maintaining a secured and protected environment. All infrastructure components such as hubs, routers, wireless access points, etc. must be registered and approved by CaTS before connecting to the campus network.

Zone 1

Zone 1, the most secure zone, will house servers and computers that either store university protected information or require constant access to protected information. In addition, departmental sub-networks and their associated computers may be placed in this zone by a department that requires greater network security. All servers for administrative applications will be placed in this zone.

Zone 2

Zone 2 will serve the campus at large. General access to this zone will not be permitted from outside the university network. There will only be access to specific services and general access to these systems (except from systems/users in zone 1) will not be allowed. Systems in this zone will be scanned for correct configuration, O/S security patches, etc.

Zone 3

Zone 3 will be a high security public server zone. This zone will contain University mission critical servers that require access from all locations on or off campus. CaTS will maintain the servers in this area for all campus users who have a need for secure remote access to data/applications. In general, servers in this area will not store protected data locally but will act as front ends to the servers in the most secure zone.

Zone 4

The fourth zone is designated for departments who have servers that require access from outside the University network. Access from all systems in zones 1-3 will be given to all servers/services. The servers in this zone may access systems only in zone 2 by requesting that access from CaTS. Most departmental web and file sharing servers will be placed in this zone. It is the responsibility of the system administrators that servers in this zone must be maintained for correct configurations, O/S patches, etc.

Zone 5

Zone 5 is for the university residence halls, dial-up and wireless networks. This is the least secure zone on the University network. Zone 5 includes any network that is either not protected or has devices that do not meet CaTS minimum level of security criteria. Systems in zone 5 will be scanned as appropriate, for correct configuration, O/S security patches, etc.

All network access will be authenticated. WSU will use its campus login and password to authenticate network usage in addition to e-mail, dial-up, laboratory and classroom access and other services.

Secure protocols such as secure shell, secure socket layer (SSL) and virtual private networks (VPN) will be required for server access. Insecure telnet and ftp will not be available.

Desktop Standards

CaTS shall develop and maintain standards, procedures and guidelines that shall be enforced in order to safeguard the computing environment all the way to the client’s desktop.

Desktops or workstations are devices connected to the WSU network using an IP address in the Wright State University domain and are generally intended to be used by a single client. In addition to the CaTS supported hardware and software standards, CaTS will require that software patches and anti-virus applications for all desktop or workstation operating systems, such as Microsoft, Macintosh and UNIX, be installed. The software updates must be applied in a timely manner.

Vendors drop support for older versions of operating systems after newer operating systems are developed. When this happens it is the customer’s responsibility to run a currently supported software environment. Computers that cannot or do not choose to participate in the automatic patching process will be identified and placed in zone 5. Computers that do not meet the minimum security criteria will also be placed in zone 5.

Clients introducing new machines into the campus network must register their machines. Those machines will be checked for infections, cleaned, and updated before being placed into the proper protected zone. This applies also to machines that are removed from the network and reintroduced.

Incident Response

CaTS shall develop and maintain an Incident Response Policy, process and security standards for the investigation, control and prevention of computer incidents. A computer incident is an event that disrupts normal operating procedures. Computer intrusions such as viruses, denial-of-service attacks, theft of information or an identity, or any unauthorized or unlawful network activity are examples of computer incidents.

If a threat or virus infiltrates the protection of a zone and propagates, the hostile traffic will be restricted within distinct network segments by implementing access control lists that will isolate the segment from the rest of the network, reducing the risk of cross-infection. Machines within the protected environment identified as infected or compromised will be immediately removed from the network until it can be certified that the infection/compromise has been removed.

Education

The security of university resources and information is the responsibility of all network users. CaTS will provide security-related information to the university via Quickbits articles, security web pages, notification of potential threats, and technical security advice for new computer applications.

Definition of Terms

Secure Shell: The Secure Shell is a program designed as a replacement for telnet and remote shell (rsh) with strong encryption.

Secure sockets layer (SSL): SSL is a plug-in technology that supports authentication between TCP/IP sockets, or more simply, for applications that use IP, such as web browsers. SSL combines the use of an encrypted connection and authentication of server certificates (client certificate verification is optional) to provide secure communications.

Virtual Private Networks (VPNs): VPN's use strong authentication and encrypted channels to make sites appear as a single virtual network, in a secure manner, even though they are separated by the Internet or another public switched data network.

The University mailserver is a secure, highly available messaging environment to safeguard the university communications. It filters emails for viruses or attachments known to be damaging and removes them from the email.