The Printer Working Group
Imaging Device Security Working Group
http://www.pwg.org/ids

The Business Case for NAC and Hardcopy Devices

Do you know where your printers are and who they're talking to?

Introduction

Enterprise class networks are beginning to deploy new network security protocols and tools designed to gather and assess the health of client computers and other devices on the network. These assessment protocols go beyond simply checking that the device or user possesses the correct credentials to access the network. Instead they validate the network health of a system by gathering and assessing health attributes such as operating system version, security patch levels, antivirus definition levels, system configuration, etc.

Modern hardcopy devices behave as complex servers and clients running multiple applications. By standardizing common Health Assessment attributes for these powerful devices (Network Printers, Multi-Function Devices, Network Scanners, etc.) should be incorporated into commercial network security tools. When health assessment support is provided for modern imaging devices, commercial network security tools will be able to offer more complete network security.

Network Access Control

Network Access Control protocols and systems provide a method for restricting network access to systems and devices, based on a set of health criteria, such as OS version, anti-virus status, application support, patch level, etc. Based on the values of these criteria, a system or device may be restricted to a non-trusted network zone, pending resolution of problems. Three of the major protocols designed for Network Access Control are:

Microsoft Network Access Protection (MS NAP)

Internet Engineering Task Force's Network Endpoint Assessment (IETF NEA)

Trusted Computing Group's Trusted Network Connect (TCG TNC)

Hardcopy Device Security Threat Exposure

As hardcopy devices have evolved, they have gained increasing levels of communications and file handling capabilities. These capabilities are no longer limited to just local document printing, scanning and copying. Increasingly, these devices are connected to corporate networks and use these networks to receive and transmit corporate data and documents and perform user activities.

Document Repository

Modern hardcopy devices also function as file servers and are used to store sensitive company documents and information for later retrieval. File access may be limited to non-accessible local storage or the device storage may be network accessible through various network file server protocols such as CIFS, SMB, NFS, etc.

Email Client and Server

Corporate documents can be sent from and received by hardcopy devices using standard email protocols. Scanned documents can potentially be sent to arbitrary email destinations, while an email containing potentially dangerous binary data could be received by a device.

FTP Client and Server

In the same manner as dangerous emails, potentially dangerous files could be sent to a device that provides an FTP server. Corporate documents could be transferred to arbitrary FTP destinations.

HTTP Web Server

Many hardcopy devices provide an embedded HTTP Web Server to allow remote configuration of the device and transfer of files. If unprotected, this capability could expose the device to a potentially insecure reconfiguration. Since some devices allow the transfer of documents through the web server potentially dangerous files could be transferred out of the corporate network.

HTTP Web Browser

In addition to file and document server functionality, hardcopy devices can include web browsers to allow user to access local and remote web sites and services. Web access can used to send documents outside a corporate network and to retrieve documents from outside the corporate network

Fax Modem

The fax modem provided by some hardcopy devices also presents a potentially insecure method of transmitting documents into and out of the corporate environment.

User Authentication

The enabling of user login and accounting information means that hardcopy devices now have access to corporate authentication services such as Active Directory and LDAP servers.

Downloadable Applications

Some advanced hardcopy devices provide a mechanism for user and system applications to be downloaded and executed on the device. Each of these applications presents a potential security threat to the system and network. Some method of monitoring and restricting the use of these applications is necessary.

As a result of this increased functionality the level of potential susceptibility of modern hardcopy devices to security threats and network attacks has greatly increased. It is no longer possible for network and security administrators to assume that a typical hardcopy device is a safe, localized stand-alone device that does not warrant excessive concern. Rather, these devices are just as capable of providing remote data transmission and the resulting exposure to threats as a user's desktop system or a corporate server.

PWG Imaging Device Security

Currently, it is not possible for a network or system administrator to detect or monitor all of the hardcopy devices that reside on the network, nor automatically determine whether they present potential security threats. While it is possible to monitor and validate devices on an individual basis, having hardcopy devices incorporated within an organization's network security tools can provide immense benefits to the network and system administrator.

To facilitate a unified approach to ensuring the network health of a hardcopy device, the PWG has defined a set of Health Assessment Attributes designed to enable device security assessment. By incorporating support for these Health Attributes in their security tools, a security vender can provide tools that present a more complete picture of network and device security. By using the security tools that provide hardcopy device support, a company can monitor and assess the hardcopy devices on their network in the same manner as they assess their user systems and servers. The level of this assessment may range from locating and identifying devices on the network to actively assessing the threat level of a device, and either remediating potential issues or isolating the device from the corporate network, thus eliminating the potential security threat.