Device Hardening, Vulnerability Remediation & Mitigation for Security and Compliance

A New Net Technologies Whitepaper

Mark Kedgley

CTO - New Net Technologies

The PCI DSS demands Device Hardening...

"Establish firewall and router configuration standards.."

"Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards."

"Always change vendor-supplied defaults before installing a system on the network—for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts."

"Change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission."

Introduction

All security standards and Corporate Governance Compliance Policies such as PCI DSS, GCSx CoCo, SOX (Sarbanes Oxley), GLBA, NERC CIP, HIPAA, HITECH, ISO27000 and FISMA require IT systems to be secure in order that they protect confidential data.

This whitepaper explores one of the key dimensions to securing devices through the process of 'hardening', and examines the various means available to audit devices and maintain them in a hardened, secure state.

There are a Number of Buzzwords Being Used in this Area - Security Vulnerabilities and Device Hardening?

'Hardening' a device requires known security 'vulnerabilities' to be eliminated or mitigated. A vulnerability is any weakness or flaw in either the software design, implementation, or administration of a system that ultimately provides a mechanism by which IT systems can be infiltrated and compromised.

There are two main areas to address in order to eliminate security vulnerabilities – configuration settings and software flaws in program and/or operating system files.Eliminating vulnerabilities will require either 'remediation' - typically a software upgrade or patch for program or OS files - or 'mitigation' - a configuration settings change. Hardening is required equally for servers, workstations, and network devices such as firewalls, switches, and routers.

How do I Identify Vulnerabilities?

A Vulnerability scan or external Penetration Test will report on all vulnerabilities applicable to your systems and applications.

You can buy in 3rd Party scanning/pen testing services – pen testing by its very nature is done externally via the public internet as this is where any threat would be exploited from.

Vulnerability Scanning services need to be delivered in situ on-site. This can either be performed by a 3rd Party Consultant with scanning hardware, or you can purchase a 'black box' solution whereby a scanning appliance is permanently sited within your network and scans are provisioned remotely.

Of course, the results of any scan are only accurate at the time of the scan which is why solutions that continuously track configuration changes are the only real way to guarantee the security of your IT estate is maintained.

> *"All the firewalls, Intrusion Protection Systems, Anti-virus and Process Whitelisting technology in the world won't save you from a well-orchestrated internal hack where the perpetrator has admin rights to key servers or legitimate access to application code - file integrity monitoring used in conjunction with tight change control is the only way to properly govern sensitive payment card systems."*

File Integrity Monitoring and the PCI Data Security Standard

The PCI DSS (Payment Card Industry Data Security Standard) specifies the following:

Requirement 11.5 "Use File-Integrity Monitoring or Change-Detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)."

However, Requirement 1 specifies *"maintain a firewall configuration to protect cardholder data"*, Requirement 2 *"Do not use vendor-supplied defaults for system passwords and other security parameters"*, Requirement 6 *"Develop and maintain secure systems and applications"* and in fact, the need to track and assess the impact on IT system security is at the heart of any Security Standard or Policy like the PCI DSS.

Host integrity monitoring software serves as an essential early-warning system and can provide the first indication of a break-in or compromised host.

When properly configured and deployed, this type of software is a powerful addition to the layers that defend your infrastructure in depth.

As a minimum, for any Windows devices 'touching' cardholder data, including EPoS equipment, the System32 and/or SysWOW64 folder should be governed as well as key application program folders.

It is important to verify all adds, changes, and deletions of files as any change may be significant in compromising the security of a host. Changes to monitor for should be any attribute changes and the size of the file. Remember, trojans are designed to impersonate existing system files and will always 'look' and usually behave like the genuine exe, dll or driver file, albeit with some nasty extra functions too!

Similarly, for Linux and Unix hosts, the /etc/ and /usr/bin/ directories and their constituent files must be tracked for integrity together with all relevant application binary and configuration files.

File Integrity - Guaranteed

However, since we are looking to prevent one of the most sophisticated types of hacks, we need to introduce a truly infallible means of guaranteeing file integrity. This calls for each file to be 'DNA Fingerprinted', typically generated using a Secure Hash Algorithm. A Secure Hash Algorithm, such as SHA1 or MD5, produces a unique, hash value based on the contents of the file.

The concept, therefore, is that a file integrity baseline must be established. Any File-Integrity Monitoring system works by comparing file attributes, filesizes, and hash signatures from one time to another. The assumption, therefore, is that the initial baseline is for a vulnerability-free, completely uncompromised host and application.

This means that even if a program is modified to expose payment card details, but the file is then 'padded' to make it the same size as the original file and with all other attributes edited to make the file look and feel the same, the modifications will still be exposed.

The schematic on the next page illustrates how such an algorithm generates a unique hash for a file.

So Tight Change Management is Essential for Ensuring we Remain Compliant?

Indeed – Section 6.4 of the PCI DSS describes the requirements for a formally managed Change Management process for this very reason. Any change to a server or network device may have an impact on the device's 'hardened' state and therefore it is imperative that this is considered when making changes.

Using a continuous configuration change tracking solution provides an audit trail and delivers the concept of 'closed loop' change management – the detail of the approved change is documented, along with details of the exact changes that were ***actually*** implemented. Furthermore, the devices changed will be re-assessed for vulnerabilities and their compliant state confirmed automatically.

What about Internal Threats? Cybercrime is Joining the Organized Crime League which means this is not just about Stopping Malicious Hackers Proving their Skills as a Fun Pastime!

Firewalling, Intrusion Protection Systems, AntiVirus software, and fully implemented Device Hardening measures will still not stop or even detect a rogue employee who works as an 'inside man'. This kind of threat could result in malware being introduced to otherwise secure systems by an employee with Administrator Rights, or even backdoors being programmed into core business applications.

Similarly, with the advent of Advanced Persistent Threats (APT) such as the publicized 'Operation Aurora' hacks that use social engineering to dupe employees into introducing 'Zero-Day' malware.

'Zero-Day' threats exploit previously unknown vulnerabilities – a hacker discovers a new vulnerability and formulates an attack process to exploit it. The job then is to understand how the attack happened and more importantly how to remediate or mitigate future re-occurrences of the threat. By their very nature, anti-virus measures are often powerless against 'zero-day' threats.

In fact, the only way to detect these types of threats is to use File-Integrity Monitoring technology. See the other NNT whitepaper **'File-Integrity Monitoring – The Last Line of Defense of the PCI DSS'** for more details, but here is a brief summary.

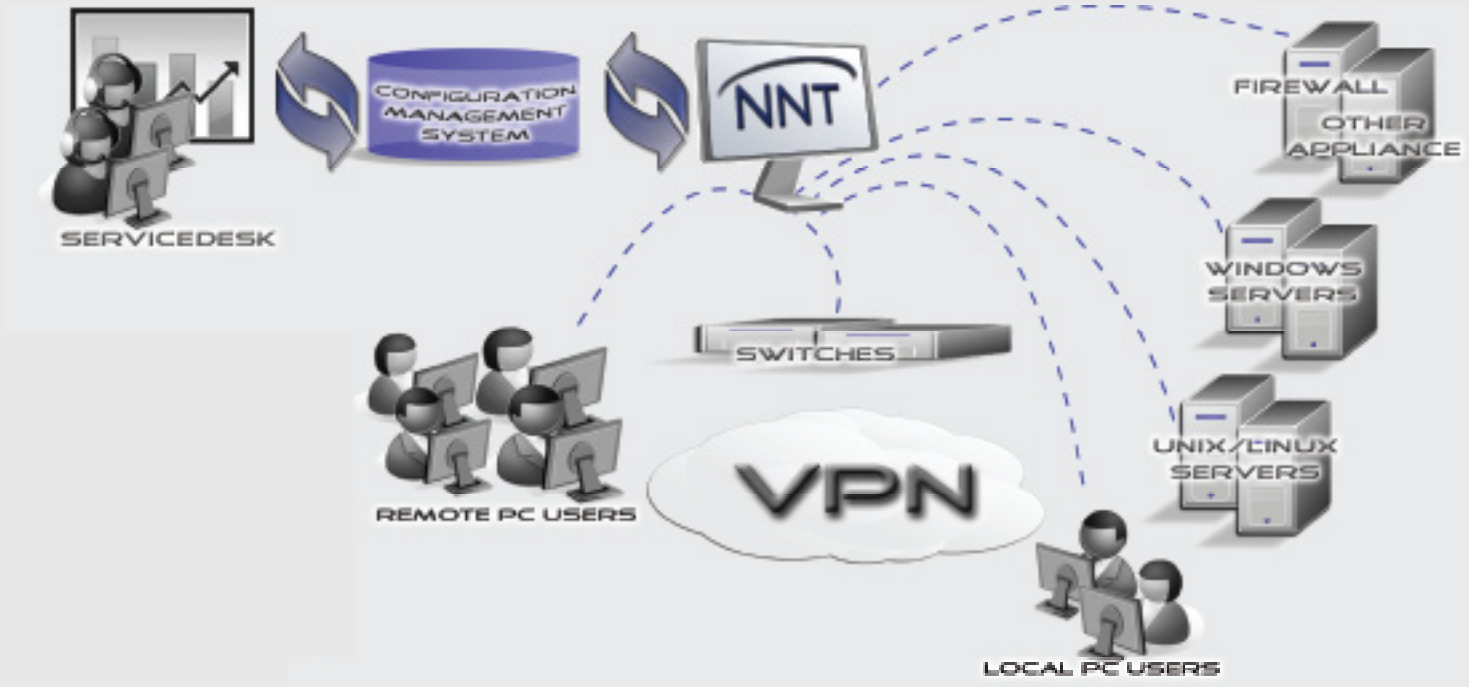
Clearly, it is important to verify all adds, changes, and deletions of files as any change may be significant in compromising the security of a host. However, since we are looking to prevent one of the most sophisticated types of hack we need to introduce a completely infallible means of guaranteeing file integrity.

This calls for each file to be 'DNA Fingerprinted', typically using a Secure Hash Algorithm. A Secure Hash Algorithm, such as SHA1 or MD5, produces a unique, hash value based on the contents of the file and ensures that even a single character changing in a file will be detected.

This means that even if a program is modified to expose payment card details, but the file is then 'padded' to make it the same size as the original file, and with all other attributes edited to make the file look and feel the same, the modifications will still be exposed.

What Do NNT Provide?

- Device Hardening Templates can be applied for all Security & Governance Policies, providing a fast Compliance Audit of all Devices
- Devices are then continuously tracked for Configuration Changes where vulnerabilities may be re-introduced
- Changes tracked include registry keys and values, file system and file integrity, user accounts, process and service white and blacklists, installed programs, performance vital signs, text-based configuration files
- All Planned and Unplanned Changes are detected and documented
- Any breach of Compliance Rules reported, including File Integrity Changes
- All platforms and environments supported, all network devices and appliances



About NNT

New Net Technologies (NNT) is the leading provider of Secure Ops, which leverages security through System Integrity along with Intelligent Closed Loop Change Control, focused on helping organizations reduce their security risk, increase service availability and achieve continuous compliance. NNT delivers its Secure Ops suite by combining: System Configuration Hardening, Closed Loop Change Control, Vulnerability Management and Event Log Management. These core security disciplines are defined by the SANS Institute as the essential Critical Security Controls for any cyber security initiative.