Device Hardening, Vulnerability Remediation and Mitigation for Security Compliance

Produced on behalf of New Net Technologies by

STEVE BROADHEAD

BROADBAND TESTING

www.nntws.com

NNT™
SECURITY THROUGH SYSTEM INTEGRITY
NOW PART OF netwrix

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.

Operation Aurora - The bar is raised for hackers with the Advanced, Persistent Threat

Operation Aurora has been widely reported and its effectiveness acknowledged by a number of high-profile targets including Google, Adobe and Juniper Networks.

The attack is seen as a grim warning of what is possible if hacking is well-planned and orchestrated. In this example, the aim appears to have been industrial espionage.

Project Aurora used targetted social engineering to infiltrate the workstations of key users withing the organizations attacked. A trojan masquerading as a windows dll was installed and sensitive intellectual property intelligence was stolen over a prolonged period of time.

source: searchsecurity.com

What is the difference between 'remediation' and 'mitigation'?

'Remediation' of a vulnerability results in the flaw being removed and fixed permanently i.e. software update or patch. Patch management is increasingly automated by the Operating System and Product Developer – as long as you implement patches when released, then in-built vulnerabilities will be remediated.

As an example, the recently reported Operation Aurora, classified as an Advanced Persistent Threat or APT, was successful in infiltrating Google and Adobe. A vulnerability within Internet Explorer was used to plant malware on targeted users' PCs that allowed access to sensitive data. The remediation for this vulnerability is to 'fix' Internet Explorer using Microsoft released patches.

Vulnerability 'mitigation' via Configuration settings ensures vulnerabilities are disabled. Configuration-based vulnerabilities are no more or less potentially damaging than those needing to be remediated via a patch, although a securely configured device may well mitigate a program or OS-based threat.

The big problem with Configuration-based vulnerabilities is that they can be re-introduced at any time – just a few clicks are needed to change most configuration settings.

How often are new vulnerabilities discovered?

Unfortunately, all of the time! Worse still, often the only way that the global community discovers a vulnerability is after a hacker has discovered it and exploited it. It is only when the damage has been done and the hack traced back to its source that a preventative course of action can be formulated.

There are various centralized repositories of threats and vulnerabilities on the web such as the MITRE CCE lists http://cce.mitre.org/ and many security product vendors compile live threat reports or 'storm center' websites.

So all I need to do is to work through the checklist and then I am secure?

In theory, yes, but there are literally hundreds of known vulnerabilities for each platform and even in a small IT estate, the task of verifying the hardened status of each and every device is an almost impossible task to conduct manually.

Even if you automate the task by using a vulnerability scanning tool, you will still have work to do to mitigate and remediate vulnerabilities.

But this is only the first step. Let's consider a typical configuration vulnerability, for example, Windows Servers should have the Guest account disabled. We run a scan, identify a server where this vulnerability exists, so we mitigate the vulnerability by disabling the Guest Account. As a result, we have hardened this server.

However, if another user with Administrator rights then re-enables the Guest Account, the server will be left exposed. The only time you will identify that the server has been rendered vulnerable is when you next run a scan which may not be for another 3 or even 12 months.

There is another factor that hasn't yet been covered which is how do you protect systems from an internal threat – more on this later.

> *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 IT systems*
>
> *Phil Snell, CTO, NNT*

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.

File-Integrity Monitoring is a mandatory requirement for PCI DSS compliance.

What Do NNT Provide?

- Device Hardening Templates can be applied for all Security and 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

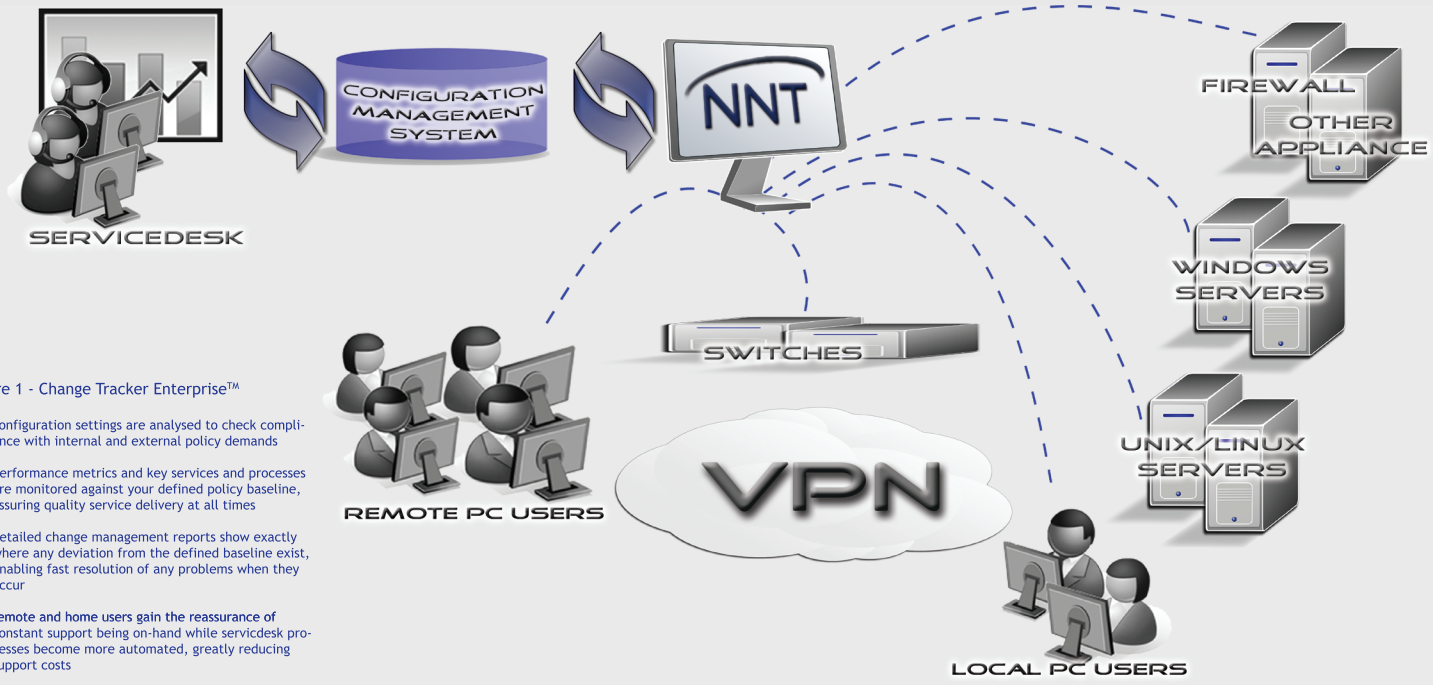

Figure 1 - Change Tracker Enterprise™

configuration settings are analysed to check compliance with internal and external policy demands

performance metrics and key services and processes are monitored against your defined policy baseline, assuring quality service delivery at all times

detailed change management reports show exactly where any deviation from the defined baseline exist, enabling fast resolution of any problems when they occur

remote and home users gain the reassurance of constant support being on-hand while servicdesk processes become more automated, greatly reducing support costs

Conclusion - The NNT View

Device hardening is an essential discipline for any organization serious about security. Furthermore, if your organization is subject to any corporate governance or formal security standard, such as PCI DSS, SOX, GLBA, HIPAA, NERC CIP, ISO 27K, GCSx Co Co, then device hardening will be a mandatory requirement.

- servers, workstations and network devices need to be hardened via a combination of configuration settings and software patch deployment
- changes to a device may adversely affect its hardened state and render your organization exposed to security threats
- file-integrity monitoring must also be employed to mitigate 'zero-day' threats and the threat from the 'inside man'
- vulnerability checklists will change regularly as new threats are identified

NNT can help – Change Tracker and Log Tracker Enterprise solutions will provide continuous configuration auditing, ensuring that any change to the hardened state of a device will be identified clearly and simply. NNT solutions provide

- configuration hardening
- change management
- centralized event log correlation
- file integrity monitoring

NNT Change Tracker and Log Tracker Enterprise - Compliance Clarified

- Audit Configuration Settings - The core function of NNT Change Tracker Enterprise is to first understand how your IT estate is configured
- Compare Audited Settings Against Policy - Configuration settings are assessed for compliance with any policy or standard relevant to your organization and deviations highlighted
- Continuously Monitor Configuration Settings - Configuration attributes are then monitored continuously for all changes, both from a compliance standpoint and from a general change management/control standpoint
- Change Management Process Underpinned - Authorized changes approved via the formal change management process are reconciled with the original RFC to ensure the correct changes were implemented accurately
- The Change Management 'Safety Net' - All unplanned changes are flagged up for review immediately to mitigate security vulnerabilities or service delivery performance degradation
- SIEM Event Log Correlation - Centralize and correlate event logs messages from all windows, unix/linux, firewall and IPS systems

For more details, or to arrange a free trial of NNT Change Tracker please contact us

About NNT

NNT build the world's best solutions for tracking and managing change, managing and protecting users, maintaining system performance and ensuring availability across the entire enterprise.

Understanding and managing the day to day changes within your environment is critical to establishing and maintaining reliable service. NNT Solutions are affordable and easy to use.

NNT help you establish and maintain a 'known and compliant' state for your IT systems. Including: PC, Network, Software, Host Machine and Database.

www.nntws.com