

**"Highest Performance
Lowest Price"**

Microsoft
GOLD CERTIFIED
Partner

GFI WHITE PAPER

Automating vulnerability management for PCI DSS compliance

A practical approach to network security and PCI DSS compliance

This white paper identifies the problems encountered in addressing network security risks through vulnerability management. It describes how automated vulnerability management contributes to compliance with industry standards such as the Payment Card Industry Data Security Standard (PCI DSS) and assists you in proactively identifying security weaknesses before these are exploited.



Sign up to GFI's FREE SMB-Zone Newsletter

Receive FREE invites to SMB focused content such as IT Advice,
Topical White Papers, MVP Tips and Tricks, Webcasts and much more!



Automated event log management for PCI DSS compliance

Introduction

Vulnerability management is a risk management discipline that addresses the dangers of e-commerce and information systems. It can be defined as the regular auditing of hardware and software components in IT infrastructures, the discovery of weaknesses and their resolution. Considered by many IT Professionals as a complex and time consuming process, vulnerability management is one of the most loathed and neglected tasks in their charges.

Network vulnerability management is however not an option anymore: Industry standards such as the PCI DSS, consistently underline the importance of managing network vulnerabilities and mandate it as an obligatory task in the compliance processes.

This paper addresses the need for effective network vulnerability management. It describes the aches and pains normally associated with this process and sheds light on how automation can assist IT professionals in mastering this discipline, reduce costs and augment PCI DSS compliance efforts.

- Introduction..... 2
- What is PCI DSS?..... 2
- New trends: Dynamic Zombie botnets..... 3
- What is network vulnerability management? 3
- What is the connection between PCI DSS and vulnerability management? 4
- The aches and pains of vulnerability management..... 5
- GFI LANguard..... 6
- Conclusion 6
- About GFI..... 6

What is PCI DSS?

Until a PCI DSS is a binding collection of rules that promote IT security processes in organizations that handle payment card information. PCI DSS aims to reduce financial fraud through heightened network security capabilities of whoever processes payment card information, and was designed because of three distinct factors that fuel financial fraud:

- E-commerce, which helps overcome geographical boundaries and, often, any protection offered by local laws and regulations.
- The high availability of “plastic money” for consumer purchases in all industrialized nations.
- An indifference to security best practices by all businesses that store and/or process unprotected payment card details.



Automated event log management for PCI DSS compliance

To counter credit/debit card fraud, the 5 major card companies (Visa International, MasterCard Worldwide, American Express, JCB and Discover Financial Services) designed a strong security framework to reinforce payment card transaction security. The result of their efforts was the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS compliance is the irrefutable responsibility of all businesses handling cardholder data including retail, mail orders, telephone orders and e-commerce – irrespective of business size.

New trends: Dynamic Zombie botnets

Botnets can be defined as networks of compromised computers which can be controlled by a single master. The number of nodes (also known as zombies) of these botnets can run into millions and these machines make use of different software vulnerabilities to gain full access to the infected hosts and add it to their existing array of zombies. Computer hackers had long been using botnets to launch DoS (denial of service) attacks and distribute network hacking attacks. Computer criminals had also been using botnets for money-making schemes, such as stealing credit card information and scamming pay-per-click advertising companies.

Seeing huge potential in botnets, spammers started financing hackers to make use of zombie machines. Hackers were able to offer services such as renting of botnets for a few minutes or hours and collections of email recipients (spam lists). The anti-virus industry noticed correlations between the spam industry and botnets. Not only were malware writers allowing spammers to make use of their creations, but they were writing malicious code to specifically suit their needs. An unholy alliance had been created.

What is network vulnerability management?

Security weaknesses lead to a continuous stream of security updates being issued by the developers of software solutions on a periodical basis. Due to the frequency and the amount of security updates released, systems administrators find it an arduous task to stay on top of this demanding process. This neglect enables hackers to exploit un-patched systems and launch network attacks most commonly through worms and viruses. One such notorious case is the Mytob worm and its derivatives. Notwithstanding the fact that Mytob spreads using known vulnerabilities for which a fix has existed since August 2004, this worm is still active to date and firmly holds the seventh position in the April 2007 top twenty virus list (Viruslist.com, [Virus Top 20 for April 2007](#)).

Targeted attacks are also an ever-increasing threat to business continuity which systems administrators must factor in their defense strategy. Malicious individuals who know of missing security updates within an organization's infrastructure can exploit such weaknesses through malicious software that enables them to gain access to networks. Such targeted attacks are often not noticed until long after these have happened and the repercussions of such attacks are already being felt.

The term 'network security' is often misinterpreted as pertaining exclusively to missing patches and security updates. Network security goes way beyond that however – for there are a multitude of attack vectors and weaknesses that must be taken in account. Lack of due diligence efforts and human error are security weaknesses in themselves and can be the direct cause of severe security breaches. This raises questions like: Why, despite all the breaches and threats that afflict networks, do systems administrators leave services running on default vendor passwords? Why, despite the fact that updated anti-malware solutions are the key to network wide protection, don't IT professionals update anti-virus and anti-malware solutions with the latest signatures? Why do companies allow the uncontrolled use of portable devices on their networks? Don't they know that these can be used maliciously to take out sensitive corporate data or bring in and install peer-to-peer (P2P) applications to smuggle pirated music, download unlicensed software and other unacceptable files on



Automated event log management for PCI DSS compliance

the network? All this leads to disruptions in day-to-day business activities and exposes companies to extensive legal liabilities.

Vulnerability management is the process that identifies all of these issues; a self-assessment exercise that identifies, categorizes and provides ways and means to resolve these weaknesses, while tackling security from various angles and attack vectors. It is blatantly clear that this is an essential part of any network security due diligence process and therefore it comes as no surprise that the Payment Card Industry Security Standards Council ingrained vulnerability management as an integral part of the PCI DSS compliancy requirements

What is the connection between PCI DSS and vulnerability management?

Through PCI DSS, the addressed issue of security is defined as being only as strong as its weakest link. The general idea governing PCI DSS aims to:

- Build and maintain a secure network
- Protect cardholder data in transit or at rest
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test your IT infrastructure
- Maintain an information security policy.

In order to achieve these principles, PCI DSS defines 12 requirements. Systems administrators have to fulfill them and demonstrate their efforts in fulfilling them. Requirement 1 for example, specifies that firewalls must be installed and maintained to protect cardholder data from outsider attacks. To fulfill it, IT professionals have to scan their networks, validate firewall setup and ensure that configuration settings do not compromise network security. Requirement 6 on the other hand defines the development and maintenance of secure systems and applications – a vulnerability management activity which entails ensuring that all network components are updated with the latest vendor-supplied security patches.

Vulnerability management however extends to all 12 PCI DSS requirements range; it goes beyond network security mechanisms and reaches to all IT infrastructure components and environments where payment card data is stored, processed or transmitted. This includes:

- Core network-security components such as firewalls, routers, Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS)
- Network segments such as Demilitarized zones (DMZ)
- Servers and business systems hosting DNS services, NTP services, SMTP/POP3/IMAP and other email services, authentication handling, Active Directory policies, web servers and database servers amongst others
- Internal or web-facing applications including off-the-shelf and custom-built software.



Automated event log management for PCI DSS compliance

- A completely in-house solution
- A hosted solution in which the archive is maintained at a third party's data center.

The aches and pains of vulnerability management

Failing to implement strong vulnerability management methods on all the above-listed components puts corporations in breach of PCI DSS and exposes them to security threats from both outside and inside the corporation. The repercussions from damage arising through such breaches are not only limited to PCI DSS. Corporations can fall foul of local or national laws and regulations such as those set up and imposed by the Federal Trade Commission or their local equivalents. These often result in fines and legal proceedings over and above those imposed by PCI DSS!

Notwithstanding it being a mandatory process, IT professionals often find vulnerability management a daunting, repetitive task prone to human error. All hardware and software components on a corporate network have to be scanned; the information gathered into a central repository, consolidated, understood and acted upon. To fulfill this charge, automation is the key that enables IT professionals to overcome challenges such as the following.

Challenge 1 – Thousands of checks on each and every computer:

The notorious **TJX breach** which was made public earlier this year makes the case for vulnerability management. According to Gartner's Vice President and Senior Fellow John Pescatore, the network security weaknesses that led to the exposure of over 45 million credit and debit card records could have easily been detected through a network vulnerability scan ([SCMagazine.com](#)). Organized crime does not target only big companies. Speaking at an IT security event at London's House of Lords on November 2006, former White House security adviser Howard Schmidt urged that "Small and mid-sized enterprises have to realize that just because they are small, it doesn't mean they won't be targeted. Bad guys target wherever they can get money" ([CNET News.com](#)). In February 4, 2007, the web site of Johnny's Selected Seeds (a relatively small 100 employee seed company in Winslow, Maine, US) was hacked by an intruder and over 11,500 credit/debit card records were electronically stolen ([MaineToday.com](#)). Apparently, the breach was noticed on February 18, when two customers called the company claiming that their credit cards had been compromised with fraudulent charges. Automating network vulnerability scans bolsters consistency, reduces human error, simplifies the identification of network weaknesses and keeps you ahead of threats.

Challenge 2 – Too much information on too many computers: In March 2007, nearly 9 million pieces of sensitive customer records were stolen from Dai Nippon Printing Co, by a sub-contracted worker ([DarkReading.com](#)). This information, which included credit card numbers, was taken out of the company using portable storage media. Scanning routines have to include whatever dangerous instances lie outside of published vulnerability definitions. State of the art vulnerability management solutions provide extensive network auditing capabilities that enumerate rogue hardware and software which could be potential hazard to network indemnity – information that is otherwise not readily available.

Challenge 3 – Patch management is a hit or miss affair: With the number of critical security updates released by Microsoft alone reaching the 104 mark in 2006, systems administrators have good reasons to feel overwhelmed with patch management! Through automated patch management solutions corporations can ensure that missing patches are automatically downloaded in a timely fashion. Not only can patches be automatically deployed/ "pushed" to target computers, they can also be rolled back to bring stability to the IT infrastructure if the need arises.



Automated event log management for PCI DSS compliance

Challenge 4 – Default vulnerability management tools are limited: A case in point is Microsoft Windows Server Update Services (WSUS); a solution that handles the download of missing Microsoft updates without any support for vulnerability scanning, network auditing and reporting operations. This creates an additional challenge, which administrators must overcome – the correlation of results. In the case of separate specialized solutions, administrators must also make sense out of vulnerability scan results, network audit results and patch management information by manually correlating them. Additionally, in most cases, reporting is limited and therefore the administrator would need to waste more time compiling reports manually – often through a cut and paste operation.

Challenge 5 – Complying with standards is an arduous process: The only way to achieve compliance is through extensive reporting that lays out how vulnerability management is performed and provides tangible proof of compliance. Problems arise with the amount of reporting required and in the archival of such data. Once again, automation facilitates the life of systems administrators through the provision of features that enable scheduled report generation and automated distribution – reinforcing compliancy efforts and saving time, which is as precious as money!

Overcoming all the challenges through automation is one facet of the complete solution. Other features, such as a comprehensive and authoritative vulnerability definition database and an ability to consolidate different tasks in a single product also assist systems administrators in identifying even more weaknesses thus keeping the corporate network security in perfect shape. Systems administrators require tools that not only automate but also integrate vulnerability management within their daily process with the least invasive procedures possible; a solution such as GFI LANguard Network Security Scanner.

GFI LANguard

GFI LANguard is an award winning, OVAL certified solution that detects, assesses, reports and rectifies vulnerabilities present on the network. From within a single solution it provides vulnerability scanning and auditing of heterogeneous networks, fully-fledged patch management capabilities as well as unsurpassed reporting features through a dedicated ReportPack.

A version of GFI LANguard specifically customized for PCI DSS compliance is also included within the GFI PCI Suite. This suite also includes GFI EventsManager, an event log management solution, together with a package of tailor-made reports. For more information about GFI LANguard and the GFI PCI Suite, and how these products assist your business to achieve PCI DSS compliance visit: <http://www.gfi.com/pci/>.

Conclusion

Today's IT professionals cannot abscond from vulnerability management duties; these are ingrained in both due diligence efforts and PCI DSS compliance obligation. In the past, monitoring for network vulnerabilities was an arduous task for any network administrator. Today, solutions such as GFI LANguard introduce automation features that assist IT professionals in fulfilling critically important network vulnerability scanning with the least possible effort, whilst reducing costs and the likelihood of human error.

About GFI

GFI is a leading software developer that provides a single source for network administrators to address their network security, content security and messaging needs. With award-winning technology, an aggressive pricing strategy and a strong focus on small-to-medium sized businesses, GFI is able to satisfy the need for business continuity and productivity encountered by organizations on a global scale. Founded in 1992, GFI has



Automated event log management for PCI DSS compliance

offices in Malta, London, Raleigh, Hong Kong, and Adelaide which support more than 200,000 installations worldwide. GFI is a channel-focused company with over 10,000 partners throughout the world. GFI is also a Microsoft Gold Certified Partner. More information about GFI can be found at <http://www.gfi.com>.



Sign up to GFI's FREE SMB-Zone Newsletter

Receive FREE invites to SMB focused content such as IT Advice,
Topical White Papers, MVP Tips and Tricks, Webcasts and much more!

© 2009 GFI Software. All rights reserved. The information contained in this document represents the current view of GFI on the issues discussed as of the date of publication. Because GFI must respond to changing market conditions, it should not be interpreted to be a commitment on the part of GFI, and GFI cannot guarantee the accuracy of any information presented after the date of publication. This White Paper is for informational purposes only. GFI MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor and their product logos are either registered trademarks or trademarks of GFI Software Ltd. in the United States and/or other countries. All product or company names mentioned herein may be the trademarks of their respective owners.