File Integrity Monitoring
Challenges and Solutions

Introduction (TOC page)

A key component to any information security program is awareness of data breaches, and yet every day, hackers are using malware to gain access to corporate records…undetected. The impact is significant, as illustrated in the case of Heartland Payment Systems, which lost $300 million in market capitalization and $30 million in direct costs when the breach of approximately 100 million credit card accounts went undetected for 18 months.

This whitepaper discusses the importance of file integrity monitoring, which facilitates the detection of malware as well as insider threats, utilizing Heartland as a case study. It also discusses file integrity monitoring as a critical component of PCI-DSS compliance, and shows how NetIQ addresses both security and PCI compliance challenges through its Change Guardian products.

Introduction

If there was ever an era where the saying “you can’t be too careful” rings true, it’s this one. Every year, despite growing awareness and implementation of protective security measures, data breaches are hitting the headlines more and more. The numbers are scary: 285 million records were compromised in 2008. Even more frightening is the fact that that these breaches are happening right under the noses of information security managers, as evidenced by cases such as Heartland Payment Systems, where a breach of approximately 100 million credit card accounts went unrecognized for 18 months.

One of the critical questions that must be answered, in order to solve this problem, is “why?” Why are these breaches going undetected? What can be done to maintain the kind of surveillance required to identify and stop these attacks before they are able to cause insurmountable damage? One of the most effective solutions is to implement file integrity monitoring.

File Integrity Monitoring: A Critical Piece in the Security Puzzle

File integrity monitoring (FIM) is an important component of any effective integrated information security program. By detecting unmanaged access and changes to system files, it reduces the risk of:

- Data breaches – from insiders, privileged users, and attacks using malware
- System instability – caused by unplanned or unauthorized changes to system configuration
- Poor performance – often caused by changes outside of managed change control processes
- Compliance failure – resulting from an inability to demonstrate due care and a lack of capability to monitor access to sensitive data

It has become even more of a critical piece in the security picture as data breaches using custom malware have increased. According to a 2009 Data Breach Investigations Report by Verizon Business, the most successful data breaches have been those in which attackers exploited some mistake committed by the victim, hacked into the network, and installed malware on a system to collect data. The use of custom malware in these attacks, which was used in the Heartland breach as well as other major credit card breaches, more than doubled in 2008.

Because custom malware successfully bypasses basic anti-malware controls, it frequently goes undetected. According to Forrester Research, the best way to reduce the risk of breach from this type of attack is to deploy file integrity monitoring tools to provide immediate alerts if unauthorized software, such as custom malware, is being installed.

In addition to serving as a safeguard against security breaches, the Payment Card Industry Data Security Standard (PCI-DSS) specifically calls for the deployment of file-integrity monitoring software in order to alert personnel to unauthorized modification of critical system files, configuration files, or content files. It is not surprising that this mandate is starting to be enforced: According to Verizon Business, over 80% of data breach victims surveyed in its 2009 Data Breach Investigations Report were not compliant with PCI-DSS.

Analysis of a $300 Million Loss

Of all the security breaches in the past decade, the most famous is that of Heartland Payment Systems. The magnitude of the breach was immense: security experts estimate that 100 million credit cards issued by 650 financial services companies may have been compromised. The financial impact has been earth-shattering: a $300 million loss in market capitalization and over $30 million in direct losses. But those statistics alone are not what have the information security world rocked. It's the fact that the breach went undetected for 18 months, and even then it was not discovered by Heartland's internal security team.

So the question is: How did this happen? How can a hacker gain access to millions of records and still go undetected? The answer, in this case, is malware.

According to the Department of Justice indictment of the Heartland hacker Albert Gonzalez, "On or about November 6, 2007, GONZALEZ transferred a computer file to the Ukrainian Server named 'injector.exe' that matched malware placed on both Heartland and Company A's servers during the hacks of those companies."

Figure 1 (*anatomy of a custom malware attack* - source – Forrester Research), illustrates how a custom malware attack, such as the one orchestrated against Heartland, is played out.

(insert illustration)

First, a hacker exploits a vulnerable server on the credit card processor's cardholder data network (CHDN) and installs a data sniffer, which may remain dormant in the system for weeks or months before the actual attack takes place. It is not detected by anti-malware because it has been custom designed with a unique signature that is not recognized by the security software, which operates using the signatures of known viruses, worms and Trojans.

Once the hacker is ready to move, the sniffer is fired up. The store sends credit card information for processing to the credit card switch, which then transfers credit card information to the processor. At this point, the malware sniffs traffic destined for the encryption appliance and the hacker is then able to retrieve packet captures from the malware and retrieve the credit card information.

If the breach is detected at all, it is usually through back-end monitoring by credit card companies through a technique known as Common Point of Purchase (CPP), which is typically used to triangulate fraud. By this time, the damage is done. Such was the case with Heartland, whose credit card brands sounded the breach alert…18 months after the intrusion actually occurred.

Stopping Malware in its Tracks

The easiest way to see why file integrity monitoring is so critical in the prevention of data breaches through custom malware attacks is by looking at a timeline of events leading up to and following a data breach. In its 2009 Data Breach Investigations Report, Verizon Business found that in just under half of their cases in 2009, there was at least some indication of pre-attack research, most often in the form of system footprinting, scanning and enumeration. After breaching the perimeter, almost 50% of hackers were able to compromise the system in a matter of minutes or hours. Conversely, it took victims weeks and even months to discover the breaches in about 75% of cases. In the vast majority of cases, breaches were discovered by a third party, not by internal security staff.

The speed with which systems and files are compromised, once the perimeter is breached, underscores the importance of a solid FIM solution. FIM allows enterprises to track deviations from their "golden image" approved software builds and file system structures. In the case of system files on business-critical systems or sensitive data files, real-time alerts for changes can be set, enabling the immediate recognition of a problem that can then be analyzed and responded to.

By using FIM, the modification of files, caused by the custom malware installation, would immediately trigger an alert. This change could then be investigated and the malicious software removed immediately, rather than remaining in the system while the hacker prepares for his attack. If the malware were deployed immediately, the real-time alert to file changes would enable a security time to significantly cut the response time and contain any damages incurred.

A Case for Corporate Compliance: PCI DSS

If security weren't a big enough issue, compliance is another reason for file integrity monitoring. The Payment Card Industry (PCI) Data Security Standard (DSS) is a contractual requirement for businesses that handle cardholder information for Visa, MasterCard, Discover, American Express and Diner's Club. The PCI-DSS specifies FIM primarily in Requirement 11.5:

> "Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly."

The intent of PCI 11.5 is to give companies a solid defense against the exploitation of critical resources within the CHDN, especially servers. For companies to ensure the protection of critical systems, they must know and be able to document changes to files and file systems, including:

- Who made the change
- What exactly was changed – files, registry or configuration settings
- When it was changes
- What the value was before the change
- What the value was after the change
- If this change was authorized as part of the change management process

PCI requirements 10 and 12 also encompass FIM, mandating inclusion of FIM alerts into policy. PCI-DSS 10 mandates file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts. It also requires that companies review logs for all system components at least daily in order to demonstrate knowledge of what is occurring within the system and to discover any anomalous activity. PCI-DSS 12 specifically includes file-integrity monitoring systems in its mandate for incident response policies to include provisions for monitoring and responding to alerts.

Managing FIM for Maximum Security:
Change Guardian from NetIQ

Whether the concern is a crippling malware attack or an insider threat, reducing risk to sensitive data and vital infrastructure is critical. The greatest threat comes from unmanaged changes to files and systems that weaken enterprise security and leave systems vulnerable.

NetIQ Change Guardian products provide real-time detection of unmanaged changes to files, system configurations, and Active Directory, to ensure your security teams can proactively protect sensitive corporate information and customer data both from malicious attacks or accidental damage. They provide the information necessary to make intelligent decisions, fast, to limit the risk of corporate data loss and maximize the return on your existing security investments.

NetIQ's real-time file integrity monitoring approach is to:

- Provide real-time detection of changes to files
- Enable alerting even if the content was simply viewed and not changed
- Integrate that alerting into leading SIEM solutions such as NetIQ Security manager
- Ensure the alerting process provides rich information such as when the change was made, who made the change, what was changed, and what the state was before the change
- Detect changes on your most important platforms: Microsoft Windows, Active Directory (including Group Policy objects), Unix and Linux.

For period assessment of less critical files, NetIQ's approach is to present configuration information and system baselines that enable administrators and security teams to easily identify which files have been changed and when. This places the changes in the context of broader systems configuration and compliance assessments.

The approaches are complementary, and can both be easily integrated into broader security and compliance management programs to enable correlation and analysis of file and systems changes within the broader security landscape.

In all cases, further integration with organizational ticketing systems provides a key check to automate the identification of unauthorized changes. It also offers the ability to provide automated remediation, or remediation tracking, to ensure that potentially damaging changes are rolled back.

Working Together: Change Guardian and NetIQ Security and Compliance Solutions

Unmanaged change to the configuration of critical systems and infrastructure represents a significant and growing risk to the security of organizational data, customer information and system stability. NetIQ Change Guardian enhances your ability to detect any unmanaged changes and respond efficiently to vastly reduce the risk of malicious activity and to support comprehensive data protection.

Beyond simple file integrity monitoring lies the much broader problem of system integrity monitoring. While it is essential to identify unmanaged changes to files, such monitoring must be part of a broader security and compliance management program.

NetIQ provides an integrated solution that enables security teams to build a more complete security and compliance infrastructure that is scalable and reduces workload. NetIQ Change Guardian works in conjunction with NetIQ Aegis for security workflow automation and NetIQ Secure Configuration manager for compliance and entitlement reporting, to form a powerful, integrated, automated solution for security and compliance management. NetIQ Change Guardian also integrates tightly with security information and event management (SIEM) solutions such as the award-winning NetIQ Security Manager in order to present correlated, rich and relevant information to security and compliance teams. Together, these products help companies not only protect their data, but also comply with important regulatory mandates such as those in PCI-DSS.

As a result of this tight integration, security teams can identify immediately when a system housing critical data is altered in order to stop a custom malware attack. They can equally quickly correlate such changes with changes to Active Directory or Group Policy that might indicate that a privileged user is the source of an insider attack.

Conclusion

Cases such as Heartland illustrate the critical importance of properly deploying a FIM solution, in order not to be caught unaware of the installation of malicious software. FIM could have foiled some of the most noteworthy breaches in recent memory. FIM is also an important component of PCI compliance, something that is sometimes overlooked. In order to effectively maintain both security and compliance, FIM software should also be integrated with SIEM solutions, in order to provide correlation with other security events and ensure that critical data and systems stay secure.

Our file integrity monitoring solution, NetIQ Change Guardian, provides you with real-time detection and alerting for changes to files and systems configurations for critical hosts. In addition to reducing the risk for data breaches and insider attacks, it provides the “who, what, when and how” for changes to Active Directory and Group Policy objects. Leveraged in conjunction with traditional SIEM solutions, this group of products provides a powerful and effective way to reduce time spent gathering information, accelerate decision making, and reduce the risk of breaches..

For more information on how to address your requirements for file integrity monitoring, and how to extend your monitoring to include full system integrity monitoring, visit www.netiq.com or call your local NetIQ representative or partner.