PRISM MICROSYSTEMS

The Top Ten Insider Threats and How to Prevent Them

The importance of consolidation, correlation, and detection
Enterprise Security Series

EventTracker
www.prismmicrosys.com

White Paper

8815 Centre Park Drive

Columbia MD 21045

877.333.1433

The Threat From Inside

In years past most attention in the security group was focused on preventing outsiders from gaining access to the corporate network. This remains a real and constant danger to companies as threats from malware and cyber-criminals become more powerful and sophisticated every day. Over the last couple of years however there has been an increasing focus on the threats posed by insiders – individuals who need and have access to critical data. The increasing dependence on automated systems and advancements in technology like small, cheap portable USB storage devices have given these individuals the ability to inflict massive damage if they so choose. Increasingly data has pointed to the fact that although insider threats are less in number, when they occur the damage is generally far greater.

With the slow economic recovery, companies have been forced to make painful reductions in staff, pay, and benefits leading to widespread worker dissatisfaction. This has led to an increase in the number of people for whom internal hacking and data theft is appealing, and has caused an explosion in malicious internal activity. According to a study conducted by KPMG insider data theft has tripled since 2007 and further research from the Ponemon Institute, a Tucson based research group, indicates that 60% of people that leave their jobs voluntarily or involuntarily take corporate data with them when they leave.

So what is the IT security group to do? Advances in technology have enabled massive advances in productivity making the business far more competitive, and these technology advancements have become part of the core business culture. But with the advancement has come increased risk. From devices that can enable personnel to quickly copy and remove gigabytes of data on a device the size of a person's little finger, to administrator privileges that enable trusted users to do practically anything,

and then almost completely disguise the record of their activity. The ability to inflict great harm is certainly present and requires internal security staff to be ever more vigilant on both - the signs of insider abuse and the compromising of security processes that can open easy avenues to make insider abuse possible.

Prism Microsystems, a leading Security Information and Event Management (SIEM) vendor has developed a number of best practices to monitor for indications of insider abuse, as well as activities that can open the gates to insider abuse. This monitoring, although helped by SIEM technology can be accomplished in large part by simple review and manual detection.

Data Leakage Enabled By USB Devices

The proliferation of writeable media devices such as USB thumb drives and CD/DVD-W has created security challenges in private networks — In fact, much of the more serious theft of organizations' data today is from internal sources, and a very convenient and efficient way to accomplish this is by utilizing these devices to copy confidential data. This often takes a few seconds, and since it can be easily done from a desktop, physically limiting access to the servers is not a complete solution. So the question becomes, how does an organization protect itself against data leakage from such endpoints and internal threats, such as maliciously infecting the network with spyware and viruses borne on such media?

When it comes to data leakage threats, USB devices can be some of the hardest to detect. These devices have become so widespread and small enough that physical detection has become impractical and harder if not impossible, so we must rely on software or Group Policy to help govern their usage. Going to extreme measures to stop these devices is not feasible (e.g. super glue in USB slots). The use of flash drives is not a harmful act; it's what happens to the data that causes the problem.

Recent press articles report that in many cases data leakage was accidental, caused by devices being lost or stolen. In these cases employees were simply trying to be productive and work from home when the devices came up missing. There are other articles that show how data leakage can be malicious in nature such as trade secrets being disclosed to rival companies or patients being harmed by the leak of confidential medical records to the public, just to name a couple. When a user decides that they wish to harm a company by taking sensitive information off-premises, there is little that System Administrators can do. USB devices can be hidden anywhere and can hold large amounts of data. Restricting their usage will help stop unauthorized users from copying company data.

With the use of a SIEM and log management solution such as EventTracker, you have the ability to not only detect these flash drives, but also disable them while leaving other USB devices active. Another benefit is that you have the ability to track data written to, deleted from, modified or copied on to these drives. It is critical to not only monitor USB flash drive usage on your servers but also at the workstation level since most cases of data leakage via USB devices come from users who do not have direct access to servers.

With this simple remedy in place companies can save themselves public embarrassment, the loss of trade secrets, customer data, customer confidence as well as financial losses.

Hijacking the Local Administrators Group

Most System Administrators keep a close eye on who is in their Active Directory Domain Administrator group, but what about the local Administrator group on each Windows system? Most of the time, the local group is ignored. When a user is in the local Administrator group on a system they are effectively a super user and have complete rights to do anything on that system. Once Administrators discover that there has been a change to the local Administrator group on a system it's often too late and the damage may have already been done.

Like with other items being discussed in this whitepaper, there is malicious intent and non-malicious intent. A harmless example is the savvy user who wants to defrag their machine to try to speed things up. Administrator rights are needed, so this user gets added to the local Administrator group so they can run defrag instead of someone from the IT department. A malicious act would be a user convincing IT to let them have admin rights so they can "defrag my machine" but then use those rights to install root-kits, hacking tools, etc. Sometimes users are added to the local Administrator group even though it is against company policy. Adding users to this group is also a favorite attack point for hackers, both inside and outside the organization.

Monitoring when a user is added to a local Administrator group can save companies a lot of time and money. Turning on the correct audit policy and pushing the policy down to the workstation level, while using a log management solution, will ensure that you know of these changes when they happen. Alerts that watch for changes to the Administrator group will let IT staff know immediately when these types of changes take place.

Hijacking the Domain Admins Group

Most companies have written policies about who can be in the Domain Admins group and have turned on the correct auditing (Audit Account Management), but most System Administrators do not check event logs to make sure a violation of policy has not occurred.

When someone gains access to the Domain Admins group they essentially have "the keys to the castle". In the previous example, a user with local Admin rights wreaked havoc on a single system. In this example they can wreak havoc on the entire enterprise. Keeping tight control over this group is vital and knowing in real time about any change (add or delete) to this group is a must.

A single malicious change using Domain Admin privileges can stop users from being able to complete their daily work or allow others to gain access to sensitive data. The wrong system being shutdown during critical parts of the day can cause problems for System Administrators as well as the company.

What can be done to counteract these changes? Having an event log monitoring solution will allow you to set alerts so that you can watch for these events and remedy the situation before costly damage is caused

Unauthorized Application Install

Unauthorized applications can open systems to attack, remote control, etc. Each application installed can have different effects on system performance. Older versions of software can contain security holes, memory leaks or other unknown risks. Leaving

these applications unchecked can pose problems for System Administrators, Developers and users.

Windows does not generate events when applications are installed, but if an application needs a service to run you can track when these services are created. This by no means catches everything. Object Access auditing will miss these installs when not setup correctly and moreover, can result in a high volume of events written to the event logs. Turning on full auditing is not recommended because of the enormous amount of noise events that will be generated.

Unauthorized Application Usage

The use of unauthorized applications can lead to many problems such as the use of unlicensed software, outdated versions or malicious programs that open up security holes. Not all programs require an install and tools used by hackers to infiltrate systems are especially likely not to require an install. Tracking software usage is crucial to augment tracking for software installation.

You can turn on Audit Process Tracking through the Audit Policy to watch for the usage of any application. This can result, however, in a large volume of events generated and will require an Administrator to check the event log and manually correlate the "Process Created" and "Process Ended" events to determine how long the application was used. This can be a laborious task.

With a SIEM and log management solution, Administrators have the ability to monitor application usage without the use of Windows Audit Policy and see applications used and the length of time they were used for.

Unauthorized Deletion of Corporate Data

File deletes can cause serious problems for companies in many obvious ways. The only way to truly recover from either a malicious or inadvertent case is with the use of timely and correct backups. It is critically important to prevent further unauthorized deletions by determining the culprit responsible for the deletion, The only way to accomplish this is by being able to determine who, how and when these files were deleted.

Without auditing there is no way of answering any of these questions. Object Access Auditing on key files and folders is crucial. It should be noted that it is not advisable to choose Full Control as this can lead to an influx of events that can be very confusing.

By the time someone figures out that files are missing it's already too late. But if you have the correct auditing turned on AND you are monitoring your event logs you can detect when an excessive amount of deletes occur. Now the question becomes what is excessive? Just by looking at the logs how do you know when this excessive threshold has been met? Is this threshold based on the enterprise as a whole, or on each system or user? And how often are the logs being reviewed for these conditions?

This is where real time alerting can help. Utilizing event correlation, as a part of the SIEM and log management solution allows policies such as excessive deletion thresholds to be set as rules and programmatically monitored for in real time. Real time alerting enables instant notification which can often prevent more widespread data loss.

Abuse of the Administrator Account (local and domain)

Every Windows system and network has Administrator accounts which are prime targets for both inside and outside hackers. For preventing inside abuse the main problem is these are "general" accounts and often multiple people have access to them making it nearly impossible to determine the actual user. In many companies the use of these general accounts is prohibited by policy, however in all cases keeping a handle on the usage of these accounts is vital. Several Windows audit policies can be enabled to help you keep track of their usage including Audit Account Management, Audit Logon Events and Audit Account Logon Events.

There are elements in some of these events that can help track down what systems the use of the Administrator account originated from. But once again you need to be monitoring each and every log from ALL systems. Depending on the size of your organization this can be a daunting task.

With the use of the real time alerting capability of a SIEM and log management solution you can be alerted when anyone tries to log in with the Administrator account (either Local or Domain). By watching for logon events you can determine from which system the account is being used and whether it is the local Administrator account or the Domain Administrator account. Anyone who needs Administrator rights should not use these accounts but instead have their own account that has Administrator rights. This way you can track changes to the domain, systems and users.

Logon Failures from Administrator Account (local and domain)

As we discussed in the last section, monitoring logons from the Administrator account is important. Watching for logon failures from these accounts is just as important. These failure events can help to identify hack attempts before the intruder gains access to your systems.

With a log management solution you will be able to detect these failures from one central location very quickly, allowing you to take preventive action to keep intruders and threats at bay.

Unauthorized Access to Someone Else's Mailbox

When talking about data leakage one area that should not be overlooked is email. With employees using email to send vital company information back and forth, keeping sensitive information from getting into the wrong hands is difficult. Email scanning is often used to discourage such behavior however this still leaves the possibility of hijacking another user's email account to transmit documents. Because of this Microsoft has made changes to Exchange to help reduce the ability of System Administrators to add a user to someone else's Inbox on a widespread scale. But these changes can still be done on a one by one basis.

There are times when System Administrators will need to give a user or users access to someone else's Inbox for legitimate reasons. These are not the conditions that should cause concern, what you should be concerned with are times when these rights are granted without approval. Knowing what to track via your Audit Policy and using a log management solution can help you detect when someone has gained unauthorized access to another user's Inbox. By configuring an alert that notifies you when this condition is met, you will be able to proactively rectify the situation, instead of reacting after data has been leaked.

Excessive Resource Access Failures

Every corporate network has shared folders. Users need access to shared documents, spreadsheets and other data and as System Administrators we must create these shares and put in place security measures to control who has access and what type of access they have.

Turning on the correct Object Access Auditing can tell you not only when people are accessing these shares but also when unauthorized users are trying to gain access. Now we all know that users will inadvertently select the wrong network share from time to time. These are one-offs and not a problem. The real problem comes from repeated attempts by a user or several users trying to gain access to resources. Setting thresholds through your log management solution can help in detecting these excessive resource access failures.

A SIEM and log management solution with a Correlation Engine helps you watch for these thresholds, which can be set at the enterprise, system, user or resource level. You have the ability to configure an alert to notify the correct team member to react to the situation.

About EventTracker

EventTracker is a scalable, enterprise-class Security Information and Event Management (SIEM) solution for Windows systems, Syslog/Syslog NG (UNIX and many networking devices), SNMP V1/2, legacy systems, applications and databases. EventTracker enables "defense in depth", where log data is automatically collected, correlated and analyzed from the perimeter security devices down to the applications and databases. To prevent security breaches, Event Log data becomes most useful when interpreted in near real time and in context. Context is vitally important because often the critical indications of impending problems and security violations can only be learned by watching patterns of events across multiple systems. Complex rules can be run on the event stream to detect signs of such a breach. EventTracker also provides real-time alerting capability in the form of an email, page or SNMP message to proactively alert security personnel to an impending security breach.

The original log data is also securely stored in a highly compressed event repository for compliance purposes and later forensic analysis. For compliance, EventTracker provides a powerful reporting interface, scheduled or on-demand report generation, automated compliance workflows that prove to auditors that reports are being reviewed and many other features. With pre-built auditor grade reports included for most of the compliance standards (FISMA, HIPAA, SOX, GLBA, PCI, and more); EventTracker represents a compliance solution that is second to none. EventTracker also provides advanced forensic capability where all the stored logs can be quickly searched through a powerful Google-like search interface to perform quick problem determination.

EventTracker lets users completely meet the logging requirements specified in NIST SP 800-92 Guide To Computer Security Log Management, and additionally provides Host Based Intrusion Detection , Change Monitoring and USB activity tracking on Windows systems, all in an off the shelf, affordable, software solution.

EventTracker provides the following benefits

- A highly scalable, component-based architecture that consolidates all Windows, SNMP V1/V2, legacy platforms, Syslog received from routers, switches, firewalls, critical UNIX servers (Red Hat Linux, Solaris, AIX etc), Solaris BSM, workstations and various other SYSLOG generating devices.

- Automated archival mechanism that stores activities over an extended period to meet auditing requirements. The complete log is stored in a highly compressed (>90%), secured (Sealed with SHA-1 checksum) archive that is limited only by the amount of available disk storage.

- Real-time monitoring and parsing of all logs to analyze user activities such as logon failures and failed attempts to access restricted information.

- Alerting interface that generates custom alert actions via email, pager, console message, etc.

- Event correlation modules to constantly monitor for malicious hacking activity. In conjunction with alerts, this is used to inform network security officers and security administrators in real time. This helps minimize the impact of breaches.

- Various types of network activity reports, which can be scheduled or generated as required for any investigation or meeting audit compliances.

- Host-based Intrusion Detection (HIDS).

- Role-based, secure event and reporting console for data analysis.

- Change Monitoring on Windows machines

- USB Tracking, including restricted use, insert/removal recording, and a complete audit trail of all files copied to the removable device.

- Built-in compliance workflows to allow inspection and annotation of the generated reports.

About Prism Microsystems

Prism Microsystems, Inc. delivers business-critical solutions to consolidate, correlate and detect changes that could impact the performance, availability and security of your IT infrastructure. With a proven history of innovation and leadership, Prism provides easy-to-deploy products and solutions for integrated Security Management, Change Management and Intrusion Detection. EventTracker, Prism's market leading enterprise log management solution, enables commercial enterprises, educational institutions and government organizations to increase the security of their environments and reduce risk to their enterprise. Customers span multiple sectors including financial, communications, scientific, healthcare, banking and consulting.

Prism Microsystems was formed in 1999 and is a privately held corporation with corporate headquarters in the Baltimore-Washington high tech corridor. Research and development facilities are located in both Maryland and India. These facilities have been independently appraised in accordance with the Software Engineering Institute's Appraisal Framework, and were deemed to meet the goals of SEI Level 3 for CMM.

For additional information, please visit http://www.prismmicrosys.com/.