

Log Analysis vs. Insider Attacks

By Anton Chuvakin

This article covers using log and audit trail analysis to detect and investigate insider attacks and abuse.

You have a firewall in place, right? Even an Intrusion Detection System? Your security policy is nicely written and posted all over the company. You accept the fact that nobody is totally safe, but you think you can manage risks successfully. Can your engineers access payroll records if they really want to? Can your system administrator encrypt the access control data and hold the company hostage after being fired? These and other question point us towards insider attacks and abuse.

As widely believed, insider threats account for up to 70% of the information security-related incidents. Most information security losses are due to theft of proprietary or customer information, the task most likely performed by insiders. Surveys over the past few years have demonstrated that the average damage from an outside intrusion was \$60,000, while losses caused by the average insider attack exceeded \$2.7 million. Companies were known to go bankrupt due to the theft of their source code or lose business due to mayhem caused by ex-employees. Moreover, this trend will continue as more critical information is created and used in digital form.

So, what exactly is this dreaded “threat from within”? Internal risks cover a wide variety of human and computer factors that threaten the IT environment.

Types of insider threats

An “insider” is typically an employee, contractor, business partner or anybody who has legitimate access to company resources, all the way down to physical access to the outside of the building’s loading dock.

Insiders can violate any of the three “letters” from the information security triad - CIA: *Confidentiality, Integrity and Availability*. Examples might include theft or disclosure of proprietary information (violates confidentiality), unauthorized modification of company data (breaks data integrity),

and denial of service attack or destruction of company information assets (undermines availability). Attacks can be motivated by a wide array of reasons, both rational (money, status, power) and irrational (revenge, frustration, emotional pain, personal problems).

We can, however arbitrary it might sound, classify insiders by their intent into malicious and non-malicious insiders. Malicious insiders might want to eavesdrop on private communication, steal or damage data, use information in a violation of company policy or deny access to other authorized users. They can be motivated by greed, need for recognition, sabotage (both for hire and to improve their standing at the expense of others), desire to make themselves irreplaceable for the job (by creating problems only they can fix), revenge or other intense negative emotional state. Unstable emotional states in IT employees is a new popular subject among psychologists. This research might eventually shed some light on how insider threats originate. Disgruntled employee is a favorite character in the inside threats game. His or her game is to “undo” the “wrongs” done to them by the company or a particular employee by causing damage to them or even to extract financial benefits at the expense of those parties.

Non-malicious insiders are users making mistakes that compromise security. Users motivated by their desire to “explore” the company network or to “improve” how things work with blatant disregard to security regulations are also in this category. Having no malicious intent, they can still present a serious danger to the enterprise since they can open a way for outside attackers, erroneously destroy information or otherwise degrade integrity and availability of computing resources. Another category of non-malicious insiders would be an insider operating under control of a malicious outsider, such as a hacker using social engineering, blackmail or threat of violence. Many hackers claim that they only rarely had to resort to technical means of attacking systems since usually people

just gave them the required data. At the very least, you should recognize that social engineering is a way to easily convert a much harder outside attack into an easy inside one.

Thus, violations, committed by insiders, can be loosely divided into three levels:

1. Mistakes – honest but no less deadly for security
2. Crimes of opportunity – probably preventable by awareness
3. Malicious premeditated crimes – the hardest to stop, but the most rare

The question then becomes, what methods can a company use to manage these internal threats?

Managing internal threats

There are three distinct categories of typical methods for managing the risk of internal threats – technological, administrative and legal, and psychological. The overall efficiency of them, even combined together, is far below the existing techniques for network perimeter defense, effective against external attacks.

Experience shows us time and again that technical methods appear to be the least efficient for fighting insider threats, especially on the preventative side. Intrusion detection, personal firewalls, end-to-end encryption software was supposed to thwart or significantly mitigate the threat from within. However, it only helps with a limited range of threats; one should keep in mind that any encryption scheme is only as secure as its endpoints and its keys. If one can read another person's email by looking over his shoulder, how is your fancy 256-bit encryption making email more secure? Intrusion and anomaly detection systems are promising tools to distinguish attack attempts from normal network traffic even if no vulnerability is exploited (as it is often the case for insider attacks). Unfortunately, current anomaly detection research does not allow for a reliable detection. The systems sometimes produce a flood of false alarms, i.e., taking a normal network behavior pattern for an intrusion. These systems might help address a sizeable portion of insider network-based attacks when they mature. The value of intrusion detection systems can be significantly increased by configuring them to report to a centralized log analysis solution. In this case, one is able to correlate the IDS data with other logs sources and to use the log collection for incident investigation.

Legal means include various non-disclosure clauses, legal warnings and general fear of prosecution. From an administrative standpoint, a company's information security policy is important to stopping insider attacks, since it outlines the acceptable use of information systems in the company. Separation of duties is yet another administrative control. This is similar to military procedure when more than one person is needed to launch a ballistic missile. If a single person is responsible for making backups, storing them, verifying them, delivering them to an off-site storage, it creates a catastrophic

single "point of failure." If that administrator develops an emotional instability or just a strong dislike for his supervisor, disastrous consequences are soon to follow. Technology that has a potential to "make or break" the company should not be controlled by a single person. The shortcoming of legal and administrative methods is that most of the legal protection mechanisms work to stop the "crime of opportunity" type of offenses and not the malicious, premeditated crimes. A mole, specially planted to discover company secrets, an insider hoping for a big financial gain or a person under intense emotional pressure or blinded by a desire for revenge is often more risk-tolerant and thus likely to ignore legal warnings.

As far as psychological profiling goes, the methods used to track computer crimes committed by insiders are similar to the one used to track serial killers and terrorists. Personnel security audit is one known way to approach internal threats by studying the potential perpetrators using profiling techniques, pre-employment screening, detection of risky character traits and their tracking, security awareness training and effective intervention by human resources specialists. The obstacles to the widespread use of these techniques are high costs, complex technical challenges and the isolated position of most information security groups within corporate bureaucracies.

Making insider attacks less damaging

These methods are all important parts of a company's security against insider attacks. But the fact of the matter is that, at present, there is no single piece of technology or policy that can reliably detect insider attacks as they are happening. Technical controls, access controls based on a well-written security policy, employee monitoring – these have met with varying degrees of success but none of them on their own create airtight insider security within an organization or even guarantee detection of all insider attacks in time. The question then becomes, is there a way to handle insider incidents better that is effective and efficient?

There is a way to track insider activity – *authorized or not* – to provide a continuous fingerprint of everything that happens within the security perimeter. All users, whether trusted and non-malicious or malicious, leave traces of their activity in logs. If an employee opens a file that they need to use to finish a report during the workday, there is a log of this activity. Likewise, if someone accesses a database and downloads data after business hours, there is a log of that activity. By analyzing these logs, organizations can gain insight into insider behavior and activity and can help investigate, detect, or even predict and prevent insider attacks.

Let's review how various types of logs can be used for detecting and investigating insider attacks, as defined above. We will go through a few common types of logs and illustrate how they can help in the discovery and investigation of insider-related incidents.

Firewall logs

While considered to be purely operation and not “insider-focused,” firewall logs are often extremely helpful as a proof of network connectivity. They directly help answer the following questions, critical during any insider investigation (of course, the usual assumption is that logging of accepted connections through the firewall needs to be enabled):

- Where did the data go?
- What did the system connect to?
- Who connected to the system and who did not?
- How many bytes were transferred out?
- Who was denied trying to connect to the system?

Overall, firewall logs, while extremely voluminous, provide a useful way to track insider activities on the network in the absence of more robust network monitoring tools.

Network IDS logs

These are the favorite of security personnel. IDSs are supposed to be for intrusion detection, but they certainly will not accomplish it in most cases of insider attacks. However, IDSs will likely record various suspicious things that might be occurring during the incident. For example:

- Access to administrator accounts of systems and applications
- Outbound malware connectivity (for cases where insiders did use malware to do their bidding)
- Access and attacks against the IDS sensor itself (from the inside)

Overall, IDS logs are much less useful for insider attacks compared to regular hacker or external attacks. Still, IDS logging should not be discounted and can be used as a set of mildly suspicious indicators to be correlated with other data sources, such as system and application logs that record activities, not attacks.

Server logs

Server logs, such as those from Unix, Linux, or Windows, truly shine in cases of insider incidents. Given that an attack or abuse might not involve ANY network access and happen purely on the same system (with attackers using the console to use the system), server – and also application – logs shed the most light on the situation. However, just as with firewall logs, these do not talk of “attacks” and “exploits” but of activities (which means they are not inherently good or bad). Relevant logged activities on a server include:

- Login success/failure
- Account creation
- Account deletion
- Account settings and password changes
- File access (read/change/delete)

- (On Windows) Various group policy and registry changes

Overall, server logs provide a key piece of the puzzle for both investigating insider attacks by providing a record of system activities as well as changes (in some cases) and authentication and authorization decisions. File access logs are probably more insightful than the rest of the log types above since they give granular information on information access by the computer users (in many cases, inside attackers will be after data), but such logs are usually created in much larger numbers. In addition, server logs are useful for early indications for insider attacks, not only as evidence for investigations.

VPN logs

Another often enlightening source of log data for insider abuse is VPN logs. In a few known cases, an employee (or an ex-employee) was engaging in nefarious activities from home after work hours, thereby, creating a detailed and incriminating trail of his activity, if only the target organization would care to look at logs. VPN logs might also contain references to resources accessed within the company as well as evidence of application use over VPN. As with system logs, network logins and logouts are also useful during insider-related investigations. Some of the useful VPN log messages are:

- Network login success/failure
- Network logout
- Connection session length, number of bytes moved

Overall, VPN logs are indispensable for cases where a trusted insider committed his misdeed while “working” from home. In addition, alerting on unusual VPN access patterns can help discover insider abuse early on.

Proxy logs

Somewhat unusual for insider investigation, web proxy logs are also useful for cases where the information was stolen or leaked over the web. Proxy logs can reveal the following activities:

- Connection to a specific website
- Data uploads
- Webmail access
- Some types of HTTP tunneling for data theft
- Spyware activities

Overall, web proxy logs are extremely useful when the suspected insider was using the company connection for data theft or other network abuse, including emailing the confidential information out or using tunneling over HTTP protocol. However, as with network IDSs, the use of encryption decreases the value of such network logs.

Database logs

As we move higher up the stack, database logs and audit trails begin to come into play. These logs are less frequently col-

lected and analyzed but usually prove very useful in cases related to data theft and unauthorized access. Databases log a dizzying array of different messages, including:

- Database data access
- Data change
- Database structures and configuration change
- Database starts, stops, and other administration tasks

Overall, database logs are useful for both internal and external attacks where database data theft, access, change, or destruction are involved. Such logs are very detailed and can help piece together what information was gathered. They can also be used for various types of anomaly detection to find “out of character” behavior (sometimes associated with insider abuse) and then alert on it. In addition, database logs are the sole source of information on Database Administrator (DBA) activities – and DBAs cannot “go bad,” can they?

Conclusion

Insiders will remain a primary information security risk for the foreseeable future. A number of diverse factors (technical, administrative, psychological) contributing to the problem make it one of toughest challenges in information security. Analysis of log data from a variety of sources is essential to tracking insider activity as well as investigating, detecting, or, in the future, even predicting and thus preventing insider

attacks. Centralized collection and subsequent analysis (via pattern matching, correlation, or anomaly detection) of all logs and audit trails is of crucial importance as well.

However, it is also important to remember that IT security is made up of many working parts, and you can not disregard other methods of dealing with insider attacks. Only by making use of a well-balanced prevention program that includes technical (protective hardware and software, sophisticated centralized log and audit data analysis, online communication monitoring), administrative (legal disclaimers, awareness programs, proper termination handling), and psychological (employee screening and profiling, training managers in identifying the internal threats) measures, one can hope to mitigate the risks. That way, an internal threat will become just another factor in information security management rather than an unstoppable force that can destroy the company.

About the Author

Dr. Anton Chuvakin, GCIA, GCIH, GCFE, a recognized security expert, is an author of a book Security Warrior and a contributor to Know Your Enemy II, Information Security Management Handbook, Hacker's Challenge 3 and an upcoming book on PCI. His current role is Chief Logging Evangelist with LogLogic, a log management and intelligence company. He may be reached at achuvakin@loglogic.com and www.chuvakin.org.