How Better Log Monitoring Can Prevent Data Breaches

Recent high-profile data breaches reaffirm that the threat from data thieves is both persistent and pervasive. Could better log monitoring mitigate or even prevent these types of security catastrophes?

February 24, 2015 - Evidence suggests that high-profile data losses at major retailers such as Home Depot, Sony, Target and Michaels Stores are a major ongoing trend, not a one-and-done anomaly of the IT infrastructure on which most companies rely.

The wholesale loss of millions of customers' personally identifiable information (PII) to hackers and other ne'er-do-wells creates a crisis of public confidence that can directly impact corporate financial results -- and yes, Virginia, IT professionals really can lose their jobs in the aftermath of such corporate hacking incidents.

Rather than re-examining how these attacks could have been prevented in the first place -- if that's even possible -- we posit that the mitigation of these events isn't purely about prevention; it's about detecting intrusions at the earliest possible moment and reacting immediately to limit any data loss.

A key tool in recognizing data intrusions is the lowly log file, a standard feature of almost every operating system, application, server platform and related software in the corporate IT world.

Isolated Is as Isolated Does

Like many others in IT, we used to firmly believe that only an isolated computer -- that is, one that is not connected to an internal corporate network or to the Internet -- is totally immune to hackers. However, the Stuxnet malware attack on the Iranian nuclear program in 2010 proved that even computers on a totally isolated internal network can be infected with malware, in this case most likely via a previously infected USB drive that was used to load software updates onto industrial process computers controlling centrifuges used in the uranium enrichment process.

It was an epiphany to see that what we used to call the venerable "sneakernet" -- moving software between computers via a floppy drive, USB drive or other removable media -- is still exposing isolated computers to destructive malware, even in the highest-security environments imaginable.

As a matter of fact, many companies disable USB ports and removable drives on corporate computers precisely to avoid such a circumstance. We are pretty confident that all USB ports and drives that use removable media on those "isolated" Iranian process logic controllers have in the intervening years been turned off or perhaps even physically removed.

The Log Ride

Log files have always been the lowest-tech, most verbose way to monitor the health and operation of IT software and hardware. In many cases, the level of log file messages can be configured from no log messages written, all the way up to highly detailed log file messages that can track every activity occurring to or within your software and hardware.

The good thing about log files is that you can easily create gigabytes of data just by configuring log files to collect said data. The problem is that finding specific information and pertinent warnings in those gazillions of log file messages is a daunting task. Log file parsing software has been available for many years, but just installing and configuring log file monitoring on your mission-critical IT components isn't going to produce much valuable information, owing to the sheer amount of data that log files can capture.

Protect and Serve(rs)

Step 1 is to turn on log file auditing for all hardware and software in your infrastructure. Step 2 is to acquire log file monitoring software that can parse those log files and create alerts, constantly vigilant for any indication of network intrusions or malware attacks.

That said, though we have no specific knowledge of the internal IT environment of any of the recent victims of corporate data loss, we'd wager that most if not all of the targeted IT shops had log file monitoring software installed. Yet those tools still did not raise sufficient alarms to prevent ongoing data loss after the initial intrusion, even though some of the harvesting of PII from the hacked companies may have gone on for weeks or months.

If an Intruder Breaches a Network in the Forest ...

Unfortunately, enabling log messages for collection and configuring log file levels is just the beginning of the process to detect intruders and their malware payload. Turning on the notification feature of your log file monitoring software is the next logical step. But if administrators are notified of every single hiccup in a server, application, device or other software component, human nature dictates that the administrators will likely begin to ignore important log file alerts just because of the high volume of notifications they receive. What's really needed in this situation is a log file aggregation tool that will collect all IT log files in a single back-end database, where further analysis and correlation can be performed.

When shopping for a log file aggregation tool, be sure that the tool comes preconfigured to detect common intrusion log messages, including external attempts to open IP ports, any changes to administrative passwords, and any access of PII or other mission-critical data. Those types of log file messages should be either built-in defaults or easily configurable in your log file aggregation software. But each IT environment and each application likely has unique log files messages that must be collected and analyzed, so the capability to easily add additional log file rules to match specific intrusion or malware indicators is an absolute must.

Hang Together or Hang Separately?

The last step to better protection from intrusion and malware for your networks and applications is the act of correlating the collected log file messages. This is the most likely breakdown point for many of the data-loss events that have dominated the headlines in recent years. The detection of intrusions or unauthorized data access will be greatly enhanced by correlating logged events on multiple server, network or application components.

If an administrator sees unauthorized attempts to access sensitive data or if an external attack on an obscure IP port is logged, you might or might not recognize those as related symptoms of an attempted intrusion.

However, if your log file aggregation and correlation tool can show you that an IP port is breached, followed by an unauthorized or failed admin login attempt on a sensitive server,

followed by someone accessing a back-end database that houses PII, that's an example of a chain of alerts that should be viewed as a single intrusion thread.

Log file aggregation and correlation is an excellent strategy to minimize the exposure and mitigate ongoing damage that can be caused by intruders and the malware they introduce on your network. Automation is the key to building robust intrusion- and malware-detecting processes, but also remember that alerts will do no good if a human being doesn't pay attention to those warnings and act accordingly to protect digital assets.

Your company is depending on it.

http://www.cio.com/article/2887924/security0/how-better-log-monitoring-can-prevent-data-breaches.html