Herding Cats:
Pointing to Logging Strategy

November 2008

BrandenWilliams
SECURE BUSINESS GROWTH

When Friday afternoon rolls around, most of the readers of this column are thinking about logging and log management. With the weekend giving you a temporary reprieve from the world, why wouldn't you spend some precious brain cycles thinking about one of the most critical components of security management?

Businesses rarely stop when the office is empty. Customers don't stop buying, and the bad guys don't stop trying to subvert the controls you manage just because you went home. All of the work you put into security during the week must stand up to the short, two day vacations that most of us get at the end.

The foundation of early detection starts with strategic logging. So do operational things like capacity planning, or any sort of analysis of IT applications within an environment. You must understand what events are occurring, and the order they occur.

So if this task is so important, why do companies fail spectacularly when it comes to logging?

Logging and log management is yet another part of IT operations that is viewed as overhead as opposed to value. In order to enable logging, that takes computing cycles. Some machines are already at capacity and suffer significant performance hits when logging is enabled[1]. After you generate all these logs, you have to think about sending them somewhere. Logs on endpoints are useful, but not nearly as useful as a centralized solution that allows you to correlate hundreds or thousands of log sources. Sending logging information in from the field costs bandwidth. Finally, you are going to need a place to store all of this stuff. Storing logging information costs disk space.

Organizations subject to compliance standards like PCI-DSS make things worse when they deploy point solutions on various platforms simply to get a checkmark in their compliance box. Last month I talked about organizational silos, but deploying logging tools in point solutions creates "IT silos"! Mainframe systems are siloed from mid-tier systems, and those are siloed from the desktop world. Point solutions are useless outside of compliance-driven initiatives and will cost you more to maintain in the long run.

The basic mistake that companies make when trying to deploy logging is they only think about two states of logging; on or off. While moving the logging switch from circle to stick is required for this whole thing to work, logging everything does you no good. Information overload leads to apathy which leads to careless security which leads to a breach. Anyone want to comment on how well their intrusion detection systems are tuned such that they add value to the organization?

Well, we're all listening…

The challenge to good logging is choosing the correct things to log, and having them log from the most optimal source. Technically, you could track access to resources over multiple mediums. Firewalls, routers, applications, databases, and even operating systems can all generate logs that lead to duplication and information overload. Should firewalls track access to sensitive data by themselves? Absolutely not, but some could with the appropriate rules in place.

What's better is to have an application or a database track the access, and have real-time

FOOTNOTES

[1] **COUGH* Point of Sale *COUGH**

analysis performed on the logs generated. Suzie in Customer Service will typically access one credit card number every five to ten minutes. If she is accessing five to ten numbers in one minute, you know something is amiss.

To create an enterprise strategy, you must first understand the business. Our role is to support the business (and occasionally prevent someone from swimming in shark infested waters). Once you understand the business, you must determine what the logging limitations are of the technologies driving the business. This is not easy and will require digging through technical manuals and working with engineers from multiple vendors to get the data that you need.

After you know the capabilities of the systems in your environment, you must figure out the optimal place to capture logging information that tells you what you need to know. Sometimes this will require you to invest in supplemental software or hardware, other times you may be able to make do with what you have[2]. Regardless, you will need to invest in some technology to collect and analyze the logs intelligently by either purchasing third party services or doing in-house development.

Logging shouldn't be a drain on your IT infrastructure. If you left strategy on the side of the road, the path to logging Zen will be impossible to follow. Before you buy that next point solution for a compliance initiative, stop and think if your actions will support the greater logging good!

FOOTNOTES

[2] *Thank YOU syslog()!*

Contact information for requests for permission to reproduce or distribute materials available through this course are listed below.

About the Author:

Branden R. Williams, CISSP, CISM, CPISA/M, has been making a name for himself in the Information Technology and Security arena since 1994, as a high school Junior. Now, a graduate of University of Texas, Arlington earning his BBA in 2000 with a concentration in Marketing and the University of Dallas, where he earned an MBA in Supply Chain Management & Market Logistics, in 2004, Williams is sought after as both an Adjunct Professor and Information Technology & Security Strategy Leader in the corporate world.

Williams regularly assists top global retailers, financial institutions, and multinationals with their information security initiatives. Read his blog at or reach him directly at http://www.brandenwilliams.com/.