Health IT Security Journal

Volume 3, No. 1

A publication of the HITSF

Logs that matter following a data breach

No Assumption of Privacy

HITSF Journal

Volume 3, No. 1

HITSF

IN THIS ISSUE

This journal is a publication of the Health Information Technology Security Forum.

The Health IT Security Forum is an International Security Organization that dedicated to help healthcare organization in securing their privacy data, confidential information, medical devices and will be recognized for the passion of its members in conducting multidisciplinary research and development in the area of Healthcare IT Security and e-Health.

Letter from the editor

Dear readers,

We are proud to present another issue. This issue of the Health IT Security journal offers insight into information security for healthcare practitioners. We hope you will enjoy it and we welcome your feedback. Please send questions and feedback to editor@healthitsecurity.org

- Hadi Syahrial

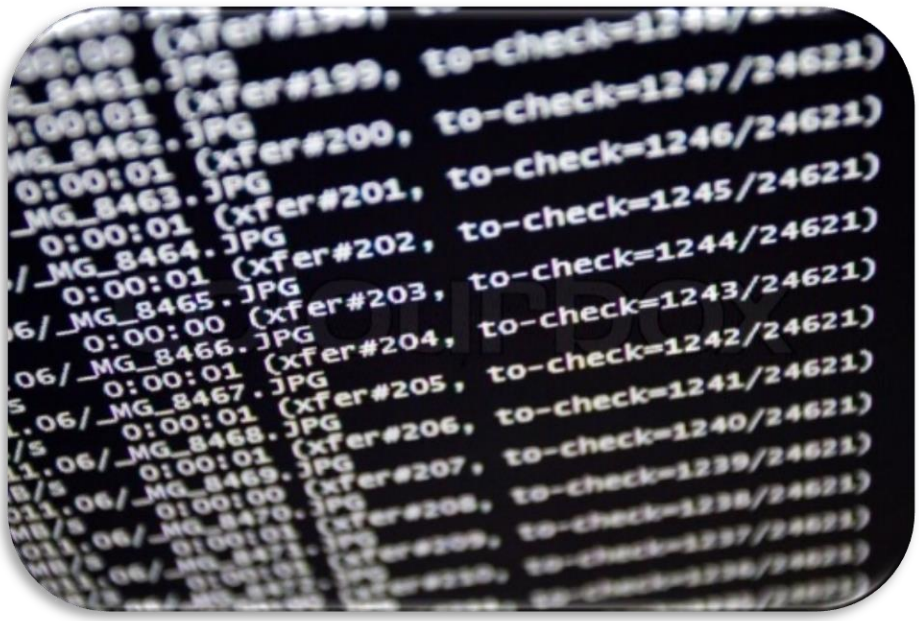
Disclaimer

The author(s) of each article appearing in this Journal is/are solely responsible for the content thereof; the publication of an article shall not constitute or be deemed to constitute any representation by the Editors that the data presented therein are correct or sufficient to support the conclusions reached or that the experiment design or methodology is adequate.

www.healthitsecurity.org

Logs that matter following a data breach

by Eric Vanderburg



There are a lot of things that log files can tell you about a security incident such as a data breach. After all, logs are generated whenever there is system activity, even when it is just a failed login, if they are enabled. So whenever a data breach happens, you can use logs to determine exactly what happened. Analyzing them can be likened to performing forensics of a crime scene. Logs help put together an electronic fingerprint of the attack.

The main caveat is that logs have to be enabled to be of any use to your investigation. In doing so, you must specify the severity level and the so-called verbose level. The former specifies how severe an event should be for a log message to be created, while the latter specifies the level of detail captured in a log message.

But why log?

- The first reason for logging is to ensure accountability. Since log identifies certain events associated with a certain account, it would be easy to pinpoint who is at fault, who needs to be re-trained or who needs disciplinary action.

- The second reason is to reconstruct an event. Certain log files provide footprints for a particular event, including a security breach. Using log messages and reviewing them chronologically, you can re-create what happened before, during and after a particular event.

- Lastly, you can log to detect intrusions. When logs are reviewed diligently, you can know if someone is trying to hack into your database, whether from the outside or the inside. This can not only raise the alarm, but prompts you to improve database security.

There are several logs that are useful following a breach.

Syslog

Syslog is a stream of information generated from log files created for activities that take place. Firewalls, routers, switches and other services can be configured to send their log data to a syslog server. In some cases, these devices may maintain logs of their own but many times, such devices have limited storage and must stream their logs elsewhere in order for them to be retained for analysis.

When managed correctly, a syslog can show you logs of when devices or software is misconfigured, who access data or changed configurations, or whether administrators are abusing privileged access. Log data typically contains a timestamp, source, event code, description, and other information.

But because large database generate a huge amount of syslog data, a lot a few important events are lost in the significant volume of messages, most of which are informational. But you can identify events that matter to a breach through programs that integrate log data and correlate events. Such systems are known as Security Information and Event Monitoring (SIEM) systems.

Event Logs

Event logs are specific to an application or operating system. For example, Microsoft Windows has the following event logs:

- Application (program) events. Events are classified as error, warning, or information, depending on the severity of the event. An error is a significant problem, such as loss of data. A warning is an event that isn't necessarily significant, but might indicate a possible future problem. An information event describes the successful operation of a program, driver, or service.

- Security-related events. These events are called audits and are described as successful or failed depending on the event, such as whether a user trying to log on to Windows was successful.

- Setup events. Computers that are configured as domain controllers will have additional logs displayed here.

- System events. System events are logged by Windows and Windows system services, and are classified as error, warning, or information.

(Source: http://windows.microsoft.com/en-us/windows/what-information-event-logs-event-viewer#1TC=windows-7)

Through log management, you can use event logs to determine which systems or applications were compromised, which

security system failed, and various information about the attack, such as the vector used, whether it was internal or external, and whether it was detected but not prevented.

Based on the information gathered, you can be able to identify the cause of the breach and then find ways to prevent a similar occurrence.

If there has been an incident, the first step is to preserve the log data that is available so that it is not overwritten by the system. This information could prove useful as evidence.

About the Author:
Eric Vanderburg

Director, Information Systems and Security, JurInnov Ltd.

Eric Vanderburg understands the intricacies inherent in today's technology and specializes in harnessing its potential and securing its weaknesses. He directs the efforts of multiple business units including Cyber Security, eDiscovery, Computer Forensics, Software Development, IT and Litigation Support at JurInnov, an eDiscovery and eSecurity consulting firm. Vanderburg holds over thirty vendor certifications and is completing a doctorate in information assurance. He has dedicated much of his career to designing and implementing systems, policies and procedures to enhance security, increase productivity, improve communications and provide information assurance. He has been invited to speak at conferences and events on technology and information security and he is active in promoting security and technology awareness through various publications. Look for his latest book, "Storage+ Quick Review Guide", due for publication with McGraw Hill in December of 2013.

No Assumption of Privacy

By Ramana Gaddamanugu

We live in a world where privacy is almost a thing of the past. Changes in technology and our culture have traded privacy for convenience or effervescent feelings of security. Privacy is the process through which an individual's actions are kept out of the public view or knowledge. The problem is that we need our privacy. We were not meant to reside in a world where everything is tracked, monitored, or published and we should not have to.

The need for Privacy is not human alone; even animals tend to keep some of their actions or interactions private but relative to human's far superior intellectual and speech capabilities combined with relatively far higher permutations and combinations of activities, animals have a relatively lower understanding as well as need for a lower amount of privacy than humans do.

Whilst human instincts, actions, motives and activities might be theoretically stable over time, there is a remarkable increase in the impact or consequences of actions due to enabling technologies, resulting from remarkable decrease in the timeframes for successive innovations and hence, the remarkable increase in the continuous "self-feeding" enhancements in technologies.

Technology

The increase in technological advances have been great. For example, Doctors are able to perform heart transplants as almost routine procedures; humans have also been able to travel to the moon and return safely as well as go to the deepest depths of the oceans.

Effects

However, the increase in innovation and technology has also had its "side-effects" on humans and other animals. For example, pollution has led to social, environmental, medical etc. adverse consequences. Another example would be that technological enhancements have enabled faster de-forestation, leading to ever-increasing loss of animals' lives and their ways of life. Similarly, the increase in technology has also led to a remarkable decrease in individuals' privacy.

The effects of these side-effects have manifested in numerous ways. For example, ever-increasing pollution has led to increase in certain types of ailments and diseases; de-forestation has led to loss of natural habitat for animals which has been resulting in ever increasing unnatural confrontations between humans and other animal species. Similarly, the loss of privacy has led to numerous side-effects such as loss of rights granted by the constitution such as non-violation of individuals' privacy without adequate due cause.

The effects of a loss of privacy are great and it is something we should be concerned about. Don't let privacy continue to be a thing of the past.

About the Author:

Ramana Gaddamanugu

Ramana Gaddamanugu is a privacy and fraud expert. He is a certified fraud examiner and a chartered accountant.