INITIAL POST

Security management has become a herculean task because of the ever-increasing sophistication of threats and number of cyberattacks. Keeping an eye on the systems they are responsible for protecting, requires security analysts to deal with large amounts of inconsistent log data from a wide variety of sources (e.g., network devices like firewalls, routers/switches and web & database servers etc.).

(Ekelhart et al., 2018)

Why Logging is needed? – Benefits:

There are numerous ways in which log management can help a business:

- It aids in keeping detailed computer security logs for an adequate time frame.
- Reviewing and analyzing logs on a regular basis helps find and fix security breaches, policy infractions, fraud, and other operational issues.
- Auditing and forensic analysis
- There are few compliance requirements which mandates for log management
    - FISMA (Federal Information Security Management Act of 2002)
    - HIPAA (Health Insurance Portability and Accountability Act of 1996)
    - SOX (Sarbanes-Oxley Act)
    - PCI-DSS (Payment Card Industry Data Security Standard).

How to keep Log Data secure? - Challenges

Integrity and availability protection of log data can be done in various ways:

- Limited privilege access to log data
- Archived of files protection through file encryption
- Secure mechanism for log-data in transit – from source to the log servers
- Avoiding logging unwanted sensitive data

(Karen Kent, Murugiah Souppaya, N.D.)

Attackers are actively scanning the networks to exploit log-related vulnerability like Log4j (**CVE-2021-44228 , CVE-2021-45046, and CVE-2021-45105**). Log4Shell, a software vulnerability in ApacheLog4j 2 which is a popular Java Library for logging error messages in applications, was rated as critical vulnerability by Apache because of the extensive use of JAVA across IT platforms /applications

(Berger 2021) (CISA 2021)

REFERENCES:

1. Ekelhart, A., Kiesling, E. and Kurniawan, K. (2018). Taming the logs - Vocabularies for semantic security analysis. Procedia Computer Science
2. Karen Kent, Murugiah Souppaya [N.D]: Guide to Computer Security Log Management https://www.govinfo.gov/content/pkg/GOVPUB-C13-52c3b5520393598b18782a7b55fde7e6/pdf/GOVPUB-C13-52c3b5520393598b18782a7b55fde7e6.pdf

3. Berger [December 2021]: What is Log4Shell? The Log4j vulnerability explained https://www.dynatrace.com/news/blog/what-is-log4shell/?utm_source=google&utm_medium=cpc&utm_term=log4j%20vulnerability%20explained&utm_campaign=uk-application-security&utm_content=none&gclid=CjwKCAjwiuuRBhBvEiwAFXKaNJd3hLzYlujXuVbTIP63_IioBFvzAYOePxfft2D6ded7EXfaTu4j4BoCrHAQAvD_BwE&gclsrc=aw.ds]

4. Mitigating Log4Shell and Other Log4j-Related Vulnerabilities [December 2021]

   https://www.cisa.gov/uscert/ncas/alerts/aa21-356a

PEER RESPONSE

Hello Iason,

Thanks for your informative post-

I agree that the Logging is required to fulfil compliance and regulatory requirements (like PCI-DSS) in many of the cases. It takes more than six months, on an average, for an enterprise to realize that the environment has been compromised. And it's only the retained logs which are helpful in analyzing the full impact of the breach. Also, the retained logs must be secured, centralized and archived for long term storage as per the requirement.

(Using Logs for Security & Compliance, 2016)

Application logs must be stored and becomes invaluable information for identifying incidents, monitoring and providing information for unusual conditions. It can also be used for audit trails and compliance monitoring.

(OWASP Cheat Sheet Series, N.D)

REFERENCES:

Using Logs for Security & Compliance: (2016)

https://www.rapid7.com/blog/post/2016/02/04/using-logs-for-security-compliance-part-2/

OWASP Cheat Sheet Series(N.D.)

https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html

Hello Gokul,

Thanks for your detailed and informative post-

I agree that the logging is required for audit trails, identifying incidents, to fulfil compliance and regulatory requirements.

Retained logs are helpful in assessing the full impact of the breach as it takes a long time for the organization to realize that the environment has been attacked.

(Using Logs for Security & Compliance, 2016)

As you rightly mentioned that the logs come from different sources and in different formats, just to add to that point, the retained logs must be secured / encrypted, centralized and properly integrated. Depending on the compliance requirements, logs should be archived for long term storage.

Integrity & log data availability protection of log data can be done by:

- Limiting privilege access, protection through file encryption
- Data security for log-data in transit – from source to the log servers
- Avoiding logging unwanted sensitive data

(Philip, 2021)

REFERENCES:

1. Using Logs for Security & Compliance: (2016)

https://www.rapid7.com/blog/post/2016/02/04/using-logs-for-security-compliance-part-2/

2. Philip Duff (2021): Managing long term log retention

https://techcommunity.microsoft.com/t5/azure-storage-blog/managing-long-term-log-retention-or-any-business-data/ba-p/2494791