INSUFFICIENT LOGGING AND MONITORING

18-01-2022

Eekelen,Stijn S.H.P.A. van
Stijn.vaneekelen@student.fontys.nl
459346

Inhoud

Why is logging and monitoring so important?

Logging is an important way to monitor your application for strange occurrences like unauthorized access for example. With good logging and monitoring you can see the cause of past /recent data breaches and perform work to prevent / investigate them. On the following source (Hdiv, 2021) they even say “Exploitation of insufficient logging and monitoring is the bedrock of nearly every major incident. Attackers rely on the lack of monitoring and timely response to achieve their goals without being detected.” Which indicate that this is a really big problem that every developer should keep in mind when developing their applications.

Impact

Not being able to keep up with threads and even when logging is setup when monitored incorrectly will not prevent any data breaches or provide useful data.

Examples

Both (Hdiv, 2021) and (Radhakrishnan, sd) give some really good examples and I don’t think it will benefit this investigation rapport to add them in a separate section so check them out if your interested.

How to prevent?

- Ensure all login, access control failures, and server-side input validation failures can be logged with sufficient user context to identify suspicious or malicious accounts, and held for sufficient time to allow delayed forensic analysis.
- Ensure that logs are generated in a format that can be easily consumed by a centralized log management solutions.
- Ensure high-value transactions have an audit trail with integrity controls to prevent tampering or deletion, such as append-only database tables or similar.
- Establish effective monitoring and alerting such that suspicious activities are detected and responded to in a timely fashion.
- Establish or adopt an incident response and recovery plan.
- Ensure all login, access control failures, and server-side input validation failures can be logged with sufficient user context to identify suspicious or malicious accounts, and held for sufficient time to allow delayed forensic analysis.
- Ensure that logs are generated in a format that can be easily consumed by a centralized log management solutions.
- Ensure high-value transactions have an audit trail with integrity controls to prevent tampering or deletion, such as append-only database tables or similar.

- Establish effective monitoring and alerting such that suspicious activities are detected and responded to in a timely fashion.
- Establish or adopt an incident response and recovery plan.
- Secure the logs
- Store the logs in accordance with the compliance and business requirements
- Properly monitor user activity, anomalous behaviour with automation and alerting
- Log review should be closely monitored
- Logs should not be deleted or modified

Conclusion

If logging or monitoring of the logs is insufficient it is nearly impossible to detect a potential active or finished data breach which is really dangerous and can cause a lot of damage in both the present and the future when those leaks become public compromising user data and risking huge fines. With the above list with things to implement and lookout for you can prevent a lot of such attacks to a certain extend and every developer should think about implementing them.

Bibliography

Hdiv. (2021, 09` 10). *Insufficient Logging & Monitoring*. Retrieved from hdivsecurity.com: https://hdivsecurity.com/owasp-insufficient-logging-and-monitoring

Radhakrishnan, R. (n.d.). *OWASP Top 10 : Insufficient Logging & Monitoring*. Retrieved from siemba: https://www.siemba.io/post/owasp-top-10-insufficient-logging-monitoring