Auditing and Logging

Security 2018

What is Auditing ?

An information security audit occurs when a technology team conducts an organizational review to ensure that the correct and most up-to-date processes and infrastructure are being applied.

What is Auditing ?

When auditing you try to discover what is really going on for example:

- Find security issues (outdated software, poor security, etc.)

- Evaluate systems, processes, risks and controls

- Enable people to make informed decisions

How do you discover what is really going on in a network ?

- Identify the topology of the network
- Identify all hosts on the network
- Determine services running on all hosts
- The configuration of all services and applications on the host
- Look at logs

Logs: *An audit log is a document that records an event in an information technology system.*

What is logging ?

- A log is a record of sequential data such as:
  - Audit logs
  - Transaction logs
  - Connections logs

- And generated by :
  - Operating system
  - Databases
  - Firewalls
  - Antivirus
  - Routers

Vulnerabilities:

An application is deemed to be potentially vulnerable if there is insufficient logging and auditing, detection, and monitoring, with effective responses. Areas where a lack of logging is potentially dangerous to your environment include:

- Warnings and errors that are not logged, or warnings and errors that produce no meaningful output.
  Ambiguous and unclear logs are also not helpful to system administrators and developers.

- Auditable events such as user logins, failed login attempts, and unlogged activities such as high-value transactions and system related changes.

Vulnerabilities: cont..

- Important logs of critical applications and APIs are overlooked when auditing and system logs are set up, meaning that entire systems can go on without ever being monitored, causing massive potential for security breaches in critical IT systems.
- Logs being stored only locally gives intruders an opportunity to edit the logs and remove any evidence of their activities in your environment.
- Alerts and responses that are not implemented correctly, or at all.
- Applications might not have ant detection, logging or alerting systems built into them, meaning that attacks go unnoticed by system administrators.

Benefits of Auditing and logging:

- Logging user actions can help [companies] improve security in a variety of ways because it provides a way for administrators to reconstruct events, detect intrusions, and analyze problems such as poor performance or unexpected system behavior. The following includes other ways audit logging can reinforce an enterprise's security. *Next slide*

- Documenting what resources were accessed, audit log entries usually include destination and source addresses, a timestamp and user login information.

- Security logs and reports provide you with an electronic record of suspicious activities and help you detect patterns that may indicate attempted or successful external penetration of the network, as well as internal attacks.

Benefits of Auditing and logging: cont..

ways audit logging can reinforce an enterprise's security:

- Detect Security Breaches:

  Having detailed audit logs helps companies monitor data and keep track of potential security breaches or internal misuses of information

- Assess System Damages:

  Audit trails can be used to reconstruct events after a problem has occurred. Damage can be more easily assessed by reviewing audit trails of system activity to pinpoint how, when, and why normal operations ceased.

Benefits of Auditing and logging: cont..

ways audit logging can reinforce an enterprise’s security:

- Aid in Recovery Processes:

  Understanding how and why a system crash or an intrusion occurred is pertinent to avoiding similar outcomes in the future.

  Audit logs can help in situations regarding data loss or corruption by allowing administrators to reconstruct data files through the changes recorded in the logs.

Benefits of Auditing and logging: cont..

- Protect data by maintaining visibility and responding quickly to timely security alerts.
- Auditing and logging of security-related events, and related alerts, are important components in an effective data protection .
- you can use auditing to monitor user activity.
- Alerts provide immediate notification when security events occur.

Examples:

- Microsoft business services and products provide you with configurable security auditing and logging options to help you identify gaps in your security policies and mechanisms and address those gaps to help prevent breaches.

- Microsoft services offer some (and in some cases, all) of the following options: centralized monitoring, logging, and analysis systems to provide continuous visibility; timely alerts; and reports to help you manage the large amount of information generated by devices and services

References:

- https://www.microsoft.com/en-us/trustcenter/security/auditingandlogging?fbclid=IwAR2VZAcqwI4yOaVFDEdRRahau6nU5wTiQqmw9Ow_UAdFVk_R8efqM3w2WLI

- https://www.digicert.com/blog/the-security-benefits-of-audit-logging/

- *https://www.techopedia.com/definition/10236/information-security-audit*

- http://www3.kau.se/kurstorg/files/a/55E2E9B11d97b3115AKOFF962F40/Audit&Logs.pdf