A09-2021 Security Logging and Monitoring Failures

It is the lack of adequate logs or the inability to monitor critical security-related events, which hinders the detection, analysis, and response to security incidents. This can include:

- Lack of key activity logs.
- Insufficient, incorrect, or inaccessible logs during an incident.
- Ineffective or absent monitoring of critical events.

Examples: An application that does not log failed login attempts, making it difficult to identify a brute-force attack.

Severity

- Facilitates prolonged attacks: Lack of monitoring allows attackers to operate undetected for long periods.
- Hinders incident response: Without adequate logs, it is almost impossible to determine how an attack occurred or what data was compromised.
- Impact on reputation and compliance: Many regulations (such as GDPR or PCI DSS) require event logging and monitoring; their absence can lead to legal penalties.

Mitigation

- Log analysis: Use log analysis tools to identify patterns and anomalies in security logs.
- Threat intelligence: Integrate threat intelligence information into monitoring systems to detect known malicious activities.
- Incident response: Develop a clear and concise incident response plan that includes procedures for investigating and containing security incidents.
- Logging and monitoring policy: It is very important that companies have logging and monitoring policies, so that those responsible for the systems can have a correct handling of this type of problems.