Oracle Database Testing Results

Kaneshia Lovick • 11.07.2022
Security Analyst
Client:Toll Road Authority

Overview

Oracle Databases Test Results

11.07.2022

Findings:

A presentation of vulnerability findings, of our Toll Road Authority Client.

- Improper Auditing
- Encryption Not Widely Used
- Monitoring of Logs Not Occuring

Risks

Severity

Recommendations

Improper Auditing - Topic area 1

Risks 1

- Not able to track and understand how records are used.
- Higher risks or fraud and less accrediability of client.

Severity 2

- Severity of improper auditing is high, as it can go against database compliance standards.
- Can cause a client to not have accurate records of financials and errors that need to be fixed are not corrected.

Encryption Not Widely Used - Topic area 2

Severity 2

Risks 1

- Unauthorized access to database data stored in files.
- Information that is not encrypted has a risk of being deleted or stolen. IE: Tables

- This risk would be severe as database servers are at higher risks of breach due to the servers holding, the clients most valuable assets. IE: Financial records
- Database servers is the key to solving issues of information management.

Monitoring of Logs Not Occurring- Topic area 3

Risks 1

- Non compliance of lack of monitoring
- Can allow attackers to perform brute force, phishing and denial of service attacks.
- Attackers more persistent.

Severity 2

- High severity as it is harder for client to detect and mitigate breaches.
- Can cost client more time and money.
- Accountability is questioned,

Recommendations

Topic Area 1

- Provide training/ awareness to client about auditing and provide a auditing guideline.
- Follow up with training of client staff if needed.

Topic Area 2

- Security training and awareness of client, if needed.
- Provide data encryption services to client, to encrypt all data, tables and securing database with a master key.
- Encryption of data at rest and data in motion.

Recommendations

Topic Area 3

- Security & awareness. Create context of baseline traffic, to help understand how to identify suspicious activity.
- Automate monitoring and alerts.
- Implement splunk tool as it assists in monitoring performance, allowing security to react quickly to threats.

Solution: Splunk, The Engine For Machine Data