Rahul Balaji (11449565)

Incidence Response Plan

Introduction

The purpose of this document is to guide the team through a plan and help them respond to a security incident that has compromised the function of the system and also to serve as a handbook to the incident response team on what actions to take to resolve the incident depending on which layer of the system architecture has been breached. The incidence response plan has been structured on varying levels based on which part of the system has been compromised or breached. The design of the system's architecture has been placed below for your reference (refer fig 1 in next page).

The architecture was designed as part of a team (Group 3 - Gabrielle), and will serve as the baseline for the incidence response plan categorization.

Before we begin with the plan for incidence response, remember that human emotions and actions also pay an important role in the security of a system. In the face of an incident, remember the 3 C's of response,

Control the situation at hand !
Coordinate the effort for incidence response !
Communicate between teams actively on any findings !

With that in mind, as long as we stick with a response plan and stay vigilant, we can actively respond to any threats and take care of them while sustaining minimum damage. With each component of the architecture, we will follow the flow of the kill chain for incidence response which is defined by lockheed martin as,

- Detect : Determine whether an intruder is present.
- Deny : prevent the disclosure of information.
- Disrupt : Stop the outbound traffic to attacker.
- Degrade : Counter, command and control the situation.
- Deceive : Interfere with command and control.
- Contain : Network segmentation changes.

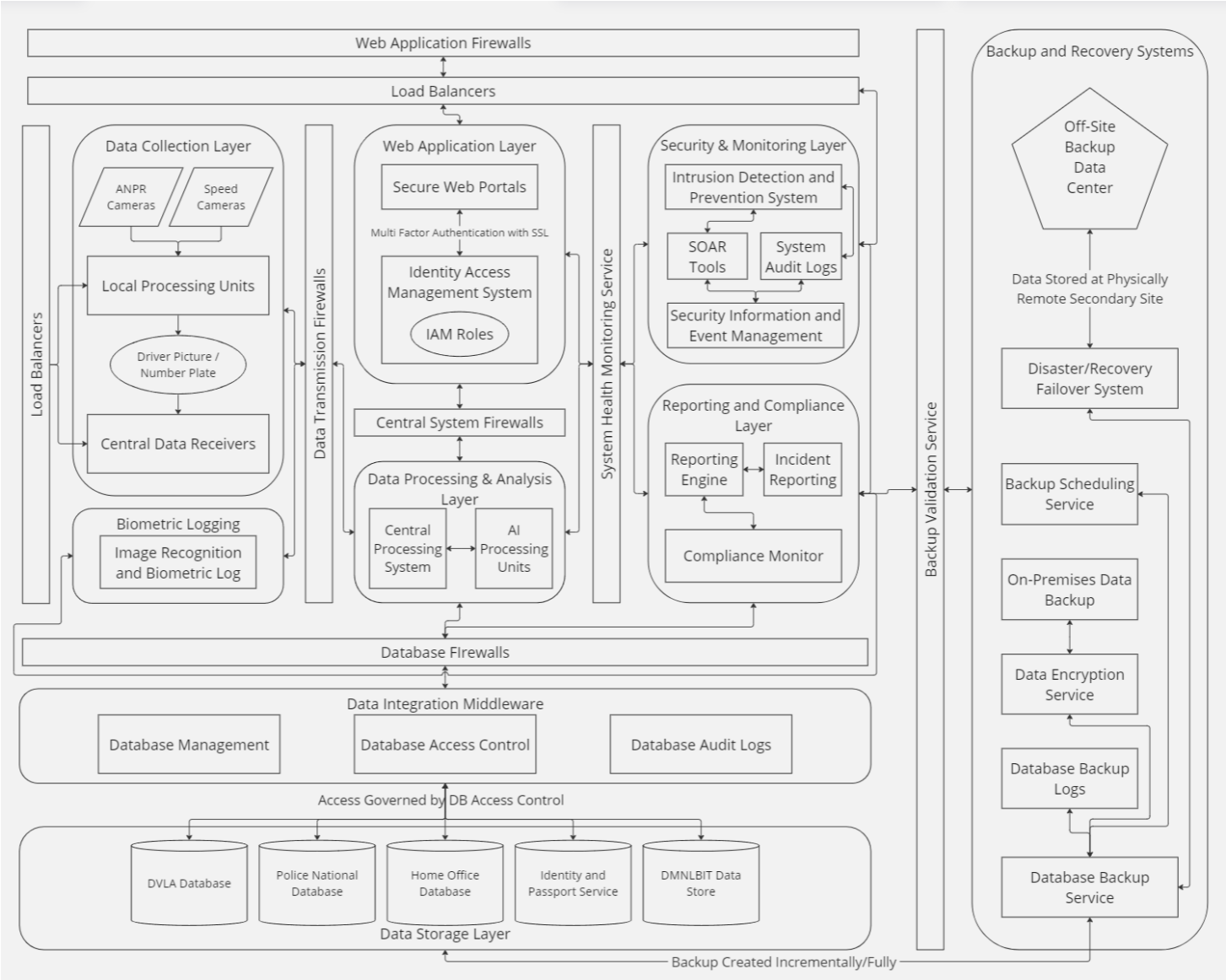

Fig1 . System Architecture

Response Plan

Data Collection Layer

Scenario 1 - endpoint sensors compromised

Indicators of compromise :

The ANPR sensors and the cameras are firing off repeatedly even though the traffic rules are being followed by the drivers.

The ANPR sensors and the cameras are not capturing data of the offenders who violate traffic laws.

The data from ANPR sensors and cameras are being routed through some unknown proxy server to the central data receivers, or the data does not reach the central data receivers.

Response :

Step 1 : check the logs via the security and monitoring layer for the endpoint machine that is displaying signs of compromise.

Step 2 : Shut down the end point and then cut off any incoming data received from the end point.

Step 3 : Monitor any other end point devices that are in nearby area to the compromised end point device.

Step 4 : Notify the maintenance department to check if the machine has been physically tampered with.

Step 5 : If the machine was not tampered with physically, retrieve any connection and network logs that are stored on the compromised device and analyse the logs for any suspicious connection requests outside the system.

Step 4 : If any suspicious connection was found, block any further requests that may be received from the external machine again in future using its network host artefact / Domain name / IP address.

Step 5 : Restart the endpoint and restore it’s connection to the system.

Step 6 : If any of the machines and/or data has been stolen and/or misused, file a report after the system is up and running and take further actions to maintain compliance.

Scenario 2 - unauthorised access to Central Data Receivers

Indicators of Compromise :

The central data receivers, receive no data captured by the endpoint devices.

The network logs show a connection request from an unknown source to the central data receiver.

The central data receiver sends data to a destination port that is not the data processing and analysing layer.

Response :

Step 1 : Block the connection between the central data receiver to the data processing and analysing layer.

Step 2 : Analyse the connection request logs given to the central data receivers, and any outgoing destination ports that the receiver has been communicating to other than the central processing unit.

Step 3 : Block that particular machine that has made the connection requests by using its Ip address or network artefacts so that it cannot make any further requests to exfiltrate data any further.

Step 4 : Restart/Recover the central data receiver so that the system is up and running again.

Step 5 : If any data has been stolen and/or misused, file a report after the system is up and running and take further actions to maintain compliance.

Data Processing and Analysis Layer

Scenario - Processing system shut down due to power loss / technical difficulties

Indicators of Compromise :

There is no report generated, no decisions taken on wether offence is created.

Response :

Step 1 : Call the IT support system and have the servers checked for any hardware/technical faults.

Step 2 : Ensure that the software is working as intended once the system is restarted.

Step 3 : If the software is corrupted due to some external reason, file a report for inspection by the software testing team and restore the software using onsite backup facility once all logs of system failure has been recorded.

Web Application Layer

Scenario - Stolen credentials and malicious login attempt

Indicators of Compromise :

Too many login attempts by one account.

An accessed account has been requesting information that they are normally not given access to.

Suspicious login activity reported by the original user of the account.

Response :

Step 1 : Identify the credentials used, block the particular account from gaining access until incident is resolved.

Step 2 : contact the user the login credentials are linked to and check if they made the login attempt, and if they still possess the secondary device they need for the multi-factor authentication.

Step 3 : If the attempt was not made by the user, change the password (and username if viable) of the user, and then securely provide them the new details over a trusted channel.

Step 4 : Ensure that old username and password is deleted from system if changed, and they can no longer be used to try and login into the system again.

Data Integration Middleware Layer

Scenario - Data is being Exfiltrated.

Indicators of Compromise :

Internal Employee who is authorised to access the database is requesting data at an unusual rate without proper evidences captured by speed camera and number plate readers.

Although the access control ensures that each layer accesses only the data it is authorised to, there may be cases where a threat actor gained access to the database via escalation of privileges. If there is a machine/user that is not on the list of known database admin workstations that is requesting information, it is surely an indicator of compromise.

Response :

Step 1 : First, block the workstation/user account that is requesting/receiving access of data so that they cannot access any further records in the databases.

Step 2 : Launch an investigation on the user linked to the account if they are an internal employee, by viewing the Database Audit Logs, gaining insight on what information they requested to be given and why they requested it.

Step 3 : If the incident is a false positive, unblock the account and continue. If it is a true positive for abusing rights on viewing sensitive data, file a formal report and complaint for further escalation of offence.

Step 4 : If the account reported is not on the list of known admins, delete the account to prevent any further access to the database and analyse the activities of the account on the system to trace the person associated to the account using digital forensics.

Data Storage Layer

Scenario - The data stored is corrupted/lost

Indicators of Compromise :

The data records are missing.

The data records cannot be accessed.

Physical Damage to the hardware/bare metal that stores the data.

Response :

Step 1 : Scan the database immediately for any vulnerabilities/malwares.

Step 2 : Send the database audit and access logs to the forensic team with server data for the forensic team to investigate the cause of loss of data.

Step 3 : Conduct a scan on the backup data stored on-site for any signs of tampering/change since last backup.

Step 4 : If scan concludes backup data is not tampered with, then use the on-site backup data to restore the database.

Step 5 : generate and file an incident report if there has been any major findings as to why the incident occurred.

Backup and Recovery Systems

Scenario - Backup files corrupted / Backup not done properly

Indicators of Compromise :

Periodic backup tests fail.

Response :

Step 1 : If offsite backup has failed the periodic test, scan the current on-site backup, test it and process it for off-site backup.

Step 2 : if onsite backup has failed the test, scan the current deployed stable version of code and then process it for onsite backup, and test it.

Miscellaneous Scenarios

Scenario - 1 Forced physical breach into any onsite locations

Indicators of Compromise :

Any unauthorised person on the onsite premises without proper documentation of their permission for entry.

Missing any physical asset that is supposed to be onsite.

Response :

Step 1 : Alert physical security to scan the premises immediately for suspicious individuals.

Step 2 : Check CCTV footages, and entry records for clues on identifying the person who entered the premises.

Step 3 : File a formal complaint in case of any missing assets.

Scenario 2 - Ransomware attack

Note : While it is not illegal to actually pay to resolve ransomware attacks, know that it should only be the last resort. Because of the nature of the system architecture, none of the databases with the sensitive data can be affected by the ransomware attack as access to users ends at the web application layer, where they can view final offence records. This scenario entails for a ransomware attack that has taken over and encrypted the website application, thus disrupting access to users.

Indicators of Compromise

The website has been hacked and the threat actors block access to website, holding it for ransom.

Response

Step 1 : Deploy another website portal for authentication and viewing of offence records using the onsite backup for the website on a different domain.

Step 2 : Notify the internal employees and users about the situation and urge them to use the other website now hosted for use until the ransomware situation is resolved.

Step 3 : Follow institution protocols for resolving ransomware attacks, either by trying to crack the encryption and scanning for any exfiltration attempts, or by paying the ransom.

Step 4 : File a formal complaint and collaborate with other public sources to identify the ransom group if needed.

Scenario 3 - Natural Disasters / Fires

Step 1 : Move away from premises immediately an safely towards designated assembly points that have been debriefed during the periodic safety trainings.

Step 2 : Alert the local emergency response team / fire department.

Step 3 : Report any missing person from the teams if not present at any assembly point.

Lecture Reflections

Colin Williams on Homo Cyborgia

It changed the way i thought about Artificial Intelligence. Gave me a new perspective on the question “Are you a human or a Robot ?” that left me thinking quite a bit. Also introduced me to the book published by Professor Norbert Wiener, Cybernetics.

Tim Armit on Resilience

Gave me the valuable insight of also considering all aspects of security, which also includes diaster recovery plans and accounting for accidents in ways i never thought of before. Having backups stored in different far away locations, thinking about physical security guards onsite, and also on social engineering methods that are not digital are some things i picked up on this lecture.

Sarah Clarke on Supplier Governance

AI incidents and what they are, how we can regulate AI and the need for regulations in this new emergent field being a heavily discussed topic. Security is everyone's responsibility in a company, and each one of us need to play the part.

Alan Jenkins on Leadership

Leadership and what it takes to run a company. The roles of a person higher up in the ladder is much more concerned with compliance and business continuity than the everyday system planning and running security scans on the system and entails more than making architecture and system design decisions. A CISO is a strategist, a advisor, a guardian and a technologist.

DI Dan Giannasi - NWROCU on Digital Forensics

Learnt what is digital forensics. How an investigation is conducted. Where even the slightest of traces left behind by your digital footprint can be a valuable information in a investigation. Also learnt about the challenges of understanding new and complex technologies and keeping up to date to remain ahead of criminals.

Fay Coxon on The Rocky Road to the IoT Horror Show

The main takeaway was how little security is prioritised in iot devices and how easily they can be hacked and information can be stolen from them. There is a need for extensive pentesting as a requirement for these devices before they can be trusted with sensitive data. I really liked the quiz.