MGS650 Reading Response 2: The 18 CIS Controls

Attack Summary:

A database belonged to the Department of Medical, Health and Family Welfare of a state in India had a breach revealing huge PII data including but not limited to name, email, DOB, gender, phone number, education level, area of specialization, functional area, employment history, current employer, current salary etc of nearly 12.5 million medical records related to both doctors and patient data.

The exposed database of stored data mostly included information regarding pregancy, sex determination tests, whistleblowing documents comprising complaints against tests, information of doctors, medical centers, inventory information of medical equipment such as ultrasound machines and other medical equipment that could have been used to determine an unborn child's sex.

Data was seen to be scrapped as part of a massive scraping operation by an anonymous person or organization. It was reported that the database was accessed after scanning the internet or by using OSINT tools such as shodan.io to search for unprotected and publicly indexed MongoDB servers which were hosted on Amazon AWS. Database files were later replaced by a ransom note with attackers' contact information. It was reported as the attacker(s) using a script that automates to access, export, delete a MongoDB database and then create the said ransom note. These kinds of remotely accessed security breaches in MongoDB servers are prevalent and are referred to as Mongo Lock. The database was able to be removed and secured by the Indian Computer Emergency Response Team (CERT), within the time period of three weeks.

From 18 ‘CIS Controls v8’ CIS Control 3, CIS Control 6, CIS Control 7, CIS Control 8, CIS Control 12 and CIS Control 16 were lacking. As an ideal security consultant, mentioned CIS control must be consdiered top priority for implementation to protect public databases with PII.

Corrective Measures:

CIS Control 3 - Data Protection

- Sub control 3.10 states to configure MongoDB to encrypt sensitive data in transit which can include transport layer security(TLS)/Secure Socket Layer (SSL) and Open Secure Shell(OpenSSH).
- Similarly, sub control 3.11 states to encrypt sensitive data at rest on servers, databases and applications containing sensitive data. This can be done through server-side encryption(storage layer encryption).In summary this control ensures protection of MongoDB data files, configuration files, auditing logs, and key files using file-system permissions.

CIS Control 6 - Access Control Management

- Sub control 6.3 requires multi factor authentication for all externally exposed applications or third party applications. This ensures authentication and access control for already present passwordless MongoDB servers.
- Sub control 6.7 addresses centralizing access control for all enterprise assets through a directory service or SSO provider that would act as a safeguard against wrongful access to the databases.

CIS Control 7 - Continuous Vulnerability Management

The key sub controls include CSC 7.1, and CSC 7.6. Sub control 7.1 addresses establishing and maintaining a vulnerability management process with documentation for all the enterprise assets. This documentation should be reviewed and updated annually to adapt to the current risk requirements.

Sub control 7.6 states organizations must perform automated vulnerability scans of all externally-exposed enterprise assets using security content authentication protocol compliant tools on a monthly or frequent basis.

CIS Control 8 - Audit Log Management

The key sub controls include CSC 8.3 and CSC 8.8. Sub control 8.3 ensures adequate audit log storage is maintained. This is essential to track changes and access to database configurations and data. This is essential to establish and maintain an audit log management process which is of paramount importance while recording system events, connection events here on MongoDB instance. Sub control 8.8 directs to collect command-line audit logs that access internal data. This control oversees collection of logs to a central log store that contain DB authentication attempts that match to the source IP address.

CIS Control 12 - Network Infrastructure Management

The key sub control CSC 12.3 states to securely manage network infrastructure by measures such as implementing version-controlled-infrastructure-as-code, disable direct SSH root access, use of secure network protocols, such as SSH and HTTPS.

CIS Control 16 - Application Software Security

The key sub controls include CSC 16.1 and CSC 16.7. Sub control 16.1 addresses the entirety of establishing and maintaining a secure application development process that includes secure application design standards, developer training, securing coding and maintaining practices, vulnerability management and application security testing procedures. Sub control 16.7 directs to use standard industry recommended hardening configuration templates for application infrastructure components that includes servers, databases, PaaS, SaaS components.

References:

Cimpanu, Catalin. “Indian Govt Agency Left Details of Millions of Pregnant Women Exposed Online.” *ZDNet*, ZDNet, 1 Apr. 2019, https://www.zdnet.com/article/indian-govt-agency-left-details-of-millions-of-pregnant-women-exposed-online/

“Security Checklist.” *Security Checklist - MongoDB Manual*, https://docs.mongodb.com/manual/administration/security-checklist/#enable-access-control-and-enforce-authentication.