KariAnn Harjo

ITSE 1450

Module 9 Discussion 2

Database security should be more granular and data-centric compared to the broader system security. It requires implementing robust access controls that limit data access based on user roles and the principle of least privilege, ensuring individuals can access only the data necessary for their job functions. Encryption of data at rest and in transit is also crucial for databases, as it ensures that even if data is intercepted or the system is breached, the information remains unintelligible without the proper decryption keys.

For web-based data designs, security concerns are heightened due to the potential exposure to a wider range of threats over the internet. It necessitates additional measures such as web application firewalls, rigorous input validation to prevent SQL injection attacks, and the use of secure, authenticated APIs for data access. Regularly updating and patching the database management systems and web applications to close any known vulnerabilities is also essential.