Comprehensive Review of Cybersecurity Threats and Mitigation Strategies to Secure Health Data for a Full-Stack Web Application

Tigist Berhe| Computer Science | Advised by Dr. Heather Guarnera

Overview

The healthcare industry is a prime target for cyber threats because healthcare organizations possess a large amount of sensitive patient data, including **personally identifiable information (PII)** and **protected health information (PHI).** Data breaches cost the healthcare sector an average of $9.23 million per incident. Healthcare organizations increasingly rely on web applications to store and manage sensitive patient data, robust cybersecurity measures are crucial to protect against data breaches, identity theft, and disruptions to patient care.

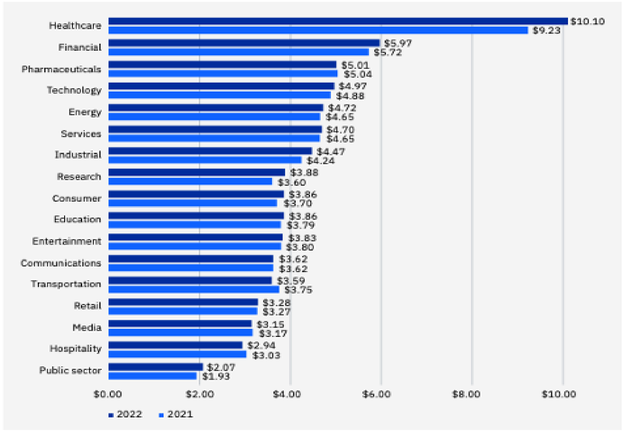
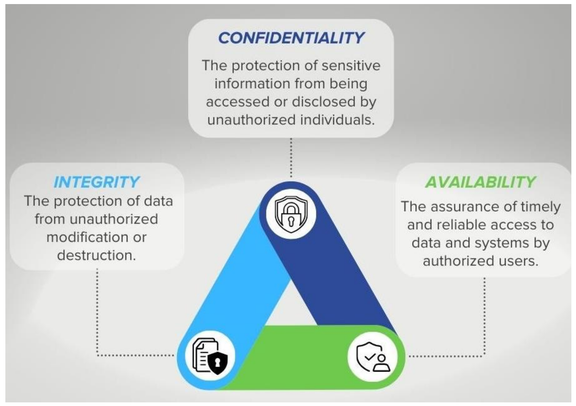


Figure 1. Average Cost of Data Breach by Industry [1]

67% of healthcare cyberattacks impact patient data and 48% impact patient care [3], therefore safeguarding patient information is essential to maintaining patient trust and ensuring the uninterrupted delivery of medical services.

Cybersecurity Threats

The CIA (Confidentiality, Integrity, Availability) triad is a fundamental principle in cybersecurity that addresses cybersecurity threats and is a crucial principle that forms the main security structure and policies of organizations.



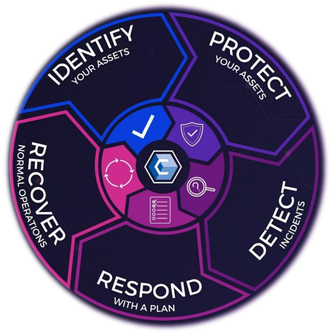
SQL injection: Attackers can exploit database vulnerabilities to access, modify, or delete sensitive patient data, compromising integrity and confidentiality.
Malware attacks: Malicious software can disrupt operations, steal data, and potentially harm patients by tampering with medical devices.
Phishing: Deceptive emails and websites trick users into revealing credentials, enabling unauthorized access to patient records and sensitive information, leading to data breaches and identity theft.

Figure 2. Types of Cyber Security Attacks in Healthcare

Mitigation Strategies

- **Risk Assessments:** conducting assessments to identify vulnerabilities
- **Security Awareness Training:** train employees on cybersecurity practices, social engineering, and phishing attacks.
- **Incident Response Plan:** to respond to security incidents efficiently.
- **Compliance with Regulation:** adheres to relevant regulations like HIPAA

Figure 3. Steps to Mitigate Attacks



Threat Modeling

Threat modeling is a process by which potential threats, such as structural vulnerabilities, can be identified, listed, and prioritized from a hypothetical attacker's point of view.

Figure 3. General Threat Modelling Steps

- **STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege)** provides a structured, goal-oriented approach to identifying threats against each system component.
- **PASTA (Process of Attack Simulation and Threat Analysis)**takes an attack-centric perspective, focusing on data (asset) protection and risk mitigation.

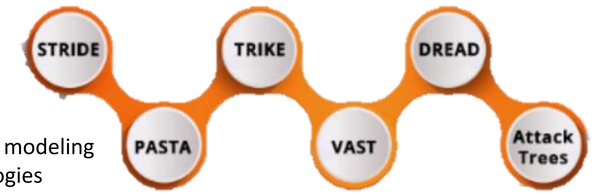


Figure 4. Threat modeling Methodologies

Implementation

The full-stack application is designed with security as a fundamental principle, integrating **input validation** to prevent injection attacks, **two-factor authentication** for robust access control, and **password hashing** for secure credential storage. **Audit logging** and **auto-session logout** mechanisms ensure traceability and mitigate unauthorized access risks. The database is structured in **3NF** to maintain data integrity and support efficient access control. These measures form a resilient shield, protecting patient data against a spectrum of cyber threats.

Conclusion

- Cybersecurity measures go beyond just application features and require a comprehensive approach.
- Understanding networks and their vulnerabilities is crucial.
- Integrate threat modeling and advanced security techniques during early stages of development.
- A well-structured plan for mitigation, prevention, and recovery strategies is crucial.

References:
1. Intraprise Health. (2023, April 6). Cybersecurity Nightmares: The cost of healthcare cyberattacks in 2023. https://intraprisehealth.com/the-cost-of-cyberattacks-in-healthcare/
2. Varghese, J. (2023, November 23). What is Web Application Security Testing? Astra Security Blog. https://www.getastra.com/blog/security-audit/web-application-security-testing/
3. William Stallings. Computer security principles and practice. 2015
4. Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. Handbook of applied cryptography. CRC press, 2018
5. Lynne Coventry and Dawn Branley. "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward". In: Maturitas 113 (2018), pp. 48–52