Spotting_OpenMRS_Threats_&_Weaknesses

Task:

Brainstorm at least 5 threats and 5 vulnerabilities for our OpenMRS system. Don't worry about being too detailed. For threats, ask "Who or what could intentionally or accidentally harm our system or data?" For vulnerabilities, ask "Where are we weak or exposed?" Jot them down in two columns (**Threats** vs. **Vulnerabilities**). This quick brainstorm will flex your risk-thinking muscles!

Answer:

6 **Threats** to our OpenMRS system.

1. Insider data misuse.
2. Power outage.
3. Natural/Accidental threats like hardware failure or software bugs causing data corruption.
4. Unauthorized access due to weak session management. Lack of authentication timeouts or session expiration increases the risk of unauthorized access if a user leaves a session open.
5. Hackers on the internet might target patient data and malware could infect the system, or a ransomware attack could attempt to encrypt the OpenMRS database.
6. Man-in-the-Middle (MitM) Attack. If network traffic between OpenMRS clients and servers is not properly encrypted, attackers on the same network could intercept, alter, or steal sensitive data in transit.

6 **Vulnerabilities** in our OpenMRS system.

1. OpenMRS Coding flaws.
2. No encryption on backups.
3. Process weakness like lack of staff training (falling prey to phishing).
4. No antivirus.
5. Lack of backup power or replication.
6. Configuration weaknesses - AWS S3 bucket with backups isn't set to private (data leak), or default passwords left in place on the OpenMRS admin account.

Reflection Prompt:

Which potential threat to OpenMRS concerns you the most, and why? Take a moment to consider which "bad scenario" feels most realistic or scary in our case study (e.g., a hacker breach vs. an insider misuse vs. system failure). This helps reveal what you (or your organization) might be most anxious to protect against.

Answer:

There are several potential threats that worry me. However, I think most concerning right now is **Insider Data Misuse** which is particularly concerning for several reasons:

1. **Prevalence and Impact**: Insider threats are common in healthcare, with a large percentage of data breaches attributed to insiders, often due to negligence or curiosity rather than malice. This can lead to unauthorized access, data theft, or misuse, compromising patient confidentiality and trust.

2. **Difficulty in Detection**: Insider threats can be extremely challenging to detect because they originate from within the organization. Insiders often have legitimate access to systems and data, making it harder to distinguish between authorized and unauthorized actions.
3. **Regulatory Consequences**: Insider breaches can lead to significant regulatory fines and reputational damage, especially under HIPAA, which emphasizes accountability and proper handling of PHI.
4. **Variety of Insider Threats**: Insider threats can range from accidental disclosure to intentional data theft or manipulation, making them a broad and persistent risk that requires ongoing vigilance and mitigation strategies to stay ahead of the curve.

With these factors in mind, addressing insider threats through education, monitoring, and strong access controls is crucial for protecting patient data and maintaining compliance with HIPAA regulations.