Threat Modeling for Healthcare Provider's Patient Database

• System Overview

The healthcare provider's patient database stores sensitive information such as personal identifiable information (PII), medical records, treatment history, and payment details. The database is accessed by healthcare professionals, administrative staff, and occasionally by patients through a web portal.

• Assets

The primary assets that need protection include:

- **Patient Medical Records**: Diagnoses, treatment history, lab results, prescriptions, etc.
- **Personal Identifiable Information (PII)**: Names, addresses, Social Security numbers, dates of birth, contact details.
- **Payment Information**: Billing details, insurance information, and payment history.
- **Login Credentials**: Usernames, passwords, and authentication tokens used to access the system.

• Potential Threat

- **Unauthorized Access**: Attackers may attempt to gain access to sensitive data by exploiting weak authentication mechanisms or leveraging compromised credentials.
- **Data Breaches**: Sensitive patient data could be leaked or exposed, leading to legal and financial repercussions.
- **Insider Threats**: Employees or contractors with legitimate access to the system may intentionally or accidentally misuse the data.
- **Malware/Ransomware Attacks**: Attackers might deploy ransomware to encrypt patient data and demand ransom for decryption keys.
- **Data Tampering**: An attacker might modify or delete medical records, affecting patient care and trust in the system.
- **Denial of Service (DoS) Attacks**: An attacker might flood the system with traffic, rendering it unavailable for patients and healthcare providers, disrupting operations.
- **Man-in-the-Middle (MitM) Attacks**: Interception of data transmissions between the healthcare provider's system and external users could lead to data leaks.

- **Vulnerabilities**
    - **Weak Password Policies**: Simple, easily guessable passwords or a lack of multi-factor authentication (MFA).
    - **Unpatched Software**: The system may use outdated software, making it vulnerable to known exploits.
    - **Improper Access Controls**: Insufficient role-based access control (RBAC) that allows users to access data they shouldn't.
    - **Misconfigured Firewalls or Security Groups**: Misconfigurations that leave the system vulnerable to external threats.
    - **Unencrypted Data**: Data stored in plain text or transmitted without encryption could be intercepted or compromised.
    - **Third-Party Dependencies**: Reliance on third-party software or services could introduce vulnerabilities if those are compromised.

- **Potential Attacks and Exploits**
    - **Phishing Attacks**: Attackers could use social engineering tactics to obtain login credentials from employees.
    - **SQL Injection**: If the system does not properly sanitize user inputs, attackers might inject malicious queries to access or modify the database.
    - **Credential Stuffing**: Attackers may use previously leaked credentials to attempt unauthorized logins.
    - **Privilege Escalation**: Attackers might exploit system vulnerabilities to gain higher-level access and modify or delete data.
    - **Zero-Day Exploits**: Unknown vulnerabilities in the software that are exploited before patches are available.

- **Risks**
    - **Data Exposure**: Unauthorized parties gain access to sensitive data, leading to identity theft or medical fraud.
    - **Reputation Damage**: A breach could severely damage the healthcare provider's reputation, leading to loss of trust from patients and stakeholders.
    - **Legal and Regulatory Penalties**: Non-compliance with healthcare regulations like HIPAA can result in hefty fines and legal actions.
    - **Service Disruption**: Interruptions in access to patient data could delay treatments and disrupt operations.

- **Financial Loss**: Ransomware attacks could lead to financial losses, whether through ransom payments or recovery efforts.

• Impact

- **Patient Safety**: Altered or unavailable medical records can lead to improper treatments, potentially harming patients.
- **Regulatory Compliance**: Non-compliance with healthcare regulations such as HIPAA could lead to investigations, fines, and sanctions.
- **Loss of Business**: Patients may lose trust in the healthcare provider and switch to competitors, resulting in financial losses.

• Mitigation Strategies

- **Implement Strong Authentication**: Enforce strong password policies and implement multi-factor authentication (MFA).
- **Regular Software Updates and Patching**: Ensure the system is regularly updated to mitigate vulnerabilities.
- **Encrypt Sensitive Data**: Both in transit (using HTTPS/TLS) and at rest to protect against data theft.
- **Access Controls and Auditing**: Implement role-based access control (RBAC) and regularly audit access logs to detect suspicious activity.
- **Security Awareness Training**: Conduct regular training for staff to recognize phishing attempts and handle sensitive data securely.
- **Network Security**: Use firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to detect and block malicious traffic.