Threat Modeling in Healthcare System

Threat: There are lots threats involved in the health care system. Below there some of the list

* Malware: Malicious software such as ransomware, viruses that may slowdown the system or lock the database.
* DDoS Attack: Overloading systems by unnecessary traffic.
* Phishing Attacks: Social engineering tactics to steal credentials or gain unauthorized access.
* Insider Threats: Employees or contractors with access to sensitive information may misuse it intentionally or unintentionally.

Vulnerabilities: Weakness may present in the system that may not be addressed. Series of vulnerabilities are:

* Outdated software: There may be some security flaws in unpatched software.
* Weak Authentication: There may be no multi factor authentication enabled may prone to brute force or password guessing attack.
* Poor Configured Networks. There may be some of the open ports present in the networks that may be exploited by the attackers or may be using HTTP protocol for website.
* Insufficient encryption: Data in hospital is crucial, not encrypting data with proper technology or algorithms may lead to data breach.
* Legacy System: Using older hardware may lead to hardware vulnerability which is fixed only by changing that hardware.
* Social engineering: Here staff may click on malicious links lead to phishing etc.

Attacks: Using vulnerabilities, attackers intrude in the system, exfiltrating the data etc. Following attacks are:

* Ransomware attack: Encrypting data and demanding a ransom for decryption.
* SQL Injection: Exploiting vulnerabilities in web applications to gain access to databases.
* Credential Stuffing: Using stolen credentials to access accounts.
* Man-in-the-Middle (MitM) Attacks: Intercepting communications between healthcare providers and systems
* Data Breaches: Unauthorized access to patient records and other sensitive data.

Risks: What are consequences after attack happens . Risks are,

* Data Loss: Loss of critical patient data due to cybersecurity.
* Operational Disruptions: Interruption of healthcare services, leading to delayed or missed treatments.
* Patient Safety Risks: Compromised systems affecting patient care and safety.
* Financial Loss: Costs associated with breaches, fines for non-compliance, and loss of reputation.

Exploits: There are number of consequences due the attacks by the attackers.

* Remote Code Execution : Exploiting vulnerability to run malicious code on victim system.
* Zero-day Exploits: Attacks using unknow vulnerabilities .
* Privilege Escalation : Gaining higher lever access to perform unauthorized actions.
* Supply chain attack: Targeting third-party vendors to compromise the healthcare provider’s systems.

Assets:

* Electronic Health Records (EHR): Digital version of patient charts, including medical history, diagnoses, and treatment plans.
* Medical Devices: Connected devices like pacemakers, insulin pumps, and imaging equipment.
* Healthcare IT Infrastructure: Servers, databases, networks, and applications.
* Patient Data: Personal and medical information of patients.
* Staff Credentials: Login information and access rights of healthcare workers.
* Research Data: Clinical trial data, research outcomes, and intellectual property.

Impacts:

* Compromised patient data: Exposure of sensitive patient data .
* Disruption in Healthcare Services: Inability to provide timely care due to system outages .
* Reputational Damage: Loss of trust in the healthcare provider, leading to patient and partner dissatisfaction.
* Financial Penalties: Fines and legal costs due to non-compliance with regulations.
* Patient Harm: Potential for physical harm if medical devices are compromised or if treatment is delayed.