-: AIIMS Data Breach (2022) – A Major Cyberattack in India: -

Overview

The All-India Institute of Medical Sciences (AIIMS), Delhi, suffered a massive ransomware attack in November 2022, disrupting its digital services for two weeks. This was one of the biggest cyberattacks on India's healthcare sector.

Key Details of the Attack:

- **Date:** November 23, 2022
- **Type of Attack:** Ransomware & Data Breach
- **Attack Method:** Hackers encrypted hospital servers and demanded a ransom of ₹200 crore in cryptocurrency.
- **Impact:**
    - 40 million patient records were compromised, including sensitive details of VIPs, politicians, and military officials.
    - AIIMS had to switch to manual operations for weeks.
    - 5 physical servers were severely damaged, leading to a complete system failure.
- **Suspected Attackers:** Chinese hackers (**APT41**, an advanced persistent threat group) were suspected, though no official confirmation was made.

Legal Implications Under IT Act, 2000

Since the AIIMS breach involved ransomware, data theft, and disruption of critical infrastructure, several sections of the **IT Act, 2000** are applicable:

- **Section 43, 66, 66B, 66C, 66D, 66F, 70 and 72**

Section 43	Unauthorized Access & Damage to Computer System	● Gained unauthorized access ● Compensation can be claimed for financial and operational damages

Section 66	Computer related offences (Hacking with Criminal Intent)	• involved unauthorized access, data theft, and destruction of records
Section 66B	Dishonestly receiving stolen computer resource or communication device	• personal and medical records were stolen
Section 66C	Identity Theft & Fraudulent Use of Credentials	• patient records were misused or sold on the dark web
Section 66D	Cyber Fraud (Impersonation for Financial Gain)	• Attacker misuse the data for financial fraud, ransom demands, or identity theft
Section 66F	Cyber Terrorism	• Since AIIMS is critical healthcare infrastructure
Section 70	Protection of Critical Information Infrastructure	• AIIMS falls under Critical Information Infrastructure (CII) as it serves millions of patients, including government officials.
Section 72	Breach of Privacy and Confidentiality	• Personal medical records were leaked or sold

-: Attack Model Design on AIIMS Data Breach: -

1. Threat Actor (Attacker Group):
    a. Reconnaissance Specialists
    b. Phishing Experts
    c. Exploit Developers
    d. Persistence & Lateral Movement Team
    e. Data Exfiltration & Encryption Team
2. Motivation of Attack:
    a. Primary motive: cyber-Espionage & intelligence Gathering
        i. Highly sensitive data i.e. medical records of politicians, military officials, and diplomats.
        ii. It could use health data for blackmail, surveillance, or intelligence operations.
    b. Secondary motive: Infrastructure Disruption and Psychological Warfare
        i. By shutting down Digital services
        ii. Fear & uncertainty
    c. Financial motive (False Flag Random Demand)
3. Attack Pattern:
    a. Reconnaissance (Information Gathering)
    b. Initial Access (Phishing & Exploits)
    c. Credential theft & Privilege Escalation
    d. Lateral Movement & Data Exfiltration
    e. Ransomware Deployment & System Lockdown
    f. Covering Tracks & Persistence
4. Entry Point (How attackers Got into the system):
    a. Primary entry point is phishing & Social Engineering
    b. Secondary entry point: Exploiting Unpatched Software
    c. Third Entry Point: Third-party IT Vendor Compromise
5. Impact on AIIMS, India:
    a. 40 million patient records compromised, including VIPs, military officers and government officials.
    b. AIIMS digital services were down for two weeks, causing delay in patient treatment.
    c. Financial loss due to system restoration costs and forensic investigation
    d. It has huge impact on National Security & Economic loss

AIIMS Data Breach (2022) - MITRE ATT&CK Mapping

Click here for details