AIIMS Cyber-Attack

Published On: 01-12-2022

In News: Securing our Networks: AIIMS cyber-attack is a wake-up call for national security. Ransomware attack increasing in India.

What is Ransomware?

Ransomware is a type of malware. It restricts user access to his computer files until a ransom is paid to unlock it. The file/Data in the infected computers gets locked up in such a way that the user cannot access them anymore. It then demands payment in cryptocurrency Bitcoin to retrieve the locked files.

Last year, A Ransomware named WannaCry has attacked 75,000 computers worldwide in 99 countries. WannaCry has used a hacking tool named Eternal Blue. The hacking tool Eternal Blue gives unprecedented access to all computers using Microsoft Windows. It was developed by NSA to gain access to computers used by terrorists and enemy states.

What are the forms of Cyber-Attack?

A cybersecurity threat is a malicious act that includes threats like computer viruses, data breaches, and Denial of Service (DoS) attacks. A cyber threat damages data, steals data, or disrupts digital life in general.

1. Global Examples of Cyber Attacks:
2. The advent of the Stuxnet Worm in 2010 resulted in large-scale damage to Iran's centrifuge capabilities.
3. In 2012, data from Saudi Aramco Oil Company computers were wiped out by Iranian operatives by employing malware.
4. The ransomware attack on Colonial Pipeline in 2021 was the largest cyberattack on an oil infrastructure.
5. Indian Examples of Cyber Attacks:
6. The data from an exam for the recruitment of police officers in 2019 in India was hacked which resulted in a leak of sensitive information of all the participants.
7. In 2021, a huge leak of customer data was experienced by the famous pizza brand namely, Dominos, India.
8. In 2021, the records of over 10 crore users were leaked from India-based digital payment company MobiKwik.

AIIMS Cyber-Attack:

- Halting access: The organisation's critical data is encrypted so that they cannot access files, databases, or applications stored on the main and backup servers of the hospital.
- Ransom demand: The attackers have made an undisclosed demand to be sought in cryptocurrency in exchange for a key that would decrypt the data.
- Multi-agency investigation: The extent and threat of the attack is so much that multiple agencies like Delhi Police, the Centre's Computer Emergency Response Team (CERT-In), the Ministry of Home Affairs, and even the National Investigation Agency have joined the probe.
- Contingency plan: Meanwhile, AIIMS Delhi has decided to get four new servers from the Defence Research and Development Organisation (DRDO) to be used on an immediate basis to provide e-hospital facility for patients.

Challenges faced by cybersecurity frameworks:

- Rising cyber espionage: Some nation-states have very strong cyber-attack capabilities and use them fairly readily in a world where large-scale conventional wars have become less likely.
- The cyber domain is especially anarchic, which means that the “cyber strong can do what they can, and the cyber weak must suffer what they must.”
- It also permits extreme asymmetry, enabling small countries like Israel and Singapore, or regimes like North Korea, to wield vastly disproportionate power within the domain.
- Investments in cybersecurity discourage lower-grade attackers and divert them to seek softer targets elsewhere. This, in turn, means that Indian networks must be as well-defended as their foreign peers, as a relative weakness will make us more attractive targets.
- Cybersecurity and cyber defence require the government, private sector, academia, civil society and citizens to collaborate intimately in a non-hierarchical, networked fashion.
- Lack of understanding of comprehensive cyber strategy. Bars development of effective international laws and norms.

Way Forward:

- Creating strong privacy and data protection laws: which keep both corporate and state power in check.
- Civil-military cooperation: requiring the government to have “tentacles” in telecom and private networks. Civil-military collaboration requires unambiguous civil-military separation.
- Generating trust: To create trust, we must clearly define rights, legal roles and responsibilities of the government, private sector and citizens, and scrupulously respect them. Measures like declaring cyber strategies, creating formal structures, appointing experts and allocating budgets, can only work in an environment of mutual trust.
- Well trained cybersecurity personnel and equipment: to be embedded across public, private and academic networks.
- Follow ‘3-2-1 backup’ approach: Healthcare entities must save 3 copies of each type of data in 2 different formats, including 1 offline. This is an industry best practice to make healthcare institutes cyber secure.