Celebration of Cyber Jaagrookta (Awareness) Diwas (CJD)

(on the first Wednesday of every month

commencing April,2022 onwards)

Central Mine Planning & Design Institute Ltd.
RANCHI

Cyber Attack

Part-1

4th May, 2022

What is a Cyber Attack?

It’s a malicious and deliberate attempt to breach information systems in order to benefit from disrupting the victims’ networks.

Broad types of Cyber Attacks

Un-targeted cyber attacks

In un-targeted attacks, attackers indiscriminately target gullible devices, services and users. There’s no specific target and machines or services with vulnerabilities are attacked. Internet, by design, indirectly aids this.

Targeted cyber attacks

In a targeted attack, devices are singled out because of specific interest in them. The groundwork for the same may take time, but a targeted attack is often more damaging than an un-targeted one.

Malware

- Malware describes malicious software like spyware, ransomware, viruses, and worms. Malware breaches a network through a vulnerability, usually when a user clicks a dangerous link or email attachment which in turn installs risky software.

Phishing

- Phishing is the act of sending fraudulent communications that appear to come from a reliable source. Typically email is used. The goal is to steal sensitive information or to install malware on the victim’s machine. Phishing is a very common cyber threat.

MiM

- Man-in-the-middle (MiM) attacks, also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction with the intention of interrupting the traffic to steal data.
- Two common points of entry for MitM attacks:
- 1. On not so secure public Wi-Fi, attackers can insert themselves between a visitor's device and the network.
- 2. On an infected device, an attacker can install software to steal information.

DoS

- A denial-of-service attack bombards systems, servers, or networks with excessive traffic to consume resources and bandwidth. As a result, the system struggles to fulfill legitimate requests. When multiple compromised devices are used to launch this attack, that's called distributed-denial-of-service (DDoS) attack.

Insider Threat

- An insider threat does not involve a third party but an insider. Usually, it’s an individual from within the organization who has lots of information on the organization. Insider threats have the potential to cause serious disruptions.

Zero-Day Exploit

- A Zero-Day Exploit happens after the announcement of a new network vulnerability which has no immediate solution. The vendor notifies the vulnerability so that the users become aware. Usually, this news also reaches the attackers.

Drive-by Attacks

- In these types of attacks, hackers insert malicious scripts into various websites and end up getting access to all the confidential documents of the users who visit the websites.

Brute Force

- It’s a method of randomly trying out different passkeys or passwords for unlocking the victim’s system. It is one of the oldest types of cyber attacks and is still prevalent.

This campaign shall continue……….