Types of Cybersecurity Attacks

1. DoS and DDoS Attacks

A denial-of-service attack is designed to overuse the resources of a system to the point where it is unable to reply to legitimate service requests. A distributed denial-of-service (DDoS) attack also seeks to drain the resources of a system. A DDoS attack is initiated by a vast array of malware-infected host machines controlled by the attacker. With a DoS attack, the target site gets flooded with illegitimate requests. Because the site must respond to each request, its resources get consumed by all the responses. This makes it impossible for the site to serve users as it normally does and often results in a complete shutdown of the site.

2. MITM Attacks

Man-in-the-middle (MITM) attack makes it possible for an attacker to eavesdrop on the data sent back and forth between two people, networks, or computers. It is called a “man in the middle” attack because the attacker positions themselves in the “middle” or between the two parties trying to communicate. In effect, the attacker is spying on the interaction between the two people.

3. Phishing Attacks

A phishing attack occurs when an attacker sends emails that seem to be coming from trusted, legitimate sources in an attempt to grab sensitive information from the target. Phishing attacks combine social engineering and technology and are so-called because the attacker is, in effect, “fishing” for access to a forbidden area by using the “bait” of a seemingly trustworthy sender. To execute the attack, the attacker may send a link that brings you to a website that then fools you into downloading malware such as viruses or giving the attacker your private information. In many cases, the target may not realize they have been compromised, which allows the attacker to go after others in the same organization without anyone suspecting malicious activity.

4. Trojan Horses

A trojan horse attack uses a malicious program that is hidden inside a seemingly legitimate one. When the user executes the disguised program, the malware inside the Trojan can be used to open a backdoor into the system through which hackers can penetrate the computer or network. An unsuspecting user may welcome an innocent-looking application into their system only to usher in a hidden threat.

5. Eavesdropping Attacks

Eavesdropping attacks involves the attacker intercepting traffic as it is sent through the network. In this way, an attacker can collect usernames, passwords, and other confidential information like credit cards. This is a type of MITM attack. One of the best ways of preventing them is by encrypting your data, which prevents it from being used by a hacker.

6. Malware Attack

Malware is a software that infects a computer and changes how it functions, destroys data, or spies on the user or network traffic as it passes through. Malware can either spread from one device to another or remain in place, only impacting its host device. Several of the attack methods described above can involve forms of malware, including MITM attacks, phishing, Trojan horses. In a malware attack, the software must be installed on the target device. This requires an action on the part of the user. Therefore, in addition to using firewalls that can detect malware, users should be educated regarding which types of software to avoid, the kinds of links they should verify before clicking, and the emails and attachments they should not engage with.