PHYSICAL ATTACKS

How Can a Cyberattack Be Physical?

It's no longer true to think of the digital world created by computers as being in a vacuum from the real one. Since computers are tangible objects, physical assaults may be possible against them. Attackers may physically interact with the computer during these attacks, or they may use physical objects like flash drives or smartcards.

Malicious USB Devices

When it comes to physical strikes, smart cards don't get to have all the fun. Malware is frequently distributed through USB drives, also referred to as flash drives. Some malwares can execute immediately automatically and discreetly as soon as the disk is plugged into a computer, even though it is packed in a way that needs a user to manually start it.

However, dangers don't just exist with storage devices: Malicious USB charging stations and cables have been reported in the past. One instance featured a USB charging cord for an electronic cigarette that had a tiny chip buried within the connector that was infected with malware. Without the user's knowledge, it would try to install its payload of malware onto the machine when plugged in.

Furthermore, this is not just a simple trick. Malicious USB devices were initially used to spread Stuxnet, a cyberweapon intended to attack Iranian nuclear enrichment facilities. The centrifuges used to process uranium were subsequently physically destroyed by the virus, demonstrating that cyberattacks can have both physical consequences and physical delivery.

Physical Hacking

An attacker's options expand when they have physical access to a computer. For instance, it might be challenging to steal a password from a secure computer using only digital means. However, the process gets significantly simpler if an attacker can physically install a keylogging device.

By simply unplugging an unencrypted hard drive from one computer and inserting it into another one that can access its information, OS-based security can be disregarded for unencrypted hard drives. It is considerably simpler to search through computer and mobile phone hard drives and locate intriguing or unique files thanks to specialized digital forensics tools. Even though a lot of this software is designed for ethical hackers, it can still be used maliciously in the wrong hands.

Externally accessing a computer's running RAM is one of the trickiest and most sophisticated methods for obtaining information from it. Though challenging and requiring incredibly specialized tools, this is doable.

A network may appear secure behind a firewall, but a hacker with physical access to a network port may connect a microcomputer to the network and then to cellular data. Networks are not immune to physical attacks. The attacker will then be able to target machines on that network without going via the firewall thanks to the microcomputer acting as a backdoor into the system.

(Not So) Smart Cards

Physical hacking attempts frequently target smart cards. It's quite simple to steal information from various types of them because they're frequently utilized for finances or gaining access to secure regions.

One method, known as skimming, involves an attacker using a false card reader to copy or skim data from a card. Credit cards are frequently used for this, but ID cards and other smart card kinds can also use it. In places with little surveillance, like ATMs or petrol pumps, these skimmers are frequently physically affixed to real card readers.

Smart cards can also be "cloned," which goes one step further and involves writing data to a blank card to make a duplicate of an existing smart card. While this information can be obtained via skimming, some smart card kinds are considerably simpler to copy: Smart cards that employ RFID technology can be copied without direct physical contact, and hardware that can fit in a backpack and automatically take the data from any nearby RFID cards is available.

Some penetration testers use this type of cloning as a common tactic. For example, they might browse their phone while sitting on a bench in front of a target building with their backpack next to them. The moment an employee sits down on the same bench, their credit card information is taken.

Conclusion

Security online is crucial. However, in the context of cybersecurity, physical security cannot be disregarded. It's critical to understand how physical attacks can jeopardize assets whether you're managing security for a huge company or yourself.

It is a good idea to enforce security regulations that forbid plugging in unknown USB devices by turning off unused USB ports in machines' BIOS. Keycard cloning can be prevented with the use of RFID blocking wallets and more secure smart cards that do more than just hold data.