**CYBER SECURITY**

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, security includes both cybersecurity and physical security. Cybersecurity includes controlling physical access to the hardware, as well as protecting against harm that may come through network access, data and code.

Elements of cyber security include:

* Application Security
* Information Security
* Network Security
* Operational Security
* Business continuity planning

One of the most problematic elements of cybersecurity is constant evolving nature of security risks. The traditional approach has been to focus most resources on the most crucial system components and protect against the biggest known threats, which necessitated leaving some less important system components undefended and some less dangerous risks not protected against. Such an approach is insufficient in the current environment. According to Forbes, the global cybersecurity market reached $75 billion for 2015 and is expected to reach high upto $170 billion in 2020.

**Different types of Cyberattacks:-**

Denial-Of-Service Attack: Denial of service attacks are designed to make a machine or network resource unavailable to its intended users. Attackers can deny service to individual victims, such as by wantedly entering a wrong password enough consecutive times to cause the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once.

Direct-Access Attack: An unauthorized user gaining physical access to a computer is most likely able to directly copy data from it. They may also compromise security by making operating system modifications, installing software worms, covert listening devices or using wireless mice.

Backdoor: A backdoor in a computer system, a cryptosystem or an algorithm, is any secret method of bypassing normal authentication or security controls. They may exist for a number of reasons, including by original design or from poor configuration.

Phishing: Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details directly from users. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Preying on a victim's trust, phishing can be classified as a form of social engineering.

**Recent Cyber Attacks:**

* Ransomware: WannaCry ransomware attack was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. The attack began on Friday, 12 May 2017, and within a day was reported to have infected more than 230,000 computers in over 150 countries. Parts of the United Kingdom's National Health Service (NHS), Spain's Telefónica, FedEx and Deutsche Bahn were hit, along with many other countries and companies worldwide. Shortly after the attack began, Marcus Hutchins, a 22-year-old web security researcher from North Devon in England, who blogs as "MalwareTech", discovered an effective **kill switch** by registering a domain name he found in the code of the ransomware. This greatly slowed the spread of the infection, effectively halting the initial outbreak on Monday, 15 May 2017.

WannaCry propagates using Eternal Blue, an exploit of Windows Server Message Block protocol. Microsoft eventually discovered the vulnerability, and on Tuesday, March 14, 2017, they issued security bulletin MS17-010, which detailed the flaw and announced that patches had been released for all Windows versions that were currently supported at that time, these being Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2012, and Windows Server 2016, in addition to Windows Vista.

**Kill Switch:** The software contained a URL that, when discovered and registered by a security researcher to track activity from infected machines, was found to act as a "kill switch" that shut down the software before it executed its payload, stopping the spread of the ransomware. The researcher speculated that this had been included in the software as a mechanism to prevent it being run on quarantined machines used by anti-virus researchers.

On 19 May, it was reported that hackers were trying to use a “Mirai” botnet variant to effect a distributed attack on WannaCry's kill-switch domain with the intention of knocking it offline. On 22 May, MalwareTechBlog protected the domain by switching to a cached version of the site, capable of dealing with much higher traffic loads than the live site.

* Petya: Petya was first discovered in 2016. The malware targets Microsoft Windows-based systems, infecting the master boot record to execute a payload that encrypts a hard drive's file system table and prevents Windows from booting. It subsequently demands that the user make a payment in Bitcoin in order to regain access to the system.

In June 2017, a new variant of Petya was used for a global cyberattack, primarily targeting Ukraine. On 27 June 2017, a major global cyberattack began utilizing a new variant of Petya. Kaspersky Lab reported infections in France, Germany, Italy, Poland, the United Kingdom, and the United States, but that the majority of infections targeted Russia and Ukraine, where more than 80 companies initially were attacked, including the National Bank of Ukraine. ESET estimated on 28 June 2017 that 80% of all infections were in Ukraine, with Germany second hardest hit with about 9%.

Petya utilizes a payload that infects the computers master boot record, overwriting the Windows bootloader, and then triggering a restart. On the next startup, the payload is executed, which encrypts the Master File Table of the NTFS file system, and then displays the ransom message demanding a payment made in Bitcoin. During this process, text purportedly output by ‘chkdsk’, is displayed on-screen, suggesting that the hard drive's sectors are being repaired. The original payload required the user to grant it administrative privileges; one variant of Petya was bundled with an alternate payload known as Mischa, which is used if Petya fails to install. Mischa is a more conventional ransomware payload that encrypts user documents, as well as executable files, and does not require administrative privileges to execute. The earlier versions of Petya disguised its payload as a PDF file, attached to an e-mail.