International Journal of Emerging Technology and Innovative Engineering
Volume 4, Special Issue 4, April 2018 (ISSN: 2394 – 6598)
Paper Received on:17.03.2018
Paper Published on:27.03.2018

CYBER SECURITY

A.K.Santhosh Madhavan (9917004133)
Email ID: smartsandy6119@gmail.com
Surya Velavan.C.G (9917004155)
Email ID: surya.velavan.9@gmail.com

Cybersecurity, **computer security** or **IT security** is the protection of computer systems from the theft and damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide.

Cybersecurity includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection. Also, due to malpractice by operators, whether intentional or accidental, IT security is susceptible to being tricked into deviating from secure procedures through various methods.

The field is of growing importance due to the increasing reliance on computer systems and the Internet, wireless networks such as Bluetooth and Wi-Fi, the growth of "smart" devices, including smartphones, televisions and tiny devices as part of the Internet of Things.

VULNERABILITY

A vulnerability is a weakness in design, implementation, operation or internal control. Most of the vulnerabilities that have been discovered are documented in the Common Vulnerabilities and Exposures (CVE) database.

INFORMATION SECURITY

To manage the information security, five steps should be taken: Pre-evaluation, strategic planning, operative planning, implementation, and post-evaluation.

- Pre-Evaluation: to identify the awareness of information security within employees and to analyze the current security policy.
- Strategic Planning: to come up with a better awareness program, clear targets need to be set. Clustering people is helpful to achieve it.
- Operative Planning: a good security culture can be established based on internal communication, management-buy-in, and security awareness and a training program.
- Implementation: four stages should be used to implement the information security culture. They are commitment of the management, communication with organizational members, courses for all organizational members, and commitment of the employees.

SYSTEM AT RISK

The growth in the number of computer systems, and the increasing reliance upon them of individuals, businesses, industries and governments means that there are an increasing number of systems at risk.

ATTACKER MOTIVATION

As with physical security, the motivations for breaches of computer security vary between attackers. Some are thrill-seekers or vandals, some are activists, others are criminals looking for financial gain.

COMPUTER PROTECTION

In computer security a countermeasure is an action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

VULNERABILITY MANAGEMENT

Vulnerability management is the cycle of identifying, and remediating or mitigating vulnerabilities, especially in software and firmware. Vulnerability management is integral to computer security and network security.

REDUCING VULNERABILITIES

It is possible to reduce an attacker's chances by keeping systems up to date with security patches and updates, using a security scanner or/and hiring competent people responsible for security.

REGULATIONS PASSED IN INDIA FOR CYBER SECURITY

Some provisions for cyber security have been incorporated into rules framed under the Information Technology Act 2000.

The National Cyber Security Policy 2013 is a policy framework by Ministry of Electronics and Information Technology (MeitY) which aims to protect the public and private infrastructure from cyber attacks, and safeguard "information, such as personal information (of web users), financial and banking information and sovereign data". CERT- In is the nodal agency which monitors the cyber threats in the country.

Every 40 seconds, a company gets hit by a ransomware

The scars of Wannacry have not healed yet, but there comes a new ransomware attack to haunt the cyber world again. Petya, another ransomware has hit organizations. Unfortunately, 2017 is being swept by the ransomware wave and this does not seem to end.

2017's BIGGEST CYBER ATTACK

WANNACRY

2017 witnessed the biggest ever cyber attack in the Internet history. A ransomware named Wannacry stormed through the network. It targeted computers running Windows OS that are not up-to-date and brought computer systems from Russia to China and the US to their knees.

PETYA

The second massive cyber attack, a variant of the ransomware Petya re-emerged using the same Eternal Blue exploit and hit organizations worldwide, especially Ukraine. It is found to exploit MS Office and SMBv1 vulnerabilities and has worm capabilities, which allows it to spread quickly across infected networks.

Fireball:

Fireball is a Chinese malware that affected nearly 250 million computers worldwide with India among the worst-hit countries. This Cyber attack was designed to hijack browsers and turn them into zombies. It is capable of executing any code on infected machines, resulting in a wide

range of actions from stealing credentials to dropping additional software nasties.

JOB MARKET

Cybersecurity is a fast-growing field of IT concerned with reducing organizations' risk of hack or data

- Security analyst
- Security engineer
- Security architect
- Security administrator
- Chief Information Security Officer (CISO)
- Chief Security Officer (CSO)
- Security Consultant/Specialist/Intelligence

ADVANTAGES OF CYBER SECURITY

- PROTECT system against viruses, worms, spyware, and other unwanted programs.
- Protection against data from theft.
- Protects the computer from being hacked.
- Minimizes computer freezing and crashes.
- Gives privacy to users.

DISADVANTAGES OF CYBER SECURITY

- Firewalls can be difficult to configure correctly.
- Incorrectly configured firewalls may block users from performing certain actions on the Internet, until the firewall configured correctly.
- Makes the system slower than before.
- Need to keep updating the new software in order to keep security up to date.
- Could be costly for average users.

Cyber Security can be used for good and also for bad purposes, but it is according to the user accessing the system. Nowadays, it is being one of the part of the internet field as a good purpose of making security to each and every sites and computers. Cyber Crime branch is trying hard to stop the opposition of the attackers for their wealth.

Maybe, this becomes a better place for security or a disastrous area to lose all of the user's identity.