CYBER SECURITY

Law

Vishwanatha
shravani

ABSTRACT

Continuous protection of organisation's digital information is important.Organisations face a complex threat landscape with an increasing rate of cyberattacks. Mobility, bring your own device,virtualisation, the cloud, and social media have opened new doors into an organisation. cyber security expertise and experience are needed to secure the organisation. Take advantage of comprehensive digital security solutions that span your IT infrastructure, on premises and in the cloud, to respond swiftly to any security incident.

KEYWORDS

INTRODUCTION:

As the technology is increasing day by day, many people fall victim to cyber theft. This high development of technology and the availability of internet to most of the public broadens the pathway of cyber-crime. Cyber-Security was once not a serious issue. But, now many people are complaining about their credit card information getting stolen or sudden drop of credits in their bank account.

The internet has become the integral part of today's generation of people. Many people share their information out in the web through social networking sites like Facebook, Twitter, Instagram etc. Internet has touched every aspect of life right from the beginning to the present. As people share their personal information online; most of their accounts get hacked by cyber-criminal or in other world's black hat hackers. And, trusting internet nowadays isn't a wise thing to do.

With the growing use of the internet by people, protecting sensitive information has become which must be taken into consideration, quite seriously. Otherwise, the internet can be one of the dangerous places to visit if one's sensitive information isn't being protected. If a computer doesn't have proper security controls then it has high chances of getting infected by malwares, malicious logic and hence, any type of information in that computer can be accessed easily within moments. And, there are many millions of websites on internet which are infected with malwares and spy-programs. Which allows a hacker to gain illegal access to the specific computer, once the computer has browsed the domain name of the malicious website or if the spy-program is downloaded into the computer. It is very important to stay secure while you are online or else it might be very risky to lose your personal information.

Cyber-attacks can be caused due to negligence and vulnerabilities. One can be a victim of cyber-attack due to his own ignorance of the vulnerabilities which his system shows. Which also means that one can stay secure online by blocking ways by which a hacker can come. He can do this by installing an anti-virus (such as, Avira, Norton, MacAfee, Kaspersky etc.), updating the application which he uses for browsing internet etc. Few other ways are, not surfing websites that isn't secure. Well, this might sound a minor thing. But, it's one of the most important things which must be followed in order to stay secure online. According to a study conducted on 2012, most of the internet users don't bother whether the website they visit is secured or not. Due this, many of the information registered on the website gets duplicated. Such as, credit card initials while making a purchase, their official email password while linking their account. All these can prove fatal if the hacker gets all this personal information.

One more thing what a person can do to stay secure is; by not clicking a link or downloading an application, which is sent via mail to him by an unauthorized person. If the email shows up in spam folder then also he shouldn't open it. In case, if the person downloads the application then his anti-virus must be turned on, in order to scan the downloaded application. Otherwise, his PC could be vulnerable to viruses and malware program. If he doesn't have an anti-virus and he downloads the application then what's going to happen is; his monitor screen suddenly flashes and shuts down. And, when here starts his PC, he notices that it doesn't function as it used to before. These symptoms are cause of the presence of virus inside his desktop.

We as a human tend to ignore things most of the time. And, this can be very dangerous when it comes to surfing web online and downloading applications. Hackers make use of paths which we tend to ignore. And, most of the attacks which we receive from them can be brutal. In earlier this year, there were a team of black hat hackers who created a ransomware were called Wannacry. Within moments of its release to the internet, many multimillion companies including FedEx and Amazon faced huge loss. This ransomware is so powerful that it spreads through a connected network.

For example, you have logged into some website and you see an ad which says "Click here to win $20,000. Only few contestants will be chosen for this draw. Hurry!! ". So, due to your interest in the draw. You tend to click it. So, while you are directed to another website through the link; a new application gets downloaded without your notice and it initiatives the launch of its written commands. Your screen flashes in a moment and all you notice is a message saying that "All your files have been encrypted and in order for you to decrypt it, you will have to pay sum of $300 in bit coins. If you don't make a payment within 3 days to the give address then the amount will be double for each day. If you are unable to make the payment within 7 days then, all your files will be lost!". This is exactly what happens when Wannacry ransomware gets into your computer.

Nowadays hackers are so good in their field. That they wipe out traces of crime in such a way; that it is almost impossible to find the cyber-criminal. If you are one of the targets of a hacker. He always tries his best to keep track of you. And, once you fall into his hands then that's the biggest mistake you have ever made. If a hacker gets into your network, say Wi-fi then he can manipulate its security setting and also have detailed log about your browsing. He can also get access to the devices that are connected to your Wi-fi. And, in case if one of your computers has your personal information then he can access it within moments. In order, to get around this issue of a hacker getting in your home network; first, you should make sure that all the devices connected into your network are all trusted devices. And, it is recommended that you must have a strong WPA2 security password. Or else, if you are using any other security type like WEP, then the password can be cracked within minutes. The next step is to regularly update your router's firmware (security settings). Regularly updating router's firmware can literally keep hackers from getting into your network. Also, keep in mind that if you disable your firewall then no matter how much you update your firmware. It's of no use until your firewall is enabled.

Normally, what firewall do is; they block the data coming from outside the network. They pretend as a thick layer of filter that denies the penetration of unwanted or harmful data that comes from the internet. So, in order to have a strong firewall, all you need to do is block all the outbound connection and allow all the inbound connection. This makes sure that the data on the internet can be accessed through inbound connection. But, no user will be able to penetrate into you network unless and until he is connected to your network. Meaning, blocking the outbound connection, you make the firewall stronger in such a way that other users who aren't connected to your network won't be able to access your files or see the devices connected to your network.

What cyber security can prevent

The purpose of cyber security is to help prevent cyber attacks, data breaches and identity theft and can aid in risk management. When an organization has a strong sense of network security and an effective incident response plan, it is better able to prevent and mitigate cyber-attacks. For example, end user protection defends information and guards against loss or theft while also scanning computers for malicious code.

Types of cyber security threats:

The process of keeping up with new technologies, security trends and threat intelligence is a challenging task. However, it's necessary in order to protect information and other assets from cyber threats, which take many forms.

- **Ransomware** is a type of malware that involves an attacker locking the victim's computer system files typically through encryption and demanding a payment to decrypt and unlock them.
- **Malware** is any file or program used to harm a computer user, such as worms, computer viruses, Trojan horses and spyware.
- **Social engineering** is an attack that relies on human interaction to trick users into breaking security procedures in order to gain sensitive information that is typically protected.
- **Phishing** is a form of fraud where fraudulent emails are sent that resemble emails from reputable sources; however, the intention of these emails is to steal sensitive data, such as credit card or login information

Elements of cyber security:

Ensuring cyber security requires the coordination of efforts throughout an information system, which includes:

- Application security.
- Information security.
- Network security.
- Disaster recovery/business continuity.
- Planning.
- Operational security.
- End-user education.

One of the most problematic elements of cyber security is the continually evolving nature of security risks. The traditional approach has been to focus resources on crucial system components and protect against the biggest known threats, which meant leaving components undefended and not protecting systems against less dangerous risks.

Reasons for Commission of Cyber Crimes:

There are many reasons which act as a catalyst in the growth of cybercrime. Some of the prominent reasons are

a. Money: People are motivated towards committing cybercrime is to make quick and easy money.

b. Revenge: Some people try to take revenge with other person organization/society/caste or religion by defaming its reputation or bringing economical or physical loss.

This comes under the category of cyber terrorism.

c. Fun: The amateur do cybercrime for fun. They just want to test the latest tool they have encountered.

d. Recognition: It is considered to be pride if someone hack the highly secured networks like defense sites or networks.

e. Anonymity: Many time the anonymity that a cyber space provide motivates the person to commit cybercrime as it is much easy to commit a cybercrime over the cyber space and remain anonymous as compared to real world. It is much easier to get away with criminal activity in a cyber-world than in the real world. There is a strong sense of anonymity than can draw otherwise respectable citizens to abandon their ethics in pursuit personal gain.

f. Cyber Espionage: At times the government itself is involved in cyber trespassing to keep eye on other person network/country. The reason could be politically,economically socially motivated.

Cyber laws in India:

India has enacted the first I.T. Act, 2000 based on the UNCITRAL model recommended by the general assembly of the United Nations.

Offences under IT act are:

- Tampering with computer source document.
- Hacking with computer systems, data alterations.
- Publishing obscene information.
- Un-authorized access to protected systems.
- Breach of confidentiality and privacy.
- Publishing false digital signature certificates.

Benefits of cyber security:

Benefits of utilizing cyber security includes:

- Business protection against malware, ransomware, phishing and social engineering.
- Protection for data and networks.
- Prevention of unauthorized users.
- Improves recovery time after a breach.
- Protection for end-users.
- Improved confidence in the product for both developers and customers.

Prevention:

- Use hard to guess passwords.
- Use anti-virus software and firewalls-keep them up to date.
- Don't open email or attachments from unknown sources.
- Backup your computer on disk or CD often.

Recommendations:

- Fostering Linkages.
- Creation liaison with international community will create sharing of experiences and good practices.
- The value of fostering co-operation internationally with other countries/regions and parties needs to be enhanced.
- Co-operation between governments.

CONCLUSION:

I would like to conclude by saying that, there is no 100% security in today's era. Nor, will there be in the future. So, don't expect an un-authorized user not to have accessed your files if connected to you network. Or in other words, don't think that they can't access any of your files. And, always update your systems and network's security settings. Always make sure that your anti-virus performs full system-scan every week. So, that your desktop stays virus and malware free.

REFERENCES:

1. www.wikipedia.org
2. www.avtest.org
3. www.billmullins.blogspot.com
4. www.digit/forum.com
5. www.antivirusnews.com