International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

Cyber Security : Impact and Preventions

Manvee Bansal, Jaspreet Kaur, Amanpreet Kaur, C.K Raina

Adesh institute of technology, Kharar, Chandigarh, Punjab, India

ABSTRACT

Cyber Security has become very important in today world, as a result of which various methods are adopted to bypass it. Cyber administrators need to keep up with the recent advancements in both the hardware and software fields to prevent their as well as the users data. This paper outlines the various attack methods which are used, as well as various defense mechanisms against them.

Keywords : Cyber Security, Computer security, IT security, Fraud, Child pornography, Bullying, Cyber stalking, Copyright infringement

I. INTRODUCTION

CYBER SECURITY

"Cyber security is a national security" Computer security, also known as cyber security or IT security, is the protection of computer systems from the theft or damage to the hardware, software or the information on them, as well as from disruption or misdirection of the services they provide. Cyber security refers to protecting the websites domains or servers from various forms of attack.

Network security is important in every field of today's world such as military, government and even in our daily lives. Having the knowledge of how the attacks are executed we can better protect ourselves. The architecture of the network can be modified to prevent these attacks, many companies use firewall and various polices to protect themselves. Network security has a very vast field which was developed in stages and as of today, it is still in evolutionary stage. To understand the current research being done, one must understand its background and must have knowledge of the working of the internet, its vulnerabilities and the methods which can be used to initiate attacks on the system. Internet has become more and more widespread, in today's world internet is available everywhere in our house, in our workplace, mobiles, cars everything is connected to the internet and if an unauthorized person is able to get access to this network he can not only spy on us but he can easily mess up our lives. It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and injection, and due to malpractice by operators, Whether intentional, accidental, or due to them being tricked into deviating from secure procedures. The field is of growing importance due to the increasing reliance on computer systems and the Internet in most societies, wireless networks such as Bluetooth and Wi-Fi and the growth of smart devices, including smart phones, televisions and tiny devices as part of the Internet of Things.

CYBER CRIME

What is Cybercrime?

Cybercrime is a bigger risk now than ever before due to the sheer number of connected people and devices. You often hear the term 'cybercrime' bandied about these days, as it's a bigger risk now than ever before due to the sheer number of connected people and devices. But what is it exactly? In a nutshell, it is simply a crime that has some kind of computer or cyber aspect to it. To go into more detail is not as straightforward, as it takes shape in a variety of different formats. We've put together this guide with some interesting and often alarming facts, to make it a little easier to digest:

Cybercrime: The facts

- ✓ Cybercrime has now surpassed illegal drug trafficking as a criminal moneymaker
- ✓ Somebody's identity is stolen every 3 seconds as a result of cybercrime
- ✓ Without a sophisticated security package, your unprotected PC can become infected within four minutes of connecting to the Internet.
- ✓ Criminals committing cybercrime use a number of methods, depending on their skill-set and their goal. Here are some of the different ways cybercrime can take shape:

    - ✓ Theft of personal data
    - ✓ Copyright infringement
    - ✓ Fraud
    - ✓ Child pornography
    - ✓ Cyber stalking
    - ✓ Bullying

As you can see, cybercrime covers a wide range of different attacks, that all deserve their own unique approach when it comes to improving our computer's safety and protecting ourselves. Symantec draws from all the different interpretations of cybercrime and defines it concisely as "any crime that is committed using a computer network or hardware device".

The computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime. The crime may take place on the computer alone or in addition to other locations. The broad range of cybercrime can be better understood by dividing it into two overall categories, defined for the purpose of this research as Type I and Type II cybercrime. Let's take a look at them both:

Type 1 cybercrime:-

- ✓ Usually a single event from the perspective of the victim. An example would be where the victim unknowingly downloads a Trojan horse virus, which installs a keystroke logger on his or her machine. The keystroke logger allows the hacker to steal private data such as internet banking and email passwords.
- ✓ Another common form of Type 1 cybercrime is phishing. This is where the victim receives a supposedly legitimate email (quite often claiming to be a bank or credit card company) with a link that leads to a hostile website. Once the link is clicked, the PC can then be infected with a virus.
- ✓ Hackers often carry out Type 1 cybercrime by taking advantage of flaws in a web browser to place a Trojan horse virus onto the unprotected victims computer
- ✓ Any cybercrime that relates to theft or manipulation of data or services via hacking or viruses, identity theft, and bank or e-commerce fraud.
- ✓ Type 2 cybercrime:-

- ✓ Type 2 cybercrime tends to be much more serious and covers things such as cyber stalking and harassment, child predation, extortion, blackmail, stock market manipulation, complex corporate espionage, and planning or carrying out terrorist activities.
- ✓ It is generally an on-going series of events, involving repeated interactions with the target. For example, the target is contacted in a chat room by someone who, over time, attempts to establish a relationship. Eventually, the criminal exploits the relationship to commit a crime. Or, members of a terrorist cell or criminal organization may use hidden messages to communicate in a public forum to plan activities or discuss money laundering locations, for example.

More often than not, it is facilitated by programs that do not fit under the classification crime ware. For example, conversations may take place using IM (instant messaging) clients or files may be transferred using FTP.

II. METHODS AND MATERIAL

MANAGEMENT OF CYBER SECURITY RISKS

The risks associated with any attack depend on three factors: threats (who is attacking), vulnerabilities (the weaknesses they are attacking), and impacts (what the attack does). The management of risk to information systems is considered fundamental to effective cyber security.

What Are the Threats?

People who actually or potentially perform cyber attacks are widely cited as falling into one or more of five categories: criminals intent on monetary gain from crimes such as theft or extortion; spies intent on stealing classified or proprietary information used by government or private entities; nation-state warriors who develop capabilities and undertake cyber attacks in support of a country's strategic objectives; "hacktivists" who perform cyber attacks for nonmonetary reasons; and terrorists who engage in cyber attacks as a form of non-state or state-sponsored warfare.

What Are the Vulnerabilities?

Cyber security is in many ways an arms race between attackers and defenders. ICT systems are very complex, and attackers are constantly probing for weaknesses, which can occur at many points. Defenders can often protect against weaknesses, but three are particularly challenging: inadvertent or intentional acts by insiders with access to a system; supply chain vulnerabilities, which can permit the insertion of malicious software or hardware during the acquisition process; and previously unknown, or zero-day, vulnerabilities with no established fix. Even for vulnerabilities where remedies are known, they may not be implemented in many cases because of budgetary or operational constraints.

What Are the Impacts?

A successful attack can compromise the confidentiality, integrity, and availability of an ICT system and the information it handles. Cyber theft or cyber espionage can result in ex filtration of financial, proprietary, or personal information from which the attacker can benefit, often without the knowledge of the victim. Denial-of-service attacks can slow or prevent legitimate users from accessing a system. Botnet malware can give an attacker command of a system for use in cyber attacks on other systems. Attacks on industrial control systems can result in the destruction or disruption of the equipment they control, such as generators, pumps, and centrifuges.

III. RESULTS AND DISCUSSION

PREVENTIONS

Keep your computer current with the latest patches and updates:-

One of the best ways to keep attackers away from your computer is to apply patches and other software fixes when they become available. By regularly updating your computer, you block attackers from being able to take advantage of software flaws (vulnerabilities) that they could otherwise use to break into your system. While keeping your computer up-to-date will not protect you from all attacks, it makes it much more difficult for hackers to gain access to your system, blocks many basic and automated attacks completely, and might be enough to discourage a less-determined attacker to look for a more vulnerable computer elsewhere.

More recent versions of Microsoft Windows and other popular software can be configured to download and apply updates automatically so that you do not have to remember to check for the latest software. Taking advantage of "auto-update" features in your software is a great start toward keeping yourself safe online.

Make sure your computer is configured securely:-Keep in mind that a newly purchased computer may not have the right level of security for you. When you are installing your computer at home, pay attention not just to making your new system function, but also focus on making it work securely.

Configuring popular Internet applications such as your Web browser and email software is one of the most important areas to focus on. For example, settings in your Web browser such as Internet Explorer or Firefox will determine what happens when you visit Web sites on the Internet.

Choose Strong Passwords and Keep Them Safe

Passwords are a fact of life on the Internet today—we use them for everything from ordering flowers and online banking to logging into our favorite airline Web

site to see how many miles we have accumulated. The following tips can help make your online experiences secure:

- ✓ Selecting a password that cannot be easily guessed is the first step toward keeping passwords secure and away from the wrong hands. Strong passwords have eight characters or more and use a combination of letters, numbers and symbols (e.g., # $ % ! ?).
- ✓ Keep your passwords in a safe place and try not to use the same password for every service you use online.
- ✓ Change passwords on a regular basis, at least every 90 days. This can limit the damage caused by someone who has already gained access to your account. If you notice something suspicious.
- ✓ with one of your online accounts, one of the first
- ✓ steps you can take is to change your password.

Protect your computer with security software

Several types of security software are necessary for basic online security. Security software essentials include firewall and antivirus programs. A firewall is usually your computer's first line of defense-it controls who and what can communicate with your computer online. You could think of a firewall as a sort of "policeman" that watches all the data attempting to flow in and out of your computer on the Internet, allowing communications that it knows are safe and blocking "bad" traffic such as attacks from ever reaching your computer.

The next line of defense many times is your antivirus software, which monitors all online activities such as email messages and Web browsing and protects an individual from viruses, worms, Trojan horse and other types malicious programs.

Protect your Personal Information

Exercise caution when sharing personal information such as your name, home address, phone number, and email address online. To take advantage of many online services, you will inevitably have to provide personal information in order to handle billing and shipping of purchased goods. Since not divulging any personal information is rarely possible, the following list contains some advice for how to share personal information safely online

Keep an eye out for Phony Email Messages

Things that indicate a message may be fraudulent are misspellings, poor grammar, odd phrasings, Web site addresses with strange extensions, Web site addresses that are entirely numbers where there are normally words, and anything else out of the ordinary. Additionally, phishing messages will often tell you that you have to act quickly to keep your account open, update your security, or urge you to provide information immediately or else something bad will happen. Don't take the bait.

Don't respond to email messages that ask for personal information

Legitimate companies will not use email messages to ask for your personal information. When in doubt, contact the company by phone or by typing in the company Web address into your Web browser. Don't click on the links in these messages as they make take you to a fraudulent, malicious Websites.

Pay attention to privacy policies on Web sites and in software

It is important to understand how an organization might collect and use your personal information before you share it with them

Guard your Email Address

Spammers and phisher sometimes send millions of messages to email addresses that may or may not exist in hopes of finding a potential victim. Responding to these messages or even downloading images ensures you will be added to their lists for more of the same messages in the future. Also be careful when posting your email address online in newsgroups, blogs or online communities.

Review Bank and Credit Card Statements Regularly

The impact of identity theft and online crimes can be greatly reduced if you can catch it shortly after your

data is stolen or when the first use of your information is attempted. One of the easiest ways to get the tip-off that something has gone wrong is by reviewing the monthly statements provided by your bank and credit card companies for anything out of the ordinary.

IV.CONCLUSION

"Nothing is secure it will only if either the system is not working or not in use" As internet has become a huge part of our daily life, the need of cyber security has also increased exponentially from the last decade. The most important thing that we want to secure the system is only awareness. As more and more users connect to the internet it attracts a lot of criminals. Today, everything is connected to internet from simple shopping to defense secrets as a result there is huge need of cyber security. Billions of dollars of transactions happens every hour over the internet, this need to be protected at all costs. Even a small unnoticed vulnerability in a network can have disastrous affect, if company's records are leaked it can put the users data such as their banking details and credit card information at risk, numerous software's such as intrusion detection have been which prevents these attacks, but most of the time it's because of a human error that these attacks occur. Most of the attacks can be easily prevented, by following many simply methods as outlined in this paper. As new and more sophisticated attacks occur, researchers across the world find new methods to prevent them. Numerous advancements are being made in the field of network security both in the field of hardware and software, it's a continuous cat and mouse game between network security analyst and crackers and as the demand of internet shows no signs of decreasing it's only going to get a lot harder.

V. REFERENCES

[1]. National workshop on cyber security at Punjab University.
[2]. https://in.norton.com/cybercrime-prevention/promo
[3]. https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101
[4]. https://in.norton.com/cybercrime-victim/promo
[5]. https://in.norton.com/cybercrime-crimeware/promo
[6]. https://www.fbi.gov/investigate/cyber