International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 04 | April - 2022 Impact Factor: 7.185 ISSN: 2582-3930

RESEARCH PAPER ON CYBERSECURITY

Subhangani
Student, Department of CSE, Dronacharya College of Engineering, Gurgaon, Haryana, India

ABSTRACT

We live in the digital era. We use the internet and electronic media for paying bills, purchasing any items, watching a movie, doctor's prescription, ordering food, and everything else. Due to this widespread use, there are innumerable incidents of security breach, fraud, malicious attack, etc. reported. To keep the internet age well-ordered and safe for users we need cybersecurity. It protects you from cyber-criminals, hackers, criminal syndicates, insiders, script kiddies, hacktivists and anybody who wants to damage you or your asset financially, mentally or engage in data theft online.

Introduction

In daily life we use information for various purposes and use the network for communication and exchange information between different parties. In many cases this information is sensitive so we need to take care that only authorized parties can get that information. We general users are almost ignorant as to how those random bits of 1's and 0's reach securely to our computer. For a hacker, it is a golden age. With so many access points, public IP's (Internet Protocol), and constant traffic and tons of data to exploit, cybercriminals are having one hell of a time exploiting vulnerabilities and creating malicious software for the same. Above that, cyber-attacks are evolving by the day. Hackers are becoming smarter and more creative with their malware and how they bypass virus scans and firewalls still baffles many people.

Therefore, there must be some sort of protocol that protects us against all those cyberattacks and makes sure our data does not fall into wrong hands. For maintaining such privacy, it requires some mechanism or physical device which ensures that it is safe. Such mechanisms or physical devices are known as *security systems*.

Cybersecurity

Privacy and security of the data will always be top security measures that any organization takes care of. We are presently living in a world where all information will be maintained in digital or cyber form. Today's generation spends most of their time on social networking sites to interact with their friends and family. Cyber-criminals would continue to target social media sites to steal personal data. Not only social networking sites but also during bank transactions a person must take all the security measures. The figure below shows the data breaches in various companies.

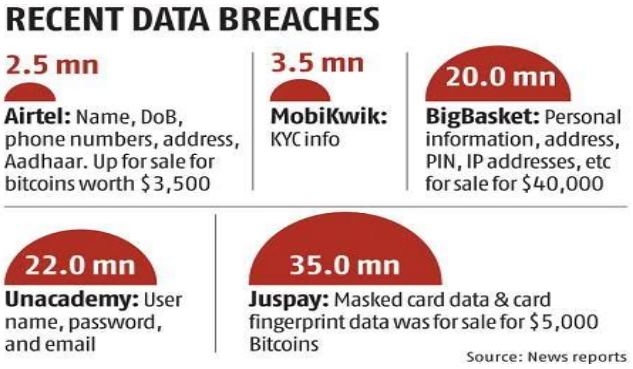

Fig.1

Computer Security is the protection afforded to an automated information system in order to attain the applicable objective of preserving the *integrity*, *availability*, and *confidentiality* of information system resources. Computer security introduces three key objectives that are at the heart of computer security.

How does Cyber Security make working so easy?

As digital transformation and hyper-convergence create unintended gateways to risks, vulnerabilities, attacks, and failures, a cyber resiliency strategy quicky becomes necessary for your business. A cyber resiliency strategy helps your business to reduce risks, financial impact and reputational damages. The more your data and applications traverse an increasingly interconnected infrastructure of on-premises, public cloud and multi cloud environments, the more ways cyber attackers can disrupt the continuity of your business. The complex nature of hybrid multi cloud environments expose your critical data and system configurations to higher levels of risk than ever before, so much so that the likelihood of a successful cyberattack has become an absolute certainty. No matter how vigilant your IT security team may be, a cyberattack will eventually lead to a business disruption in the form of an outage, data theft or data corruption—causing reputational damage and financial fallout. So, Cybersecurity tools help to defend against those risks and make our work very easy. It protects business-critical applications and data, and helps accelerate recovery from data breaches or similar disruption.

Types of Cyber Security Threats

Phishing Attacks

These attacks are mainly executed by sending a large number of emails to different users requesting them to click a fake link or provide sensitive information.

Sometimes a phishing email will be disguised as a legitimate and trustworthy software program. The sender will often request you to click a link and type in your password, which they will steal and use to hack into your accounts.

Denial-of-Service Attacks

A denial-of-service (DoS) attack is a type of cyber-attack often conducted on a business or large computer system. These cyber-attacks are carried out by flooding a network or data center with large amounts of traffic to slow down their systems, so they cannot perform their normal services for legitimate users.

Once the system becomes unusable, a cyber attacker might employ other methods of gaining access to sensitive information.

Malware

Malware is short for malicious software, and there are many different types that can affect your computer system. You might have heard the terms trojan, worm, and virus. These terms explain how malware infects your computer.

- Worm – This type of malware is a singular piece of software that reproduces and spreads from computer to computer.
- Trojan – This type of malicious code does not reproduce, but it is disguised as a type of program the user would normally install. Once the user clicks on the fake executable file, the program is implanted into the hard drive and causes damage from there.
- Virus – This type of malware attack uses a standalone software program as its vehicle. The virus implants a piece of malicious code into the program and forces it to take malicious actions against the user's computer system.
- Spyware– This type of cyber threat spies on an unsuspecting user and gathers information from their computer systems without them knowing. Sometimes spyware will log your keystrokes or monitor the information you send and receive online.

Ransomware

It is a type of malicious software. It is considered to extract currency by blocking contact to records or the PC system until the deal is paid. Paying the ransom does not ensure that the records will be recuperated or the system returned.

Goals of Cybersecurity

The definitive objective of cybersecurity is to defend the data from actuality stolen or cooperated. To attain this, we aspect at 3 important goals of cybersecurity.

Confidentiality covers two concepts.

- Data Confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

- Privacy: Assures that individual's control or influence what information related to them may be collected and stored and by whom that information may be disclosed.

Methods to safeguard Confidentiality:

- Data encryption
- Two or Multifactor verification
- Confirming Biometrics

Integrity covers two concepts.

- Data integrity: Assures that systems work promptly and service is not denied to unauthorized users.
- System integrity: Assures that the system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Availability assures that systems work promptly and service is not denied to authorized users.

- Threat: A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a danger that might exploit vulnerability.

Cyber Security Solutions

1. Use strong password and review for change password regularly: The concept of Username and Password is fundamental way of protecting the data. This is one of the first measures for security.
2. Antivirus protection and firewall: Antivirus (AV) protection software has been the most prevalent solution to fight malicious attacks. AV software blocks malware and other malicious viruses from entering your device and compromising your data. Using a firewall is also important when defending your data against malicious attacks. A firewall helps screen out hackers, viruses, and other malicious activity that occurs over the Internet and determines what traffic is allowed to enter your device.
3. Two-Factor or Multi-Factor authentication: It is a service that adds additional layers of security to the standard password method of online identification. It is an additional authentication method such as OTP, verification code or fingerprint.
4. Malware scanners: This is the software that usually scans all files and documents present in the system for malicious code and harmful viruses like viruses, worms, and Trojan horses.
5. Aware of phishing frauds: A few important cyber security tips to remember about phishing schemes include:

- Bottom line – Do not open emails from people you do not know
- Know which links are safe and which are not – hover over a link to discover where it directs you to. Copy the link and search it to various tools and check whether it is malicious or not.
- Be suspicious of the emails sent to you in general – look and see where it came from and if there are grammatical errors. Sometime the “from” in sender is different from actual sender that is envelope sender.
- Malicious links can come from friends who have been infected too. So don’t click on that.

Conclusions

Computer security is important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. The most important thing is awareness on the individual level. Due to lack of awareness, it is difficult to regulate these crimes. Laws along with individual awareness can help to make less vulnerable to cybercrime. The latest and disruptive technologies, along with the new cyber tools and threats that become known each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no perfect solution for cyber-crimes but we should try our level best to minimize them.

References

- https://www.business-standard.com/
- https://cipher.com/blog/10-personal-cyber-security-tips-cyberaware/
- https://www.thehindu.com/news/national/cybercrime-went-up-by-500-per-cent-during-pandemic-chief-of-defence-staff/article37457504.ece
- https://www.kyndryl.com/in/en/services/business-continuity/cyber-resilience?gclid=Cj0KCQiAjc2QBhDgARIsAMc3SqSozN6jyTcgIuHPhi-ukE7_Msz-RfL_nugo4fhoruVX17b-XAeNRu8aAs_lEALw_wcB&gclsrc=aw.ds
- https://triadanet.com/different-types-of-cyber-security/