International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 05 | May -2020 ISSN: 2582-3930

Cyber Security

Neenu Ann Sunny
Department of Computer Applications
Saintgits College of Applied Sciences Pathamuttom Kerala India

Abstract :Cyber security is a necessary consideration for information technology as well as Internet services. Whenever we think about the cyber security we think of 'cybercrime' which is
increasing day by day. Various governments and companies are talking many measures to prevent the cybercrime. . It refers to the body of technologies, processes, and it may also be referred to as information technology security. The field is of growing importance due to increasing reliance on computer systems, including smart phones, televisions and the various tiny devices that constitute the Internet of Things.

Keywords: IT security, Internet of things (IOT).

➢ INTRODUCTION

Cyber security is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, etc. Cyber security is the protection of Internet-connected systems, including hardware, software, and data from cyber attacks. It is made up of two words one is cyber and other is security. Cyber is related to the technology which contains systems, network and programs or data. Whereas security related to the protection which includes systems security, network security and application and information security. It is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access. It may also be referred to as information technology security.

➢ What is Cyber Security ?

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

➢ WHY DO WE NEED CYBER SECURITY ?

The range of operations of cyber security involvesprotecting information and systems from major cyberthreats. These threats take many forms. As a result, keeping pace with cyber security strategy and operations can be a challenge, particularly in government and enterprise networks where, in their most innovative form, cyber threats often take aim at secret, political and military assets of a nation, or its people. Some of the common threats are :[1]

- **Cyber terrorism**
  Cyberterrorism can be also defined as the intentional use of computers, networks, and public internet to cause destruction and harm for personal objectives. Experienced cyberterrorists, who are very skilled in terms of hacking can cause massive damage to government systems, hospital records, and national security programs, which might leave a country, community or organization in turmoil and in fear of further attacks. The objectives of such terrorists may be political or ideological since this can be considered a form of terror.

- **Cyber warfare**
  Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.

- **Cyber spying**
  Cyber spying is the act or practice of obtaining secrets and information without the permission and knowledge of the holder of the information from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet, networks or individual computers through the use of proxy servers.**[3]**

➢ Who are Cyber Criminals ?

Cyber criminals, also known as hackers, often use computer systems to gain access to business trade secrets and personal information for malicious and exploitive purposes. Hackers are extremely difficult to identify on both an individual and group level due to their various security measures, such as proxies and anonymity networks, which distort and protect their identity. Cybersecurity experts assert that cyber criminals are using more ruthless methods to achieve their objectives and the proficiency of attacks is expected to advance as they continue to develop new methods for cyber attacks. The growth of the global cyber criminal network, which is largely credited to the increased opportunity for financial incentives, has created a number of different types of cyber criminals, many of which pose a major threat to governments and corporations.

- **Identity Thieves**

Identity thieves are cyber criminals who try to gain access to their victims' personal information – name, address, phone number, place of employment, bank account, credit card information and social security number. They use this information to make financial transactions while impersonating their victims. Identity theft is one of the oldest cyber crimes, gaining prominence during the early years of the Internet. Initially, these cyber criminals leveraged basic hacking techniques, such as modifying data and leveraging basic identity fraud to uncover the desired information. Today, the practice has progressed in scope and technique due to advances in computing, and now, many identity thieves can hack into a government or corporate database to steal a high-volume of identities and personal information. This expansion of strategy has resulted in major losses for companies and consumers, with recent studies indicating that approximately $112 billion has been stolen by identity thieves over the past six years.

- **Internet Stalkers**

Internet stalkers are individuals who maliciously monitor the online activity of their victims to terrorize and/or acquire

personal information. This form of cyber crime is conducted through the use of social networking platforms and malware, which are able to track an individual's computer activity with very little detection. The motives for such attacks can differ depending on the cyber criminal, but many internet stalkers seek to acquire important information that they can use for bribery, slander, or both. Businesses should be aware of internet stalkers, as well as the strategies that they utilize, in case their employees are ever victims of this cyber attack. If left unaddressed, internet stalkers could cause emotional distress to the team or even obtain data for blackmail.

- **Phishing Scammers**

Phishers are cyber criminals who attempt to get ahold of personal or sensitive information through victims' computers. This is often done via phishing websites that are designed to copycat small-business, corporate or government websites. Unsuspecting computer users often fall prey to such activities by unknowingly providing personal information including home addresses, social security numbers, and even bank passwords. Once such information is obtained, phishers either use the information themselves for identity fraud scams or sell it in the dark web. It's important for businesses to constantly be aware of phishing scams, particularly scams that may be trying to copycat their own business site. Such sites can tarnish the company's reputation and brand, which could potentially lead to a decrease in earnings.

- **Cyber Terrorists**

Cyber terrorism is a well-developed, politically inspired cyber attack in which the cyber criminal attempts to steal data and/or corrupt corporate or government computer systems and networks, resulting in harm to countries, businesses, organizations, and even individuals. The key difference between an act of cyberterrorism and a regular cyber attack is that within an act of cyber terrorism, hackers are politically motivated, as opposed to just seeking financial gain.[3]

➢ **How To Maintain Effective Cyber Security**

Historically, organizations and governments have taken a reactive, "point product" approach to combating cyber threats, produce something together individual security technologies – one on top of another to safe their networks and the valuable data within them. Not only is this method expensive and complex, but news of damaging cyber breaches continues to dominate headlines, rendering this method ineffective. In fact, given the area of group of people of data breaches, the topic of cyber security has launched to the top of the priority list for boards of directors, which they seeked as far as less risky way. Instead, organizations can consider a natively integrated, automated Next-Generation Security Platform that is specifically designed to provide consistent, prevention-based protection – on the endpoint, in the data centre, on the network, in public and private clouds, and across Saabs environments. By focusing on prevention, organizations can prevent cyber threats from impacting the network in the first place, and less overall cyber security risk to a manageable degree. [1]

➢ **What Cyber Security Can Prevent**

cyber security can 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 serious of these attacks.[1].

➢ **Types of Cyber Security Threats**

new technologies, security trends and threat intelligence is a challenging their task. However, it should be in order to protect information and other assets from cyber threats, which take many forms.

- **Social Engineered Trojans**

Social engineering, in the context of information security, is the psychological manipulation of people into performing actions or divulging confidential information. This differs from social engineering within the social sciences, which does not concern the divulging of confidential information.

- **Unpatched Software**

Unpatched software refers to computer code with known security weaknesses. Once the vulnerabilities come to light, software vendors write additions to the code known as "patches" to cover up the security "holes." Running unpatched software is a risky activity because by the time a patch emerges, the criminal underground is typically well-aware of the vulnerabilities.

- **Phishing**

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

- Network traveling worms

Network travelling worms are computer programs that can harm and damage computer networks once they gain access to them.

- **Malware**

Malware, or malicious software, is any program or file that is harmful to a computer user. Types of malware can include computer viruses, worms, Trojan horses and spyware. These malicious programs can perform a variety of different functions such as stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity without their permission.

➢ **What does a security analyst do ?**

An information security analysts protects to safe the company's systems and networks by planning and carrying out measures of security. They create disruptive solutions to prevent critical information from being stolen, damaged, or compromised. Their primary responsibility is to keep a business or organizations data, clients, employees, and any virtual stored information safe from cyber attacks or hacking of anysort.[1]

➢ **What are the consequences of cyber attack ?**

Cyber attacks can cause electrical blackouts, failure of military equipment and breaches of national security secrets. They can result in the theft of valuable, sensitive data like medical records. They can disrupt phone and computer networks or paralyze systems, making data unavailable.

➢ **THE LEVEL OF CYBER RISK**

As combating cyber-threats has become a highly politicized issue, official statements about the level of threat must also be seen in the context of different bureaucratic entities that compete against each other for resources and influence. , psychological research has shown that risk perception is highly dependent on intuition and emotions, as well as the perceptions of

experts (Gregory and Mendelsohn 1993). Cyber-risks, especially in their more extreme form, fit the risk profile of so-called „dread risks", which appear uncontrollable, catastrophic, fatal, and unknown[1].

➢ REDUCING CYBER – IN - SECURITY

Common Cyber Attacks: Reducing The Impact helps organisations understand what a common cyber attack looks like and explains why all organisations should establish basic security controls and processes, to protect themselves from such attacks.It can be read alongside the recently updated 10 Steps to Cyber Security, which offers more comprehensive guidance on the practical steps organisations can take to improve the security of their networks and the information carried on them The paper does not provide a comprehensive review of sophisticated or persistent attacks, nor a detailed analysis of how those attacks occurred.

Common cyber attacks at-a-glance

The downloadable info graphic below summarises the security controls you can apply to reduce your organisation's exposure to a successful cyber attack.

NCSC Cyber Attacks Infographic
The threat landscape

Before investing in defences, many organisations often want concrete evidence that they are, or will be targeted, by specific threats. Unfortunately, in cyberspace it is often difficult to provide an accurate assessment of the threats that specific organisations face.However, every organisation is a potential victim. All organisations have something of value that is worth something to others. If you openly demonstrate weaknesses in your approach to cyber security by failing to do the basics, you will experience some form of cyber attack.

Reducing your exposure to cyber attack

Fortunately, there are effective and affordable ways to reduce your organisation's exposure to the more common types of cyber attack on systems that are exposed to the Internet. The following controls are contained in the Cyber Essentials, together with more information about how to implement them:

- boundary firewalls and internet gateways - establish network perimeter defences, particularly web proxy, web filtering, content checking, and firewall policies to detect and block executable downloads, block access to known malicious domains and prevent users' computers from communicating directly with the Internet
- malware protection - establish and maintain malware defences to detect and respond to known attack code
- patch management - patch known vulnerabilities with the latest version of the software, to prevent attacks which exploit software bugs
- whitelisting and execution control - prevent unknown software from being able to run or install itself, including AutoRun on USB and CD drives
- secure configuration - restrict the functionality of every device, operating system and application to the minimum needed for business to function
- password policy - ensure that an appropriate password policy is in place and followed

- user access control - include limiting normal users' execution permissions and enforcing the principle of least privilege

If your organisation is likely to be targeted by a more technically capable attacker, give yourself greater confidence by putting in place these additional controls set out in the 10 Steps to Cyber Security:

- security monitoring - to identify any unexpected or suspicious activity
- user training education and awareness - staff should understand their role in keeping your organisation secure and report any unusual activity
- security incident management - put plans in place to deal with an attack as an effective response will reduce the impact on your business

Raising your cyber defences

The Internet can be a hostile environment. The threat of attack is ever present as new vulnerabilities are released and commodity tools are produced to exploit them. Doing nothing is no longer an option. Protect your organisation and your reputation by establishing some basic cyber defences to ensure that your name is not added to the growing list of victims.

CONCLUSION

More highly skilled workers in cybersecurity roles would help the nation respond more robustly to the cybersecurity problems it faces. All organizations need to understand their threat environment and the risks they face, address their cybersecurity problems, and hire the most appropriate people to do that work.

REFERENCES

[1].Overview of cyber security Department of Computer Technology, Sri Krishna Arts & Science College, Coimbatore IJACCE VOL.7 ISSUE 11.NOVEMBER 2018 .

[2]ijcsmc volu.3 issue 2 feb 2014 cyber security –Trend and chanllenges.

[3].Google Seracher

[4].Daniel, Schatz,; Julie, Wall, (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215. Archived from the original on 28 December 2017.

[5].Rouse, Margaret. "Social engineering definition". Tech Target. Archived from the original on 5 January 2018. Retrieved 6 September 2015.

[6].Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017)."Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215.

[7]."Reliance spells end of road for ICT amateurs", 7 May 2013, The Australian

[8].Stevens, Tim. "Global Cyber security: New Directions in Theory and Methods". Politics and Governance. 6 (2).doi:10.17645 /pag.v6i2.1569.

[9]."Computer Security and Mobile Security Challenges". researchgate.net. Archived from the original on 12 October 2016. Retrieved 4 August 2016. Pp-1-35

[10]."Distributed Denial of Service Attack". csa.gov.sg. Archived from the original on 6 August 2016. Retrieved 12 November 2014. 12- 22

[11].Wireless mouse leave billions at risk of computer hack: cyber security firm Archived 3 April 2016 at the Way back Machine.

[12]."Multi-Vector Attacks Demand Multi-Vector Protection". MSSP Alert. July 24, 2018.

[13].Millman, Renee (December 15, 2017). "New polymorphic malware evades three quarters of AV scanners". SC Magazine UK.

[14].Turner, Rik (May 22, 2018). "Thinking about cyber attacks in generations can help focus enterprise security plans". Informa PLC. Ovum.

[15]."Identifying Phishing Attempts". Case. Archived from the original on 13 September 2015.

[16].Arcos Sergio. "Social Engineering" (PDF). Archived (PDF) from the original on 3 December 2013.

[17].Scannell, Kara (24 February 2016). "CEO email scam costs companies $2bn". Financial Times (25 Feb 2016). Archived from the original on 23 June 2016. Retrieved 7 May 2016.

[18]."Bucks leak tax info of players, employees as result of email scam". Associated Press. 20 May 2016. Archived from the original on 20 May 2016. Retrieved 20 May 2016.

[19]."What is Spoofing? – Definition from Techopedia". Archived from the original on 30 June 2016.

[20]."spoofing". Oxford Reference. Retrieved 8 October 2017.

[21].Marcel, Sébastien; Nixon, Mark; Li, Stan, eds. (2014).Handbook of Biometric Anti-Spoofing: Trusted Biometrics under SpoofingAttacks (PDF). London: Springer.doi:10.1007/978-1-4471-6524-8. ISBN 978-1-4471-6524-8. ISSN 2191-6594. LCCN 2014942635. Retrieved 8 October 2017 – via Penn State University Libraries.