A State of the Art Review on Cyber Attacks

Raj Kumar, Ranjeev Kumar Chopra,
RIMT University, Mandi Gobindgarh, Punjab
Email id- raj.kumar@rimt.ac.in, ranjeevk.chopra@rimt.ac.in

ABSTRACT: ***Social networks, internet transactions, cloud computing, and automated procedures are driving rapid technological advancements. It is true that as technology advances, so does cybercrime, which continuously creates new attack types, tools and tactics that allow attackers to access more complicated or well-controlled settings, do greater harm, or stay untraceable at all times. Cyber-crime as defined and disclosed by specialist literature, international legislation and historical facts is the focus of this paper. Attacks recorded all over the world over the previous years are also analysed to establish patterns and trends in cyber-crime. To help businesses protect themselves against attackers, the article outlines a number of actions that may be taken based on the study' findings. This paper explains how technology can help reduce the impact of cyber assaults, but the real threat and susceptibility lies in human behaviour and psychological predispositions that can be altered via education. It discusses how cyber security model are reducing and minimising the cyber-attacks increasing the future implementation of these models.***

KEYWORDS: Cyberspace, Cyber-Attacks, Cyber-Security, Service, Threats.

INTRODUCTION

The world is inevitably heading toward digitalization, or the elimination of monetary transactions. Cyberattacks have cost the government and defence organisations a lot of money and caused a lot of downtime. Because the criminal environment in cyberspace is so different from that in real space, applying cybercrime laws like real-space laws in any society has numerous challenges. Age, for example, is a self-authenticating factor in physical space, but not in online. In cyberspace, a child under the age of 18 may easily hide his age and obtain access to restricted resources, but this would be impossible in real space. Cyber security comprises preventing, detecting, and responding to cyber-attacks in order to safeguard information[1]. A positive step towards modernisation, computer penetration in society must be better equipped to compete with technology-related difficulties. In order to detect hackers, security experts must utilise new hacking tactics and security flaws that are not commonly identified. . Defenders must understand their own network, the attacker's motivation, technique of attack or security flaw in order to prevent future assaults[2].

In the media, government sectors, and businesses, cyber security is now a hot subject. Fear mongers, who use words like "cyberwarfare" to evoke an emotional rather than an analytical response, are believed to have over-hyped and artificially inflated the issue, according to experts. The number of dangers, such as cyber-war, has been significantly overstated, according to a recent Intelligence study. Cyber security is a hot topic with fundamental concepts that can spark independent thought among academics and professionals. Many caution advocates, such as security experts, have urged for this type of discussion. So many cybercrimes are the direct result of insufficient security, not a lack of government policies. Internet identity requirements should be avoided, according to the head of the Electronic Privacy Information Center (EPIC). These nations have been subject to censorship and international human rights breaches because of the attribution requirements. There is no doubt that cyber-security is a highly significant and contemporary issue, one that warrants healthy discussion[3].

Attackers seek to undermine the confidentiality, integrity and availability of information by devising novel methods of gaining unauthorised access to computer networks, programmes, and data. Their targets range from individuals too small to medium-sized businesses to large corporations. Annual assaults are on the rise, but so are attacks that compromise the security of really large businesses, compromising information security and consumer confidence. Maximum cyber-attacks were done in the year 2013 as well as 2014, but the authors think this is not the apogee unless remedies are taken. It's important to note that technology programmes are based on a variety of published study materials. Globally, governments and security groups have taken proactive measures to minimise cyber-attacks on vital infrastructures, which are increasing in frequency. As a result of this, there is an interaction between the physical and the virtual worlds. Protection of such infrastructure is achieved by the prevention, detection and response to cyber events.[4]

Military strikes on people and government-sponsored Internet censorship were generally accepted, with physical acts laying the groundwork for cyber-events. Recent incidents involving malware that has been causing havoc on Supervisor Control and Data Acquisition (SCADA) systems may be familiar to IT experts. SCADA malware takes use of both previously unpatched weaknesses and freshly found vulnerability. On a global scale, the physical and economic repercussions of these issues might be

devastating. Although not all cyber-events result in human mortality, the economic consequences for a society can be disastrous. This year's top fraud was reported to be information and electronic data theft, up from the year before. This is despite the fact that half of the other fraud categories have declined.

A larger, updated national U.S. cyber-security policy is being established through the CNCI, which is the first in a series of steps. The first step is to create a front-line of protection against today's imminent cyber threats. Next is to defend against all threats and last is to strengthen cyber-security environment in the future. In addition, the CNCI's activities are guided by these objectives. According to a 2009 study by the US Department of Homeland Security, cyber security is an issue that transcends national lines and requires worldwide cooperation with no single organisation, country or agency claiming control. According to the study, there should be a Roadmap for Cyber-Security Research that should be followed. As a result of the aforementioned presidential orders and the second edition of the INFOSEC Research Council (IRC) Hard Problem List, the road map outlines research and development possibilities that are focused on addressing eleven “hard challenges”.

They define cyber security as "the preservation of confidentiality, integrity and availability of information in cyberspace" with a definition of "cyberspace" that includes the interaction of people, software, and services via technology devices and networks connected to it in a complex environment that does not exist in any physical form". Cyber-security is currently a hot issue, attracting a lot of conversation, interest, and attention [5].

1.1. Threats:

A larger, updated national U.S. cyber-security policy is being established through the CNCI, which is the first in a series of steps. The first step is to create a front-line of protection against today's imminent cyber threats. Next is to defend against all threats and last is to strengthen cyber-security environment in the future [6]. Among the many types of crimes, there are some that directly target computer networks or services, such as malware, viruses or denial of service attacks, as well as those that are assisted by networks or devices, but whose primary goal is independent of the network or device itself.

1.1.1.Cyber Theft:

This is the most prevalent type of cyber-attack in cyberspace today. Generically, this type of offence is referred to as "hacking." Information or assets can be stolen by utilising the internet as a tool. When a malicious script is used to crack the computer system or network security without the user's knowledge or agreement, vital data might be tampered with. It is one of the most serious cybercrimes. A large number of banks, Microsoft, Yahoo, and Amazon have fallen prey to cyber-attacks of this nature. Phishing, DNS cache poisoning and identity theft are some of the techniques used by cyber criminals to steal data and intellectual property. There are a lot of security websites that have detailed description of the various cyber threats[7].

1.1.2. Cyber Vandalism:

Cyber vandalism is the act of destroying or exploiting data rather than stealing or misusing it. In other words, it indicates that network services have been interrupted or have been discontinued. This prevents authorised users from gaining access to the network's information. When this cybercrime is activated, it damages the target system like a time bomb. Cybercrime is the purposeful introduction of malicious code, like as viruses, into a network in order to monitor, follow, disrupt, halt, or conduct any other activity without the consent of the network's owner. [8]

1.1.3.Web Jacking:

As the name implies it is the act of obtaining access to and control over another's web site in order to take over a web server. Hackers might be tampering with the site's information.

1.1.4. Telling cards Information:

By hacking into an e-commerce system and misusing credit or debit card information it is performed.

1.1.5.Cyber Terrorism:

It is done on purpose, generally for political reasons, internet-based violence is done against people.

1.1.6. Child Pornography:

It is done to produce, distribute, or access items that sexually exploit underage minors’ pornography in shared drives of community networks through the use of a computer network

1.1.7.Spam:

Violations of the SPAM Act include sending unlawful product promotion or immoral information through email in violation of the SPAM Act.

1.1.8. Cyber Trespass:

Data or systems are disrupted or damaged by legal access to network resources without alteration. Private information may be accessed without disturbing the person or network traffic can be monitored in order to gather vital information.

1.1.9. Logic bombs:

It's a case-by-case basis. These programmes are launched when a certain event is detected. The Chernobyl virus is a unique example of a logic bomb that may sleep of a certain date in history.

1.1.10. Drive *by Download*:

Search engine firms conduct a survey. Sites hosting viruses were many. Since its origin, the phrase "Drive by Download (DbD)" has been used in the software business in a variety of ways. Software programmes are automatically installed on a user's PC when accessing the internet. When malicious software is installed on a victim's computer, the goal is to gain advantage over the victim, such as stealing private information such saved passwords and personal data, or utilising the victim's computer as a botnet to disseminate harmful material.

1.1.11. Cyber Assault by Threat:

Email, videos, or phone calls are used to threaten a person's life or the lives of their family members or anyone for whose safety they are responsible (such as employees or communities). Such blackmailing might include blackmailing the victim into transferring cash through a payment service to an untraceable bank account.

1.1.12. Script Kiddies Novices:

Students who utilise scripts or programmes written by others to attack computer systems and networks to get root access and deface websites, are known as "script kiddies," "script bunny," "script cat," or "script running juveniles."

1.1.13. Denial of service:

Attacks on computer resources are known as denial of service (DoS) attacks, or distributed denial of service attacks, or DDoS attacks. The victim's machine crashes because it is overloaded with requests. Although the tactics, objectives, and targets of a DoS assault may vary, it typically involves the deliberate efforts of a person or persons to prevent an Internet site or service from working efficiently or at all, momentarily or forever. E-mail bombing is another name for this type of attack. Attacks on eBay, Yahoo!, and Amazon occurred as a result of this incident.[9]

1.2.Attacks:

Since cyber-attacks have a negative impact on essential infrastructure and data, it is important to pay attention to this issue. Cyber security risks or "cyber-attacks" accompany the expansion of technology, posing a hazard to users' security when utilising such technologies. As a result, it is difficult to recognise and prevent cyber threats and assaults. The frequent cyber-attacks and lack of data protection are preventing people from adopting the new technology. Unauthorized access to a computer is the result of hostile cyber-attacks. [10]

1.2.1 Untargeted attacks:

Untargeted attacks occur when attackers target as many users and services as they can find. This is done through identifying weaknesses in the service or network. Attacker can take the advantage of technologies like:

- Phishing: Phishing is when a phoney individual sends emails to a large number of users and asks for personal information such as passwords and credit card details in exchange for money. They encourage people to visit phoney websites and offer them excellent deals in

exchange for their efforts. Since the consumers input their personal information by clicking on the links in the email, the fraudsters are unaware that they were defrauded.

- Water holing: In order to gain access to the personal information of visitors to your website, people can create a false or dummy website or compromise an existing one.
- Ransom ware: It contains malware that encrypts discs and extorts users.
- Scanning: Attacking wide swathes of the Internet at random

1.2.2 Targeted attacks:

In the cyber realm, targeted assaults occur when attackers target specific users. Spam is the practise of sending targeted persons emails that contain harmful software links and advertisements in order to trick them into downloading dangerous software. A botnet is deployed. A DDOS (Distributed Denial of Service) attack is delivered. Taking advantage of the supply chain's weaknesses .An attack on the organization's network or software the majority of the time, attackers will initially utilise tools and techniques to explore your systems for vulnerabilities that may be exploited.

1.3.Vulnerability:

There are vulnerabilities in a system that let an intruder to execute instructions, access unauthorised data, and/or launch denial-of-service assaults on a computer. Throughout the system, vulnerabilities can be identified in a wide number of places. In addition to hardware and software flaws, there are also policy and procedural flaws in systems, as well as vulnerabilities in the system users themselves. Vulnerabilities were discovered as a result of hardware compatibility and interoperability, as well as the time and effort required to fix them. Software vulnerabilities exist in operating systems, application software, and control software such as communication protocols and device drivers. A range of variables, including human factors and software complexity, can lead to programme design mistakes. In most cases, technical vulnerabilities are the result of human frailty.

The repercussions of complacency, carelessness, and ineptitude are apparent when it comes to cyber-attacks. In 2015, an unprecedented amount of vulnerabilities were identified as weaponized zero-day exploits, and online assault exploit kits are adapting and developing them more swiftly than ever before. There will be additional vulnerabilities when more gadgets are connected.

1.4 Cyber-crime:

Any unlawful action that employs a computer as its principal method of commission and theft is referred to as cyber-crime. The United States Department of Justice has broadened the definition of cybercrime to encompass any criminal action that involves the preservation of evidence on a computer. Cyber-crimes encompass crimes made possible by computers, such as network intrusions and the spread of computer viruses, as well as computer-based versions of existing crimes, such as identity theft, stalking, bullying, and terrorism, which have become a serious concern for individuals and governments. Cyber-crime is typically described as a crime committed using a computer and the internet to steal a person's identity, sell contraband, stalk victims, or disrupt operations using malicious software. As technology continues to play an increasingly important part in people's lives, cybercrime will rise in tandem with technical advancements.

1.5 Trends changing cyber security:

1.5.1 Web servers:

Attacks on internet apps to collect data or transmit malicious code remain a threat. Cyber criminals deploy malicious malware using compromised lawful web sites. However, data-stealing assaults, which are frequently in the news, are also a serious threat. We must now put a greater emphasis on protecting web servers and web applications. Web servers are the most common way for these cyber criminals to collect data. To prevent being a victim of these frauds, always use a secure browser, especially while doing sensitive transactions.

1.5.2 Cloud computing and its services:

Cloud services are being increasingly used by all small, medium, and large enterprises these days. To put it another way, the planet is slowly nearing the clouds. This present development creates a serious challenge for cyber security since communications may circumvent established ports of inspection. As the number of applications available in the cloud grows, policy controls for web apps and cloud services will need to evolve to prevent the loss of vital information. Despite the fact that cloud services are developing their own

business models, security issues remain. Although the cloud has many benefits, it is crucial to realise that the cloud will evolve as well.

as the country's security worries grow.

1.5.3 APT's (Advanced Persistent Threats)and targeted attacks:

APT (Advanced Persistent Threat) is a form of cybercrime software that is relatively new. Network security features such as web filtering and intrusion prevention systems (IPS) have been crucial in identifying targeted attacks for years (usually after the first penetration). As attackers get bolder and employ more confusing techniques, network security must communicate with other security services in order to identify assaults. As a result, in order to avoid future threats, we must enhance our security processes.

1.5.4 Mobile Networks:

We now have the ability to speak with anyone in any part of the world. Security, on the other hand, is a key issue for these mobile networks. As consumers utilise more devices such as tablets, phones, PCs, and other devices, firewalls and other security safeguards are becoming increasingly porous, necessitating extra security considerations beyond those offered by the applications. The security of these mobile networks must be continuously considered. In addition, because mobile networks are so sensitive to cybercrime, more vigilance is required in the case of a security breach.

1.6 Impact on Victims:

Cyber-attacks are difficult, if not impossible to quantify, in terms of how much they cost their victims in terms of business, customer trust, and brand image. This is especially true because companies do not always disclose all of their information to the public, but the results show that cyber-attacks are most often associated with data loss and data theft. The most frequent forms of attacks allowed unauthorised access to information such as: complete names, birth dates, personal IDs, full addresses, medical records, phone numbers, financial data, e-mail addresses, credentials (usernames, , passwords), and insurance information.

2 DISCUSSION

This paper solely focuses on several cyber-attacks which are performed by several hackers who intend to harm someone in some way. When computer systems, technology-dependent companies and networks are targeted, it is referred to as a cyber assault. Computer code, logic, or data can be altered by malicious code in cyber assaults, resulting in disruptions that can compromise data and lead to cybercrimes such as identity theft and information theft. Alternatively, a computer network assault is known as a cyber-attack (CNA). On March 20, South Korean banks and television firms were the targets of cyberattacks. Through overwriting the Master Boot Record (MBR) and all logical drives on compromised servers, malware was able to bring down several websites and disrupt bank operations. According to media reports, 32,000 PCs had been destroyed, although the actual amount of financial loss hasn't been estimated yet. The fact that we haven't done an exact study of the reason makes it more probable that we'll suffer more harm if there are more assaults. As a result of this attack, APT (Advanced Persistent Threat) has become a major concern. However, APT is not a new technique of attacking, but a pattern of recent cyber-attacks. This paper discusses few of these kind of attacks and cyber threats which are performed nowadays by number of people to steal data of other people with the intention to harm them.

3 CONCLUSION

The most effective safeguard against cyber security events is a computer educated user, according to studies. It is important to keep in mind that the most susceptible people in a company are those who are just hired. The psychological factors that lead to user and network susceptibility are also examined in this study. It concludes that while technology can help reduce the impact of cyber assaults, the real threat and susceptibility lies in human behaviour and psychological predispositions that can be altered via education. Cyber assaults can be mitigated, but there hasn't been a definitive answer to the problem of cyber security concerns. In the future, the cyber security model will be used to minimise the threat and susceptibility of cyber-attacks on the network.

REFERENCES

[1] K. Huang, M. Siegel, and S. Madnick, "Systematically understanding the cyber attack business: A survey," *ACM Computing Surveys*. 2018, doi: 10.1145/3199674.

[2] J. Raiyn, "A survey of cyber attack detection strategies," *Int. J. Secur. its Appl.*, 2014, doi: 10.14257/ijsia.2014.8.1.23.

[3] M. M. Rana, L. Li, and S. W. Su, "Cyber attack protection and control of microgrids," *IEEE/CAA J. Autom. Sin.*, 2018, doi: 10.1109/JAS.2017.7510655.

[4] D. Stiawan, M. Y. Idris, A. H. Abdullah, F. Aljaber, and R. Budiarto, "Cyber-attack penetration test and vulnerability analysis," *Int. J. Online Eng.*, 2017, doi: 10.3991/ijoe.v13i01.6407.

[5] D. Tellbach and Y. F. Li, "Cyber-attacks on smart meters in household nanogrid: Modeling, simulation and analysis," *Energies*, 2018, doi: 10.3390/en11020316.

[6] P. Eder-Neuhauser, T. Zseby, J. Fabini, and G. Vormayr, "Cyber attack models for smart grid environments," *Sustain. Energy, Grids Networks*, 2017, doi: 10.1016/j.segan.2017.08.002.

[7] M. Uma and G. Padmavathi, "A survey on various cyber attacks and their classification," *Int. J. Netw. Secur.*, 2013.

[8] Á. M. Guerrero-Higueras, N. DeCastro-García, and V. Matellán, "Detection of Cyber-attacks to indoor real time localization systems for autonomous robots," *Rob. Auton. Syst.*, 2018, doi: 10.1016/j.robot.2017.10.006.

[9] O. A. Hathaway *et al.*, "The law of cyber-attack," *California Law Review*. 2012, doi: 10.15779/Z38CR6N.

[10] J. Valuch, T. Gábriš, and O. Hamul'ák, "Cyber Attacks, Information Attacks, and Postmodern Warfare," *Baltic Journal of Law and Politics*. 2017, doi: 10.1515/bjlp-2017-0003.