International Journal of Scientific Research and Engineering Development-– Volume 5 Issue 6, Nov- Dec 2022

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

RESEARCH RECENT CHALLENGES IN CYBER SECURITY AND THEIR SOLUTIONS

Ghone Siddhesh Jaywant

Keraleeya Samajam's Model College, Khambalpada Road, Thakurli, Dombivli (East), Kanchangaon, Maharashtra

siddheshghone821@gmail.com

ABSTRACT

The running era can be called the Internet era, because the use of the Internet is increasing every day. Eachthe coin has two sides, just like the coin of the internet. One side shows the ease ofcommunication, information sharing, marketing andbusinesses etc using the internet. On the other hand, it brings major security concerns. Cyber security isa field that promises to protect your network, data, electronic devices, servers, and computers from malicious attacks. According toby cyber security, we mean staying ahead of hackers and preventing system abuse. Hackers are getting smarter every day, which brings new challenges for cybersecurity professionals. Reports on threats such as ransomware, phishing, vulnerabilityexploits, IoT based attacks etc. are running around us most of the time these days. The current study describes a well-known common challenge and reveals some emerging challenges in cyber security andsuggests possible solutions to overcome them.

KEYWORDS

Cyber Security, Cybercriminals, Hackers, DDoS, Phishing, Malware, Ransomware, Internet of Things,Artificial intelligence, cloud risks, countermeasures, technical skills gap, anti-security tools, antivirus.

I. INTRODUCTION

Cybersecurity refers to the process of providing protection to Internet-connected systems such as computers, servers,mobile devices, electronic systems, programs and data from attack, damage or unauthorized access. In other words, Cybersecurity is a set of methods, technologies, and processes that help protect confidentiality, integrity, andavailability of computer systems, networks and data against cyber-attacks or unauthorized access. Cyber security sometimes isreferred to as information security. Cybersecurity is critical because government, military, corporate, financial, and medicalorganizations collect, process and store unprecedented amounts of data on computers and other devices Telling Fractionthis data may

be sensitive information, whether it is intellectual property, financial data, personal data or other typesdata to which unauthorized access or exposure could have negative consequences.Organizations transfer sensitive datanetworks and other devices in the course of business. It is practiced by individuals, organizations and businessesstores all types of data including sensitive data, personal information (PII), protected health information (PHI),personal information, intellectual property, data, and government and industry information systems from theft and damage.Without a cybersecurity program, it is nearly impossible for any organization to protect itself from cyber-attacks and threats.The need for cyber security is growing with the advent of new technologies such as cloud services such as Amazon Web Services and othersmany other. The current study outlines some known common challenges and reveals some new challenges in cybersecurityproposed a solution to overcome them.

II. KNOWN SECURITY CHALLENGES

Below are some well-known cybersecurity challenges

2.1 DDoS Attack:

DDoS is short for Distributed Denial of Service attack. In a DDoS attack, cybercriminals flood the network with a lotmalicious traffic that is difficult to operate normally, which in turn causes the normal operation of the website, commonly known as legitimatepackets, freeze. The purpose of a DDoS attack is to overload a server with access requests until it eventually crashesbe a denial of service. Among all other attacks, DDoS attacks are the ones that prevent clients, users from accessing everythingbenefits of the services available to them from the server side [1]. A DoS attack is an attempt by an individual or group of individualscripple online service, with serious consequences, especially for companies like Amazon and eBay that rely on themtheir online availability for business [2]. The expansion of 5G, the proliferation of the Internet of Things and smart devices, and the next shiftindustries moving their operations online have brought new points of contact for DDoS attacks, as presented in consumer McAfeethreat report. Cybercriminals are using leverage, and 2020 saw the two largest DDoS offensives everlaunched on Amazon and Google.

DDOSattacks fall into two broad categories: Flood attacks and Flash Crowd attacks. Flood DDoS attacks devourresources such as network bandwidth due tothe overwhelmingly narrow connection with high packet volume. Flash Crowd attacks usepredictable behaviour of protocols such as TCP and HTTP in favour of the attacker [2].

2.2 Phishing:

Phishing is the act of circumventing security by using an alias or the act of sending an email falsely claiming to be fromlegitimate organization [3]. This is usually combined with a threat or request for information: for example, an accountcloses, a balance is due, or the account is missing information. The email asks the recipientto provide confidential information such as bank account details, PIN or passwords; this data is then used by the website owners tocommit fraud. A phishing website looks just like a real website and the end user doesn't realize it wasredirected. However, data hacking through phishing can be avoided by not clicking on unknown links from the webforeigners [4].

Phishing attacks impact organizations and individuals and face heavy losses that include finesinformation laws and regulations, loss of reputation, recovery costs and reduced productivity [5]. Phishing in anotherdirections initiate attacks such as phone calls, instant messaging or physical letters in addition toe-mails. However, the technical onethe method includes phishing scams, phishing emails, fakewebsites, phone phishing, social media phishing [6].

2.3 Malware:

It is software that has a malicious purpose (Malicious software). Malware is uninvited from multiple sourcesvarious media such as website pop-ups, spam, e-mails, downloads from unknown sources [7]. The types of malwares arespyware, trojan horses, virus attacks, worms, adware and logic bombs; are the most widespread danger to systems [8].

A computer virus is designed to replicate and spread. The virus spreads using the victim's email account to everyone in hiscontacts. Due to the replication of the virus, the network traffic turns out to be heavy and causes the network to slow down [9]. Electronic trojanthe horse functions similarly to the well-known story of the Trojan horse that was used to get to the city of Troy. It is a malicious software thatpretends to be a legitimate program [10]. Spyware is a program that monitors activities performed on a computer system.As you browse the web, the spyware downloads and creates a simple text file using your system browser.stored on the hard disk. Later, any data save flat file save can be obtained from any web page, so the whole internet browsingthe history of the computer can be traced [11]. Another type of spyware is called a keylogger, which records all users' keystrokes. A worm virus is malicious, self-replicating software that can automatically propagate and spread over a network.Adware is advertising-supported software.

2.4 Internal Abuse:

When insiders compromise their access privileges or steal data, it is referred to as an

insider exploit. People are leaking secure data to the publicsprings. Secured data can include strategic documents, customer data and even proprietary source code. Insiders who performattacks (inside attacks) have a distinct advantage over external attackers because they have authentication to access the system andmay also be familiar with network architecture and system policies and procedures[12]. Employees are authorized to a wide range of physical equipment within a company with a single trust to prevent them from damaging or stealing it.Hardware such as hard drives thatcontained a lot of important data may bephysically destroyed or stolen from thecompany or datacan be duplicated, deleted or transferred on a USB drive. In addition, calamities such as floods, fires, terrorism or powerfailure may destroy stored data.

III. RECENT CYBER THREATS

3.1 Ransomware:

Ransomware is a family of malware that uses security techniques such as cryptography to hijack user files and related filesresources,then demands cryptocurrency in exchange for locked data [13]. Some ransomware gets into the system usingsocial engineering, malicious ads, spamming, car downloading while others try to discover vulnerabilitiesexploit, using open ports or using backdoors to get in [14]. The infection process begins by injecting malware into thenetwork computer by targeting human or technical weaknesses. Human frailties often emerge from opening and clickingspam messages, known as phishing emails. While technical deficiencies are based on various factors such as public useaccessible Wi-Fi networks, insufficient firewall protection, etc. After the infection process, cybercriminals change the file systemencrypting entire computer files and allowing the victim to see only their message andbitcoin payment process [15]. Whencybercriminals hack a computer, it is almost impossible to decrypt files unless they have a decryption algorithm or a decryptedkey. Because of this, victims tend to pay cybercriminals to recover their hostage data from criminals [16]. Ransomware isconsidered the fastest growing cyber threat attracting attention. It either encrypts files or blocks access to the system orsew. If someone is hit by ransomware, the hacker demands money depending on the criticality of the data or the sizeorganization. In this case, victims on the brink of data loss also suffer financial and productivity losses.

3.2 Cloud Risks:

Companies are moving their sensitive data from legacy data centers to the cloud, due to the flexibility & costs involved in the legacy data centre. Moving the data to the cloud needs proper configuration and security measures in place otherwise there are chances of falling into a trap. Cloud service providers are just securing

their platform, securing the companies infrastructure from theft & deletion over the cloud is the company's responsibility. With cloud services, the traditional endpoint focused security operations tools do not work as the perimeter and security gradually move away from the endpoint to cloud security controls and much of the insights are lost [17]. The five most significant cloud risks are accessmanagement, data breaches & data leaks, data loss, insecure APIs, mis-configured cloud storages.

3.3 Artificial Intelligence:

AI is generally an ally of humans using problem solving and learning techniquesunderstanding high-level activities in the functioning of human-inspired elements, decision-making and the emotional cycle [18].Artificial intelligence runs parallel to cyber-attacks and prevention. AI has revolutionized this era by acting and defending. Theone cannot ignore the fact that in addition to defence, AI also acts on the attacker's side. Biometric login is one exampleartificial intelligence. AI after much research and modelling can learn anomalies in behaviour patterns that can be used as adefensive tool. Unfortunately, these similar techniques can be used by attackers to carry out a cyber-attack. Previous generations of cyber-attacks focused primarily on data theft (extraction) and braking systems (intrusion). New formsattacks on AI systems seek to gain control over the targeted system and change its behaviour. To get control, three typesattacks are particularly important: data poisoning, tempering of categorization models, and backdoors [19]. Each of these exploitsthe ability of artificial intelligence systems to learn to change their behaviour. For example,cybercriminals can introduce carefullydesignederroneous data among legitimate data used to train the system to modify its behaviour.

3.4 Internet of Things (IoT):

The Internet of Things (IoT) is a set of interconnected objects, services, people and devices that can communicate, sharedata and information to achieve common goals in different areas and applications [20]. Companies are increasingly dependenton technology and exposes them to attacks. With the rapid adoption of the Internet of Things (IoT), security threats are also growingdrastic. The commonly accepted IoT architectureincludes three layers, namely PerceptionLayer (PL), Network Layer (NL) andapplication layer (AL). PL uses a sensor to collectinformation about an intelligent object in the environment. NL is responsible fortransmission& processing data from sensors, establishing connections with other smart things, servers and network devices. AL provides users with application-specific services and the idea of smart city, smart home, smart healthcare, etc. Attackers can exploit IoT infrastructure by creating vulnerabilities at each of these layers. IoT applications such as smart TVs, security

systems, wearable health meterscollect user information that may be accessed or shared by some hackers for illegal reasons. Security challenges in PL areeavesdropping, replaying the attack, timing the attack. Threats in NL include DoS, RFID spoofing, sinkhole attack. And finally in the AL challengesare phishing,cross site scripting, malicious form/virus attack.

3.5 Technical skills gap:

Cyber-attacks are progressing with an increasing number of sophisticated and successful targeted cyber-attacks worldwideglobe. There is an urgent demand for cyber security professionals with the appropriate motivation and skills to prevent, detect,respond to or even mitigate the effect of such threats. Recent research by the Department for Digital Culture, Media and Sport(DCMS) claims that around 48% of organizations in the UK are unable to carry out core operations as defined by the governmentCyber Essentials Scheme such as firewall setup, data storage, etc. The report also claimed that 30% of businesses have preparedadvanced cyber security skills like pen testing, forensics etc. Companies and organizations are constantly facing a serious shortagewith respected and highly qualified cyber security professionals.Lack of such expertise makes them vulnerable to cyber threats, leading to theft of sensitive information, financial loss,and reputational damage [21]. The rapid growth of technology and the technical nature of cyber-attacks is widening the gap between absencerelevant security skills and faster growth forcybersecurity professionals.

IV. SUGGESTED SOLUTIONS

4.1 DDoS Countermeasures:

One countermeasure against a DDoS attack is predictive analytics. It helps IT staff to investigate the attack, predict itprobability of occurrence and source of origin. Predictive analytics software consumed by machine learning may collectsignificant information about known cyber-attacks and can connect the results to existing security protocols. This is particularly effectivefor active DDoS mitigation, as it enables cyber security systems to identify threats and thus take proactive measures to redirectof operation before the system is affected. Another countermeasure is to back up critical data. There are othersalso countermeasures.Every single user accessing your router should be given a username and password, make sure you have RPF on your routerinterface of each static connection, disable Telnet on vtys, allow only SSH-based connections, use vtys filters to prevent publicrouters since receiving a response from your router, use TACACS (Terminal Access Controller Access Control System) for the password.verification, set up security labs, if that is not possible, set aside at least one spare router

and server to test the new service insteadimplement it directly in the live network, minimize the number of transit providers, possibly one, connect with otherlocal ISPsfor benefits such as cleaning center lease, out-of-band management, and possibly setting up better security labs [22].

4.2 Countermeasures against phishing:

The first countermeasure against a phishing attack is to educate the end user to recognize phishing and avoid accessingunauthorized links. Second, prevent a vulnerability-level attack from materializing on a user's device and detectattack once it is launched through the network layer. Finally, use enforcement law as a deterrent control to overcome attacks [23].

4.3 Countermeasures against malware:

There are many proposed countermeasures used to mitigate the effects of malware on systems. Somecountermeasures against malware are a firewall, security software, manual malware removal, and training. Firewall is protectiona mechanism that controls and monitors network traffic in and out. It allows or blocks such traffic based on security rulesdepending on his perceived threat. There are two types of firewalls, i.e., hardware and software. There are several software firewallsavailable as Check PointNext Generation Firewalls (NGFWv), SonicWall, Official G2 Survey, CiscoNext-Generation FirewallVirtual (NGFWv), FortiGate NGFW, SophosXG Firewall, Microsoft Windows firewall, Macfree, Symantec, TrenMicro, Sygare,and ZoneAlarm.There are many security software such as antivirus, internet security software and removal tools that need to be protectedanti-malware computer systems. Malware removal tools are used to scan and remove malware in a computer system. A littleremoval tools are provided by Microsoft, they are security scanner, malware removal tools, diagnostics andrecovery toolkit (DaRT) and Emsisoft Emergency Kit, Avast Free scanner and malware removal tools, malware bytes. Mainthe function of antivirus software includes scanning of executable files, real-time activities (such as downloading files,monitoringapplication activities). Here are some antivirus lists: McAfee, Symantec, Norton, AVG, Kaspersky and Quick-heal. Internetsecurity software has additional features compared to antivirus, such as: anti-spyware, family and privacy protection, maliciousdevice and platform independent website blocking and online storage security.Security awareness training should be providedemployees to recognize the various threats.

4.4 Countermeasures against internal abuse:

Data breaches are usually the result of people'spsychologicalweaknesses.To avoid internal abuse, this is importanteducate employees about warning signs of a security

breach, safe practices such as: being careful when opening emailsattachments, where they surf and what measures to take against a suspected takeover.

4.5 Ransomware Countermeasures:

As stated in an online article by Kaspersky [24], countermeasures against ransomware are: never click on dangerous links, avoiddisclosure of personal information when receiving an email, call or text message from an untrusted source, do not open suspiciousemail attachments, never use unknown USB keys, keep programs and OS up to date, use only known download sources, useVPN services on public Wi-Fi networks. In addition to these measures, the use of Antiransomware software, such as anti-virus programs, contentinternet security filters and solutions such as Kaspersky InternetSolutions, Bitdefender Total Security, McAfee Anti-virus plus, etc.protect against cyber-attacks.

4.6 Countermeasures against cloud risks:

There are various cloud security countermeasures such as firewalls, multi-factor authentication, virtual private networks(VPN) etc. Gray Stevens [25] suggests preventive measures for the five most significant cloud risks. They are: AccessManagement can be avoided by carefully designing access policies and setting up authentication and identity verification tools. Databreaches and leaks can be managed by establishing secure communications and connections. You avoid frequent data backupsData loss. Careful vendor selection limits insecure APIs. Check that the cloud storage is configured correctlyconfiguration settings.

4.7 AI Countermeasures:

Mariarosaria Taddeo, et.al., suggests three countermeasures for AI vulnerabilities.First, to ensure that reliable vendors design and develop models in-house, such as system training and test datacollected, verified and maintained directly by the system providers. For example, the cloud system may be disruptedgive the attacker access to the AI model and training data. Second, a deep method to improve the resilience of the AI system isAdversary training. Feedback loops allow the AI system to increase theirperformance by adjusting their own variablesiteratively. As a result, training adversariesbetween AI systems can help increase their resilience and promoteidentification of system vulnerabilities. Finally, parallel and dynamic monitoring helps in assessing AI robustnesssystems, the deceptive nature of attacks and the learning capabilities of targeted systems.

4.8 IoT Countermeasures:

Countermeasures for IoT proposed by Mohamed Litoussi, et. al [26] in three different layers are as follows:

- Perception layer (PL), hash-based encryption, public key infrastructure (PKI protocol), light weightcryptography can be implemented.
- NL countermeasures include an identity management framework, software-defined networking (SDN) with IoT,cooperation of node communication protocols.
- Similarly, AL countermeasures are special policies and permissions, anti-virus, anti-adware and anti-spyware,risk assessment techniques

4.9 Technical Skills Gap Countermeasures:

In 2020, when thieves can easily clone identities for any fraud, hackers can exploit any vulnerability; it will only increaseunless there is an equal number of resources with the right skills to solve the problem.Companies must invest in existing trainingemployees to prevent cyberattacks and must also hire new resources to analyze network threats. Otherwise, companies willhave to bear huge financial losses.

V. CONCLUSION

Cybersecurity is a set of methods, technologies and processes that help protect the confidentiality, integrity,and the availability of computer systems, networks and data against cyber-attacks orunauthorized access. Cyber security issometimes referred to as information security.Cyber threats and security attacks are nothing new to companies and organizations. Fortunately, in recent years they have achieved alevel of sophistication. Computer security is a critical topic as the world becomes highly interconnected, including networksused to perform critical transactions. Cybercrime continues to diverge in different ways with each new year that passesas well as information security. There are practices and technologies that companies and organizations must adoptprevent any external and internal threats.The study is being conducted to create awareness about the challenges involved in dealing with various cyber threats. These speciesAttacks also have an impact on the economy. To mitigate and manage these threats, end users must engage in education andawareness training. The complexity of the attack requires studyingpast user data and attack patterns;reformulating the approach to minimizing adverse impacts.

REFERENCES

[1] Sushmita chakraborty, Praveen kumar, Dr.Bhawnasinha , “A study on DDoS attacks, danger and its prevention” ,Pg.1. InternationalJournal of Research and Analytical

Reviews (IJRAR) E-ISSN 2348-1269, P- ISSN 2349-5138,May 2019, Volume 6, Issue 2.

[2] Anup Bhange, Amber Syad, Satyendra Singh Thakur, "DDoS Attacks Impact on Network Traffic and its Detection Approach", InternationalJournal of Computer Applications (0975 – 8887) Volume 40– No.11, February 2012.

[3] A. Summer, "Mitigating Phishing Attacks: An overview Computer Science," pp. 72-77,2010

[4] Vayansky and S. Kumar, "Phishing-challenges and solutions", Computer Fraud Security, Vol. no. 1, pp. 15-20, 2018 [5] Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf and Imtiaz Khan, "Phishing Attacks: A recent Comprehensive Study and a new Anatomy," Frontiers in Computer Science, vol. 3 March 2021, Article 563060

[6] Abdullah Fajar and Setiadi Yazid, "The intial socio-technical solution for phishing attack", Journal of Physics: Conference Series, IOP Publishing, 2020, 1502 012034

[7] Emma Megan, IEEE Computer Society, https://www.computer.org/publications/tech-news/trends/cybersecurity-threats-and-solutions - viewed on 27/06/2021

[8] Chuck Easttom, "Computer Security-Fundamentals", Third Edition, Pearson Education, Inc., 2016, ISBN-13: 978-0-7897-5746-3

[9] E. Filiol, "Viruses and Malware", Handbook of information and communication Security, 2010

[10] A. Bettany and M. Halsey, Windows Virus and Malware Troubleshooting, Berkeley, CA:Apress, 2017

[11] Mariwan Ahmed Hama Saeed, "Malware in Computer Systems: Problems and Solutions", International Journal on Informatics for Development, Vol. 9, No.1, 2020, Pp.1-8, e-ISSN: 2549-7448

[12] Shilpa Pareek, Ashutosh Gautam, Ratul Dey, "Different Type Network Security Threats and Solutions, A Review", International Journal of Computer Science(IIJCS) ISSN 2321-5992, Volume 5, Issue 4, April 2017

[13] Al-rimy B, Maarof M, Shaid S, "Ransomware threat success factors, taxonomy, andcountermeasures: A survey and research directions", Computers and Security, 2018; 74:144-166.

[14] Popli N, Girdhar A. Verma, Nishchal K, Ghosh A. K, "Behavioural Analysis of Recent Ransomware and Prediction of Future Attacks by Polymorphic and Metamorphic Ransomware". (eds) Computational Intelligence: Theories, Applications, and Future Directions - Volume II ICCI-2017. Springer, Singapore. 2018;799(4):65–80.

[15] Murat Ozer, Said Varlioglu, Bilal Gonen, Mehmet F. Bastug, "A Prevention and a Traction

System for Ransomware Attacks". 6th Annual Conference on Computational Science & Computational Intelligence (CSCI'19); Dec 05-07, 2019.

[16] I DUNCAN, "' Discombobulated and upset': Baltimore ransomware attack complicates matters for debt payers," Baltimore, may 2019 [Online]. Available: https://www.baltimoresun.com/politics/ bs-md-20190508-story.html

[17] Bharadwaj D. R., Bhattacharya A., Chakkaravarthy M., "Cloud Threat Defense – A Threat Protection and Security Compliance Solution". IEEE International Conference on Cloud Computing in Emerging Markets (CCEM) 2018.

[18] Vishal D. K. Soni, "Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA". ARTIFICIAL INTELLIGENCE IN CYBERSECURITY OF THE USA [Online], available at: https://ssrn.com/abstract=3624487

[19] Mariarosaria Taddeo, Tom McCutcheon and Luciano Floridi, "Trusting artificial intelligence in cybersecurity is a doubleedged sword", Nature Machine Intellegence, 42256-019-0109-1.

[20] Tasneem Yousuf, Rwan Mahmoud, FadiAloul, Imran Zualkernan, "Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures". International Journal for Information Security Research (IJISR), Volume 5, Issue 4, December 2015

[21] Mouheb, D., Abbas, S., &Merabti, M., "Cybersecurity Curriculum Design: A Survey". Lecture Notes in Computer Science, 93–107, 2019. [22] Sushmita chakraborty, Praveen kumar, Dr. Bhawna sinha , "A study on DDoS attacks, danger and its prevention" , pp 2. International Journal of Research and Analytical Reviews (IJRAR) E-ISSN 2348-1269, P- ISSN 2349-5138, May 2019, Volume 6, Issue 2.

[23] B.B. G. Nalin and A. G. A. Kostas, "Defending against phishing attacks: Taxonomy of methods, current issue and future directions", Telecommunication System, vol. 67, no.2, pp. 247-267, 2018 [24] AN ARTICLE BY KASPERKEY ON RANSOMWARE PROTECTION: HOW TO KEEP YOUR DATA SAFE IN 2021[ONLINE]. AVAILABLE AT: HTTPS://WWW.KASPERSKY.CO.IN/RESOURCE-CENTER/THREATS/HOW-TO-PREVENT-RANSOMWARE

[25] GARY STEVENS, "CLOUD SECURITY: 5 SERIOUS EMERGING CLOUD COMPUTING THREATS TO AVOID", MAY 26, 2020 [ONLINE]. AVAILABLE AT: HTTPS://WWW.THESSLSTORE.COM/BLOG/CLOUD-SECURITY-5-SERIOUS-EMERGING-CLOUD-COMPUTINGTHREATS-TO-AVOID/

[26] Mohamed Litoussi_, Nabil Kannouf, Khalid El Makkaoui, AbdellahEzzati, Mohamed

Fartitchou, "IoT security: challenges and countermeasures". 7th International Symposium on Emerging Information, Communication and Networks (EICN 2020), November 2-5, 2020, Madeira, Portugal.

[27] Abuagoub, Ali M A, "International Journal of Communication Networks and Information Security". Kohat Vol. 11, Iss. 3, (Dec 2019): 342-351.

[28] Malatji, M., Von Solms, S., &Marnewick, A., "Socio-technical systems cybersecurity framework". Information and Computer Security 2019. doi:10.1108/ics-03-2018-0031

