World of Science: Journal on Modern Research Methodologies

Volume 2 Issue 9, Year 2023
ISSN: 2835-3072
https://univerpubl.com/index.php/woscience

Survey on Computer Cyber Security

Chya Omer Qader [1], Dr. Ann Zeki Ablahd [2]

[1] Department of Computer Science , College of Computer Science & Information Technology, University of Kirkuk , Iraq .
e-mail. Stcha006@uokirkuk.edu.iq
[2] Technical College Kirkuk, Northern Technical University , Iraq .
e-mail. drann@ntu.edu.iq

Article Information

Received: Jul 13, 2023
Accepted: Aug 26, 2023
Published: Sep 14, 2023

Keywords: *Internet of Things, cyber Security, cybersecurity policy.*

ABSTRACT

The growing reliance on computer systems and the increasing interconnectedness of the digital world have amplified the significance of computer cyber security. This survey aims to provide an overview of the current state of computer cyber security by examining key areas of concern, emerging threats, and the measures taken to mitigate risks.

This survey begins by exploring the fundamental concepts of computer cyber security, including the importance of confidentiality, integrity, and availability of data. It delves into the various types of cyber threats faced by computer systems, such as malware, phishing attacks, data breaches, and social engineering techniques. Next, the survey investigates the common vulnerabilities and weaknesses that cyber attackers exploit to compromise computer security. This includes software vulnerabilities, weak authentication mechanisms, inadequate network security, and the challenges posed by emerging technologies like the Internet of Things (IoT) and cloud computing.

The survey then discusses the countermeasures and best practices employed to safeguard computer systems against cyber threats. It covers the implementation of firewalls, antivirus software, intrusion detection systems, encryption protocols, and regular security updates. Additionally, it highlights the significance of user awareness training and policies to promote a culture of security within organizations.

Furthermore, the survey explores the role of government regulations, industry standards, and international collaborations in promoting computer cyber security. It examines the legal and ethical aspects of cyber security, including privacy concerns, incident response, and the attribution of cyber-attacks.

Finally, the survey discusses emerging trends and future directions in computer cyber security. It touches upon topics such as artificial intelligence and machine learning for threat detection, block chain for secure transactions, and the challenges posed by the proliferation of connected devices in the Internet of Things (IOT).

1 -INTRODUCTION:

Cybersecurity has risen to the top of the priority list for organizations and governments worldwide. Unfortunately, many companies still do not have the tools and processes in place to protect themselves from cyberattacks. This article will cover the current challenges and issues confronting cybersecurity experts, as well as potential solutions to these issues. [1].

Overall, this survey gives a thorough review of computer cyber security, emphasizing the significance of proactive measures and ongoing adaptation to a shifting threat scenario [2]. Individuals and businesses may better defend themselves from cyber attacks and contribute to a safer digital world by knowing the current status of computercybersecurity

Cybersecurity is the process of securing internet-connected systems, as well as the hardware, software, and data contained inside, against unwanted access, use, disclosure, modification, and destruction. Along with the restricted network infrastructure, sensitive data like financial and personal information, intellectual property, and trade secrets must be protected. Cybersecurity includes a variety of security measures that are aimed at defending the availability, confidentiality, and integrity of information from cyberattacks [3].

On the other hand, regardless of the medium used, information security includes measures to protect data from unauthorized access, unauthorized use, disclosure, alteration and destruction. Information security versus computer security, includes both computerized systems, such as file cabinets, and non-computerized systems, such as physical papers. In addition, information security is concerned with safeguarding all kinds of data, including financial and personal information, trade secrets, and intellectual property. It entails a variety of safeguards including encryption, access control, firewalls, and security rules designed to protect data during its entire existence.

[3]

In general, information security deals with the protection of all types of data, whereas cybersecurity is focused on defending systems and networks connected to the internet against online attacks. The main goal of cybersecurity measures is to thwart cyber-attacks, which are often carried out by external threats like malware and hackers. On the other hand, information security measures concentrate on thwarting both internal and external threats and take into consideration various kinds of data storage, including physical forms of storage like paper documents. These two ideas do, however, intersect and cannot be seen independently. A cybersecurity strategy that neglects to incorporate crucial information security safeguards might lead to breaches since information security is a subset of cybersecurity..

2. Related works

" The State of Cybersecurity in Organizations: A Global Survey" by Ponemon Institute(2019):(In order to evaluate the present level of cybersecurity, the research looked into enterprises all around the world. It looked at the difficulties businesses confront with regard to cyberthreats, data breaches, and their readiness to respond to security incidents.).[1]

"Cybersecurity Threats, Vulnerabilities, and Countermeasures: A Survey" by Zawoad et al. (2018)(The many computer dangers, weaknesses, and defenses in place in computer systems were the subject of this thorough examination. We looked at issues including network security, malware research, intrusion detection, and encryption). [2]

"A Systematic Review of Internet of Things (IoT) Security: Current State, Challenges, and Countermeasures" by Alaba et al. (2020).(I paid particular attention to security concerns and difficulties with the Internet. (IoT). It explored privacy issues, hardware flaws in ICT, and suggested solutions to improve ICT security.)[3].

"The Human Factor in Cybersecurity: A Systematic Literature Review" by Renaud and De Angeli (2017). (This literary analysis explored the role of users in upholding computer security with an emphasis on the human element in cybersecurity. It covered user knowledge, behavior, training, and the influence of human factors on cybersecurity issues.).[4]

"Emerging Threats and Countermeasures in Information Security: A Survey" by Bhavsar and Parekh (2020).[5]

(In the poll, increasing challenges to information security were highlighted, including persistent and sophisticated threats, assaults on labor ransom, and zero vulnerabilities. Additionally, mitigation plans and defenses were covered. .)

These related works provide valuable insights into different aspects of computer cyber security, including organizational cybersecurity, specific threats and vulnerabilities, human factors, IoT security, and emerging trends. They contribute to the overall understanding of the field and complement the findings of the surveyed study.

3. Emerging threats

As technology improves and fraudsters use new tactics, new dangers to computer security are continually emerging. Here are c ..

- Internet of Things (IoT) Vulnerabilities:

IoT device proliferation has quickly created new security issues. Cybercriminals find IoT devices to be appealing targets because of their poor authentication and lack of appropriate update procedures. Attacks on IoT networks that aim to steal data, create botnets, or gain illegal access are new dangers that need to be dealt with..[6]

- Cloud Security Risks

As cloud computing becomes more widely used, new risks and vulnerabilities appear. There are several new dangers to cloud security that need to be looked at, including misconfigurations, unsafe APIs, data breaches, and unauthorized access to cloud resources.

- Mobile Device Exploitation
- Mobile devices are being targeted by hackers as they grow more and more ingrained in our daily lives. Among the new dangers to the security of mobile devices include malicious applications, mobile viruses, phishing scams, and unreliable Wi-Fi networks.

- Social Engineering Techniques

Attackers' methods are always changing, and social engineering is still a serious concern. This includes phishing emails, voice phishing calls, SMS phishing assaults, and impersonation techniques that take advantage of user psychology to trick them and acquire access.

- Crypto currency-Related Threats

New security issues have emerged with the growth of cryptocurrencies. Emerging risks aimed at people and businesses include ransomware that requests payment in cryptocurrency and crypto jacking, when attackers mine cryptocurrency on victims' machines without their knowledge.

- Supply Chain Attacks

In order to obtain unauthorized access or insert malicious code into a system, supply chain attacks entail compromising reputable software or hardware providers. Recent events, including the Solar Winds breach, have brought attention to the growing danger that such attacks offer.These are only a few illustrations of recent dangers to computer security. To give an up-to-date picture of the always shifting environment of cyber dangers, a thorough study should investigate these and other developing concerns.

4. Cyber Attack

Cyberattack danger increases with the development of technology. Cyber-attacks may take many different forms, endangering both people and businesses.

An effort to hack or break into a system or organization's data is referred to as a cyber-attack. Figure 1 represents the Threat – Driven Approach to Cyber-security.

Identity theft, extortion, malware, man-in-the-middle, hijacking, spam, Trojans, phishing, denial-of-service, and replay attacks are just a few of the most common attacks. forms of cyberattacks. Botnets pose a serious danger to cybersecurity among these several sorts of cyberattacks.[7]

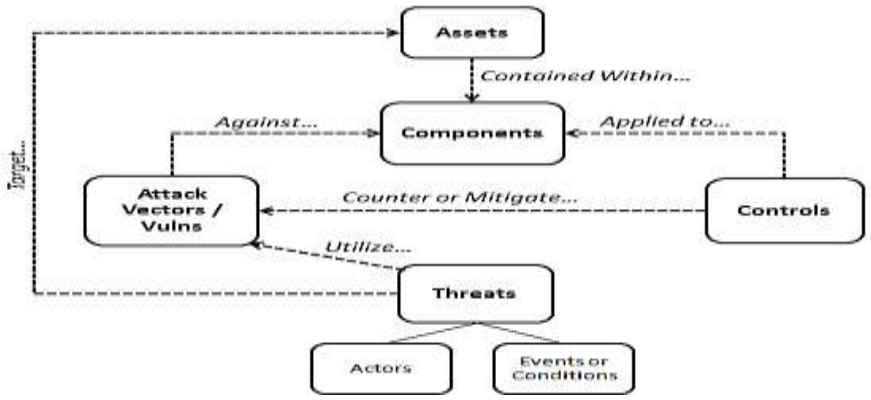

Figure 1 represents the Threat – Driven Approach to Cyber-security.

4.1 Botnets

Cybersecurity is particularly at risk from A serious danger to cybersecurity now comes from botnets. A botnet is a network of infected devices that cooperate to carry out various cyberattacks on the target system. Computers, servers, and Internet of Things hardware might all be part of this [9]. Attacks like denial of service, phishing, or DDoS are frequently used to control botnets. Since they enable communication between the bot and its creator, botnets differ from other malware in that their producers may provide commands to the bot. Because free tools are accessible for

unskilled and ignorant people to remotely penetrate devices and establish botnets, the ability to set up and maintain a botnet is no longer restricted to experienced users. Botnets represent a wide range of risks, including Denial of Service attacks, spam, phishing, ransomware, click fraud, and even bitcoin mining. Botnets serve as a useful tool for malicious attackers because they provide the ideal foundation for launching and sustaining all types of dispersed assaults. Additionally, compromised hosts unintentionally participate in destructive operations and join botnets. Because they operate beyond national borders and are challenging to detect and successfully battle, botnets pose a particularly serious danger to cybersecurity. Finally, as technology develops, the threat of cyberattacks grows more and more important. Due to their distinctive features and the ease with which even untrained persons may set them up and operate them, botnets pose the greatest danger to cybersecurity among these assaults and control them remotely.
Figure 2 represents more threats of computer systems.

Therefore, it is essential that people and businesses take precautions to defend themselves from botnet assaults by constantly upgrading their security software, putting firewalls in place, and keeping an eye on network activities. In order to address the threat posed by botnets, it is crucial for politicians to give cybersecurity measures top priority and strive toward global collaboration. By adopting these actions, we can reduce the dangers presented by cyberattacks and make sure that everyone using the internet is protected..

5. Types of Cyber Attack

A cyber-attack is any intentional, hostile attempt to undermine the security, availability, or integrity of computer systems, networks, or digital data. It entails employing a variety of tools and ways to gain unauthorized access to, modify, or destroy information. Information fraud, extortion, virus, man in the middle, and server takeover are some of the frequent forms of cyberattacks.. [10]

5.1 Information Fraud

Obtaining and using someone's personal information without their knowledge for financial gain or other nefarious objectives is a sort of fraud that is sometimes referred to as identity fraud or identity theft. It entails the illicit collection and usage of personal information, including social security numbers, credit card numbers, bank account numbers, and other identifying information...[11]
Criminals who engage in information fraud frequently collect personal information by using a variety of techniques, such as phishing emails, computer hacking, stealing actual documents, and even using social engineering to trick people into disclosing their personal information. As soon as they get the relevant information, fraudsters can engage in a range of fraudulent actions, including money fraud and identity theft.[12]
Financial fraud: involves illegal transactions, credit card fraud, creating false bank accounts, obtaining loans in the victim's name, and making purchases using payment card information that has been stolen. [12]

5.1.1 Identity Theft

The thieves may exploit the victim's name to conduct crimes while posing as the victim, file false tax returns, or ask for government benefits.[13]

5.1.2 Account Takeover

In order to steal sensitive information or engage in more fraudulent actions, fraudsters may get unauthorized access to the victim's internet accounts, including email, social media, and online banking.[14]

5.1.3 Medical Fraud

Personal information can be used to obtain medical services, prescriptions or false insurance claims, resulting in financial loss and potential damage to the victim ' s medical records. [15]

5.1.4 Synthetic Identity Fraud

In order to construct completely new identities that they may use to establish credit or engage in other fraudulent activities, thieves blend actual and made-up information in this type of fraud.[16] Information fraud may have serious repercussions for the victims, including financial loss, harm to their credit history, emotional pain, and the requirement to expend a lot of time and effort to rectify the difficulties brought on by the fraud. Individuals should safeguard their personal information, exercise caution when disclosing sensitive information online or to unknown parties, routinely check their financial accounts and credit reports, and report any suspicious activity to the appropriate Report to authorities immediately to avoid information fraud. It is also recommended to enable two-factor authentication., Use strong passwords that are not secure easily guessed, and use caution when giving out sensitive information over the phone or via email.[17]

5.2 Blackmailing

In a kind of extortion known as blackmail, a person or group makes threats to divulge or expose private, humiliating, or damaging information about another person if specific conditions aren't satisfied. The revealing of the private, sensitive, or secret material used for blackmail might endanger the victim's reputation, relationships, job, or personal life.[18]

Blackmail typically involves the following elements:

1. Threat Threats of disclosing private information or harming the victim are made by the blackmailer until certain conditions are met. Threats might include disclosing humiliating images or videos, divulging private information, revealing illegal activity, or harming someone's reputation..[19]
2. .Demand: The blackmailer states what they want to happen, which typically entails the victim making a payment or making other concessions. They could demand cash, expensive items, favors, or things the blackmailer can use as leverage..[19]
3. Coercion: Blackmailers use coercion to get victims to comply by instilling dread, worry, or anguish in them. They may exert pressure on the victim via psychological tricks, intimidation, or emotional manipulation.[20]

4. Confidentiality: Blackmailers frequently stress the need for confidentiality and caution their victims against approaching law police or other authorities. They want to keep control of the situation and keep the victim from seeking assistance or disclosing the blackmail attempt.[21]
5. Threats made verbally, in writing, through phone, email, or online chat are all examples of ways that blackmail can be carried out. Blackmailers may use stolen personal information, intimate images, or private chats gained through hacking, social engineering, or other illegal ways as a means of payment. Cyber blackmail is becoming more and more prevalent as a result of technology.[21]
6. Due of its coercive and manipulative elements, blackmail is prohibited in the majority of nations. Blackmail victims should think about reporting the occurrence to law enforcement

officials, gathering evidence if feasible, and getting legal counsel to safeguard their rights and interests. It is imperative to refuse to comply with the blackmailer's demands because doing so frequently feeds the extortion cycle and could not ensure that the blackmailer will keep their word.[19]

5.3 Malware

Any program or code designed to disrupt, damage, or gain unauthorized access to the computer system, network, or device in question, as malicious software, or simply as malicious software. Cybercriminals employ a variety of tools to produce malware, which they use with harmful purpose. Examples include viruses, worms, Trojan horses, ransomware, spyware, adware, and more.[21]

Malware's main objective is to utilize computer system flaws to its advantage or to deceive people into doing things for the attacker. Once a device or network has been compromised by malware, a number of negative outcomes might occur, including data loss, financial loss, system malfunctions, unauthorized access, identity theft, and privacy violations.[22]

Malware may spread through a number of channels, including phishing emails, infected websites, portable media, software downloads from dubious sources, and even by taking advantage of security flaws in operating systems and software. Utilizing up-to-date antivirus and anti-malware software, maintaining patch levels for operating systems and apps, being cautious when opening email attachments or clicking links, and avoiding downloading software from dubious sources are all critical steps in malware protection.[22]

5.4 Man-in-the-middle attacks

This assault can take place in a variety of settings, such as online purchases, email correspondence, voice calls, or even public Wi-Fi networks. As they provide attackers access to sensitive data like login passwords, financial information, or personal information, these assaults present serious hazards. They can also make it easier for attackers to launch additional attacks by giving them unrestricted access to or control over the compromised communication channel.[23]

To protect against man-in-the-middle attacks, it is important to adopt security measures such as:

Encryption: Using secure communication protocols, such as HTTPS for websites, ensure that data is encrypted and protected from interception or tampering.[23]

Secure Networks: As they are vulnerable to man-in-the-middle attacks, avoid connecting to public or untrusted Wi-Fi networks. Use networks with established trust and the necessary security measures.[23]

Digital Certificates: Verify the validity of digital certificates used by websites and make sure that the certificate authority from whom they were issued are reputable.To reduce vulnerabilities that attackers may exploit, keep antivirus software, firewalls, and security updates up to date on all devices.[23]

Awareness and Education: When exchanging sensitive information or gaining access to vital resources, especially in unsettling or suspicious circumstances, use caution and vigilance. [24]

By implementing these preventive measures, individuals and organizations can significantly reduce the risk of falling victim to man-in-the-middle attacks.

5.5 Server hijacking

Server compromise or server takeover refers to an attacker's unauthorized access to and control of a server. In such an attack, the attacker gains access to the server's operating system or programs,

allowing them to change their functionality, steal data, disseminate malware, or waste the server's resources..[25]

Here are some common methods used in server hijacking:

1-**Exploiting Vulnerabilities**: Attackers attempt to obtain access by exploiting known flaws in server software, operating systems, or web applications. They could take advantage of vulnerabilities in security that have not yet been addressed or configuration issues that make the server vulnerable to assault. [25]

2-**Brute Force Attacks**: Attackers test a variety of username and password combinations until they discover the right ones in an effort to guess the login credentials for the server. The main objective is often passwords that are weak or simple to guess.[25]

3-**Remote Code Execution**: For arbitrary code to run on the server, attackers take advantage of security flaws in web applications or server-side scripting. They can then take over and use the hacked application or server's privileges to carry out their orders.[26]

4-**Social Engineering**: To deceive server administrators into providing login passwords or other sensitive information, attackers may utilize social engineering tactics like phishing emails or phone calls. Then, using this information, illegal access to the system is gained. Once a server has been effectively hijacked, the attacker [27], they can carry out various malicious activities, including:

- Data Theft: Attackers are able to get access to and take control of sensitive data kept on the server, such as customer information, financial information, or intellectual property.[27]
- Malware Distribution : Hackers may exploit compromised servers as distribution hubs for malware, infecting users' computers or other connected devices.[27]
- 3-Denial of Service (DoS): Attackers may exploit the compromised server to perform denial-of-service (DoS) assaults against specific systems or networks, rendering them inoperable.[27]
- Spamming or Phishing: Large-scale spam campaigns or phishing websites that deceive users into disclosing their personal information can be sent from servers that have been hacked.[27]

To prevent server hijacking, it is crucial to follow best practices for server security, including:

1-Regular Updates and Patches: Update server operating systems, applications, and software to the most recent security patches and upgrades to fix known vulnerabilities.[28]

2-Strong Authentication: Use multi-factor authentication and require strong passwords to secure server login information.[28]

3-Access Control: Use appropriate access control measures to limit administrative rights and restrict access to just those trustworthy persons who need it.[28]

4-Monitoring and Logging: To identify and look into any shady actions on the server, put in place reliable monitoring and logging solutions.[28]

5-Security Audits: To find and fix possible vulnerabilities in server setups, conduct routine security audits and vulnerability assessments.[28]

By implementing these measures, server administrators can strengthen the security of their servers and reduce the risk of server hijacking.

Spoofing	An attacker acting as the control system could forge control messages to field devices
Tampering	An attacker staging a man-in-the-middle attack to extract and modify information going to and from the RTU
Repudiation	An attacker using IP Spoofing to hide its identity in the case of a DOS attack
Information Disclosure	An attacker finding a cross-site scripting vulnerability could inject a script that steals credentials that users enter into the web server login form
Information Disclosure	An attacker sniffing on packets sent either by field devices or control center could be able to find information on how devices are being used or the data they gather
Denial of Service	An attacker causing a denial of service through one of the open interfaces, for example TCP or HTTP flooding
Elevation of Privilege	By cracking the web server password, an unprivileged attacker could gain privileged access to the system

Figure 2 represents more threats of computer systems.

6. Cyber Security Policy

A cybersecurity policy is a set of guidelines and rules that an organization implements to protect its information technology systems, networks, and data from unauthorized access, use, disclosure, interruption, or destruction. It serves as a framework for defining how an organization manages and mitigates risks related to cybersecurity.[29]

A cybersecurity policy typically includes the following components:

- Purpose and scope: Clearly defines the objectives and scope of the policy, including the systems, assets, and personnel it applies.
- Roles and responsibilities: Identifies the individuals or teams responsible for implementing and enforcing the policy, as well as their specific duties and authorities.
- Risk assessment: Outlines the processes to determine the rating,and prioritizing cybersecurity threats to the assets of the organization and systems.
- Security controls: Specifies the security measures and controls that must be implemented to protect the organization's information and systems. This can include network security, access controls, encryption, authentication mechanisms, incident response procedures, and more.
- Data classification and handling: Provides guidelines for classifying and handling sensitive data, including data privacy, data retention, and data disposal practices.
- Incident response and reporting: Defines the actions to be performed in case of a cybersecurity incident, involving reporting procedures, containment measures, and recovery processes.

- Employee awareness and training: Emphasizes the importance of cybersecurity awareness and provides guidelines for educating employees about their roles and responsibilities in maintaining a secure environment.
- Compliance and monitoring: Describes the processes for performing routine audits and evaluations to ensure compliance with the policy, monitoring and enforcing compliance with the policy, and its effectiveness.
- Policy review and update: Establishes a mechanism for consistently evaluating and revising the policy to handle new risks, technological advancements, and modification in the organization's environment.

A well-defined cybersecurity policy helps organizations establish a proactive approach to security, minimize vulnerabilities, protect sensitive information, and respond effectively to cyber threats. It serves as a foundation for creating a a security-conscious organizational culture and aligning security practices with business goals.

7. Secure Tools to Prevent cyber-attacks:

Building a secure tools to prevent cyber-attacks involves multiple layers of protection, including network security, endpoint security, and application security. Here are some key measures that can be taken to build a more secure tool:

1-Use Secure Coding Practices: Among the most crucial measures in building secure tools is to use secure coding practices. Developers should be trained in secure coding practices and should adhere to coding standards such as OWASP (Open Web Application Security Project).

2-Use SSL/TLS encryption: SSL/TLS encryption is essential to ensure secure communication between the client and the server. HTTPS should be used for all web-based applications to encrypt data in transit.

3-Implement Multi-Factor Authentication (MFA): Multi-factor authentication is a crucial security feature that gives user accounts an additional degree of protection. Users are required to enter at least two credentials to access their accounts, such as a one-time code and a password were sent via SMS.

4- Update and patch software frequently: Frequently updating and patching crucial to keep tools secure. Developers should be proactive in identifying and fixing vulnerabilities to ensure that their tools remain secure.

5-Use Firewall and Intrusion Detection System: Firewalls and intrusion detection systems are critical components of network security. They can help to identify and prevent malicious traffic from entering the network.

5- Conduct routine security audits: Regular security audits are required to spot vulnerabilities and confirm that security controls are current.. It's recommended to conduct security audits at least once a year.

6- Provide Security Awareness Training: Training in security awareness may benefit personnel. to identify potential security threats and respond to them effectively. It should be a regular part of employee training and on boarding.

By implementing these measures, developers can build more secure tools that are less vulnerable to cyber-attacks. However, it's important to remember that security is an ongoing process that requires constant vigilance and attention to detail. Figure 3 display the estimated creasing of cyber-attack in the world until 2027.

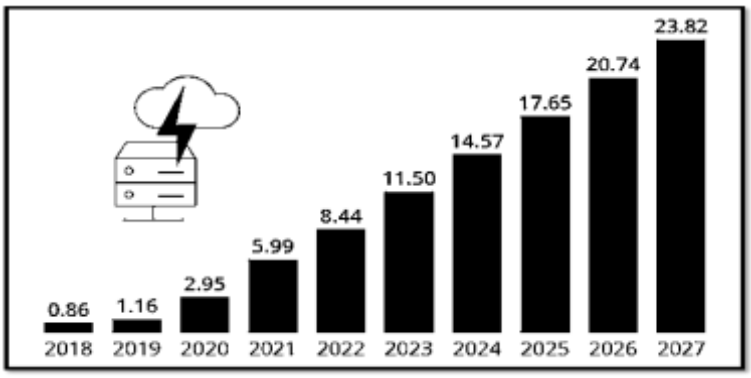

Figure 3 displayed the estimated increasing of cybercrime in the world

8. CONCLUSIONS

In conclusion, it is vital to prevent cyberattacks as they can be costly and detrimental to individuals and organizations. Thankfully, there are several tools available that can help prevent cyberattacks. For instance, endpoint security tools can help identify and prevent malware from making its way onto a device. Additionally, two-factor authentication can aid in guarding against illegal access to private information. Other tools such as network security monitoring and firewalls can also be implemented to mitigate the risk of cyberattacks.

However, it is important to note that tools alone cannot provide complete protection against cyberattacks. Cybersecurity must be viewed as an ongoing process that involves regular training, updates to security policies, and an understanding of the latest threats and vulnerabilities. Employees and users should also be educated on how to spot and evade potential dangers. In summary, while the tools discussed are a great way to prevent cyberattacks, they should be part of a comprehensive security strategy that addresses both human and technical vulnerabilities.

In conclusion, the impact of cyberattacks is far-reaching, and there is a growing need to develop better cybersecurity measures to protect against them. There are several tools available such as endpoint security, two-factor authentication, network security monitoring, and firewalls, among others that can help mitigate the risk of cyberattacks. However, users and employees need to be part of the comprehensive security strategy, and there should be ongoing training and updates to address new threats and vulnerabilities. It is crucial to recognize that cybersecurity is a continuous process that requires vigilance and proactive measures to prevent cyberattacks.

REFERENCES

1. Ponemon Institute, The State of Cybersecurity in Organizations: A Global Survey,(2019).
2. Zawoad et al., Cybersecurity Threats, Vulnerabilities, and Countermeasures: A Survey" by (2018).
3. Alaba et al ,A Systematic Review of Internet of Things (IoT) Security: Current State, Challenges, and Countermeasures, (2020).
4. Renaud and De Angeli, The Human Factor in Cybersecurity: A Systematic Literature Review, (2017).
5. Bhavsar and Parekh , Emerging Threats and Countermeasures in Information Security, (2020).
6. Ryan Turner, Python Programming book, Kindle Edition. Sqlmap tutorial for beginners hacking with SQL injection,2018.
7. Alfantookh, Abdulkader. An automated universal server-level solution for SQL injection security flaw International Conference on Electrical and Computer Engineering (ICEEC'04), 2004.

8. Chen xiao bing, Zhang Han yu, Luo Liming , Research on the technology of SQL injection attacks and detection . Comput Eng Appl.,2007.
9. .Fu, Xiang, et al. A static analysis framework for detecting SQL Injection vulnerabilities. Computer Software and Applications Conference.31st Annual International.Vol. 1. IEEE,2007.
10. Gerand Swinnen, Teach python3 book, first edition, 2013
11. .Ann Z. Ablahd, Suhair A. Dawwod / Tikrit Journal of Engineering Sciences (2020).
12. Grinberg, Miguel, Flask web development: developing web applications with python. O'Reilly Media Inc, 2014.
13. Halfond, William G., Jeremy Viegas, and Alessandro Orso. A classification of SQL-injection attacks and countermeasures. Proceedings of the IEEE International Symposium on Secure Software Engineering. Vol. 1. IEEE, 2006.
14. .Matec Web of Conference https://doi.org/10.1051/matecconf/2018173, 2018
15. .Suraj Natarajan, Melody Moh Recommending News Based on Hybrid User Profile Popularity Trends and Location, CTS, 2016..
16. Tao Han. Research on SQL injection detection method based on analytic tree - Harbin Institute of Technology, 2013.
17. The OWASP Top Ten Project OWASP_Top_Ten_Project, 2018.
18. Tian Y J, Zhao Z M, Zhang H C. Second-order SQL ,Injection Attack Defense Model, Netinfo Security,2014.
19. Valeur, Fredrik,Darren Mutz, and Giovanni Vigna ,A learning-based approach to the detection of SQL attacks. International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Springer Berlin Heidelberg ,2005.
20. Wahid Rajeh,Alshreef Abed.Anovel three-tier SQLi detection and mitigation scheme for cloud environments, ICECIS, 33-37, 2017.
21. WuShao Hua, Chen Shu bao.Web Attack Detection Method Based on Support Vector Machine Computer ,2015.
22. .Zhuang Chen, Min Guo, Lin zhou. Research on SQL injection detection technology based on SVM,2018.
23. Dr.Yusuf Perwej, Prof. (Dr.) Syed Qamar Abbas, Jai Pratap Dixit, A Systematic Literature Review on the Cyber Security International Journal of Scientific Research and Management (IJSRM),2021.
24. Sachin Kumar Tomar1 , Pawan Singh2 Cyber Security Methodologies and Attack Management , Journal of Management and Service Science, 2021.
25. Diptiben Ghelani Department of Computer Engineering, Gujrat Technological College Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review September 22, 2022.
26. Peter Eder-Neuhauser∗ , Tanja Zseby, Joachim Fabini, Gernot Vormayr Cyber Attack Models for Smart Grid Environments☆Institute of Telecommunications, TU Wien, Gusshausstraße 25 / E389, 1040 Vienna, Austria,2022.
27. Junaid Akram1 , Luo Ping1 How to build a vulnerability benchmark to overcome cyber security attacks ISSN 1751-8709 Received on 18th December 2018 Revised 14th August 2019 Accepted on 3rd September 2019 E-First on 26th September 2019.
28. C. Hemminghaus1,2, J. Bauer1 & E. Padilla1 1 Fraunhofer Institute for Communication, Wachtberg, Germany 2 University of Bonn, Bonn, Germany BRAT: A BRidge Attack Tool for

Cyber Security Assessments of Maritime Systems, Volume 15 Number 1 March 2021 DOI: 10.12716/1001.15.01.02

29. Mohamed S. Salhein elbelekia, ATTITUDES OF EMPLOYEES TOWARDS CYBERSECURITY NICOSIA, 2020.
30. Eirini Sofia Anthi, Detecting and Defending against Cyber Attacks in a Smart Home Internet of Things Ecosystem, February 2022 Cardiff University School of Computer Science & Informatics.
31. . Michael Swanagan, CISSP, CISA, CISM / Last updated: 10/16/22, How To Prevent Cyber Attacks & Threats,2022.
32. Mohammed Fakhrulddin Abdulqader&Adnan Yousif Dawod, Securing Network services and Protocols, Computer Science Department, College of Computer Science and Information Technology, Kirkuk University, Kirkuk, Iraq volume 41 issue4,2022
33. .Manuela TvaronaviÄ ienÄ), Tomas PlÄ—ta, Christos P. Beretasand Lina LeleÅ¡ienÄ— Analysis of the critical infrastructure cyber security policy, Insights into Regional Development, 2022.
34. Chovin Usman Najam ,Ahmed M. Fakhrudeen, On the performance of intrusion detection systems for the internet of things: State-of-the-Art in Research Computer Science Department, College of Computer Science and Information Technology, Kirkuk University, Kirkuk, Iraq,2022.