ABSTRACT

Cybersecurity refers to the protection of computer systems, networks, and digital information from unauthorized access, theft, damage, or exploitation. It is an increasingly critical issue in today's digital age, where businesses, governments, and individuals rely on digital technologies to store and process sensitive information.

Cyber threats come in many forms, including phishing attacks, malware, viruses, ransomware, and hacking. These threats can have significant consequences, such as data breaches, financial losses, reputational damage, and even national security threats. As a result, cybersecurity is a complex and constantly evolving field, requiring a range of skills and expertise to keep up with the latest threats and develop effective defenses.

Effective cybersecurity measures involve a combination of technical solutions, such as firewalls, encryption, and intrusion detection systems, as well as non-technical measures such as employee training, policies and procedures, and risk management strategies. Many organizations also rely on third-party cybersecurity experts to help them develop and implement effective security strategies.

In recent years, there has been a growing awareness of the importance of cybersecurity, and governments and businesses around the world have made significant investments in this area. However, cyber threats continue to evolve and become more sophisticated, and the need for robust cybersecurity measures remains as critical as ever.

In summary, cybersecurity is a vital aspect of modern society, with the potential to impact individuals, businesses, and governments in profound ways. Effective cybersecurity measures require a combination of technical and non-technical solutions, as well as ongoing education and awareness of the latest threats and trends in the field.

ACKNOWLEDGEMENT

The satisfaction that implies the successful completion of our work would be incomplete without the mention of people who made it possible.

I wish to place my deepest gratitude to our beloved Principal **Dr. R. B. Khadiranaikar,** Head of Department, **Dr. S. A. Quadri** and all the staff members of Computer Science & Engineering Department, Secab Institute of Engineering and Technology Vijayapur, for their inspiration and whole hearted support during this Seminar.

I am indebted to my **Mrs Nazeera Madabhavi** Asst. Prof. in Computer Science & Engineering Department who motivated us and guided me throughout this Seminar. She made the entire task simple with his/her valuable suggestions. My special thanks to all my friends for the timely help and kind co-operation.

Finally, no words would be sufficient to express my acknowledgement to my parents. I thank them for their inspiration, moral support. Without their encouragement this Seminar would never have been completed.

Saiyed Afak Ahmed (2SA19CS039)

CONTENTS

1 INTRODUCTION

1.1.1 CYBER SECURITY SUB DOMAIN

1.1.2 CYBER SECURITY THREATS

1.1.3 PREVENTION OF CYBER SECURITY THREATS

1.2 LITERATURE SURVEY ON RANSOMWARE ATTACK

1.3 PROBLEM STATEMENT

1.4 ARCHITECTURE OF CYBER SECURITY

2. APPROACHES AND METHOD

3. RESULT AND DISCUSSION

4. CONCLUSION

5. REFERENCES

1. INTRODUCTION

In today's digital age, cyber threats have become a significant concern for individuals, businesses, and governments. Cybersecurity refers to the protection of computer systems, networks, and digital information from unauthorized access, theft, damage, or exploitation. The increasing reliance on digital technologies has made cybersecurity a critical aspect of modern society. Cyber threats come in many forms, including phishing attacks, malware, viruses, ransomware, and hacking. These threats can have significant consequences, such as data breaches, financial losses, reputational damage, and even national security threats.

As the volume and complexity of cyber threats continue to increase, the need for robust cybersecurity measures becomes more critical. Cybersecurity professionals use a variety of tools and techniques to protect against cyber threats, including firewalls, intrusion detection systems, antivirus software, and encryption. Risk management and incident response plans are also essential components of a comprehensive cybersecurity strategy.

Cybersecurity is not just a concern for large corporations or government agencies. Small businesses and individual users are also vulnerable to cyber threats and must take steps to protect their digital assets. This can include using strong passwords, keeping software up to date, backing up critical data, and avoiding suspicious links or emails.

1.1.1 CYBER SECURITY SUBDOMAIN

Application Security:

Application security involves implementing various defenses within all software and services used within an organization against a wide range of threats. It requires designing secure application architectures, writing secure code, implementing strong data input validation, threat modeling, etc. to minimize the likelihood of any unauthorized access or modification of application resources.

Identity Management and Data Security:

Identity management includes frameworks, processes, and activities that enables authentication and authorization of legitimate individuals to information systems within an organization. Data security involves implementing strong information storage mechanisms that ensure security of data at rest and in transit.

Network Security:

Network security involves implementing both hardware and software mechanisms to protect the network and infrastructure from unauthorized access, disruptions, and misuse. Effective network security helps protect organizational assets against multiple external and internal threats.

Mobile Security:

Mobile security refers to protecting both organizational and personal information stored on mobile devices like cell phones, laptops, tablets, etc. from various threats such as unauthorized access, device loss or theft, malware, etc.

Cloud Security:

Cloud security relates to designing secure cloud architectures and applications for organization using various cloud service providers such as AWS, Google, Azure, Rackspace, etc. Effective architecture and environment configuration ensures protection against various threats.

Disaster recovery and business continuity planning (DR&BC):

DR&BC deals with processes, monitoring, alerts and plans that help organizations prepare for keeping business critical systems online during and after any kind of a disaster as well as resuming lost operations and systems after an incident.

User education:

Formally training individuals regarding topics on computer security is essential in raising awareness about industry best practices, organizational procedures and policies as well as monitoring and reporting malicious activities.

1.1.2 CYBER SECURITY THREATS

Here are some common types of cyber threats:

Malware: Malware is a type of malicious software that can infect a computer system and cause damage or steal sensitive information. Examples of malware include viruses, worms, and Trojan horses.

Phishing: Phishing is a technique used by attackers to trick users into providing sensitive information, such as usernames, passwords, or credit card details, by impersonating a trustworthy entity.

Ransomware: Ransomware is a type of malware that encrypts a victim's data and demands payment in exchange for the decryption key.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks: DoS and DDoS attacks aim to overload a system with traffic, making it unavailable to legitimate users.

Password attacks: Password attacks use various techniques, such as brute-force or dictionary attacks, to guess or crack passwords to gain unauthorized access.

Social engineering: Social engineering techniques manipulate human behavior to obtain sensitive information or access to computer systems. Examples include phishing, pretexting, or baiting.

SQL Injection: SQL injection is a code injection technique that might destroy your database. SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input.

1.1.3 PREVENTION OF SECURITY THREATS

Here are some common cybersecurity practices that can help prevent breaches:

Use strong passwords and change them regularly. Strong passwords should be at least 12 characters long and include a mix of uppercase and lowercase letters, numbers, and special characters.

Keep software up to date. Software updates often include security patches that address known vulnerabilities.

Use anti-virus and anti-malware software. These programs can help detect and remove malware from your system.

Enable firewalls. Firewalls can help block unauthorized access to your network.

Use encryption. Encryption can help protect sensitive data, such as financial information or personal data, from being intercepted by attackers.

Back up critical data regularly. Backups can help recover data in case of a breach or system failure.

Implement multi-factor authentication. Multi-factor authentication adds an extra layer of security by requiring users to provide additional proof of identity beyond a password.

Train employees on cybersecurity best practices. Employee training can help prevent human error, such as clicking on suspicious links or sharing sensitive information.

Regularly review and update access controls. Access controls should be regularly reviewed to ensure that only authorized users have access to sensitive information.

Develop and test incident response plans. Incident response plans should be in place to quickly and effectively respond to a security breach. These plans should be regularly tested and updated to ensure they are effective.

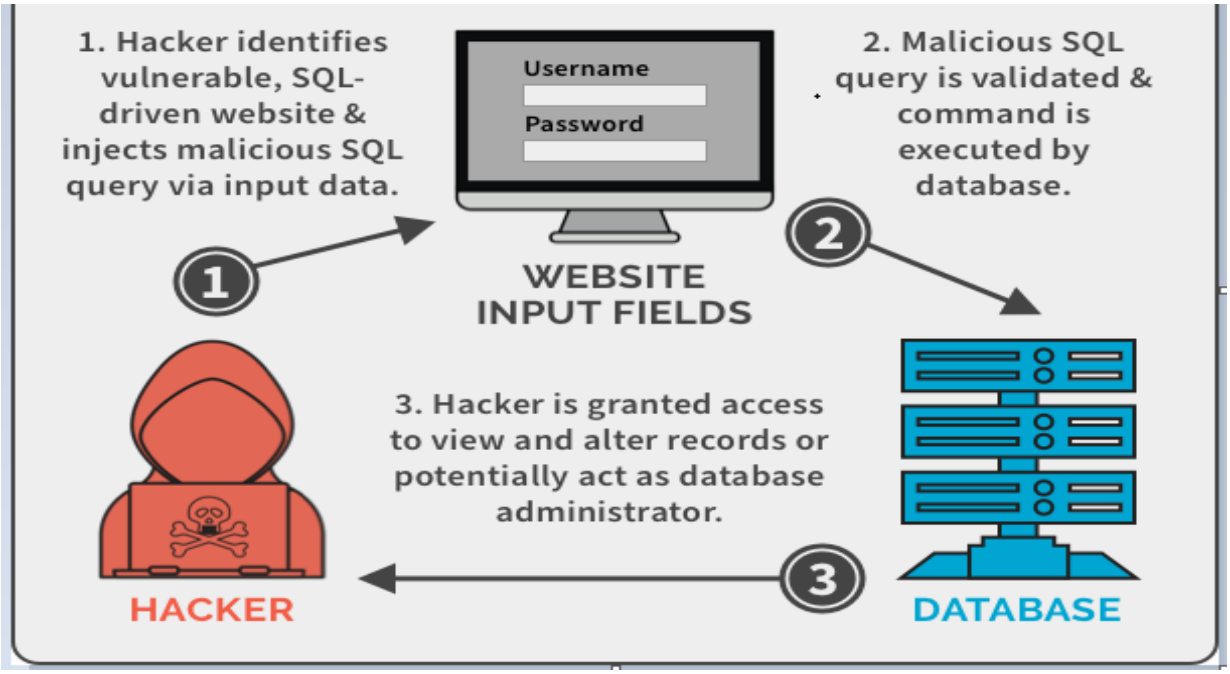


Fig 1.1.1.: SQL Injection

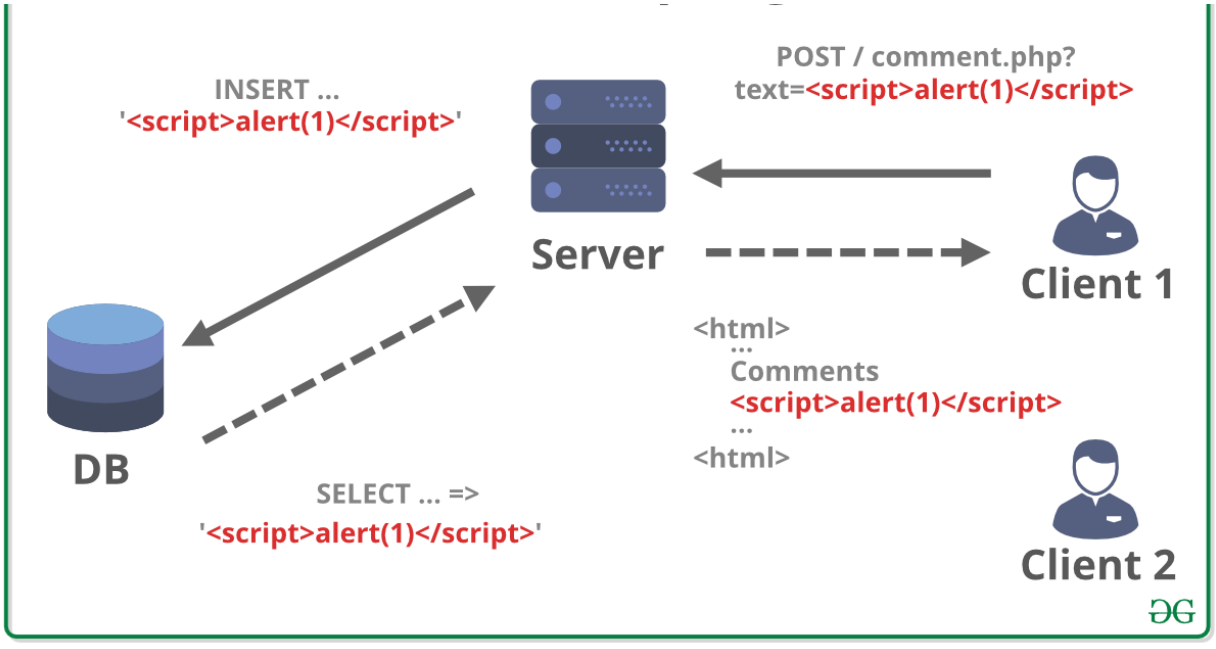


Fig 1.1.2 : Cross Site Scripting(XSS)

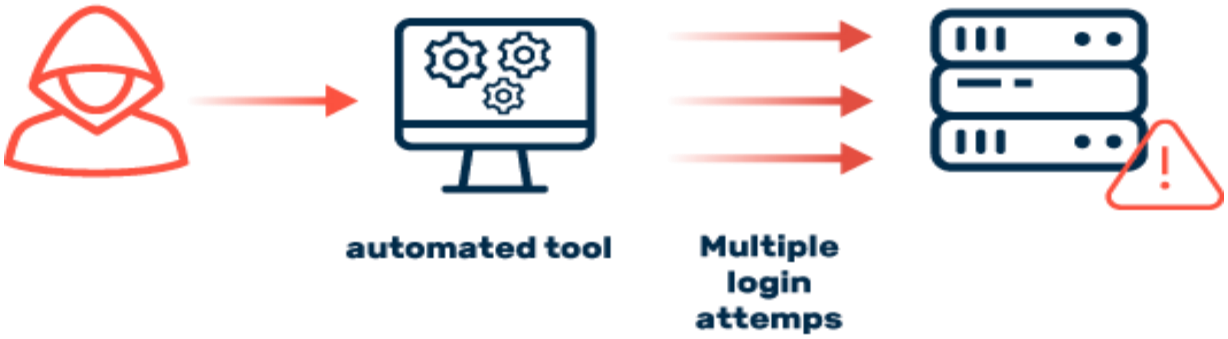


Fig 1.1.3: Bruteforce Attack

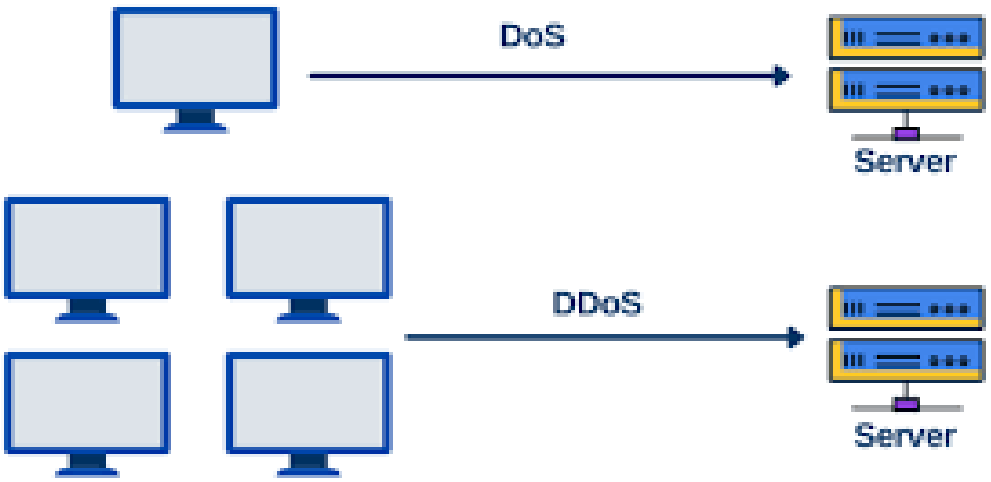


Fig 1.1.4: Denial of Service

1.2 LITERATURE SURVEY ON RANSOMWARE

Publication/Year	Title	Overview	Positive Aspects	Limitations
ELSEVIER/2016	Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization[1]	-This paper shows the life cycle and analysis of windows based Ransomware. -Also it presents evolution of ransomware for windows. -MD5 method, Cuckoo Sandbox used for malware analysis system. -RSA and AES used for encryption.	-The main purpose is to detect the ransomware by monitoring abnormal file system registry activities. - PEid tool is used for windows ransomware detection.	- To prevent the user's data from getting into un-recoverable state, a user should have incremental online and offline backups of all the important data and images.
IEEE/2016	CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data[2]	-Teslacrypt, CTB-Locker, GP code are used for CryptoDrop detection. - Ransomware is a nuisance which can be remedied by wiping the system or removing the disk and extracting the user's important data.	-CryptoDrop reduces the need for the victim to pay the ransom and represents the malware ineffective.	- CryptoDrop stops ransomware from executing with a median loss of only 10 files.
Hindawi/ 2016	The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform[4]	-Ransomware prevention technique on Android platform is proposed. - The proposed technique is designed with three modules: Configuration, Monitoring, and Processing.	- The proposed method can monitor file events that occurred when the ransomware accesses and copies files. -Ransomware classified into three types: Scareware, Lock-Screen, and Encrypting.	- It does not need to install an application such as existing prevention and reduce damage caused by unknown ransomware attacks.
IEEE/2015	Unknown Malware Detection Using Network Traffic Classification[5]	- It presents an end-to-end supervised based system for detecting malware by analyzing network traffic. -Network classification method is used.	- The proposed method analyzes DNS, HTTP, and SSL protocols, and combines different network classification methods in different resolutions of network.	- Evaluated the effect of the environment on the performance.
IEEE/2015	Fest: A Feature Extraction and Selection Tool for Android Malware Detection[6]	- FEST contains three components: AppExtractor, FrequenSel and Classifier. -FEST generally aims with detecting malware using both of high efficiency and accuracy. -AppExtractor, FrequenSel is used as the method.	- FEST only takes 6.5s to analyze an app on a common PC, which is very time-efficient for malware detection in Android markets.	-FrequenSel is definitely more suitable for feature dataset.

Fig 1.2.1: Literature survey on SQL Injection

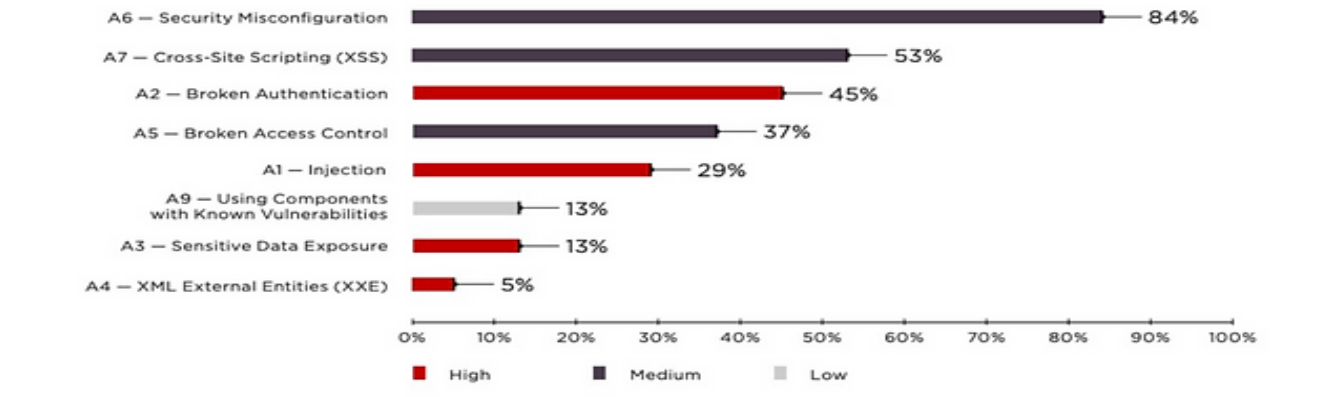


Fig 1.2.2: Types of cyber attack still possible in 2023

1.3 PROBLEM STATEMENT

Cybersecurity has become a major concern in today's digital age as organizations and individuals are increasingly relying on technology and the internet for various purposes. Cyber threats such as hacking, malware attacks, phishing, and identity theft are on the rise, and their impact can be devastating, leading to financial losses, reputational damage, and loss of sensitive information.

The problem is that cybercriminals are constantly evolving their techniques, making it challenging for organizations and individuals to keep up with the latest threats and defend against them effectively. In addition, many individuals and organizations do not have sufficient knowledge or resources to implement strong cybersecurity measures, leaving them vulnerable to attacks.

Furthermore, the increasing use of Internet of Things (IoT) devices and the rise of cloud computing have created new cybersecurity challenges. These devices are often poorly secured and can be easily compromised, providing cybercriminals with a gateway to sensitive information.

Addressing these challenges requires a coordinated effort from governments, organizations, and individuals to prioritize cybersecurity and invest in the necessary resources and technologies to defend against cyber threats. This includes increasing awareness about cybersecurity risks, implementing robust security protocols and practices, and collaborating with other stakeholders to share information and expertise to better defend against cyber attacks.

1.4 Architecture of Cyber Security

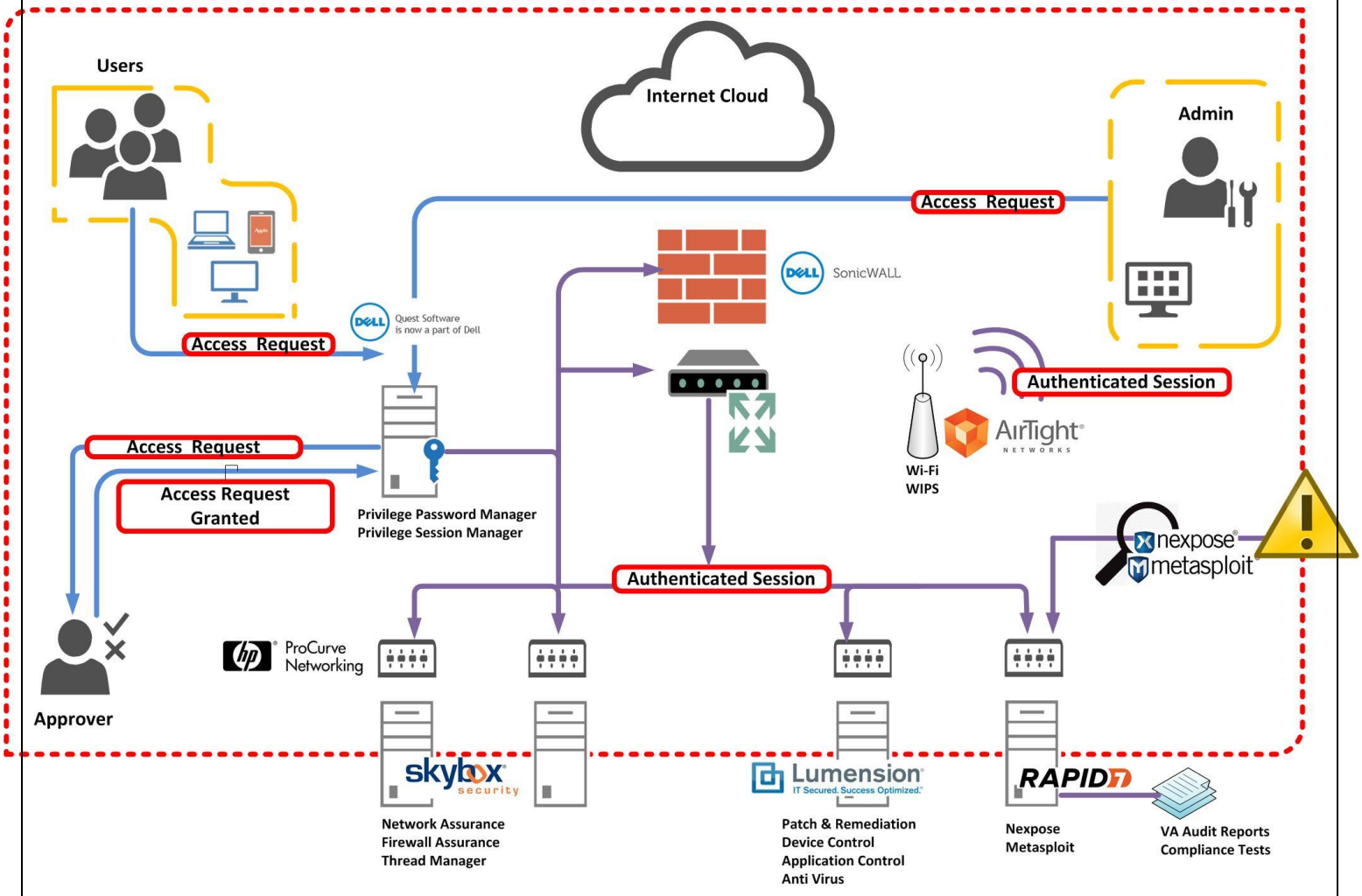


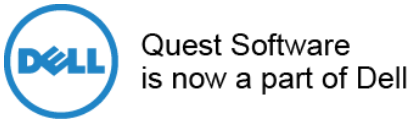
Fig 1.4: Cyber security model of a company

Rapid 7 NeXpose is the only vulnerability management solution to analyze vulnerabilities, controls, and configurations to find the who, what, and where of IT security risk. Metasploit is a computer security tools that provides information about security vulnerabilities and aids in penetration testing.

Lumension Endpoint Management Security Suite (LEMSS) solution fully protects endpoints from malware and unknown threats while enforcing the use of authorized software. With Lumension Application Control™, which is the primary component of Lumension Endpoint Protection solution, you can centrally manage, monitor, and control applications. By employing an application whitelisting approach, you can ensure that only authorized applications can run on laptops, PCs, servers, terminal services servers, and thin clients, preventing the execution of unknown or malicious code.

AirTight Wireless Security Enforcer a World class wireless intrusion prevention system that also doubles as Wi-Fi Access Point with traffic management. Locates rouges and unauthorised wireless with the ability to restrict them from local connections.

SkyBox Network Intelligence Analysis & Monitor is a network security modelling tool that checks for all firewall rules and uses AI for recursive network routing checks. It does not take up any network resources because it just models what it finds in the Firewall managers and compiles and cross checks all the rules of the entire network.



Quest One Identity Solutions empower you to control administrative access enterprise-wide. Quest One solutions for privileged account management improve efficiency while enhancing security and compliance: administrators are granted only the rights they need - nothing more, nothing less and all activity is tracked and audited.

2. APPROACHES AND METHODS OF CYBER SECURITY

Prevention: This approach focuses on preventing cyber attacks from happening in the first place. This includes implementing firewalls, intrusion detection systems, and antivirus software to detect and block malicious activity before it can cause damage.

Detection: Detection is the process of identifying and responding to a cyber attack that has already occurred. This approach includes techniques such as security analytics, threat intelligence, and log analysis to identify and investigate suspicious activity on networks and systems.

Response: In the event of a cyber attack, a response plan is necessary to minimize damage and quickly recover. This approach involves implementing incident response plans, disaster recovery plans, and business continuity plans to ensure that critical systems and data can be restored as quickly as possible.

Education and Awareness: Educating employees and end-users about cybersecurity risks and best practices is critical in preventing cyber attacks. This approach involves conducting training sessions, awareness campaigns, and phishing simulations to educate individuals about the importance of cybersecurity and how to identify and prevent cyber attacks.

Risk Management: Risk management is the process of identifying, assessing, and prioritizing cybersecurity risks and taking appropriate measures to mitigate those risks. This approach involves conducting risk assessments, implementing risk mitigation strategies, and continuously monitoring and evaluating risks to ensure that security measures remain effective.

Compliance: Compliance with industry regulations and standards is critical in maintaining strong cybersecurity. This approach involves adhering to regulations such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS).

Encryption: Encryption is a method used to secure data by converting it into a code that can only be deciphered by someone with the appropriate decryption key.

Multi-factor authentication (MFA): MFA is a security method that requires users to provide more than one method of authentication to access a system or account, such as a password and a fingerprint scan.

Vulnerability scanning: This involves using automated tools to scan networks and systems for vulnerabilities and weaknesses that could be exploited by cybercriminals.

Penetration testing: This approach involves simulating a cyber attack to test the effectiveness of an organization's security controls and identify any vulnerabilities.

Network segmentation: Network segmentation is the process of dividing a network into smaller subnetworks, each with its own security controls, to limit the spread of a cyber attack.

3. RESULTS AND DISCUSSION

Cybersecurity is a critical issue facing individuals, organizations, and governments worldwide. With the increasing reliance on technology and the growing sophistication of cyber threats, it has become more important than ever to implement effective cybersecurity measures.

The results of effective cybersecurity can be seen in a number of ways, including:

Protection of sensitive data: Cybersecurity measures such as encryption, access controls, and firewalls can help protect sensitive data from cyber attacks and data breaches.

Reduction in cybercrime: Effective cybersecurity can help reduce the incidence and impact of cybercrime, such as identity theft, fraud, and ransomware attacks.

Maintenance of business continuity: In the event of a cyber attack, having effective cybersecurity measures in place can help maintain business continuity by minimizing downtime and data loss.

Mitigation of reputational damage: Cybersecurity incidents can have significant reputational damage for organizations. Effective cybersecurity measures can help prevent such incidents and mitigate the impact if they do occur.

Compliance with regulations: Adhering to industry regulations and frameworks such as PCI DSS, HIPAA, and GDPR can help ensure that cybersecurity measures are in place and effective.

However, there are also challenges associated with cybersecurity. These include:

Cost: Implementing effective cybersecurity measures can be costly, particularly for smaller organizations with limited budgets.

Complexity: The complexity of cybersecurity can make it difficult to implement and manage effective measures, particularly for organizations with limited technical expertise.

Evolving threats: Cyber threats are constantly evolving, making it difficult to stay ahead of the curve and effectively defend against them.

Human error: Human error is a common cause of cybersecurity incidents, such as through phishing scams and weak passwords.

To address these challenges, organizations must develop a comprehensive cybersecurity strategy that incorporates a range of approaches and methods. This may include prevention, detection, response, education and awareness, risk management, compliance, and other methods mentioned earlier.

4. CONCLUSION

Cyber security is a critical aspect of modern society that requires constant attention and vigilance. The increasing reliance on technology, coupled with the growing sophistication of cyber threats, has made it more important than ever to implement effective cyber security measures.

The consequences of cyber attacks can be devastating, including data breaches, financial losses, reputational damage, and even physical harm in some cases. Therefore, it is imperative that individuals, organizations, and governments take steps to protect themselves from cyber threats.

Effective cyber security requires a comprehensive approach that includes prevention, detection, response, education and awareness, risk management, and compliance with regulations and industry standards. It also involves implementing a range of methods and techniques, such as encryption, multi-factor authentication, vulnerability scanning, penetration testing, network segmentation, patch management, cloud security, identity and access management, threat hunting, and incident response planning.

While there are challenges associated with cyber security, such as cost, complexity, evolving threats, and human error, organizations can overcome them by developing a solid cyber security strategy and prioritizing cyber security as a critical aspect of their overall operations.

In short, cyber security is an ongoing process that requires constant attention, education, and adaptation to keep pace with the changing cyber threat landscape. With the right approach and methods, organizations can mitigate the risks associated with cyber threats and protect themselves and their stakeholders from harm.

5. REFERENCES

1. National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) - Released on February 12, 2014.
(https://www.nist.gov/cyberframework)

2. Center for Internet Security Critical Security Controls (CIS Controls) - First published in 2008 and updated in 2018.
(https://www.cisecurity.org/controls/)

3. The Cybersecurity and Infrastructure Security Agency (CISA) - Created on November 16, 2018.
(https://www.cisa.gov/)

4. International Organization for Standardization - ISO/IEC 27001 - Originally published in October 2005 and revised in 2013.
(https://www.iso.org/standard/54534.html)

5. The Cybersecurity Information Sharing Act of 2015 (CISA) - Enacted on December 18, 2015.
(https://www.congress.gov/bill/114th-congress/senate-bill/754/text)

6. Verizon Data Breach Investigations Report (Verizon DBIR) - Published annually since 2008.
(https://enterprise.verizon.com/resources/reports/dbir/)

7. Symantec Internet Security Threat Report (Symantec ISTR) - Published annually since 2008.
(https://www.symantec.com/security-center/threat-report)

8. The Cybersecurity Information Sharing Partnership (CISP) - Launched in March 2013.
(https://www.cisp.org.uk/)

9. SANS Institute - Founded in 1989.
(https://www.sans.org/)

10. Information Systems Security Association (ISSA) - Founded in 1982.
(https://www.issa.org/)