IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⋇ Impact Factor 7.918 ⋇ Vol. 11, Issue 11, November 2022

DOI: 10.17148/IJARCCE.2022.111145

Cyber Security Technology use for Protect latest Technology

Dipali V. Thakare[1], L.N. Yadav[2], N.B. Jiwane[3]

Student, Computer Science & Engineering, SSCET, Bhadrawati, India[1]

Head Of Department, Computer Science & Engineering, SSCET, Bhadrawati, India[2]

Asst. Professor, Computer Science & Engineering, SSCET, Bhadrawati, India[3]

Abstract: In today's world driven by technology and connectivity, it's important to understand what cybersecurity is and be able to use it effectively. Systems, important files, data and other important virtual things are at risk if there is no security to protect them. need to do it Attackers are keeping up with the development of new technologies in cybersecurity. They use better and improved hacking techniques and target vulnerabilities in many companies. Cybersecurity is critical as military cops, government Department, financial Sectors, Hospitals, and organizations collect, practice, and store unprecedented amounts of data on PCs and other devices. A significant portion of this data may be sensitive information, such as financial data, intellectual property, personal information, or various other types of data, and unlawful access.

Keywords: Cloud,Cyber Security, Artificial Intelligence, Ramsomware

I. Introduction

Effective cyber security techniques have many layers of defense spread across networks, computers, programs, or information you want to keep non-toxic. In society, processes, people, and tools must all have alternatives to create a true defense against or after cyberattacks. An integrated threat management system automates additions to select Cisco security products to accelerate key security process functions (detection, investigation, and remediation). In the Real world most important thing need to provide security to internet user because of they don't know how his data going to connect with unauthorized person, virus attack, hackers, then cyber security protect to user data and save from malicious attacks. without any threats. Cyber security therefore addresses critical infrastructure, network security, cloud security, application security, internet of Things, and several other areas that need to be secured.

II. LITERATURE SURVEY

Consumers should know and follow basic information security principles such as choosing strong passwords, being careful with email data attachments, and protecting data. Learn about the core values of cybersecurity. Process we should have an overview of how to deal with attempted common cyberattacks respected plan can accompany you. Learn how to detect seizures, protect your organization, detect and respond to threats, and remediate successful incidents.

III. TECHNOLOGY

Technology is essential to providing individuals and organizations with the system security tools they want to used de-fend themselves against the Cyber attacks. want to used Three main objects must be threatened. Endpoint strategies such as personal computers, devices, and Routers. Systems and clouds. Shared technologies used to protect these objects include next-generation firewalls, DNS pass-through filters, malware prevention, antivirus tools, and Email Security Score. The Cyber may differ in that it connected in some way to a collection or net-work of workstations. At the same time, security means a mechanism that protects everything. The terms cyber and security thus define how defensive user information is organized during or after a malicious at-tack that may indicate vulnerability. It's a time that was covered for a while after the internet evolved as usual. Cybersecurity helps businesses and users protect sensitive data from hackers. At some point we are concerned about hacking, but in fact we use ethical hacking to invent cybersecurity in any structure. can be defined as the process of mitigating security concerns in order to protect against potential loss. The term cybersecurity was clearly required to be the security measures pro-posed to organizations that frequent users can contact via the Internet or networks. There are many tackles and techniques that can be thrown to deploy it. The most important fact about protecting information is that it is an ongoing process, not her one-time event. Organization owners should keep their materials up to date to keep risks low.

How does cybersecurity make your job easier?
We never hesitate to make our job easier by ensuring the availability of limited capital in each network where cyber Security tools are Commercials and businesses can suffer a great loss if they are not honest about the safety of their online presence. In today's connected world, everyone favors advanced cyber Defense plans. On another level, cyber security breaches can range from personal theft to extortion at-tempts to corruption of important data such as family photos.

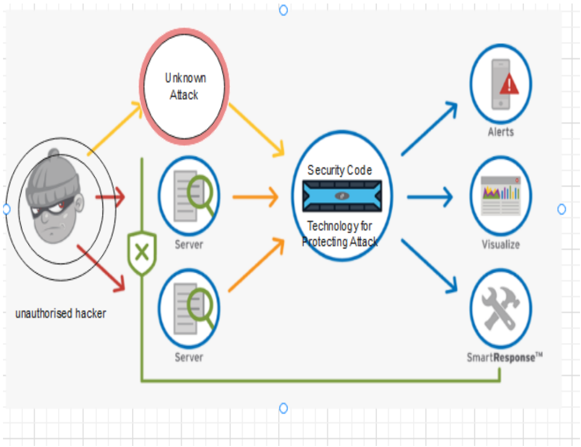

Fig. 1. Architecture of Cyber Security

IV.CYBERSECURITY WILL PROTECT FROM TYPES OF THREATS

A. Phishing

It is the distribution of fake communication samples that look like emails from a trusted source. Its purpose is to negotiate well thought out data comparable to credit card data or login data. This is the largest type of cyberattack. You can manually defend against learning or expert solutions that filter malicious email.

B. Malware

A type of software intended to obtain the rights to illegally use or compromise a system.

C. Ransomware

A type of malicious software. By blocking contact with the records or PC system until the transaction is paid, it is assumed that you are extracting the currency. Paying the ransom does not guarantee recover of recording or return of System. A tactic where your opponent tries to trick you into revealing sensitive information.

You can request payment of money or improve access to re-served information. Combining social engineering with the printed material above increases the chances of connecting via links, sending malware, or believing malicious causes.

V. PURPOSE

The majority of business operations take place over the Internet, exposing their data and resources to a variety of cyber threats. Since data and system resources are the pillars on which an organization operates, it leads to the lack of adage that any risk to these people is definitely a threat to the group itself. Threats can be anything from small code flaws to complex cloud hijacking culprits. Risk assessments and recovery cost estimates help organizations pre-pare and anticipate potential loss-es.

Therefore, it is important to have a clear understanding and articulation of each organization's cybersecurity goals in order to protect valuable data. Cybersecurity is the practice designed to protect complex data on the Internet and devices in order to protect against attack, destruction, or unauthorized access.

The goal of cybersecurity is to ensure a safe, risk-free environment that protects data, networks, and devices from cyberterrorism.

DOI: 10.17148/IJARCCE.2022.111145

VI. THE GOAL OF CYBERSECURITY

The ultimate goal of cybersecurity is to protect data from actual stolen or compromised data. To achieve this, con-sider three key cybersecurity.

A. Goals:

Protect the confidentiality of information Maintain the integrity of information Ensure that only authorized users have access to information These goals are the foundations of a complete security agenda: confidentiality, integrity and availability. (CIA) do three things. This CIA Triad model is a security model intended to guide strategies for data security within a social or organizational place.

This model is similarly referred to instead of the AIC (Availability, Integrity, and Confidentiality) triad to avoid Central Intelligence Agency bugs. The triad foundation reflects three major and important security mechanisms. CIA standards are one of the largest societal and corporate practices when making new claims, creating records, and securing access to approximate information.

All these security areas must emerge in order for the data to be completely secure. These are security strategies that we all work on together, so policy monitoring can be wrong. The CIA Triad is the largest collective standard for measuring, selecting and applying the right security panel to increase risk.

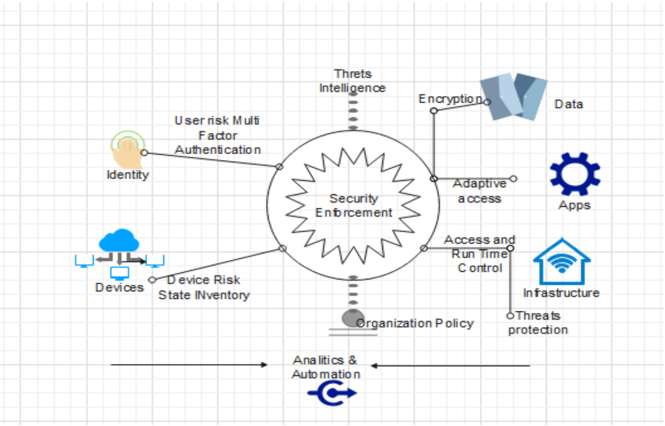

Fig.2. Cyber Security Statistics

B. Confidentiality:

Gives authorized users access to complex statistics and prevents information disclosure to unintended parties.Confidentiality is ultimately compromised if the key is private and not shared with third parties. Confidentiality Methods: Data Encryption Two or More Levels of Verification Biometric Verification

C. Integrity:

Verifies that all data is accurate. Do not switch from one reliable, broad-cast fact to another.

How to ensure integrity:

Unauthorized persons should not have access to delete records. This is also an invasion of privacy. Therefore, operator contact controls are required. A good backup should be returned soon. Need a version monitor to see who made changes.

Availability

Every time an operator requests some resource for statistics, there should not be any reports like Denial of Service (DoS). Evidence must be fully available
For example, let's say your website is in the hands of an attacker, causing a DoS and hindering accessibility. Here are the steps to maintain these goals: Classifies possessions based on their location and priority. The most important things are always kept safe. Suppress potential threats. Determining security force methodologies for each threat Monitoring all breach activity and managing data at rest and in motion. Responding to recurring maintenance and related issues. Updated risk management policy based on previous assessment.

DOI: 10.17148/IJARCCE.2022.111145

VII. ADVANTAGES

consists of many benefits.

As the term itself says, it provides security to a network or system and we all know that there are many benefits to protecting every-thing.

Securing society Cybersecurity is all about safeguarding an organizations net-work from outdoor attacks.

It marks sure that the society should achieve decent and should sense safe around its important information's.

A. Protection of complex data:

The highly Private data like student data, patient data and transactions data have to be safe from illegal access so that it couldn't be changed. It's what we can attain by Cybersecurity.

Hamper illegal access assistances us defend the system after being retrieved by some-body who is not sanctioned to contact it Data is strictly reserved and can only be created by valid users. Cyber Security provides protection in addition to data theft, protects workstations from theft, reduces PC freezes, provides operator privacy, suggests strict policies, and protects non- technical There's a problem to deal with only receipt for a protective computer that protects your computer from worms, viruses and additional unwanted programming.

protection against malicious attacks on systems, removal and/or retention of malicious bases on existing networks, termination of unlawful network access, on or after otherbases with which they may cooperate; It deals with eliminating programming and protecting complex data.

B. Cyber Security provides enhanced cyber security:

expands cyber flexibility, and accelerates industry system data and information protection. Protect your personal data, protect your network and money, and fight computer hackers and identity theft. Protects against data theft asmalicious operators cannot sabotage network construction with advanced security procedures. secure hacking technology. offers privacy and organization. This can be achieved through proper application of security rules and system protocols.

C. Accelerated Ramsomware Attack:

Cyber security Speculations updated cybercrime information and predictions that in 2021 he will fall victim ransomware attacks every 15.4 seconds. This is less than once he did in 14.2 seconds in 2019. The total cost of ransomware would exceed $21 billion for him World wide. The Cloud breaches are on the rise Cloud infrastructures are so highly secure, but customers are responsible for implementing cyber security features and configuring them appropriately. Cloud misconfigurations are a common cause of data breaches, and that number is expected to grow as more organizations adopt cloud services to support remote workers.

Increase in threats are doing target users' devices telecommuting employees utilize systems that are not patched, run and protected by her IT department at the company. This increases the company's attack surface and allows hackers to bypass border security to gain access to the system. Critical business data may be stored on these systems, further increasing the risk of data breaches.

D. Prevent From Attacks on Internet of Things (IoT):

Systems More and more organizations are implementing IoT devices and applications to collect data, remotely control and manage infrastructure, improve customer service, and more. Many IoT devices lack robust security and remain vulnerable to attack. Hackers can extend strategy mechanisms to run in botnets and influence IoT weaknesses to gain access to the network conclusion the Emergence of Cyber Security is somewhat similar to the current one. Digital capabilities interact with humanoids across essentially all aspects of politics, society, family, etc., so it is difficult to describe and the possibilities are endless.

The project was developed in the late 2010 on the notion of 'cybersecurity', a suggestion that the 'cyber' and 'security' mechanisms were more rapidly advancing This gesture for more likely to speed up than slow down, but how you do it depends a lot on the situation. This is not an article of our research process., Effort is required. I expect that in the not too distant future (if not yet), cybersecurity will be widely recognized as the "big problem" of the Internet age. It ranks high on the list of all the difficulties facing civilization as a real fear that technology companies must succeed, akin to almost existential challenges like changing weather. increase.

DOI: 10.17148/IJARCCE.2022.111145

VII. CONCLUSION

Organizations are finding themselves under the pressure of being forced to react quickly to the dynamically increasing number of cybersecurity threats. Since the attackers have been using an attack life cycle, organizations have also been forced to come up with a vulnerability management life cycle. The vulnerability management life cycle is designed to counter the efforts made by the attackers in the quickest and most effective way. This chapter has discussed the vulnerability management life cycle in terms of the vulnerability management strategy.

ACKNOWLEDGEMENT

These Research of Cyber Security can protecting to technology from Unwanted Malicious Threats. paper was partially supported and Gratefully Acknowledge received from Shri Sai College of Engineering And Technology**, Dr. Babasaheb** Technological University, Lonere India. I would like to show our Gratitude to Prof. L.N.Yadav HOD of CSE Department & Prof. N.B.Jiwane of CSE Department for Sharing Their Pearl of wisdom with us during course of this Research paper.

REFERENCES

[1]. The Art of Invisibility: The World’s Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data

[2]. Jon Erickson: The Art Of Exploitation

[3]. Practical Malware Analysis: The Hands On Guide to Dissecting Malicious Software by Michael Sikorski, Andrew Honig

[4]. Black Hat Python: Python Programming for Hackers and Pentesters by Justin Seitz

[5]. Hackers & Painters: Big Ideas From The Computer Age by Paul Graham

[6]. Assante, M., Tobey, D. (2011, February 4). Enhancing the Cybersecurity Workforce.

[7].Conklin, W., Cline, R., & Roosa, T. (2014, March 10). Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors.