ISSN: 2347-6540
International Journal of Latest Research In Engineering and Computing (IJLREC)
Volume 9, Issue 1, Page No. 11-16, 2022
www.ijlrec.com

CYBERSECURITY: CAN WE REALLY BE SAFE

Anjali Semwal[1]
MCA Student, Uttaranchal University
angelsemwal98@gmail.com
Sweta Naithani[2]
MCA Student, Uttaranchal University
snaithani13@gmail.com

Abstract- ***The research paper is about analyzing the cyber-attack which is now a days increasing repeatedly day by day and whether the current cyber security is capable of stopping these attacks. As we know that the cybercrime is increasing day to day, this is happening mainly due to the quick growth in the technology. This research paper takeover the fact of increasing the cybercrime which can now become a serious threat in our lives. This research paper holds a collection of the data related to cybercrime which is picked from the different articles, newspaper, websites and all other source related to cybercrime. It also Reflects about the different cyber security protocols used in different organization to find out the success rate of protocol. This research paper also Highlight on the challenges facing cyber security based on the field of latest technologies.***

Keywords: cyber security, cybercrime, challenges, latest technologies, Cyber Security Protocols.

1. INTRODUCTION

Now a days person can easily send & receive data through the internet. The data can be in of e-mail, audio, video or picture etc. We just have to click on a button and our data is easily shared to the internet platform. But have we ever thought of how the data is securely shared through this internet without any leakage of information to the third party? The answer is in the cyber security. Around the 59.5 percent of global population is using internet, and in which around 4.66 billion are active users. So, now this can think that how fast the internet is growing in day-to-day life. Due to with the help of this more people are connecting to the internet and sharing their private life on the internet without even thinking about the security of their data. As a consequence of this cybercrime is now a days increasing constantly. On the other side, the emerging technologies also play the important role of increasing the cybercrime. If we look into e-commerce website, about 51.7 percent of people are using mobile wallet and the remaining 48.3 percent are using different modes of payment, so for the best Agreement in this type of area good high-quality protection is required. Many organizations store their data with the cloud computing in consequences the data remain on the internet, which could become the part of the cyber-attack. cyber security is latest issue that is not only Restricted to securing the information and data in the organization, but also in various parts like cyber space etc.

When we are bringing out about distinct types of technologies example: - net banking, E-commerce, cloud server, mobile computing also required high level of security. As, we know that these technologies store and keep some valuable information with respecting their customer, so security now has become important features build up cyber security has become the basic priority for every nation so that people can be remain Protected from the cyber-attack.

1. CYBERCRIME

Cyber crime is a word which is also know as computer crime, is the use of computer to fulfill crime such as stealing identities, trafficking in child pornography, violating privacy and long-haired property. Most of the cybercrime is committed by hackers or cybercriminal to earn money in exchange of the private data. Also, the researchers ascertain that there are some emerging technology groups that are anticipated to have important impact on cybercrime over the next time:

- Blockchain and Distributed Ledger Technologies

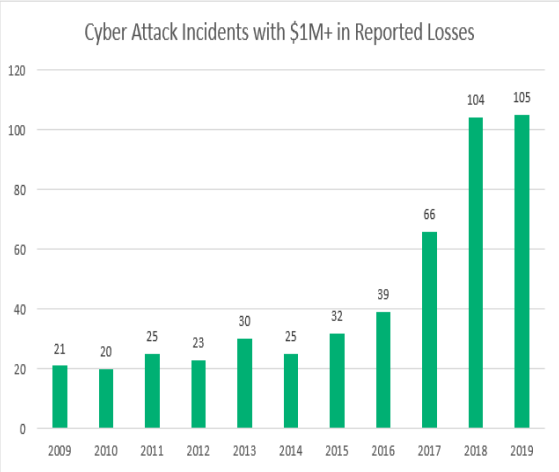
- Artificial Intelligence/ Machine Learning
- Privacy-Enhancing Technologies
- Internet of Things
- Telecommunication Infrastructure
- Autonomous Devices and Systems
- Computing and Data Storage Technologies

So as the technologies are developing day by day in a person's life the Number of cybercrimes is also increases.

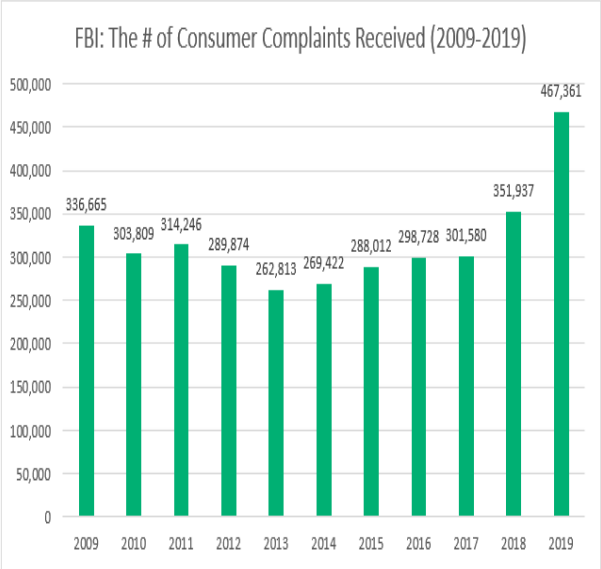
2. CYBERSECURITY

Cybersecurity is the way of technologies that is applied to keep computers, network, programs and data from the nonactive attack or hackers. It plays a essential role in the securing data online. Privacy and Security is the major priority for an organization to make sure. We are living in the planet where most of the organization's information are stored in digital or cloud form. Almost all organization uses cyber security to Secure their data online from unauthorized use. Lots of data are being transfer from one organization to another in order to exchange information. This information is being shared via internet, and here the protection of data in required so that the data does not get release to other party, whether accidental or intentional. To avoid this situation different types of cyber security protocols are used by different group. The cyber security can be divided into the following common genre.

- Network Security: It is the security of computer network from aggressors.
- Operational Security: It is the Safety of data that is stored or shared among the organization.
- Information Security: It is the safety of the confidentiality of data both in storage and in transmission of data from one basis to another.
- Application Security: It is the protection of software and devices from intimidations.
- End-User education: It the knowledge which is given to the people, to delete the suspicious email, not plug in unidentified USB drives and some other important lessons to prevent the virus entering in the secure system.



The chart over shows economic crimes of more than one million dollars over the past period. The above data has been collected by the Center for Strategic & International Studies (CSIS), which "tracks cyber-attacks on high-tech companies, government agencies and other large organization. The chart below shows how many consumer complaints occurred in the past period.



This whole scenario reveals, how cybercrime is increasing over the past Period and the challenges faced by the government to minimize the economic disasters and also spread the awareness to the people about taking precautions before sharing, uploading any of their distinctive data on the internet.

4. Cyber Security Protocols

According to an IBM study, 95% of cyber security breaches are affected by human error which means that Nineteenth out of twenty cyber breaches cannot occur if we avoid human error. Some human errors include the delivery of private information to the wrong person if they are not sensitive, putting weak passwords and sharing with the colleagues, leaving sensitive documents on the desk unattended, etc. That is why cyber security protocols should be known by employees of an organization in way to increase the posture of an organization. Cyber security protocols are action, plans, protocols and measurements that are intended to ensure that your organization is secure from hateful attacks, data breaches and other security incidents. When the attacker could use multiple ways to gain entree to your networks, so you require to apply and update regularly more than one security measure. Regard as the security of an organization in today's state of affairs, when the data is one of the most valuable assets for an organization, it is significant for the organization to take essential measure in contradiction of cyber-attack. Even small organizations fall on the locator of most hackers, because their security is not so strong and due to which they become easy targets.

Top cyber security protocols are:

Firewalls

Firewall can either be software or hardware that checks and uses incoming and outgoing network traffic to avoid unlicensed access to or from a private network. It is one of the most useful tools which assist in to screen out the hackers, viruses, spam, and worms that enter your computer through the Internet. All this data is confirmed by a firewall before it runs to the Internet. Fireball investigates data confidentiality based on preset security rules and blocks those that do not meet particular security criteria. Therefore, the firewall plays an Vital role in identifying cyber criminals and hateful attackers

Encryption

According to Verizon's statement on data contravention investigation published in 2016, 63% of all data breaches are produced by theft, sub-parse, and misplaced passwords. This is why most of the company encrypts their employee's login password for their own advantage. Furthermore, it helps the company as well as the employees to encrypt their vulnerable data, so that their data is secure from serious damage in the case of a data breach. This Gives an additional layer of security, so making the organization more securable and much more challenging for the hackers to steal their data.

Authentication of data

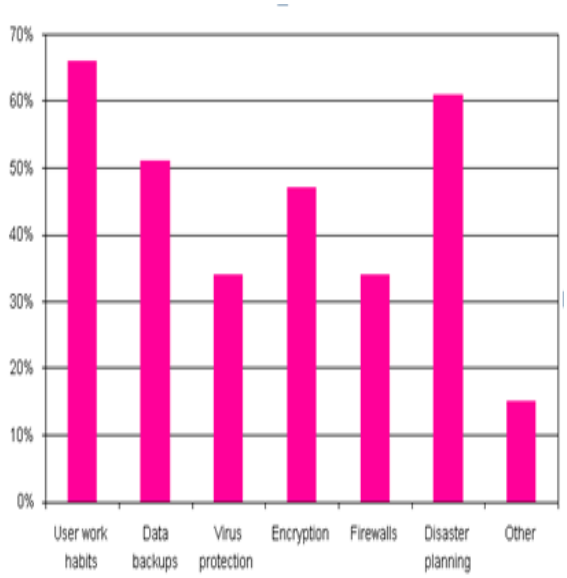
Any of data that is being downloaded from the Internet or received from an external source must always be valid and verified by the receiver, to look after whether it made from a dependable source and is reliable. This authentication of data is done by the different software presented in different devices.

Using A VPN

Whenever the employees of an Company access their systems from outside their capability, they must use the virtual private network (VPN). A VPN is a set of networks that encrypts the data take place through it, as a result it helps in improving the cyber security of an association.

Avoiding Personal Devices for Work

It is always good for an employee of a Company to avoid personal device during their work time. For more security, there should be a collection of devices to be placed in an organization which are only used for work.



5. Latest Cyber Security Technologies

Man produces technology, and it is also true that the technology is developing day to day and only the man is able to get the better of this technology. It always depends on how sensibly a Company chooses the technologies to protect cyber security. Below there is the list of some advance cyber security technologies.

Artificial Intelligence & Deep Learning

AI and machine learning could raise the effectiveness of cyber security, as the application is very similar to the working of two-factor authentication.

Two factor authentication acts as a user approval based on two to three different limits, which helps them to login to their personal details. And here AI comes into the picture which is helping users to add additional levels of information and authentication. Deep Learning is used to examine the data such as real-time communication, logs and connections to detect threats or breaches.

Behavioral Analytics

The data mining is to be used for communicative analysis. This technique is being increasingly discovered to develop improve cyber security technologies as it usually targets social media and online advertisement to the right place of audience.

Behavioral analytics improves to find out the pattern and abnormal network activities to discover the real-time cyber threats for example an abnormal increase in the data transmission from one supplier to another, which can be led in the direction of some probable cyber security problem. Mostly behavioral analytics is used for networks, where a user device has witnessed an upsurge.

Embedded Hardware Authentication

A PIN and password are not necessary for foolproof security of any kind of software or hardware. As you know that password and PIN could easily be broke by the hackers. Therefore, rooted authenticators are the Developing technologies used by most of the hardware or software to confirm a user's identity. Sixth generation v Pro Chips is introduced for which is fixed into the hardware to provide powerful user verification

Blockchain Cybersecurity

If an operation is held between two parties in a proper manner, the blockchain generates a near-hidden network for hackers and currently shows to be the best to protect against data theft.

Whenever the data is added in this, every member who is connected to the blockchain is liable for verifying the accuracy of that data.

Zero-Trust Model

Zero-Trust Model is created on a consideration that both internal and external network is already negotiated. Due to which these networks are at risk and need equal security which includes logical and physical breakdown, identifying business-critical data, mapping the flow of this data and self-control enforcement through automation and frequent monitoring

The overhead chart displays rising technologies ranked in order of importance. This shows that the administration is ready to make major investments in areas such as cyber security, even though being of high value.

6. Conclusion

Cyber security is a vast topic that becomes essential for every government worldwide to reduce the increasing level of cybercrime. This research paper demonstrates how economic crimes increase and are impacting the economics of the country. The number of consumer complaint increases in every year, the main reason behind this is human mistake. Many groups are using new technologies as well as different rules are applied to protect their cyber security. There is no perfect solution for the cyber-crime, but the essential thing is that all of us should try our level best to discovering out the solution and avoiding the cybercrime as minimum as likely for the secure future in cyber space.

REFERENCES

[1] Statista (2021). Global digital population [Online]. Available: https://www.statista.com/statistics/617136/digital-population-worldwide/

[2] Nikhita Reddy Gade, Ugander G J Reddy (2014). "A Study of Cyber Security Challenges And Its Emerging Trends On Latest Technologies [Online] Available: https://www.researchgate.net/publication/260126665

[3] Statista (2020) Share of selected payment systems as percentage of total e-commerce transaction volume worldwide in 2020, [Online]. Available: https://www.statista.com/statistics/1111233/payment-method-usage-transaction-volume-share-worldwide/

[4] Wall, D. S. 2001. “Cybercrimes and the Internet.” In Crime and the Internet, edited by D. S. Wall, 1–17. New York: Routledge. [Crossref], [Google Scholar]
[5] Rand Corporation (2021) Technological developments and the future of cybercrime [Online] Available: https://www.rand.org/randeurope/research/projects/technological-developments-and-the-future-of-cybercrime.html
[6] G.Balaji, V.S.HariPrassath, V.Sriram (16thFebrurary18) www.conferenceworld.in “Issues Based On Cyber Crime And Security” ISBN: 978-93-87793-00-2 [Online] Available: http://data.conferenceworld.in/IIMT_NHSEMH/16.pdf
[7] Casey Crane (21 February, 2021) “Cyber Attack Statistics Reported in the Last Decade” [Online] Available: https://sectigostore.com/blog/42-cyber-attack-statistics-by-year-a-look-at-the-last-decade/
[8] Logsign (2020) “Cyber Security Protocols That You Should Know” [Online]Available: https://www.logsign.com/blog/cyber-security-protocols-that-you-should-know/
[9] MickeAhola (2020) “The Role of Human Error in Successful Cyber Security Breaches” [Online] Available: https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches
[10] Incognito (2019) “Latest Cyber Security Technologies for Your Business” [Online] Available: https://ifflab.org/the-5-latest-cyber-security-technologies-for-your-business/